IBM **Security**

X-Force 脅威インテリジェンス・インデックス2022: エグゼクティブ・サマリー

IBM

目次

エグゼクティブ・サマリー

世界では、長引くパンデミック、在宅勤務や職場復帰への移行、不信感を生む地政学的な変化と格闘し続けています。これらはすべてカオスと同義であり、サイバー犯罪者はカオスの中で繁栄しています。2021年、IBM Security® X-Force®は、脅威アクターが移り変わる状況をどのように好機的に利用し、戦術や技術を導入して世界中の組織への侵入を成功させたのかを発見しました。

IBM Security X-Force脅威インテリジェンス・インデックスは、ネットワークやエンドポイントの検出デバイス、インシデント・レスポンス（IR）活動、ドメイン名の追跡など、何十億ものデータポイントから私たちが観察・分析した新しいトレンドと攻撃パターンをマッピングします。本レポートは、2021年1月から12月に収集したデータをもとに、その集大成として作成したものです。

これらの調査結果は、IBMのお客様、セキュリティー業界の研究者、政策立案者、メディア、そしてセキュリティーの専門家やビジネス・リーダーなど、より広いコミュニティーへのリソースとして提供されます。

不安定な状況と、脅威タイプと脅威ベクトルの両方の進化を考えると、攻撃者の一歩先を行き、重要な資産を強化するには、これまで以上に脅威インテリジェンスに関する洞察が必要です。

レポートのハイライト

トップ攻撃タイプ：2021年もランサムウェアがトップ攻撃タイプでしたが、X-Forceが修正したランサムウェア攻撃の割合は前年比で9%近く減少しました。X-Forceが2年目に観測した最も一般的なランサムウェアはREvil（X-ForceではSodinokibiとも呼ぶ）で、全ランサムウェア攻撃の37%を占め、次いでRyukが13%となっています。2021年のランサムウェアとIoTボットネットの攻撃は、おそらく法執行機関の活動が主な推進力となって減少しましたが、2022年に復活する可能性を排除するものではありません。

サプライチェーン脆弱性：バイデン政権によるサイバー・セキュリティーに関する大統領令、米国国土安全保障省、CISA、NISTによるゼロトラスト・ガイダンスの倍増などにより、サプライチェーンのセキュリティーは政府や政策立案者の注目を集めるようになりました。これらのガイドラインは、脆弱性と信頼関係に焦点を当てています。製造業では、脆弱性の悪用が初期の攻撃対象のトップとなり、サプライチェーンの圧力や遅延の影響を受けています。

ほとんどのフィッシング・ブランド：X-Forceは、2021年を通じてサイバー犯罪者がフィッシング・キットをどのように使用しているかを綿密に追跡しました。調査の結果、Microsoft、Apple、Googleが犯罪者が模倣しようとしたブランドの上位3位であることが明らかになりました。これらのメガブランドはフィッシング・キットで繰り返し使用されており、攻撃者はその人気と多くの消費者の信頼を利用しようとしている可能性があります。

トップ脅威グループ：イランの国民国家脅威行為者と疑われるITG17（MuddyWater）、サイバー犯罪者グループITG23（Trickbot）、Hive0109（LemonDuck）は、X-Forceインテリジェンス・アナリストが2021年に観察した最も活発な脅威グループの一部です。世界中の脅威グループは、その能力を強化し、より多くの組織に侵入しようとしていました。彼らが使用したマルウェアには、より優れた防御回避技術が組み込まれており、場合によっては、クラウド・ベースのメッセージングとストレージ・プラットフォームを介してホストされ、セキュリティー管理を通過していました。これらのプラットフォームは、正当なネットワーク・トラフィックでコマンドとコントロール通信を隠すために悪用されました。また、攻撃者はクラウド環境への移行を容易にするために、Linux版のマルウェアの開発も続けています。

主な統計

21%

ランサムウェアの攻撃の割合

ランサムウェアはX-Forceが昨年確認した攻撃タイプの第1位で、前年の23%から21%に減少しています。REvilのランサムウェア攻撃者(Sodinokibiとも呼ばれる)は、ランサムウェア攻撃全体の37%を占めていました。

17ヶ月

ランサムウェア・ギャングがブランド名の変更またはシャットダウンするまでの平均時間

X-Forceが調査したランサムウェア・ギャングは、ブランド名の変更や解散までの平均寿命が17カ月でした。最も成功したギャングの一つであるREvilは、2021年10月に31ヶ月(2年半)で終了しました。

41%

初回アクセス時にフィッシングを悪用する攻撃の割合

2021年にはフィッシング詐欺が侵入経路のトップに浮上し、X-Forceが修復したインシデントの41%がこの手法で最初のアクセスを獲得しています。

33%

2020年から2021年にかけての脆弱性悪用によるインシデント数の増加

2021年に悪用された脆弱性の上位5件のうち4件は新しい脆弱性で、その中にはLog4j脆弱性 「CVE-2021-44228」が含まれていました。この脆弱性は12月に公開されたにもかかわらず、2位にランクされました。

3倍

電話を使用した標的型フィッシング・キャンペーンのクリック効果

平均的な標的型フィッシング・キャンペーンのクリック率は17.8%でしたが、電話を使ったフィッシング・キャンペーン(ヴィッシング、ボイス・フィッシング)は3倍の効果があり、被害者の53.2%がクリックしました。

146%

新しいコードによるLinuxランサムウェアの増加

Intezerによると、ユニークな（新しい）コードを持つLinuxランサムウェアの割合は、前年比で146%増加しており、Linuxランサムウェアの革新レベルが高まっていることを示しています。

#1

製造業の攻撃ランク

2021年、金融サービスに代わって製造業が攻撃対象のトップとなり、X-Forceが昨年修復した攻撃の23.2%を占めています。攻撃タイプではランサムウェアがトップで、製造業企業への攻撃の23%を占めました。

61%

OTに接続された組織での製造業の不正アクセスの割合

昨年OTに接続された組織で発生したインシデントの61%は製造業でした。さらに、OTに接続された組織に対する攻撃の36%はランサムウェアでした。

2,204%

OTに対する偵察の増加

攻撃者は、2021年1月から9月の間に、インターネット経由でアクセスできるSCADA Modbus OTデバイスの偵察を2,204%増加させました。

74%

MoziボットネットからIoT攻撃の割合

2021年には、IoTデバイスに対する攻撃の74%がMoziボットネットから発生していました。

26%

アジアを標的とした世界的な攻撃の割合

攻撃の26%はアジアを標的としていました。アジアは2021年に最も攻撃された地域でした。

リスク軽減に関する推奨事項

本レポートで紹介した脅威は、ランサムウェアににによる深刻かつ増大する脅威、BECやフィッシングによる新たな脅威、脅威アクターが過去1年間に悪用したいくつかのゼロデイ攻撃などが強調されているため、 疑問を引き起こす可能性があります。しかし、私たちの意図は、この情報が、現在の脅威の状況をよりよく理解し、これらの脅威に対抗するために取るべき行動への信頼を築くために、組織を支援することです。

X-Forceが今日のサイバー脅威との戦いに役立つと判断したセキュリティー原則には、ゼロトラスト・アプローチ、インシデント対応の自動化、検知および対応能力の拡張などがあります。

ゼロトラストでトップの攻撃のリスクの低減を支援します

ゼロトラストは、セキュリティー問題に対する新しいアプローチであるパラダイムシフトで、セキュリティー侵害がすでに起こっていることを想定し、攻撃者がネットワーク全体を移動する際の困難性を高めることを目的としています。中核となるのは、重要なデータがどこに存在し、誰がそのデータにアクセスできるかを理解し、ネットワーク全体で強固な検証手段を構築し、適切な個人のみが適切な方法でそのデータにアクセスしていることを確認することです。

X-Forceの脅威研究者による調査では、MFAの実装や最小特権の原則など、ゼロトラスト・アプローチに関する原則は、本レポートで確認された上位の攻撃タイプ、特にランサムウェアとBECに対する組織の感受性を低下させる可能性があることが確認されています。

特にドメイン・コントローラーとドメイン管理者アカウントに最小特権の原則を適用すると、ランサムウェア攻撃者の障壁が高くなる可能性があります。これは、これらの攻撃者の多くが、被害を受けたドメイン・コントローラーからネットワークにランサムウェアを展開しようとするためです。また、MFAを導入することで、Eメール・アカウントの乗っ取りを狙うサイバー犯罪者は、盗まれた認証情報以外のさらなる認証を要求されるため、その難易度が上がります。

セキュリティーの自動化がインシデント対応を強化

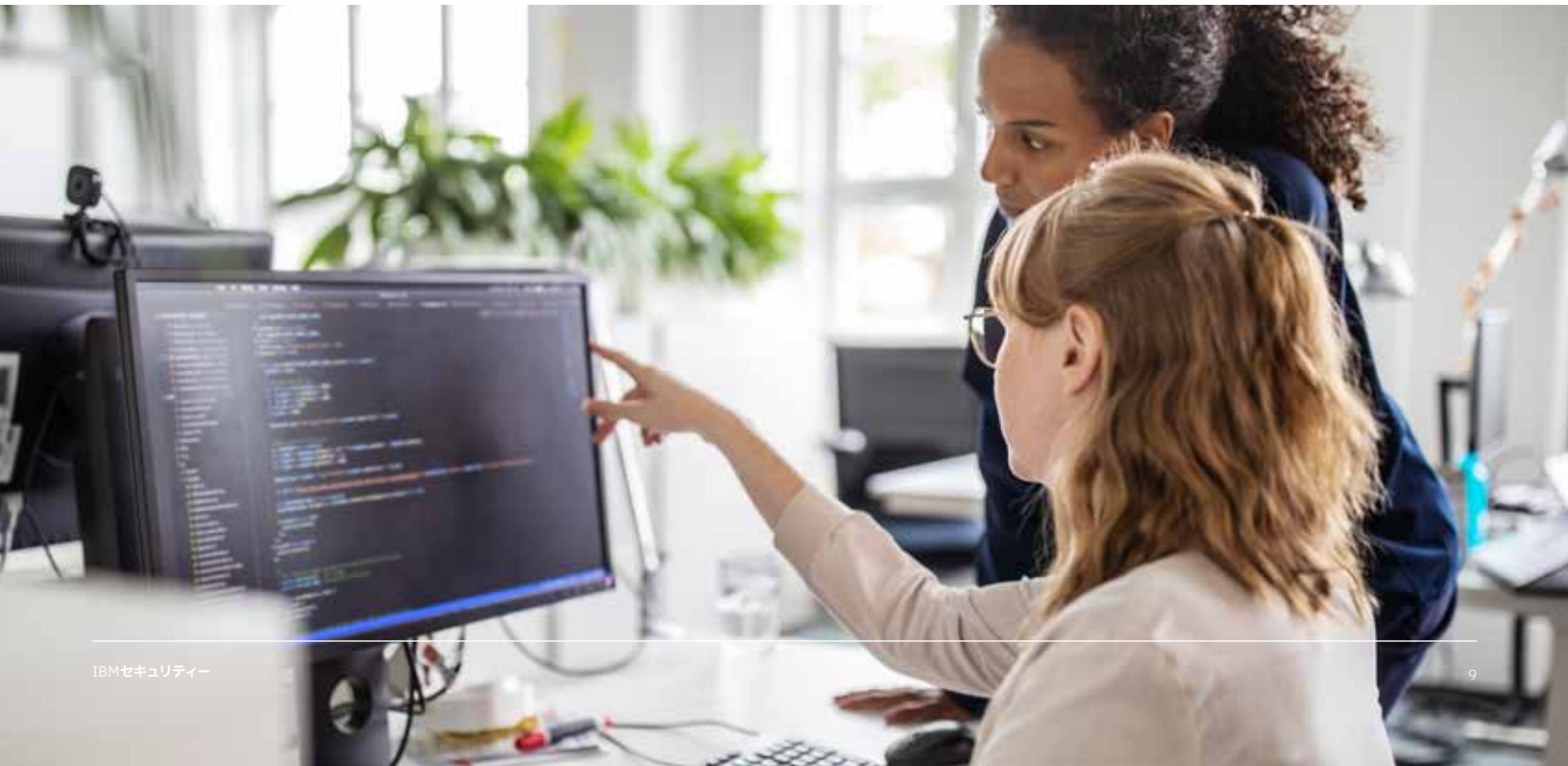
X-Forceのインシデント対応チームは、毎年、さまざまな地域で数百件のインシデントに対応し、社内のインシデント対応アナリストを支援し、さまざまな攻撃タイプに対応しています。ランサムウェアをネットワーク上にデプロイする前に攻撃者を特定して排除する場合でも、次のインシデントに備えて帯域幅を確保するために問題を迅速かつ効率的に解決する場合でも、スピードは最重要事項です。このような速いペースで進む環境では、セキュリティーの自動化が鍵となります。人間のアナリストやチームが時間を要するタスクをマシンにアウトソーシングし、ワークフローを改善するメカニズムを特定します。

2021年半ば、IBMは、セキュリティー・オペレーション・センター（SOC）のアナリストが迅速にフォレンジック調査を実施し、サイバー・インシデントに対処することを支援することを目的として、脅威ハンティング自動化ツールをOpen Cybersecurity Allianceに寄贈しました。また、X-Force IRチームは、IBM Security QRadar SOARを利用してインシデント対応機能を強化しています。

広範な検知と対応は、攻撃者よりも大きな利点を提供します

検知および対応技術、特に複数の異なるソリューションを組み合わせたExtended Detection and Response(XDR) ソリューションは、ランサムウェアのデプロイメントやデータの盗難など、攻撃の最終段階に達する前に攻撃者を特定し、ネットワークから除去する上で、組織に大きな利点を提供します。

複数のケースで、X-Force IRチームがエンドポイントの検出と応答(EDR)またはXDRソリューションをクライアントのネットワークにデプロイした場合、IRは、攻撃者の活動を特定して迅速に対処するのに役立つ追加の洞察を即座に得ることができました。XDR技術はおそらく、サーバー・アクセスやその他の攻撃タイプの増加を促進するのに役立っているとX-Forceは観測しており、攻撃者が特定され、操作が意図した結論に達する前に停止したことを示しています。



推奨

次の推奨事項には、このレポートに示されている脅威に対してネットワークのセキュリティーを強化するために組織が実行できる具体的なアクションが含まれています。

ランサムウェアへの対応計画を策定します。あらゆる業界と地域がランサムウェア攻撃のリスクにさらされており、重要な瞬間にチームがどのように対応するかによって、対応に費やされる時間と費用が大きく異なります。

- 対応計画には、即時の封じ込め措置、利害関係者および法執行当局に通知する必要がある事項、組織がバックアップから安全に保存およびリストアする方法、修復中に重要なビジネス機能を実行できる別の場所を含めます。
- ランサムウェアの攻撃の一部として、データの盗難や漏洩を想定したシナリオを計画に含めます。これは、今日非常によく使われている手口で、X-Forceが修復を行うランサムウェア攻撃の非常に高い割合で見受けられるものです。
- ランサムウェア・ドリルを使用して、組織が身代金を支払うかどうか、およびその決定の計算方法を変更する要因を検討します。
- ランサムウェアの対応計画には、クラウド関連のインシデントに対する特定のコンティンジェンシーが含まれていることを確認してください。クラウド関連のインシデントには、追加のツールやスキルが必要になる場合があります。
- マルウェアやランサムウェアの攻撃によるデータの破損を防ぐフラッシュ・ストレージ・ソリューションは、データ損失の防止、業務継続性の促進、インフラストラクチャー・コストの削減に役立ちます。
- X-ForceのDefinitive Guide to Ransomwareでは、ランサムウェアの攻撃への対応方法について、さらに詳細なアドバイスを提供しています。X-Forceのインシデント対応チームは、ランサムウェアのインシデント対応計画の構築とテストを支援するために、お客様の組織に対してRansomware Readiness Assessmentを実施することも可能です。X-Force Command Centerは、必要なビジネス対応と技術的な対応の両方を考慮して、ランサムウェア攻撃に備えて組織を準備します。

ネットワークに接続するすべてのリモート・アクセス・ポイントに、マルチファクター認証を実装します。X-Forceは、これまで以上に多くの組織がMFAをより効果的に実装していることを確認しています。これは文字通り、脅威の状況を変え、盗まれた認証情報を利用するのではなく、ネットワークを侵害する新しい方法を攻撃者に強制し、Eメールによる乗っ取りキャンペーンの効果も低下しています。

- MFAは、ランサムウェア、データ盗難、BEC、サーバー・アクセスなど、さまざまな攻撃タイプのリスクを軽減できます。
- さらに、アイデンティティーおよびアクセス管理テクノロジーによって、実装チームとエンド・ユーザーの両方にとって、MFAの実装が毎年容易になっています。

フィッシング対策に階層型アプローチを採用します。残念ながら、すべてのフィッシング攻撃を阻止できるツールやソリューションは存在せず、脅威アクターは、確立された制御を回避するためにソーシャル・エンジニアリングやマルウェア対策の検出技術を改良し続けています。したがって、フィッシング・メールを検出する可能性の高いソリューションをいくつかの階層に分けて実装することをお勧めします。

- まず、効果的なユーザーの認識と教育が重要であり、実例を含める必要があります。
- 次に、メールソフトウェア・セキュリティー・ソリューションを使用して、悪意のあるメッセージを特定してフィルタリングするタスクをマシンに行わせます。
- 第三に、万が一フィッシング・メールが送信されてきても、マルウェアや横方向の動きを素早くキャッチできるよう、行動ベースのマルウェア対策、エンドポイント検知と応答（EDR）、侵入検知・防御ソリューション（IDPS）、セキュリティー情報とイベント管理（SIEM）システムなどの防御策を実装します。

脆弱性管理システムを改善し、成熟させます。脆弱性管理は、組織のネットワーク・アーキテクチャーに最も適した脆弱性を特定することから、プロセスの途中で何も破壊することなく脆弱性を導入する方法を特定することまで、1つの芸術です。

- 脆弱性管理に特化したチームを編成し、このチームに十分なリソースとサポートが提供されていることを確認することで、潜在的な脆弱性の悪用からネットワークを確実に保護することができます。
- この評価で言及された脆弱性のうち、お客様の組織に該当するものに優先順位を付けることをお勧めします。
- IBMのX-Force Exchangeには、最も懸念される脆弱性を特定するのに役立つ脆弱性と関連する重要度レベルのリポジトリーも含まれており、X-Force Redは特別な脆弱性スキャンおよび管理サービスを提供することが可能です。

IBM Security X-Force について

IBM Security X-Forceは、ハッカー、レスポンダー、研究者、アナリストからなる脅威中心のチームです。当社のポートフォリオには、攻撃的および防御的な製品とサービスが含まれており、脅威に対する360度の視点に基づいています。X-Forceをセキュリティーのパートナーとして迎えることで、データ侵害の可能性と影響を最小限に抑えることができると、自信を持って断言することができます。

IBM Security X-Force脅威インテリジェンスは、IBM セキュリティー運用テレメトリー、調査、インシデント対応調査、商用データ、オープンソースを組み合わせることで、お客様が新たに出現した脅威を把握し、セキュリティーに関する意思決定を情報に基づいて迅速に下せるように支援します。

さらに、X-Forceインシデント対応チームは、データ侵害の影響を最小限に抑えるために、検知、対応、修復、および準備のサービスを提供します。

X-ForceとIBM Securityコマンド・センターを組み合わせることで、アナリストから経営幹部まで、今日の脅威の実態に対応できるようチームを訓練することができます。IBM Security のハッカーチーム X-Force Red は、侵入テスト、脆弱性管理、攻撃者シミュレーションなど、攻撃的なセキュリティー・サービスを提供しています。

また、IBM X-Force の研究者達が、年間を通じて、進行中の調査や分析の情報をブログ、ホワイト・ペーパー、Webセミナー、ポッドキャストで提供し、新たな脅威アクター、マルウェア、攻撃手法などについての洞察を紹介しています。さらに、X-Force脅威インテリジェンス・ソリューションを通じて、サブスクリプションをご契約いただいているお客様には、最新かつ最先端の分析結果を数多く提供しています。

IBM Security について

IBM Securityは、AI を活用した先進的で統合されたエンタープライズ・セキュリティー製品とサービスのポートフォリオ、ゼロトラストの原則に基づくセキュリティー戦略への最新のアプローチを活用して、お客様のビジネスを保護し、不確実な状況下でも、お客様が成功するよう支援いたします。さらに、セキュリティー戦略をお客様のビジネスに合わせ、デジタル・ユーザー、資産、データを保護するために設計されたソリューションを統合し、高まる脅威に対する防御を管理するためのテクノロジーを導入することで、今日のハイブリッドクラウド環境をサポートする、リスクの管理と制御を支援します。

IBMの新しいオープン・アプローチの IBM Cloud Pak for Security プラットフォームは、RedHat Open Shift 上に構築されており、広範なパートナー・エコシステムによってハイブリッド・マルチクラウド環境をサポートします。Cloud Pak for Security は、データとアプリケーションのセキュリティーを管理できるようにする、企業向けのコンテナ化されたソフトウェア・ソリューションです。データを移動することなく既存のセキュリティー・ツールを迅速に統合し、ハイブリッドクラウド環境全体にわたる脅威に対するより深い洞察を引き出し、セキュリティー対応のオーケストレーションと自動化を容易にします。

詳細については、www.ibm.com/jp-ja/securityを参照するか、IBMセキュリティー・インテリジェンス・ブログにアクセスしてください。

協力者

カミーユ・シングルトン
チャールズ・デベック
ジョシュア・チャン
デビッド・マクミレン
スコット・クレイグ
スコット・ムーア
シャーロット・ハモンド
ジョン・ドワイヤー
メリッサ・フリードリッヒ
オーレ・ヴィラドセン
リチャード・エマーソン
ギ・ヴァンサン・ジュルダン
ヴィオ・オヌート
ステファニー・カラザース
アダム・ローリー
ミシェル・アルヴァレズ
サライナ・ウッケ
ジョージア・プラシノス
ジョン・ゾラベディアン
ミッチ・メイン
リモール・ケッセム
イアン・ギャラガー
アリ・エイタン

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社

Produced in the United States of America
2022年2月