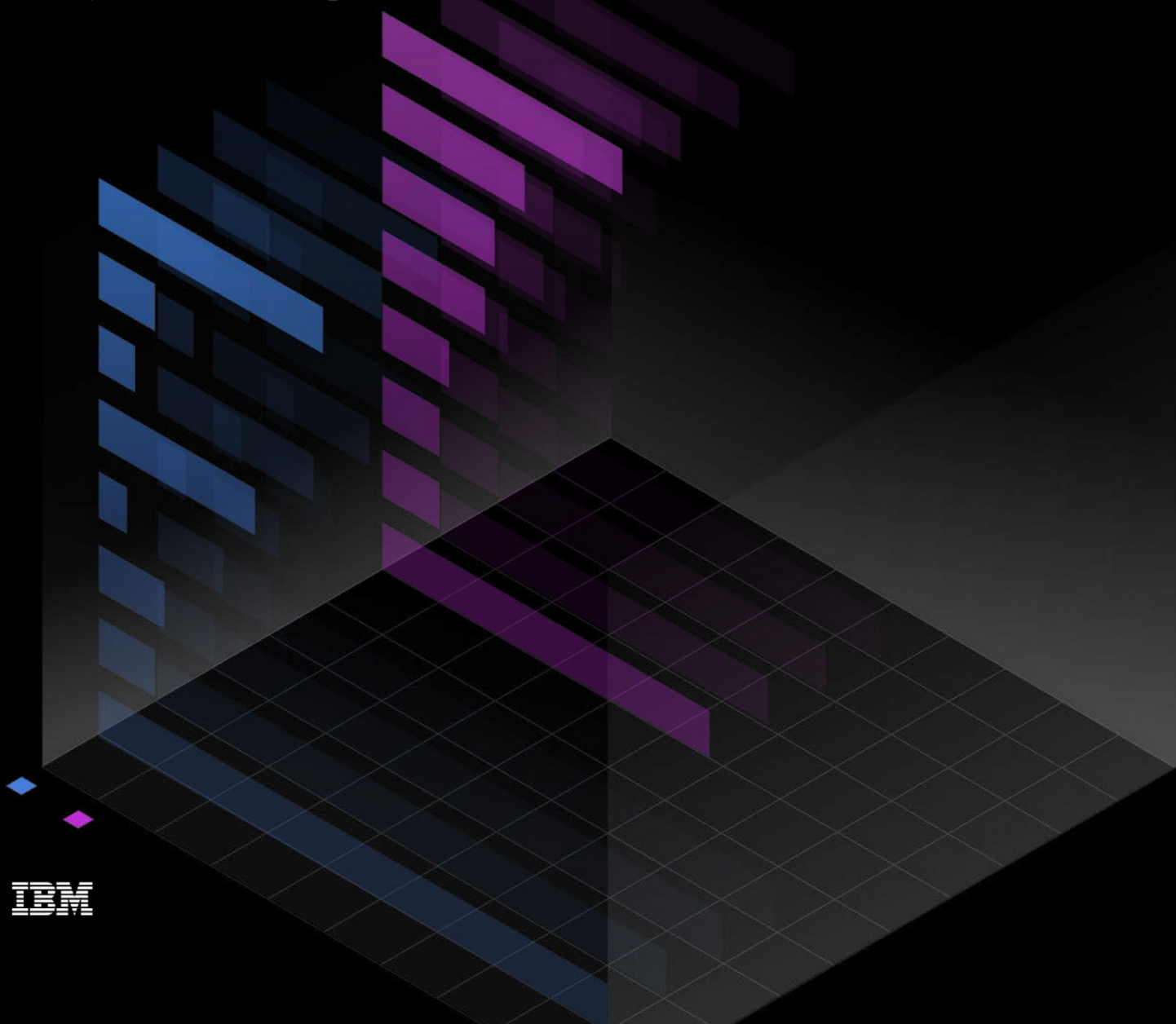
IBM Security

X-Force 脅威インテリジェンス・インデックス 2021

エグゼクティブ・サマリー



IBM

はじめに

2020 年は間違いなく近年で最も重大な転機をもたらした年、すなわち、世界的なパンデミックや経済の混乱が何百万もの人々の生活に影響を及ぼし、社会的、政治的な不安を増大させた年であったと言えるでしょう。こうした出来事はビジネスにも大きな影響を与え、多くの企業が分散型ワークフォースへと大規模な転換を図った年でもありました。

サイバーの世界においては、2020 年のこの特殊な状況が、サイバー攻撃者に、通信ネットワークの必要性を悪用する機会を与え、さらにサプライチェーンや重要なインフラストラクチャーに豊富な攻撃機会を与えてしまうことにも繋がりました。2020 年は、迅速な対応と修復を必要とする世界的に重大な脅威が検知された一年でもありました。ほとんどの攻撃は、ネットワーク監視ソフトウェアのバックドアを利用して政府や民間団体を攻撃する国家アクターの犯行によるものであり、第三者によるリスク対策の必要性と共に、そのような攻撃を予測することの難しさを浮き彫りにしました。

こうした課題に対応できるように、IBM Security X-Force は、サイバー脅威の全貌を評価し、巧妙化する脅威とそれに関連したリスク、さらにはサイバーセキュリティーの取り組みにどのような優先順位をつけるべきかを、企業にご理解いただけるよう支援しています。お客様に提供する卓越した脅威インテリジェンスに加え、IBM Security X-Force は収集した大量のデータを分析し、脅威の全貌とその変化に関する年間の調査結果である「X-Force 脅威インテリジェンス・インデックス」をリリースしています。

追跡した傾向によると、ランサムウェアの急増が続いており、2020 年に X-Force が対応したセキュリティー・イベントの 23% を占める第 1 位の脅威タイプとなりました。ランサムウェアを使用した攻撃者は、データの暗号化と公開サイトへのデータ・リークの脅威を組み合わせることで、支払いを強要する圧力を強めました。このような策略が成功したことで、2020 年にはある犯罪組織が 1 億 2,300 万ドルを超える利益をランサムウェア攻撃を通して手に入れたと X-Force は推定しています。[1]

2020 年には、製造業に携わる複数の企業が激しいランサムウェア攻撃とその他の攻撃にさらされました。最も頻繁に攻撃対象となった業界の中で、2019 年に第 8 位であった製造業は、2020 年には金融・保険業界に次いで第 2 位になりました。X-Force は、新型コロナウイルス感染症ワクチンのサプライチェーンに関与する製造業や NGO に対して、標的を絞り込んだスピア・フィッシング・キャンペーンを使用した巧妙な技術を持つ攻撃者を検知しました。

1 このレポートでは、コストの総額はすべて米ドルで記載されています。

さらに脅威アクターは、ビジネスに不可欠なクラウド・インフラストラクチャーとデータ・ストレージをサポートするオープンソースコードの Linux を標的としたマルウェアの巧妙化を進めました。2020 年の Intezer による分析では、56 もの新種の Linux マルウェア・ファミリーが検出されており、これは、他の脅威タイプで確認された革新レベルをはるかに上回るものでした。

このような中、2021 年はより良い年になるという希望を抱ける理由があります。トレンドを予測するのは難しいことですが、唯一信頼できるもの、それは変化です。増減するサイバーセキュリティーの問題に直面した際のレジリエンスを高めるためには、アクションに繋がるインテリジェンスと、よりオープンでコネクティッドなセキュリティーの未来に向けた戦略的なビジョンが必要です。

コミュニティーによって強さを生み出すという精神に基づいて、IBM Security は「X-Force 脅威インテリジェンス・インデックス 2021」をここにご案内いたします。本レポートの調査結果は、セキュリティー・チーム、リスクの専門家、意思決定者、研究者、メディアなどが、過去 1 年間に発生した脅威の状況を把握し、次に起こりうるあらゆる脅威に備えるための手掛かりとなります。

エグゼクティブ・サマリー

IBM Security X-Force は、2020 年の 1 月から 12 月までの間に、IBM のお客様や公的な情報源から収集した数十億件のデータ・ポイントを用いて、攻撃タイプや感染ベクターの分析、グローバルおよび業界別の比較を行いました。以下は、「X-Force 脅威インテリジェンス・インデックス」で発表された主な調査結果です。

23%

ランサムウェアが攻撃に占める割合

ランサムウェアは 2020 年で最もよく使われた攻撃手口であり、IBM Security X-Force が対応し、修復を支援した全インシデントの 23% を占めています。

1 億 2,300 万ドル超

ランサムウェアによる推定最高被害額

X-Force は、2020 年に Sodinokibi (REvil とも呼ばれる) ランサムウェア・アクターが単独で、少なくとも最低 1 億 2,300 万ドルの利益を得て、約 21.6 テラバイトのデータを盗んだと推定しました。

25%

2020 年の第 1 四半期の攻撃に占める最大の脆弱性の割合

脅威アクターは Citrix のパス・トラバーサルの欠陥を利用し、1 - 3 月までの 3 カ月における全攻撃の 25%、および 2020 年全体における攻撃総数の 8% で、この脆弱性を悪用していました。

35%

上位の攻撃手口に占めるスキャンとエクスプロイトの割合

脆弱性のスキャンとエクスプロイトが、2019 年に第 1 位の手口であったフィッシングを上回り、 2020 年の攻撃手口の第 1 位に跳ね上がりました。

第 2 位

最も頻繁に攻撃を受けた業界での製造業の順位

製造業は 2019 年の第 8 位から順位を上げ、2020 年には金融サービスに次いで 2 番目に多く攻撃された業界でした。

5 時間

脅威グループのサーバー上の攻撃用トレーニング動画の長さ
イランの国家アクターの操作ミスによって、X-Force の研究者は誤って設定されたサーバー上にあった約 5 時間の動画を発見し、犯罪者の手のうちを明らかにすることに成功しました。

100 人超

精度が高いフィッシング・キャンペーンの攻撃対象となった経営幹部の人数
X-Force は 2020 年の中頃に、新型コロナウイルス対策において 個人用防護具（PPE）を確保するタスク・フォースで管理と調達の役割を担う、100 人を超える上級経営幹部に接触したグローバル・フィッシング・キャンペーンを検知しました。

49%

ICS 関連の脆弱性の増加率、2019-2020
2020 年に検知された産業用制御システム（ICS）関連の脆弱性は、2019 年に比べて 49% 増加しました。

56

新種の Linux マルウェア・ファミリーの数
2020 年に検知された新種の Linux 関連のマルウェア・ファミリーの数は、過去最多の 56 件でした。これは 2019 年から 2020 年に比べて 40% の増加となります。

31%

攻撃に占めるヨーロッパの割合
2020 年に最も頻繁に攻撃対象となったのはヨーロッパで、X-Force が観測した攻撃の 31% が同地域で発生しました。その後に、北アメリカ（27%）とアジア（25%）が続きます。

将来の展望

2021 年には、新旧の脅威が混在するため、セキュリティー・チームは同時に多数のリスクを考慮することが求められます。X-Force の分析に基づいて、2021 年に優先的に考慮すべき重要事項を以下に示します。

- **リスクの範囲は 2021 年も引き続き拡大する。**新旧両方のアプリケーションやデバイスで、数千種類の新しい脆弱性が報告されるでしょう。
- **ランサムウェアによる二重の恐喝は 2021 年も引き続き発生する。**ランサムウェアの脅威アクターは、さらに巧妙な手口を使って、リークサイトでのデータの公表をちらつかせ、高額な身代金を要求します。
- **脅威アクターは、今後も様々な攻撃手口に照準を移していく。**Linux システム、オペレーショナル・テクノロジー (OT)、IoT デバイス、クラウド環境は、引き続き攻撃対象となります。こうしたシステムやデバイスへの攻撃が高度化するにつれて、脅威アクターは手法を素早く変更すると考えられます。特に注目度の高いインシデントの後は、その傾向が顕著になります。
- **どの業界にもリスクは存在する。**各業界における攻撃状況は前年から変化しています。リスクはすべての業界にあると考え、業界の枠を超えてサイバーセキュリティー・プログラムを意味のあるものに進化、成熟させていく必要があります。

レジリエンスに関する推奨事項

このレポートで説明した IBM X-Force の知見に基づいて、脅威インテリジェンスの最新情報を把握し、強力な対応能力を備えることが、あらゆる業界と国にとって、高度化する脅威から自組織を守り、被害を軽減するための効果的な方法です。

2021 年 のサイバー脅威に備えるために組織が実行できる対策として、X-Force は以下を推奨します。

脅威に反撃するのではなく、事前に脅威を阻止する。脅威インテリジェンスを活用して、脅威アクターの動機と戦術をより深く理解し、セキュリティーのリソースを優先順位付けします。

十分な備えによってランサムウェア攻撃に対処する。ランサムウェア攻撃への対応計画（ランサムウェアとデータ窃盗を組み合わせた脅迫手法への対応など）を策定し、その計画の実施訓練を定期的に行うことによって、重大な局面での対応を格段に強化することができます。

組織のパッチ管理の構造を二重にチェックする。2020 年はスキャンとエクスプロイトが攻撃手口として最も多かったことを踏まえて、インフラストラクチャーを補強し、内部での検知機能を刷新して、自動化された悪用攻撃を迅速かつ効果的に検知し遮断します。

インサイダー脅威を防止する。データ損失防止 (DLP) ソリューション、訓練、およびモニタリングによって、悪意あるインサイダーや不注意による組織への侵害を防ぎます。

組織内でインシデント対応チームを編成し、訓練する。それが難しい場合は、インシデント対応能力を有効活用し、影響力の大きいインシデントに速やかに対応できるようにします。

組織のインシデント対応計画のストレス・テストを実施し、即時対応力を身につける。インシデント対応チームが机上演習やサイバー・レンジの実体験によって重要な経験を積むことで、データ漏えい発生時の対応時間やダウンタイムを短縮でき、最終的にコストも削減できます。

多要素認証 (MFA) を実装する。アカウントの保護レイヤーを増強することは、今後も組織にとって優先すべき最も効果的なセキュリティー対策の 1 つです。

バックアップを実行、テストし、オフラインで保管する。ランサムウェア攻撃が再び多発していることを示す 2020 年のデータを踏まえて、バックアップの存在を確認するだけでなく、実際にそれをテストしてバックアップの有効性を点検することが、組織のセキュリティーを確保するうえで非常に重要です。

IBM Security X-Force について

IBM Security X-Force は、洞察、検知、対応能力を提供し、お客様がセキュリティー体制を強化できるよう支援いたします。

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、熟練した X-Force インシデント対応チームは、組織がセキュリティー・インシデントやデータ漏えいに対する制御を向上させる上で役立つ戦略的な修復対策を提供します。

X-Force は、IBM Security コマンド・センターのサイバー・レンジでの体験を通して、お客様に今日の脅威の実態に備えるための訓練を提供しています。

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、プレミア脅威インテリジェンス・プラットフォームの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。

次のステップ

IBM Security によるインシデント対応の活用について検討する

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、http://www.ibm.com/jp-ja/security をご覧ください。また、Twitter (@IBMSecurity をフォロー) や IBM Security インテリジェンス・ブログでも、より詳しい情報をご覧いただけます。

協力者

執筆責任者:
カミーユ・シングルトン

協力者:
アリソン・ウィクオフ
アリ・エイタン (Intezer)
チャールズ・デベック
シャーロット・ハモンド
チェンタ・リー
クリス・スペリー
クリストファー・キーファー
クレア・ザボエヴァ
デビッド・マクミレン
デビッド・モールトン
ダーク・ハーツ
ジョージア・プラシノス
イアン・ガラハー (Intezer)
ジョン・ゾラベディアン
ジョシュア・チャン
ケリー・ケイン
ローレン・ジェンセン
リモール・ケッセム
マーク・アッシャー
マシュー・デフィル
ミーガン・ラドナ
メリッサ・フリードリッヒ
ミシェル・アルヴァレズ
ミッチ・メイン
ニック・ロスマン
パティ・カーヒル-イングラハム
ランダル・ロッシ
リチャード・エマーソン
サライナ・ウッケ
スコット・クレイグ
スコット・ムーア

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

Produced in Japan
2021 年 3 月