IBM Security

IBM X-Force 脅威インテリジェンス・インデックス 2020

IBM

Produced by IBM X-Force Incident Response and Intelligence Services (IRIS)

目次

目次

サマリーと主要な傾向

IBM Security は、お客様が今後のサイバーセキュリティーの脅威に備えて、自社のレジリエンスを強化するためのインテリジェントな企業セキュリティーのソリューションとサービスを開発しています。

セキュリティー専門家に最も重要度の高い脅威の最新情報を提供するため、IBM X-Force は新しい脅威や攻撃者の TTP (戦術、技法、手順) についてのブログ、ホワイト・ペーパー、Web セミナー、ポッドキャストを定期的に公開しています。

IBM Security は、「IBM X-Force 脅威インテリジェンス・インデックス」を毎年公開しています。これは、過去 1 年間に IBM の各研究チームが取り上げた最も顕著な脅威をまとめ、組織の保護強化に役立つ情報をセキュリティー・チームに提供するものです。

このレポートで提示するデータと洞察は、IBM Security マネージド・セキュリティー・サービス、インシデント対応サービス、ペネトレーション・テストの取り組み、脆弱性管理サービスから得たものです。

IBM X-Force 研究チームは、何億もの保護対象のエンドポイントおよびサーバーから得たデータを、スパム・センサーやハニーネットなどお客様以外の資産から取得したデータと合わせて分析します。また X-Force 研究チームは、世界中でスパム・トラップを実施し、何千万ものスパムとフィッシング攻撃を毎日監視しています。何十億もの Web ページと画像を分析して、攻撃キャンペーンや不正なアクティビティー、企業価値の悪用を検知して、お客様と、あらゆるものがつながる社会をより適切に保護しています。

X-Force Incident Response and Intelligence Services (IRIS) は、過去 1 年間の IBM Security のソフトウェアおよびセキュリティー・サービスの分析情報を集め、2019 年は、かつての脅威が再び姿を現して新たな方法で使用されたということを示しました。

- X-Force のデータによると、2019 年にはオペレーショナル・テクノロジー (OT) を標的にしたインシデントが 2000% 増加しています。これは脅威アクターが 2020 年にかけて、製造システムを攻撃しようと関心を高めている可能性があることを示しています。

- 2019 年は、2018 年の漏えいレコード件数より 200% 以上多い、85 億件を超えるレコードが漏えいしました。この著しい増加の原因は主に、不注意な内部関係者によるものです。適切に構成されていないサーバー (公的にアクセス可能なクラウド・ストレージ、保護されていないクラウド・データベース、適切に保護されていない rsync バックアップ、オープンなインターネットに接続されたネットワーク・エリアのストレージ・デバイスなど) が原因で漏えいしたレコードは、2019 年のレコード漏えいの 86% を占めました。

- 2019 年のマルウェアの状況に目を向けると、脅威アクターがランサムウェアに回帰して、ボットネットを構築するという変化がありました。X-Force IRIS は 2019 年に 5 大陸 12 カ国、13 の業界にわたってランサムウェアが関与したインシデントに対応しました。破壊的なマルウェアのアクティビティーは急増しており、大惨事につながるマルウェアのこの傾向が引き続き脅威の増大につながることを示しています。

- X-Force IRIS が 2019 年に関わった事案における攻撃手口のトップスリーは、1 位フィッシング (31%)、2 位スキャンおよび悪用 (30%)、3 位資格情報の盗難 (29%) であり、非常に僅差でした。特に注目すべきなのはフィッシングで、2018 年ではインシデント総数の半数近くを占めていましたが、2019 年には 1/3 未満になりました。それに対し、脆弱性のスキャンおよび悪用は、2018 年にはわずか 8% であったのが、インシデントの 1/3 位までに増加しました。

- X-Force の世界のスパム・アクティビティーの分析では、スパム・メールで使用される脆弱性は依然としてごく一部であり、特に 2017-0199 と 2017-11882 の 2 つの CVE に集中していることがわかりました。これらはパッチ提供済みの脆弱性ですが、脅威アクターがスパム・キャンペーンによって悪用しようとした脆弱性の 90% 近くを占めています。

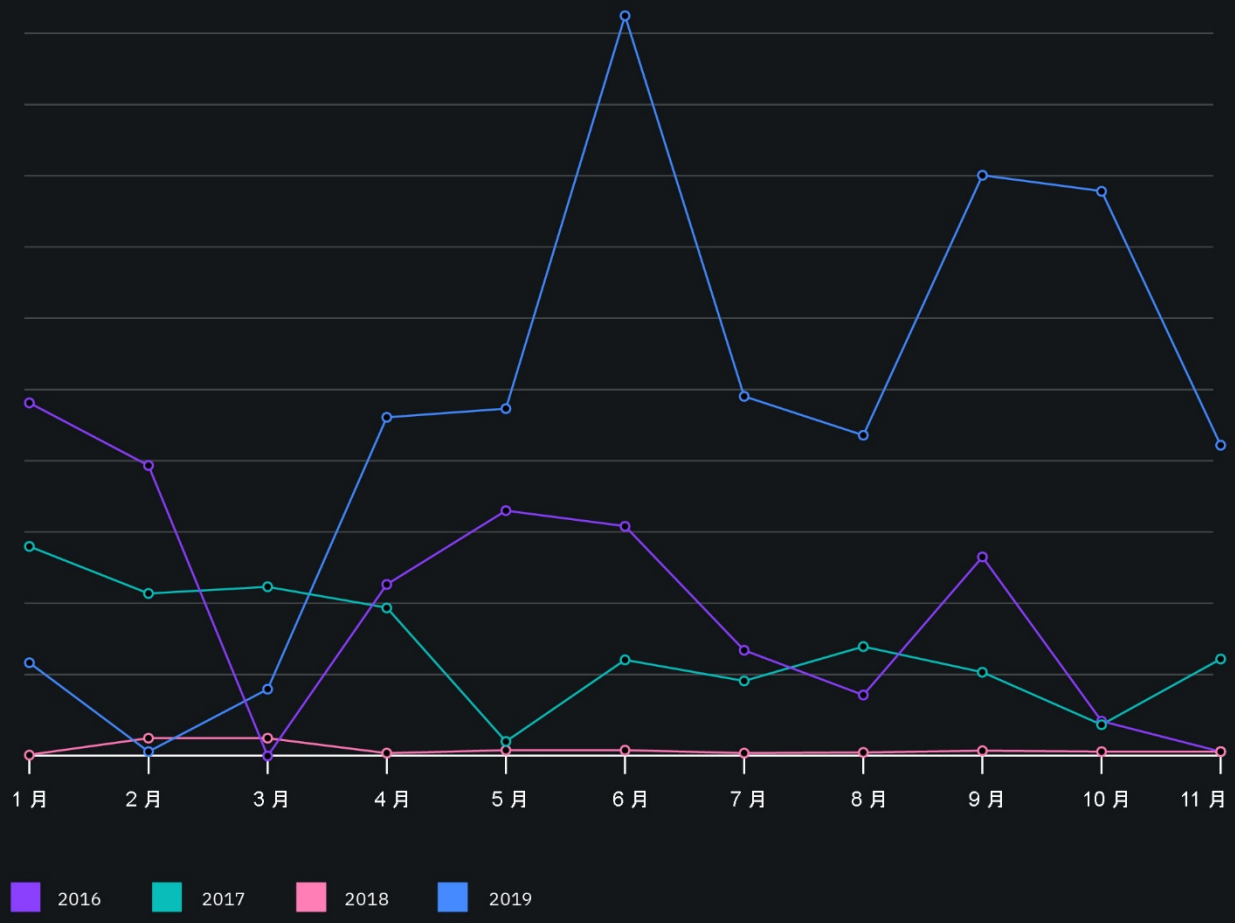
- 2019 年に最も頻繁に攻撃対象となった部門のトップは、依然として金融サービスですが、脅威アクターにとって業界に特化した標的設定の優先順位が変わりつつあることが浮き彫りになっています。小売り、メディア、教育、政府は、いずれも世界で最も頻繁に攻撃対象となった部門一覧で、順位を上げています。

- 本年の X-Force 脅威インテリジェンス・インデックスでは、地域的に見た洞察を新たに取り入れ、世界中で観測される傾向に関するデータを提供します。IBM Security は、全地域を標的とする複数の脅威アクターを引き続き追跡します。このレポートでは、各地域を標的とする主要な脅威アクター、2019 年に観測された攻撃、そして 2020 年のサイバーセキュリティーの脅威になり得そうなことについて説明します。

今年のレポートの次のセクションでは、2019 年の主要な傾向について詳しく調べ、それらの要因を掘り下げます。

標的および攻撃手口

図 1:
オペレーショナル・テクノロジー (OT) 攻撃の傾向
2016-2019 年で比較した毎月の OT 攻撃件数 (出典: IBM X-Force)



オペレーショナル・テクノロジー (OT) インフラストラクチャーを標的とする脅威の爆発的な増加

IBM X-Force のデータでは、脅威アクターが産業用制御システム (ICS) などのオペレーショナル・テクノロジー (OT) 資産を標的としたイベントが 2018 年以降 2000% 以上増えていることが示されています。実際、2019 年の OT 資産を標的としたイベントの件数は、過去 3 年間に観測されたアクティビティーの件数を超えました。

観測された攻撃の大半は、SCADA と ICS ハードウェア・コンポーネント内の既知の脆弱性の組み合わせを利用したものや、ICS を標的とした総当たりログイン戦術を利用したパスワード・スプレー攻撃が中心でした。

一部の報告によると、ICS 攻撃に焦点を当てたアクティビティーは 2 つの既知の脅威アクターと関連があり、IBM がテレメトリーで観測した攻撃タイムラインの急増と一致します。2 つの特定のキャンペーンを実行した Xenotime グループと Hive0016 (APT33) が、ICS を標的とした攻撃を拡大したとされています。

PLC (プログラマブル・ロジック・コントローラー) や ICS (産業用制御システム) のように IT インフラと OT (オペレーショナル・テクノロジー) が重なりつつある状況は、こうしたハイブリッド・インフラストラクチャーで業務を行う組織にとって、2019 年も引き続きリスク要素となりました。

IT/OT インフラストラクチャーが集約されることで、IT セキュリティーへの侵害が、物理資産を制御する OT デバイスにも及ぶようになったため、復旧にかかるコストが増加しています。例えば 2019 年前半に、IBM X-Force IRIS がセキュリティー侵害への対応を支援したある世界的な製造会社では、IT システムから始まったランサムウェアの感染がラテラル・ムーブメントにより OT インフラストラクチャーへと広がり、工場の運営を一時停止するまでに追い込まれました。攻撃は企業自体の運営に影響を与えただけでなく、世界市場にも波及効果をもたらしました。

2019 年にお客様にお届けした X-Force IRIS のセキュリティー・アセスメントでは、既存のソフトウェアやハードウェアが使用されていることが多い OT システムの脆弱性について取り上げました。パッチが適用できなくなり、公開されてから長年経過した古い脆弱性だらけの実動システムでは、OT システムがインターネット接続されていなくても、パッチが適用されていない OT システムが格好の餌食になる恐れがあります。ラテラル・ムーブメントの場合、攻撃者は最初の足場を確保し、その後にこうしたシステムにネットワーク内部からアクセスするため、比較的単純な悪用技法で被害に遭ってしまいます。

図 1 に示されるように ICS ネットワーク攻撃の傾向は、 2019 年 10 月前半以降下降していますが、世界中でさまざまな脅威アクターが製造業のネットワークに対する攻撃キャンペーンを企てて遂行していることから、ICS を標的とした攻撃が 2020 年も増加し続けると X-Force は予測しています。
2019 年には 200 件を超える新たな ICS 関連の CVE が公開されており、 IBM X-Force の脆弱性データベースからも、 ICS に対する脅威が 2020 年も引き続き増える可能性が高いことがわかります。世界中でさまざまな脅威アクターが製造業のネットワークに対する攻撃キャンペーンを企てて遂行していることから、 X-Force は ICS を標的とした攻撃は 2020 年も増加し続けると予測しています。

世界中でさまざまな脅威アクターが製造業のネットワークに対する攻撃キャンペーンを企てて遂行していることから、ICS を標的とした攻撃が 2020 年も増加し続けると X-Force は予測しています。

漏えいレコード数の劇的増加

漏えいレコードの件数は 2019 年に大きく跳ね上がり、85 億件を超えるレコードが漏えいしました。これは、2018 年同期比の 3 倍超に相当する数です。大幅な増加の第一の理由は、不適切な構成によるレコードの漏えいが前年比で 10 倍近く増加したことです。こうしたレコードは、2019 年のレコード漏えいの 86% を占めますが、2018 年に IBM が報告した内容からはかけ離れています。2018 年には不適切な構成によるレコードの露出は 2017 年から 52% 減少したことが観測され、こうしたレコードはレコード総数のわずか半数未満だったのです。

注目すべきことに、2019 年には不適切な構成によるインシデントの件数は前年比で 14 % 減少しました。この事実から、2019 年は不適切な構成による漏えいが 1 件発生した場合に影響を受けるレコードの件数が著しく増えたということがわかります。1 億件超のレコードが漏えいしたセキュリティー侵害の 3/4 近くが、不適切な構成によるインシデントでした。不適切な構成が原因で発生したインシデントの中でも専門サービス部門で発生したうちの 2 件では、漏えいしたレコード件数が 1 インシデントあたり数十億件に上りました。

このように失われたレコード数が業界全体で著しく増加していることは、通常は主な標的と考えられていなかった部門の企業でさえ、データ漏えいのリスクが高まっていることを浮き彫りにしています。

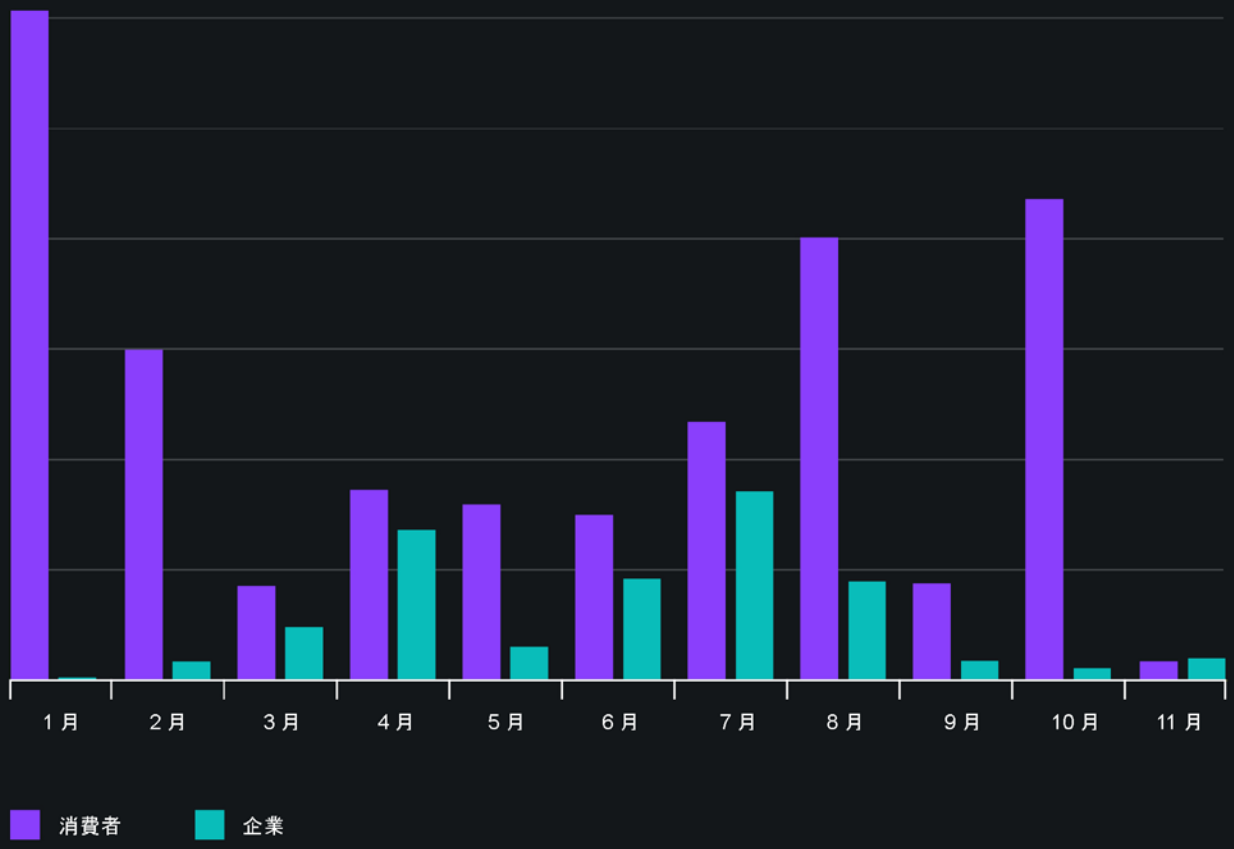
2019 年に漏えいしたレコード数

85 億

図 2:

消費者 IoT 対企業 IoT 攻撃件数

2019 年の消費者 IoT 対企業 IoT の毎月の攻撃件数 (出典：IBM X-Force)



企業における IoT デバイスが標的対象に

2020 年には 380 億超のデバイスがインターネットに接続すると見込まれます。モノのインターネット (IoT) の脅威は徐々に発展しており、消費者と企業の運用に影響を与え得る脅威ベクトルの 1 つとなっています。比較的シンプルなマルウェアと自動化された (多くの場合はスクリプト化された) 攻撃がこれを可能にしています。

悪意あるコードの IoT デバイスへの感染という観点から、IBM X-Force 研究チームは、2019 年の複数の Mirai マルウェア・キャンペーンを追跡しました。すると、標的が消費者向けのエレクトロニクスから、企業のハードウェアもターゲットとするようにシフトしたことがわかりました。これは 2018 年には観測されなかったアクティビティーです。ネットワーク・アクセスによるセキュリティー侵害を受けたデバイスを、攻撃者がピボット・ポイントとして使用し、組織内での足掛かりを築いてしまう可能性があります。

Mirai は、2016 年以降複数の攻撃者の手によって用いられている拡散型の IoT マルウェアです。多数の IoT デバイスに感染させて分散型サービス妨害 (DDoS) 攻撃を行うのに利用され、大規模な混乱を引き起こしています。IBM は 2019 年のキャンペーンについて分析を行い、Mirai マルウェアを扱う攻撃者の TTP (戦術、技法、手順) が 2018 年以降確実に変化しており、2019 年には消費者向けエレクトロニクスに加えて企業のハードウェアを標的とすることに焦点が当てられていることを発見しました。

2019 年に IoT デバイスに影響した攻撃という観点では、さまざまな種類の IoT デバイスを標的とする悪意のあるペイロードをダウンロードする命令が含まれたコマンド・インジェクション (CMDi) 攻撃が広く使用されたことが観測されました。こうした感染攻撃の大半は、スキャンして見つけたデバイスに一斉感染を試みるスクリプトにより自動化されています。標的の IoT デバイスが感染攻撃に対して脆弱である場合、ペイロードがダウンロードされて実行され、そのデバイスを巧妙に大規模な IoT ボットネットとしてしまいます。こうした攻撃を可能にする最も一般的な要因の 1 つは、粗末な辞書攻撃で簡単に推測されるようなセキュリティーの弱いパスワードや、デフォルトのパスワードを使用している IoT デバイスです。

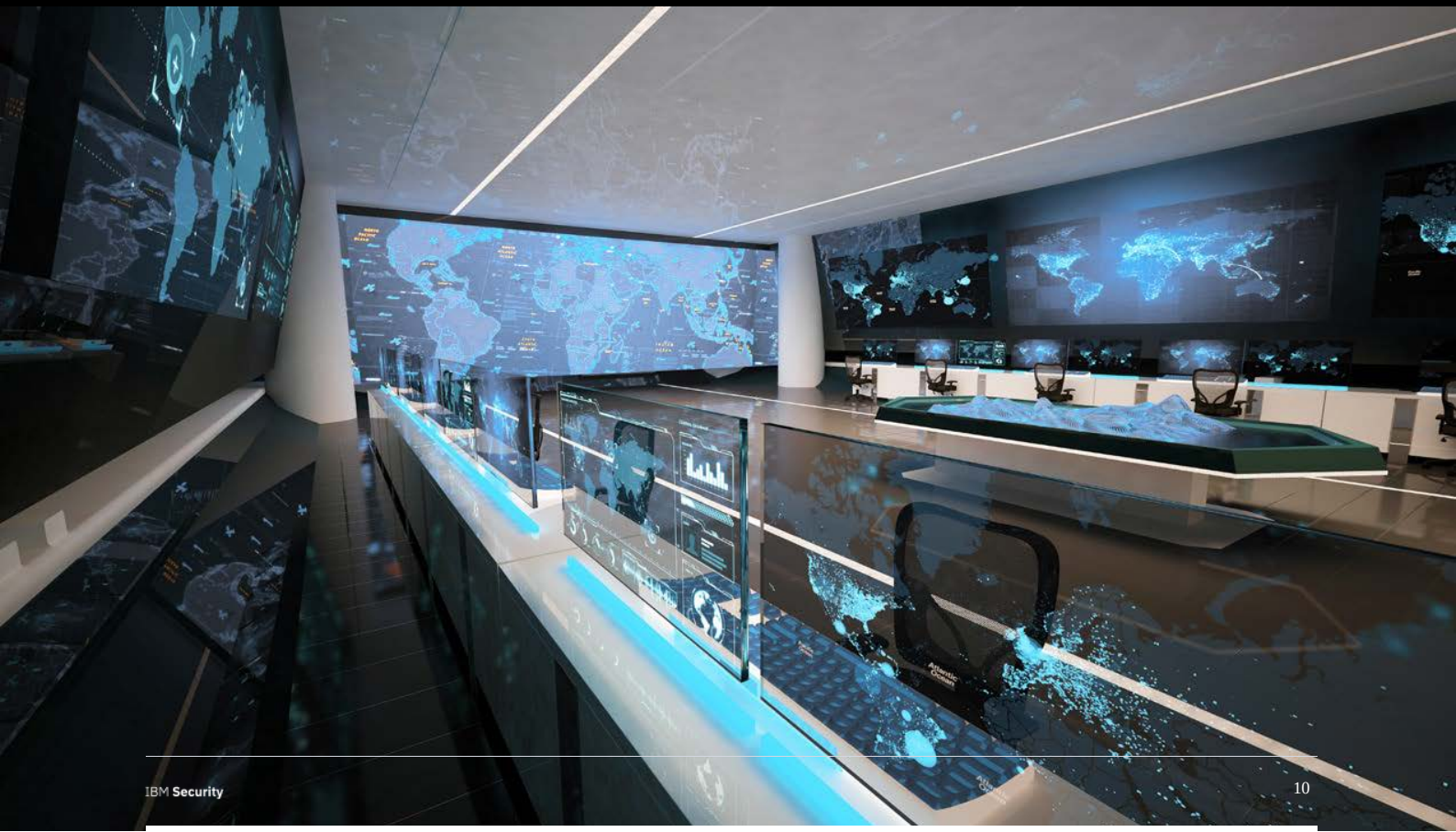
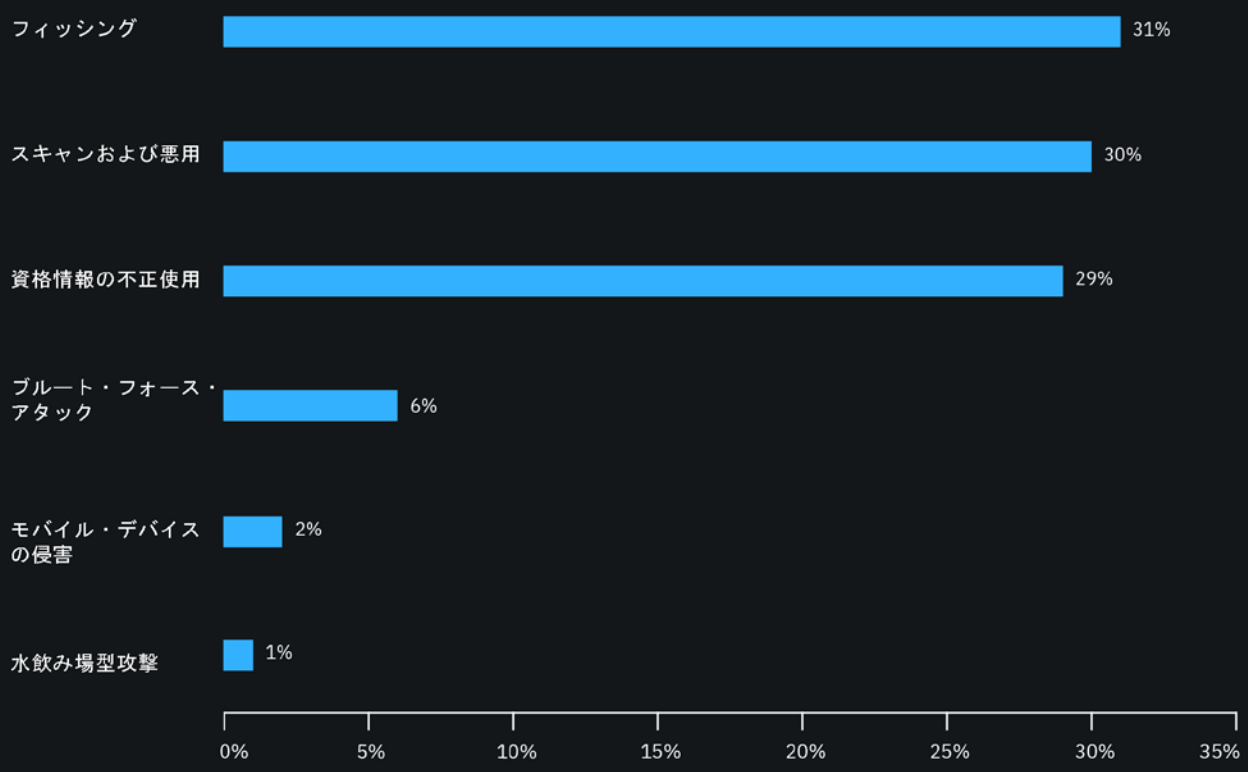


図 3:
上位の攻撃手口
2019 年の攻撃手口上位 6 つの内訳 (6 つの手口をパーセンテージで表示)(出典: IBM X-Force)

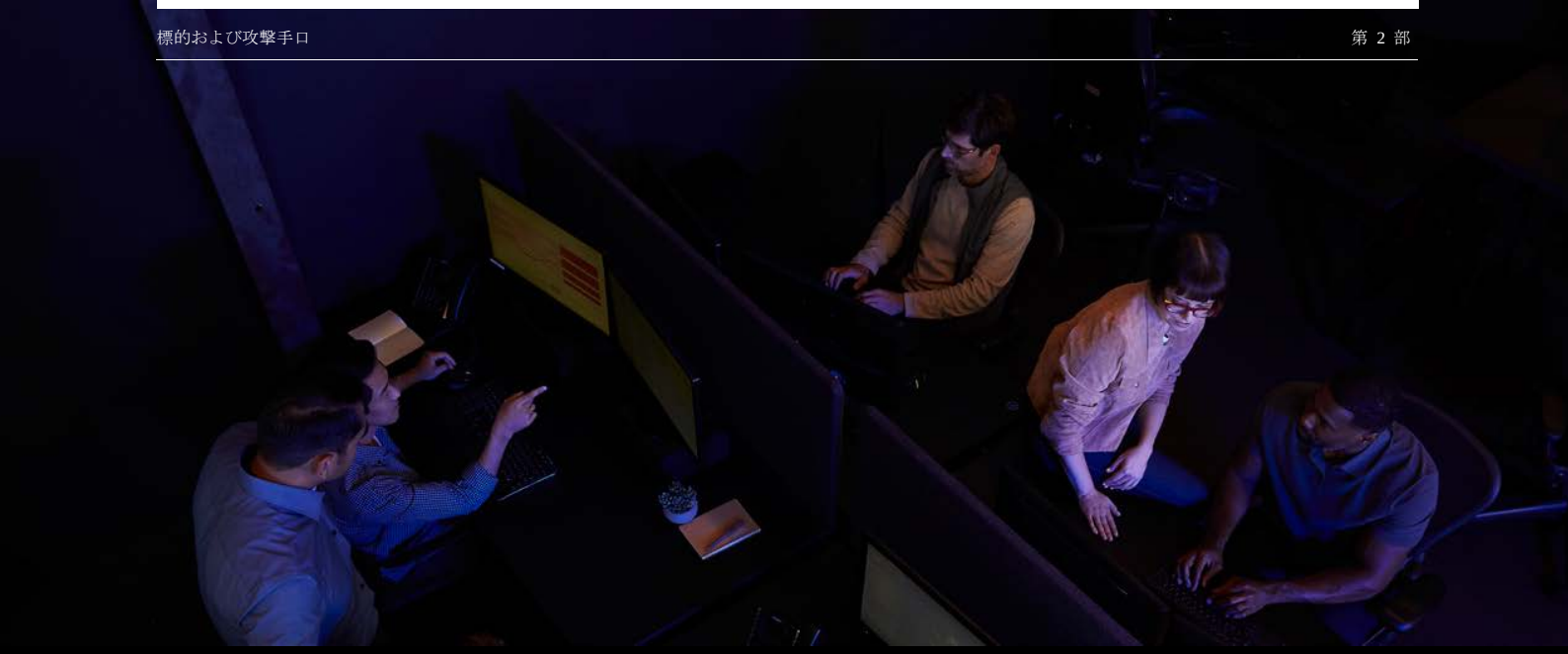


フィッシングが攻撃手口のランキング最上位に

IBM X-Force IRIS の広範囲に渡ったインシデント対応により、攻撃者の手法や動機について貴重な洞察がもたらされました。

2019 年に攻撃起点として最も頻繁に使用された手口は、31% を占めるフィッシングでしたが、2018 年には、インシデント総数の半数近くであったことに比べると減少しています。[1]

[1] 「X-Force 脅威インテリジェンス・インデックス 2019」の報告では、X-Force IRIS が分析した 2018 年の攻撃のうち 3 分の 1 近くの 29% が、フィッシング・メールによる侵害に関するものであったと書かれています。刊行後に複数のインシデントについて新たな証拠が生じ、それらを考慮すると、2018 年におけるこの数値は 44% に増加することがわかっています。



2019 年にとりわけ顕著であったのは、攻撃者が標的の環境をスキャンし、悪用できる脆弱性を探すケースが増えたことです。インシデント対応者は、30% のインシデントにこの技法が使用されていることを発見しました。インシデント総数のわずか 8% だった前年から増加しています。

脅威アクターには、スキャンして悪用する脆弱性の選択肢が多数あります。IBM X-Force は、公表されている 150,000 件を超える脆弱性について追跡しました。高度な技術を持った攻撃者はゼロデイ・エクスプロイトを開発することができるかもしれません。しかし新たな TTP を作り上げるためのリソースを費やす必要はなく、最初の足掛かりを得るのに既知のエクスプロイトが多く利用されており、最も防御が堅いネットワークの攻略用に最強の武器を取っておくことができます。さらにいうと、パッチを適用して最新状態にしていない組織を狙うだけでなく、パッチが一定期間公開されている脆弱性ですらつけこみます。例えば WannaCry 感染の実例は、最初の感染が発生し、パッチ (MS17-010) が広く公表されてから 2 年以上も観測され続けています。

脅威アクターが以前に取得した資格情報を利用して標的の組織にアクセスする資格情報の盗用は、1/3 近く (29%) に上りました。こうした資格情報の多くは、サード・パーティーのサイトから盗まれるか、標的の組織に対するフィッシングによって取得されます。脅威アクターが、盗んだ資格情報を正当なトラフィックに紛れ込ませる場合があり、これにより検知がいっそう難しくなっています。

ブルート・フォース・アタックは全ケースの 6% で前年より順位を下げ、3 位から大きく差のついた 4 位となりました。その後に、標的の組織への最初のアクセス・ポイントとして BYOD デバイスを利用するケースが 2% で続きます。

X-Force の研究者は、2019 年 6 月と 7 月に脅威アクターのアクティビティーが著しく増加しているのを観測しました。そのイベント件数は、その時点までの 2019 年の全イベント数を超える数です。アクティビティーのこの急激な増加の理由は不明ですが、夏季シーズンはスパムもよりアクティブに活動するようで、2019 年 8 月、スパム件数はそのピークを記録しました。単に脅威アクターの活動が目立ったため、簡単に検知された可能性もありますが、脅威アクターの戦術やツールの変化によって重大なアクティビティーが生成された可能性もあります。新たな脅威アクターが市場に出現すると、アクティビティーの増加は一時的に急上昇するというより、じわじわと増加すると予測されます。今回アクティビティーのピークが短期間であることからして、そうした脅威アクターが出現した結果である可能性は低いと考えられます。

マルウェアの傾向

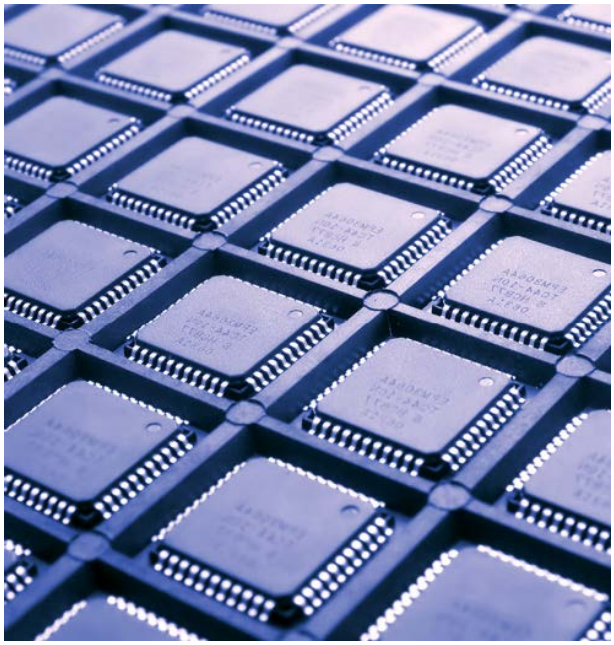
破壊的マルウェア攻撃が激増

IBM X-Force IRIS の調査によると、2019 年を通して破壊的マルウェア攻撃がより頻繁に発生し、地域とその範囲が広がりました。

サイバー犯罪者と国家アクターの両方が利用する破壊的マルウェアは、影響を受けたシステムを操作不可能にし、再構成を困難にする悪意のあるソフトウェアです。大半の破壊的マルウェアの新種は、オペレーティング・システムの実行に不可欠なファイルを削除したり上書きしたりします。少数ですが破壊的マルウェアが作り替えたメッセージを製造機器に送信し、誤動作を引き起こすケースもありました。マシンからデータをワイプしたり、暗号化して元に戻せないようにしたりする種類のランサムウェアは、破壊的マルウェアの定義に含まれます。

2018 年後半から 2019 年後半に、X-Force IRIS は、前年と同数の破壊的攻撃に対応し、こうした大惨事になり得るマルウェアによって組織が引き続きリスクにさらされることを強調しています。

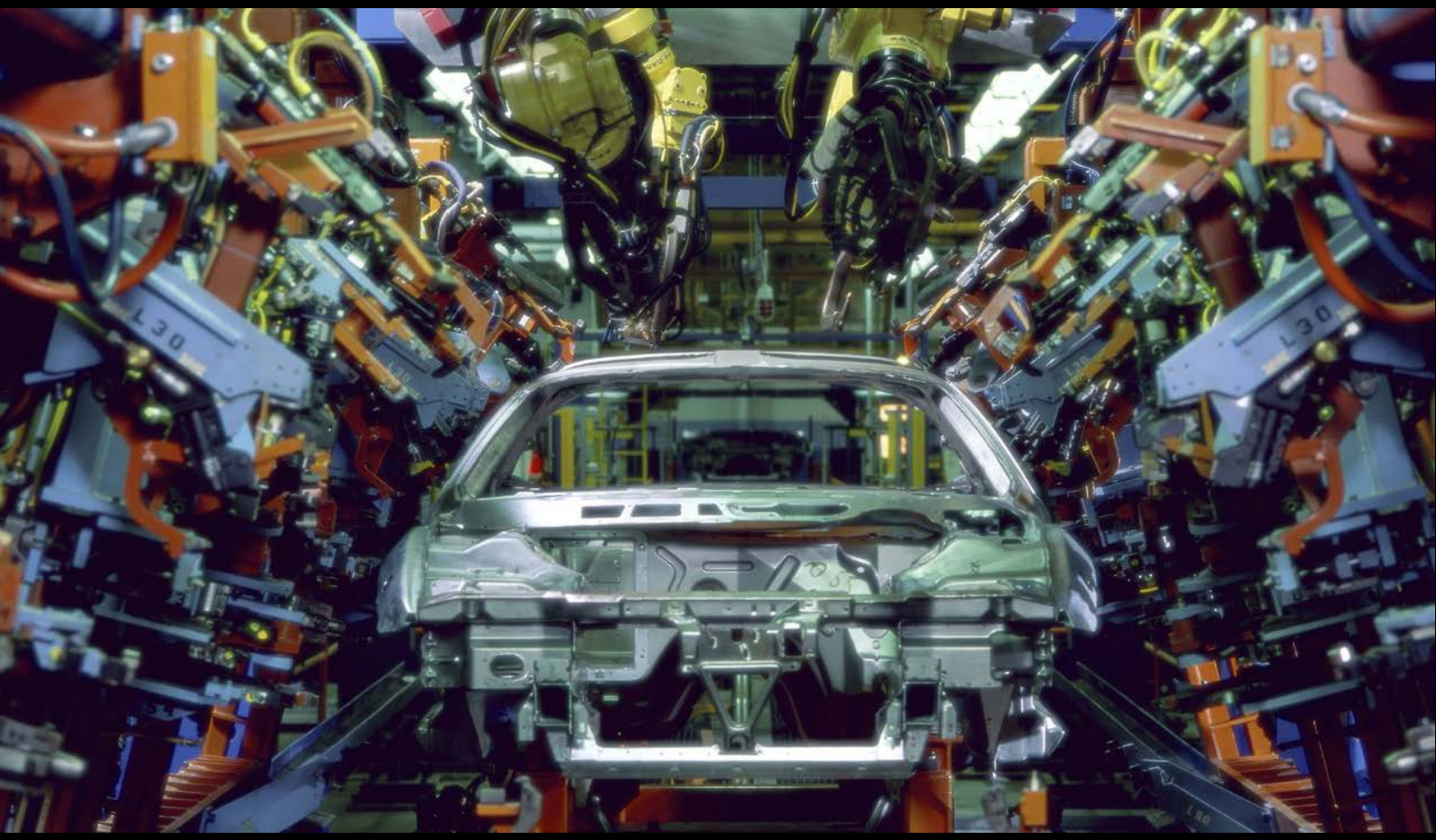
従来、破壊的攻撃は一般に国家アクターによるものでした。しかし、破壊的要素を攻撃に取り込む金銭狙いのランサムウェアが増えるという傾向が見られ、2018 年後半から 2019 年前半には LockerGoga や MegaCortex などの新種が初めて登場して破壊的攻撃を行いました。



破壊的攻撃のコストは平均 2 億 3900 万ドルと見込まれます。これはデータ漏えいの平均コストの 60 倍を超える金額です。

2019 年後半に X-Force IRIS は、新たな破壊的マルウェアを検知し、ZeroCleare と命名しました。このワイパーは中東のエネルギー部門を標的としたもので、IBM はこれをイラン関連の APT グループ ITG13[2] (別名 APT34/OilRig) によるものと見なしました。

X-Force IRIS は、企業にかかる破壊的マルウェア攻撃のコストは特に高く、大手多国籍企業となるとインシデントあたり平均 2 億 3900 万 ドルのコストを負担していると見積もっています。このコストの見積りは、米調査会社ポネモン・インスティテュートが算出した 2019 年のデータ漏えいのコスト平均の 60 倍以上です。データの窃盗や露出などのデータ漏えいと異なり、破壊的攻撃では、通常、被害に遭った組織のネットワーク上の全デバイスの最大 3/4 以上が破壊されています。



[2] ITG は、IBM Threat Group の略語であり、この用語については「最も頻繁に攻撃対象になった業界」で詳細に説明されています。X-Force では、ITG 名を使用しており、ITG 名の後に括弧で囲んで脅威グループの代替名を示しています。

2019 年に猛威を振るったランサムウェアおよびクリプトマイナー

マルウェアの新種とマルウェアを利用した攻撃の数は年間を通して浮き沈みがありますが、それでも優先すべき種類の脅威に関する洞察をご提供することは、組織のリスクに対する適切な対応をサポートすることにつながると考えています。

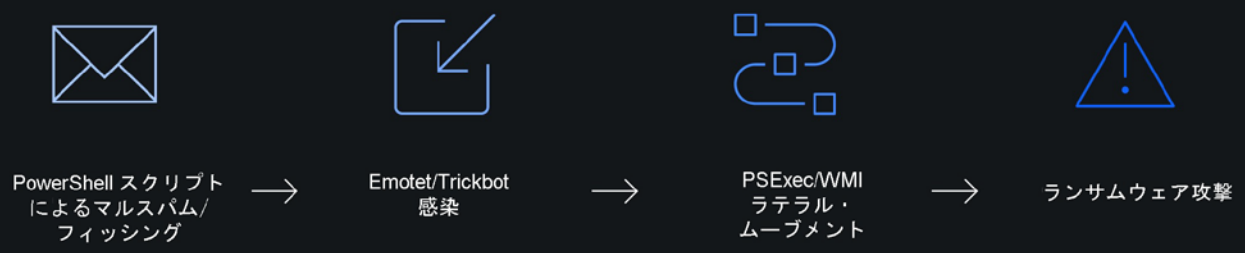
2019 年前半、IBM が観測した攻撃の約 19% がランサムウェアのインシデントに関連するものでしたが、2018 年後半のそれは攻撃のわずか 10%でした。2019 年第 4 四半期には、前年の第 4 四半期と比較して、ランサムウェアの関与が 67% 増加しました。X-Force IRIS は 2019 年に 5 大陸 12 カ国、13 の業界にわたってランサムウェアが関与したインシデントに対応しました。

この急増の原因は、2019 年に、脅威アクターの数と、さまざまな組織に対して開始された攻撃キャンペーンの数が増加したことである可能性があります。注目すべきは、地方自治体や医療機関に加えて、地方公共機関もランサムウェア攻撃の被害に遭ったことです。これらの組織に対する攻撃は、多くの場合、攻撃対象の対応準備が整っておらず、身代金を支払う可能性が高く、場合によっては公共の安全と人命の安全を確保するため攻撃から回復せざるを得ないという状況に付け込んだものです。

X-Force のデータによると、2019 年のランサムウェア攻撃の最上位の攻撃手口は Windows Server Message Block (SMB) プロトコル内の脆弱性に対するエクスプロイトを試み、ネットワーク経由で伝搬するものでした。以前 WannaCry 攻撃で使用されたこの戦術は、観測された攻撃試行件数の 80 % 超を占めます。

2019 年第 4 四半期には、2018 年の第 4 四半期と比較して、ランサムウェアの関与が 67% 増加しました。

図 4:
多段階式で展開するランサムウェア感染
多段階式感染ルーチンによるランサムウェア攻撃 (出典: IBM X-Force)



SMB プロトコルの脆弱なバージョンに対する攻撃の自動化が可能なので、脅威アクターにとっては低コストな選択肢であるというだけでなく、1 回の攻撃で可能な限り多くのシステムに影響を及ぼすよう容易に規模拡大することができます。

また脅威アクターは多くの場合、Emotet や TrickBot などのコモディティー・ダウンローダーを使用して、標的のシステム上でランサムウェアを実行しました。この技法では PowerShell を活用してマルウェアをダウンロードし、検知がますます困難な PSExec や Windows Management Instrumentation (WMI) などのネイティブ関数を使用してこれを広めていました。

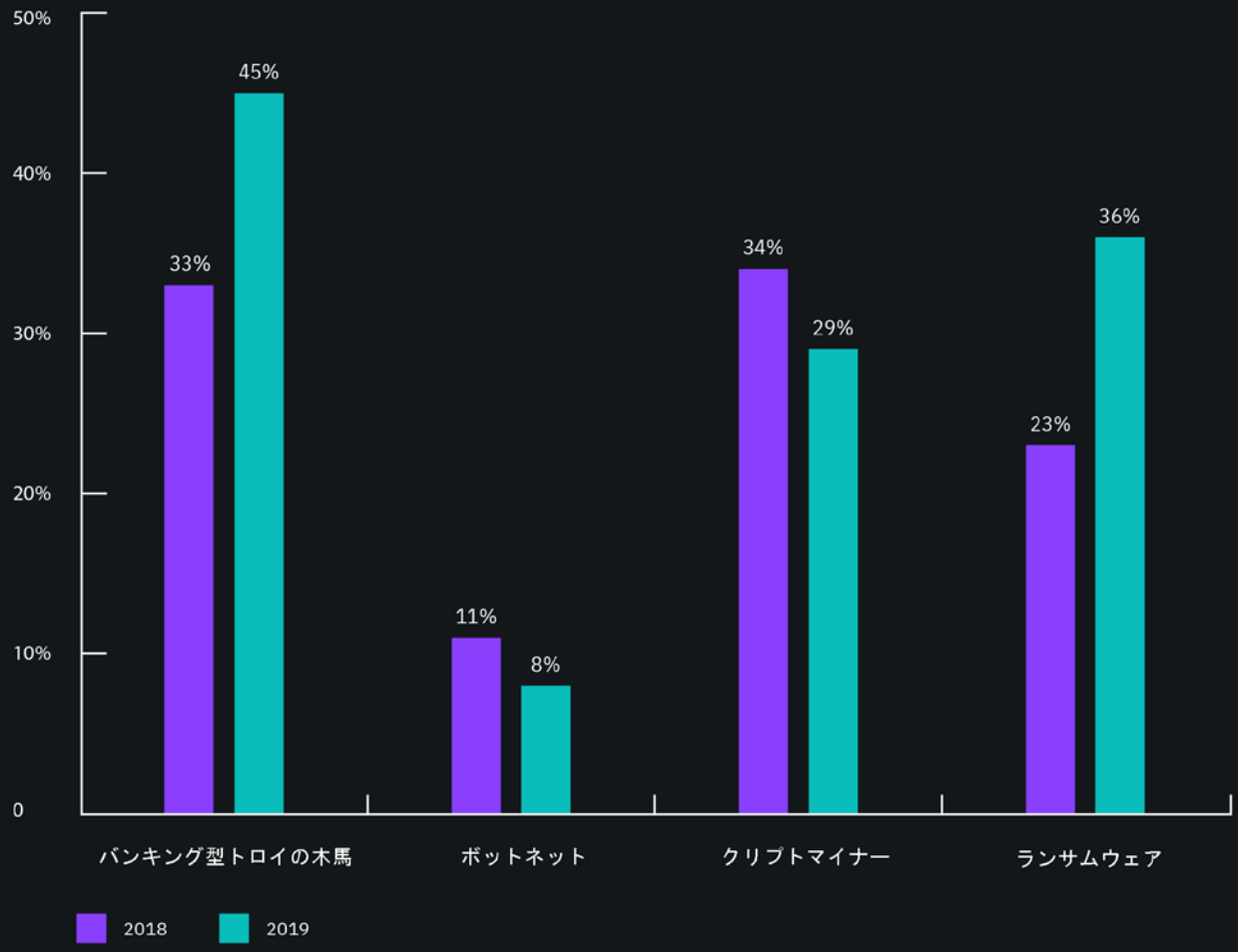
攻撃者は、ランサムウェアを使って直接攻撃するのではなく、多段階式でユーザーを感染させます。攻撃を思い通りに行い、管理機能と検知機能から逃れ、そして、被害者が支払わざるを得ないようにするべく十分な数のデバイスを包囲するランサムウェア操作の種を植えるためです。その忍耐と計画の見返りは大きく、Ryuk を使用する犯罪グループが Ryuk 攻撃によって 5 カ月間で得た金額は、370 万ドルを超えます。また、Ryuk を使った犯罪者たちが、米国内の介護施設に対して行った攻撃で 1400 万ドルを要求した例もあります。

2019 年に急増したマルウェア・タイプはランサムウェアだけではありません。2019 年に大流行したもう 1 つのマルウェア・タイプは、仮想通貨マイニング・コードです。

X-Force のテレメトリーによれば、クリプトマイニング (仮想通貨マイニング) の活動は、2019 年の中頃にこれまでにないレベルに急増し、6 月の活動量は、年の残りの 11 カ月の合計をほぼ上回っていました。

マルウェアのトレンドは、これらの操作ボットネットの動機とリソースに従って浮き沈みしますが、クリプトマイニングの急増は、マルウェア・マイナーが頻繁に使用する仮想通貨、Monero の価値が 3 倍に上昇したことに関連している可能性もあります。

図 5:
マルウェアの遺伝的コードのイノベーション
カテゴリー別の新型 (未観測) コードのパーセンテージ、2018-2019 (出典：Intezer)



2019 年のマルウェア・コードの進化における トップ・イノベーター

新しいマルウェアの変種を検知するために以前行われた X-Force とのコラボレーションを参考にして、Intezer はマルウェアの「イノベーション」を測定しています。マルウェアの遺伝学的分析技術を使用して、コードの類似性とコードの再利用度合いを調べ、すべてのソフトウェア・コードの遺伝的起源を明らかにしています。このイノベーションの測定値は、脅威アクターが新しいコードの開発にどの程度投資したかを表す指標で、攻撃者が自身の攻撃能力の拡大と検知の回避をどれくらい目指しているかを示しています。

Intezer のデータによると、2019 年、脅威アクターたちは主にバンキング型トロイの木馬とランサムウェアのコードベースの開発と進化に力を注ぐ一方で、各種のクリプトマイニング・マルウェアの修正と作成に継続的に多大な労力を割いていました。

本レポートのこのセクションは、IBM X-Force と Intezer の研究者たちが共同で執筆しました。Intezer は、マルウェアのバイナリー・コードの「遺伝学的」分析を行っています。

2019 年 はバンキング型トロイの木馬において新しいコードの割合が最も高く (45%)、次いでランサムウェア (36%) となりました。IBM はこれまで、脅威アクターの関心が、企業ユーザーに有効なマルウェア・タイプにあり、それに対して投資していることを観測してきました。これは、これらのマルウェア・タイプが 2020 年に企業を標的にする可能性があることを示しています。もしこれらのマルウェアが継続的に進化しない場合は、マルウェアの検知がさらに迅速になり、攻撃者が得る投資の見返りが徐々に少なくなるため、バンキング型トロイの木馬とランサムウェアの実行者は消滅していくと考えられます。

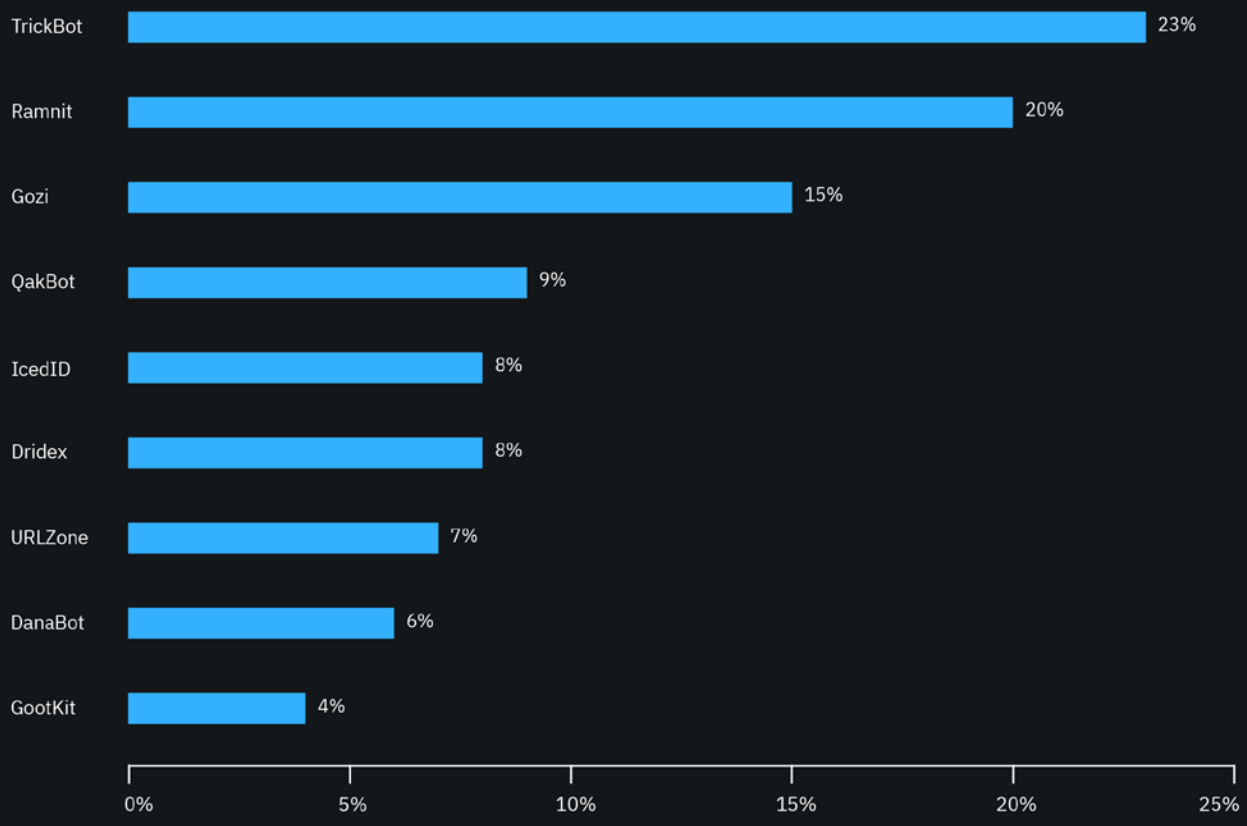
クリプトマイナーは 2019 年にイノベーションが減少したものの、マイニング活動は依然として活発に行われているため、脅迫アクターたちが従来のコードを改修して新しいバージョンのクリプトマイナーの開発を続けていると考えられます。IBM の経験に基づくと、これらの単純なマルウェア・コードは、多くの場合、別の悪意のないコードから派生しています。例えば、違法なやり方で仮想通貨を収集するように修正された XMRig などがあります。また、新しいクリプトマイナーは、IoT デバイスや感染したサーバー (CPU 性能が小型のデバイスや PC よりも高い) での仮想通貨の収集など、それぞれの目的で開発されています。

一方で、汎用的なボットネット・マルウェア (8%) のコード・イノベーションは年々減少しており、機能の修正への投資が減少していることを意味します。IBM は、スパムまたは悪意のある広告からユーザーにプッシュされるこれらのタイプのコードを観測してきました。汎用的なボットネット・マルウェアの主な役割は、感染したデバイス上に足掛かりを得ることですが、その機能は最低限で済みます。このことが、ボットネット・マルウェアのコードが大きく進化しない理由といえるでしょう。

2020 年に向かい、これらのコード・イノベーションのトレンドを見ると、継続的なコード進化を行うよう投資されているマルウェアに対して、我々は特定や封じ込めにもっと注力する必要があるといえるでしょう。

2019 年、脅威アクターたちはバンキング型トロイの木馬とランサムウェアのコードベースの開発と進化に力を注ぎました。

図 6:
上位のバンキング型トロイの木馬ファミリー
2019 年の上位のバンキング型トロイの木馬ファミリーの内訳 (9 つのトロイの木馬ファミリーの割合で表示)(出典：IBM X-Force)



バンキング型トロイの木馬とランサムウェア – 悪化の一途をたどる危険な組み合わせ

金融マルウェアは 10 年以上前から主流の問題になっており、サイバー犯罪の世界に初めて登場した商用バンキング型トロイの木馬である Zeus Trojan をはじめ、いろいろなマルウェアが増加しています。2019 年の金融犯罪の全貌のレビューでは、上位のバンキング型トロイの木馬を使用する犯罪グループについての明確なトレンドが示されています。これらのマルウェア・ボットネットは、ターゲットを絞った金額の大きいランサムウェア攻撃のチャンスを狙って使用されることが増えています。

2019 年にこのカテゴリーにおいて最も活動が激しかったトロイの木馬型マルウェアの上位 10 位は、2018 年の年間調査の結果と似ています。TrickBot、Gozi、Ramnit が上位 3 位のままです。これらのトロイの木馬は、Botnet-as-a-Service スキームや不正アクセスされた資産を介して配布されるなど、他のサイバー犯罪者にさまざまなビジネス・モデルを提供する組織化されたグループによって操作されています。

2019 年のサイバー犯罪の領域では、TrickBot を操作する犯罪グループが圧倒的に激しく活動したクライムウェア・グループでした。その活動は以下のさまざまな面で見ることができます。

- コードの更新と修正の頻度 (コード、バージョン、機能の進化)
- 感染キャンペーンの頻度と規模
- 攻撃活動の頻度と量

2019 年に高額のランサムウェア攻撃で大きなニュースとなった犯罪グループは、2015 年にサイバー犯罪の領域に高額の電信送金詐欺を持ち込んだグループでもあります。ある意味、全体的な戦略は同じであり、より大きな金額を手に入れるために企業をターゲットにするように戦術のみが徐々に修正されています。

以下は、上位のバンキング型トロイの木馬がランサムウェアに手を広げている例です。

Dridex
以前は LokiBot をユーザーのデバイスに拡散し、現在は企業ネットワークに BitPaymer/DopplePaymer をデプロイする。

GootKit
企業ネットワークに LockerGoga をデプロイした疑いがある。LockerGoga は 2019 年初頭に登場し、それ以降、企業に大きな損害を与える攻撃の一部となっている。

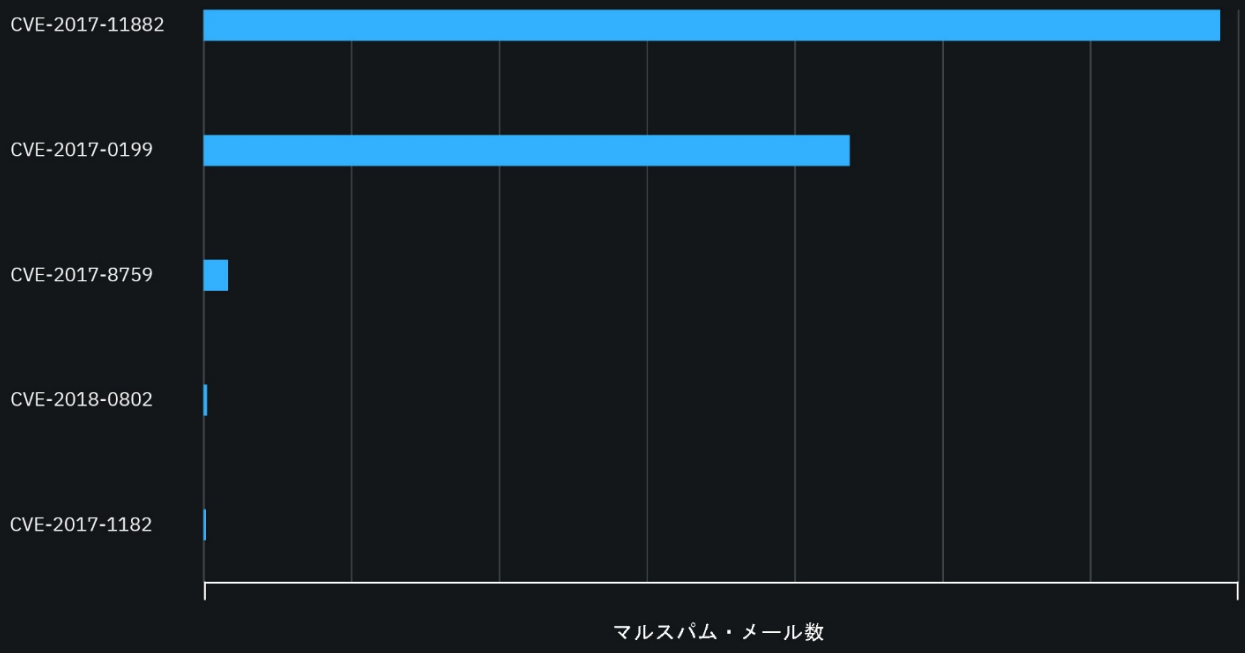
QakBot
企業ネットワークに MegaCortex をデプロイする。

TrickBot
企業ネットワークに Ryuk をデプロイする。

さらに、2019 年末のレポートによると、支払い機能のついたカードのデータの大規模盗難を中心に行ってきた ITG08 (FIN6) が、TTP も同じく多様化させているということです。この犯罪グループは現在、企業ネットワークでのランサムウェアのデプロイメントを組み込むことを目標にしています。盗難カードのデータを累積してから販売あるいは使用して金銭を得るには時間と労力がかかるのに対して、ランサムウェア攻撃は一挙に数百万ドルを入手できる可能性があります。そのため、さらに多くの犯罪グループが、ランサムウェアとサイバー恐喝を行っています。

スパムとフィッシングの傾向

図 7:
マルスパムで利用される上位の脆弱性
2019 年にマルスパム添付ファイルで利用された上位の脆弱性の内訳 (数量別)(出典：IBM X-Force)



2017 年の脆弱性が 2019 年のスパム上でも引き続き君臨

IBM X-Force は、世界中でスパム・トラップを実施し、何千万ものスパム・メッセージとフィッシング・メールを毎日監視しています。チームとテクノロジーが連携して、何十億もの Web ページと画像を分析し、不正なアクティビティーやブランドが悪用されるのを検知します。

X-Force の世界のスパム・アクティビティーの分析では、スパム・メールで使用される脆弱性は依然としてごく一部であり、特に 2017-0199 と 2017-11882 の 2 つの CVE に集中していることがわかりました。これらはパッチ提供済みの脆弱性ですが、脅威アクターがスパム・キャンペーンによって悪用しようとした脆弱性の 90% 近くを占めています。いずれの CVE も Microsoft Word に作用し、ブービートラップの仕掛けられた文書をユーザーが開くだけで感染します。

IBM のイベント・データによると、2019 年のこれら 2 つの脆弱性の使用頻度は、 他の Microsoft Word のリモート・コード実行の脆弱性の 5 倍近くに上ります。

この 2 つの脆弱性はかなりの数のスパム・メールに出現しますが、ユーザーがファイルを開く必要があるため、どの成功の程度ははっきりしません。そうは言ってもスパムは多くの場合「数の駆け引き」です。つまり数が十分であれば、成功率が小さくても脅威アクターにとっては十分に価値があります。多くのユーザーにとっては、あるいは企業にとってでさえ、問題のパッチ適用は後回しになりがちであるため、古いバグが残ったままのデバイスがいまだに見られることがあります。

古い脆弱性がよく狙われるのには多くの理由があります。取り込みやすく無料のドキュメント・ジェネレーターが使用できること、長期にわたって有効であること、悪意のある各種ペイロードをドロップできる多様性があることなどです。

古い脆弱性が引き続き利用されているということは、悪意のあるアクティビティーのロングテールを示しています。つまり、重大な脆弱性は、その公表およびパッチ公開後も何年にわたってずっと利用される可能性があるということです。

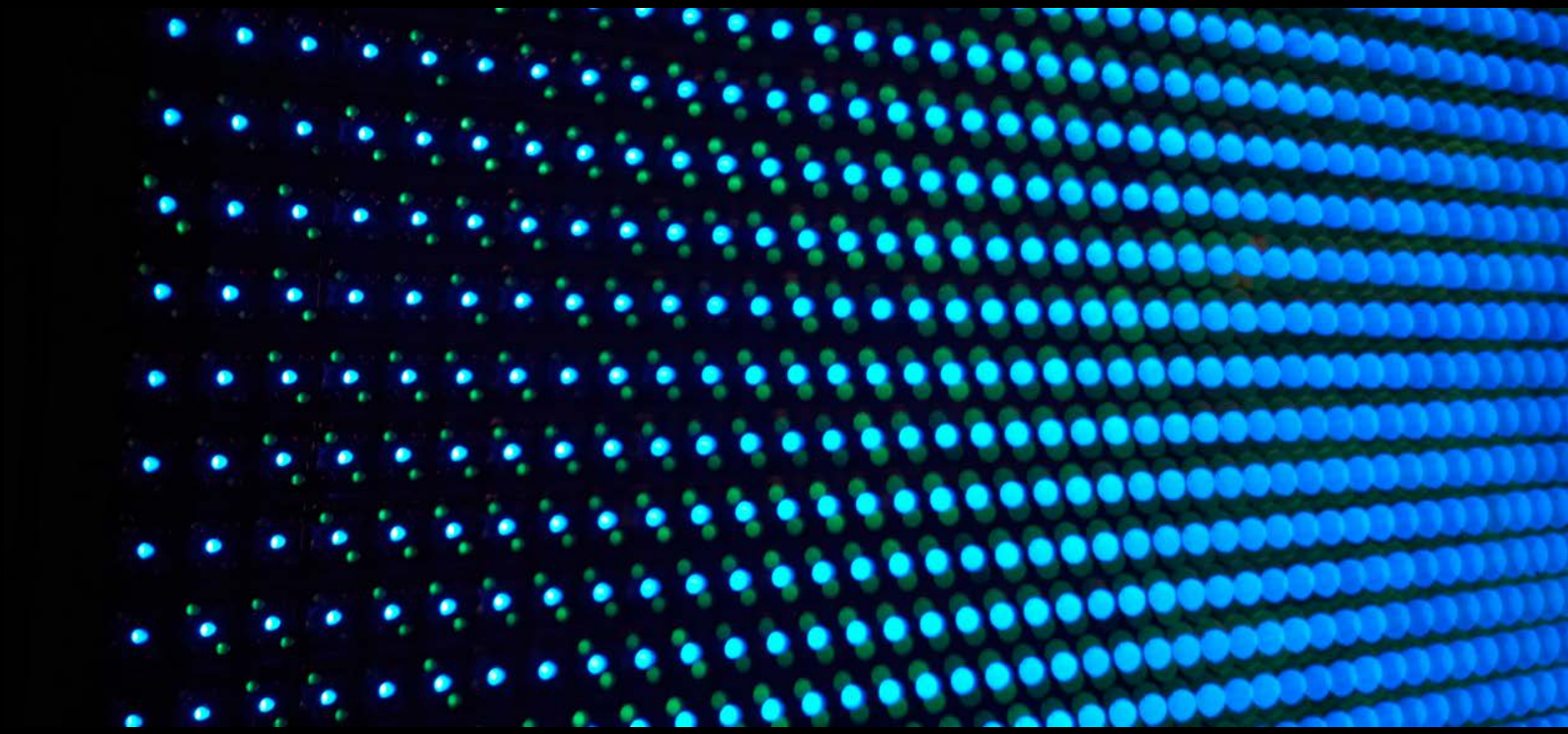
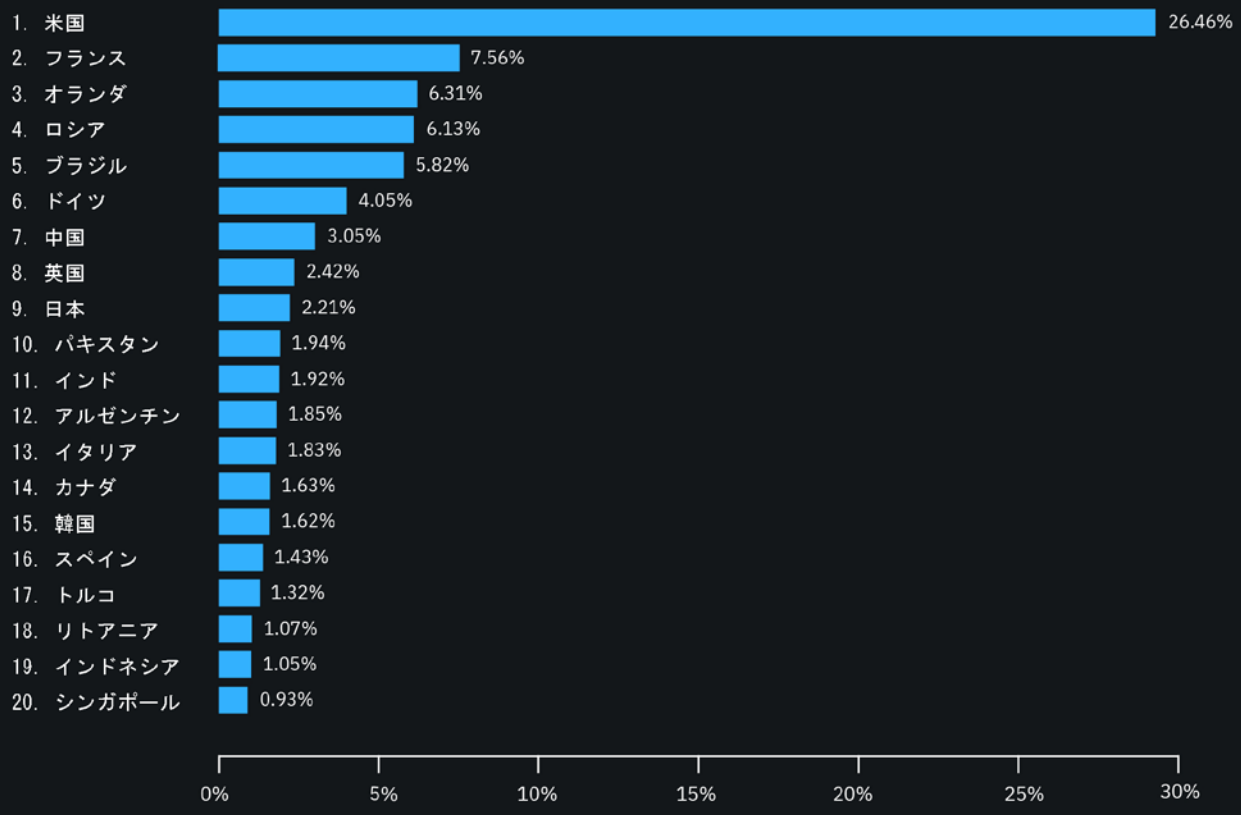


図 8:
スパム C2 ホスト国上位 20 カ国
2019 年のスパム・コマンド・アンド・コントロール（C2）サーバー数による上位 20 カ国を表示
(出典：IBM X-Force)

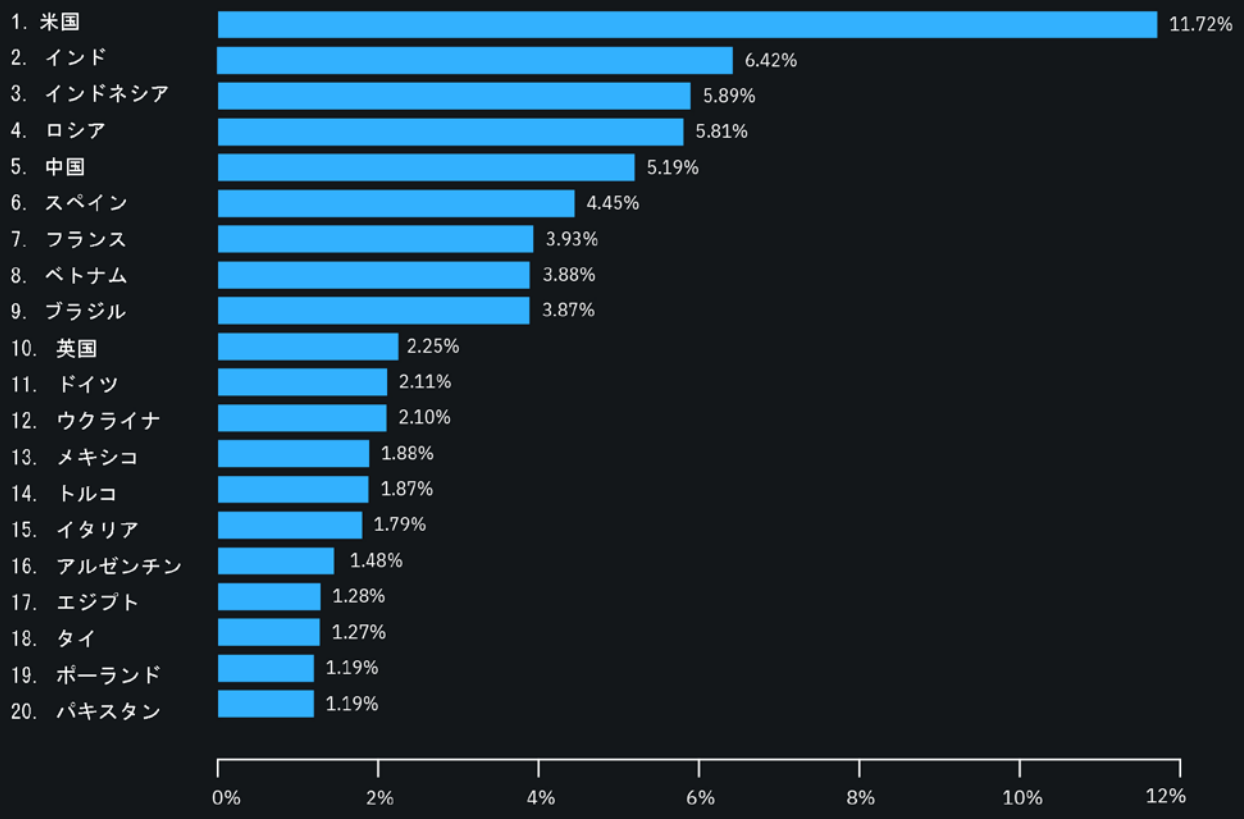


スパム・ボットネットのホスティングは欧米が中心、被害は全世界で

IBM X-Force のスパム・ボットネットに関する研究は、スパム・ボットネットのコマンド・アンド・コントロール (C2) インフラストラクチャーにリンクされた、地域固有の各種データ・ポイントについて調べています。IBM が注目したパラメーターの 1 つは、ボットネット C2 がホストされている地域です。2019 年には、C2 は主に北アメリカと西ヨーロッパの国々でホストされ、2019 年に観測された全 C2 事例の半分以上を占めていたことが分かりました。残りの C2 ホスティングはさまざまな地域に広がっていました。

多くの場合、スパム・ボットネット C2 インフラストラクチャーは、セキュリティー侵害のあったサーバー上でホストされます。北アメリカとヨーロッパのサーバーが利用されるのは、一般にこれらの国々のサーバー稼働時間は一貫して高いという共通認識と一致します。さらに、サイバー犯罪者は、標的と同地域のリソースを用いて攻撃をホストすることを好みます。標的とする地域のデバイスやネットワークは、それと同地域サーバーからのトラフィックのほうが警告を出す可能性が少ないからです。

図 9:
ボットネット被害者の上位 20 カ国
2019 年のボットネット・クライアント (被害者) 数による上位 20 カ国を表示
(出典：IBM X-Force)



地域別のスパム被害

2019 年のスパム・ボットネットの被害は世界中に広がっています。米国が最も多く、インド、インドネシア、ロシア、中国と続きます。
標的が分散しているのは、大量のスパム・キャンペーンをできるだけ多くの受信者に送りつけようとするスパム送信者の意図を表します。人口の多い国にはより多くのスパム・メールが流れ着くというわけです。

ブロックされたドメインから見える匿名化サービスの跋扈

ネットワークをオンラインの脅威から安全に守るための一般的な方法は、ユーザーや資産が、悪意のあるドメインと通信しないようにすることです。リスクを最小限に抑えるため、大半の組織はブロッキング・リストを利用して、疑わしい IP アドレスをブラックリストに載せています。同じ考えが世界中に広がっており、無料で利用可能なドメイン・ネーム・サーバー (DNS) サービス Quad9[3] は、悪意のあるサイトへの DNS 要求を毎日平均 1000 万件ブロックしています。

IBM Security の脅威に対するインテリジェンスに関連付けられた Quad9 データのサンプリングによると、スパム・メールで見つかった URL が、疑わしい DNS 要求の大多数を占めており、2019 年の全要求の 69% でした。2018 年の 77% から減少したものの、スパム URL のカテゴリーは依然として、悪意のあるドメイン全体の最も重大なカテゴリーとなっています。8% の減少は、DNS 要求の 24% を占める匿名化サービスのカテゴリーによるものと思われます。

毎日何千万件というスパム・メールをまき散らすことができる Necurs などの大規模スパム・ボットネットの恩恵を受け、メール・スパムは、依然として、潜在的なターゲットに接触する最も効率の良い方法の 1 つです。悪意のあるドメインは多くの場合、ランサムウェア、資格情報盗難スクリプト、詐欺サイトへのリンクをばらまくマルウェアを広め、正規のメールに見せかけたり、エンド・ユーザーが知っているブランドになりすましたりして、ユーザーをだますよう設計されています。

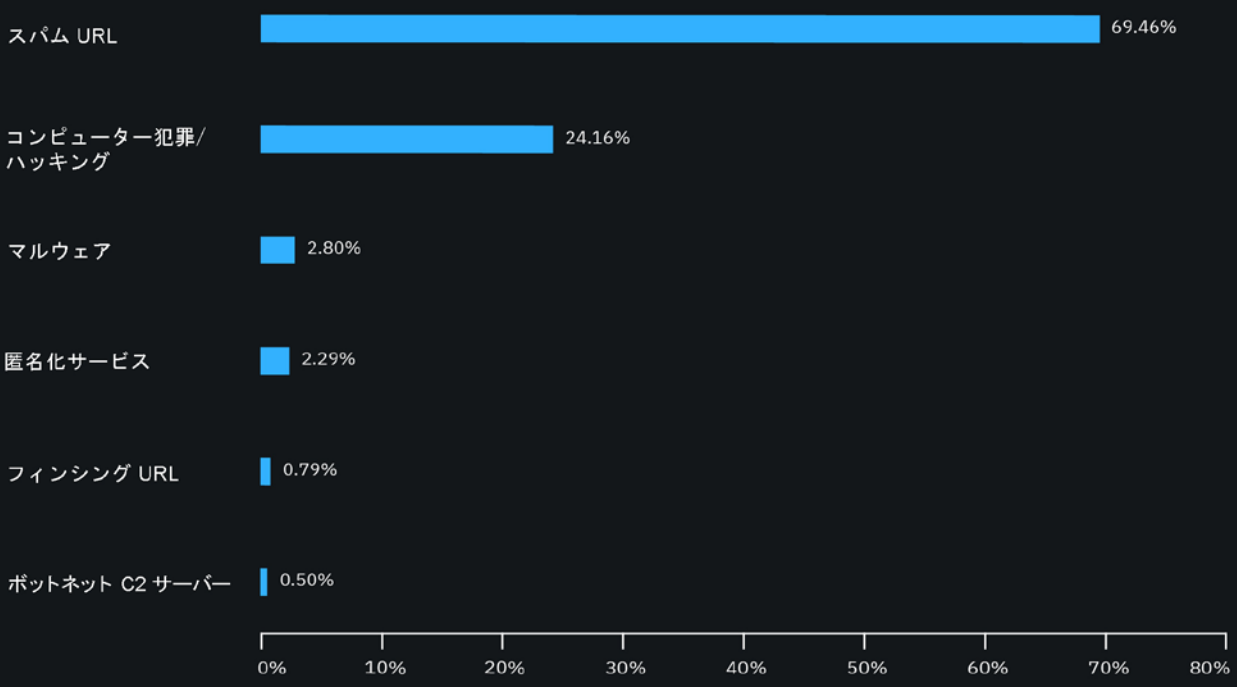
スパム・メール内に悪意のある URL へのリンクを埋め込むという手法は、最小限の労力でより広くわなを仕掛けたり、地域を特定して標的を設定したりできるため、金銭狙いのアクターに最もよく選ばれています。

図 10 のグラフは、IBM Security が 2019 年に記録した悪意のあるドメイン・タイプの分布を示しています。

メール・スパムは、依然として、潜在的なターゲットに接触する最も効率の良い方法の 1 つです。

[3] Quad9 は、IBM、Packet Clearing House (PCH)、Global Cyber Alliance (GCA) がコラボレーションして作成、後援しています。

図 10:
上位の悪意のあるドメインの脅威の種類
2019 年の上位の悪意のあるドメインの脅威の種類の内訳 (6 種類をパーセンテージで表示) (出典: IBM X-Force および Quad9)



スパム URL:
スパム・キャンペーンと関連するサイトにリンクするドメイン。多くの場合、迷惑以上の犯罪行為には関連付けられていません。

匿名化サービス:
それ以上追跡されないようにトラフィックを隠す匿名化プロバイダーにリンクするドメイン。

コンピューター犯罪/ハッキング:
Web ブラウザーの悪用スクリプトをホストするサイトなど、明らかに犯罪行為に関与していると見なされるドメイン。

フィッシング URL:
他の正規のドメインになりすまし、資格情報データなどの機密情報をユーザーから入手するドメイン。

ボットネット・コマンド・アンド・コントロール:
ボットネット・アクティビティーおよび感染する可能性のある訪問者にリンクするドメイン。

マルウェア:
既知のマルウェアをホストするドメイン。

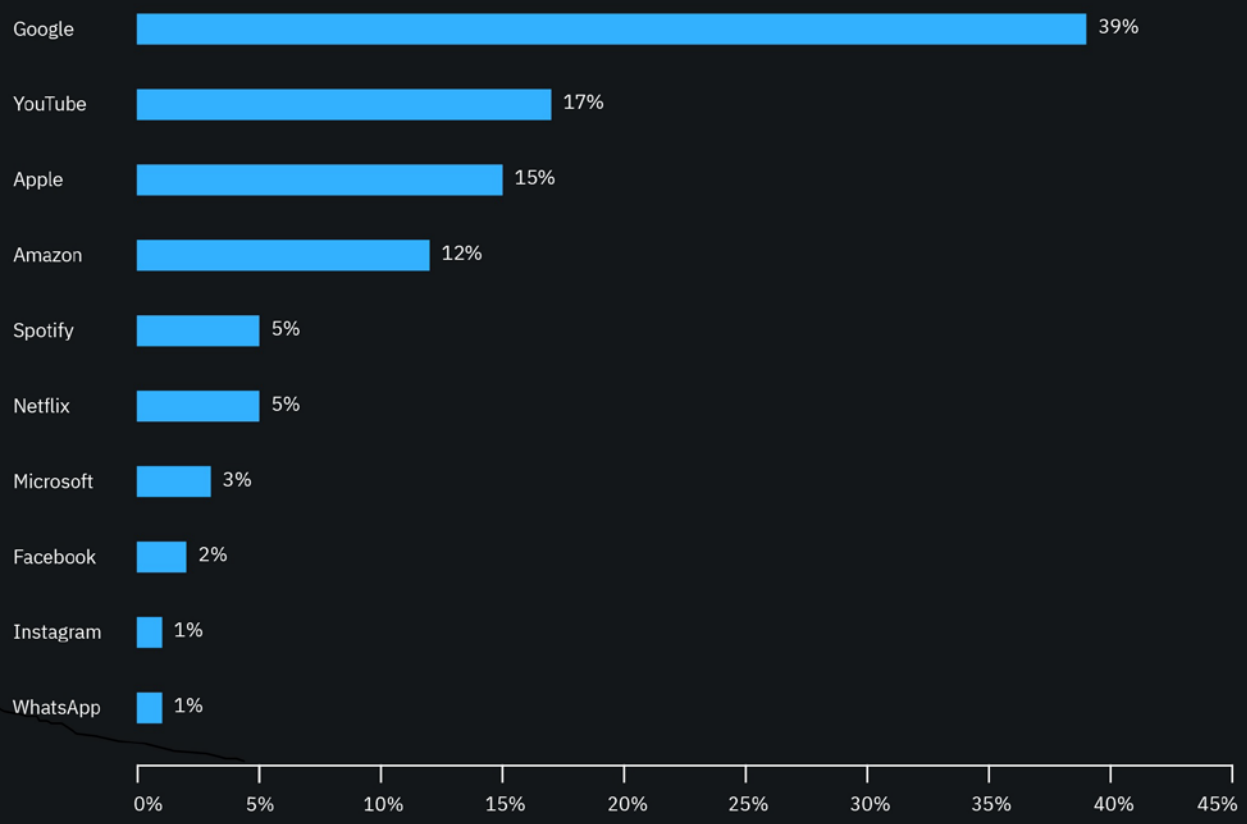
例えば、Tor のような匿名化プロバイダーでは、ユーザーは他のアクターが操作するノードを介してブラウズすることで、インターネット・トラフィックのソースを匿名化できます。匿名化サービスは、多くの場合、Web ブラウズ・アクティビティーのプライバシーを強化するという本来の目的を果たしていますが、このアクティビティーによって悪意のあるアクティビティーの追跡とブロックが困難になったり、不可能になったりすることもあります。

匿名化は、悪意のあるリンクを難読化したり、データ損失防止 (DLP) ルールを機能させずにデータを盗み出したり、リモート・サーバーの IP がブロックされる前に悪意のあるペイロードを埋め込むのに使用できるため、サイバー犯罪者が自分たちの形跡を隠すために使用する一般的な戦術です。

悪意のある DNS 要求の 4% は、犯罪者が Web ブラウザーの悪用、不正に関する情報の分散、その他のオンライン犯罪に利用する、コンピューター犯罪やブラックハット・ハッキングの Web ページに関連するものです。この数字が比較的低いのは、これらのリンクが匿名化ノードを経由して送られているか、企業のプロキシーとファイアウォールで検知、ブロックされ、シャットダウンされたためであると推測されます。

図 11:
スプーフィングされたブランド上位 10

2019 年スパムにおいてスプーフィングされたブランド上位 10 の内訳 (10 ブランドをパーセンテージで表示)(出典: IBM X-Force)



テクノロジー&ソーシャル・メディア企業がフィッシング攻撃の餌食に

フィッシングは 2019 年も引き続き主要な脅威の手口です。X-Force のデータでは、フィッシング・キャンペーンで最もよくスプーフィングされたブランドは、テクノロジーとソーシャル・メディアのプラットフォームでした。スプーフィングされたドメインは、ユーザーが見た目で判断することが難しく、多くの場合は偽名を使用された企業が使用する正規のドメインを正確に模倣したものです。本物のように見える Web サイトが元のサイトに酷似していれば、ユーザーは疑うことなく悪意のある Web サイトに個人データを漏らしてしまう可能性があります。

このデータは、2019 年に Quad9 によってブロックされた悪意のあるドメインの分析、および IBM X-Force のドメインスクワッティング検知に基づいています。

Google アカウントや Amazon アカウントを盗み出すのと違って、Instagram や Spotify などのソーシャル・メディアやコンテンツ・ストリーミング・サイトを狙っても、攻撃者はすぐに収益化可能なデータを入手できるわけではありません。しかし、ユーザーがアカウントやサービス間でパスワードを再利用することに乗じて、収集済みの資格情報を使い、同じユーザーのより価値の高いアカウントへのアクセスを狙っている可能性があります。

最も頻繁に攻撃対象になった業界

今日の脅威の全貌から分かるのは、脅威アクターの目的によって攻撃のタイプはそれぞれ特異なため、サイバーセキュリティーのリスク管理は部門ごとにかなり異なる可能性があるということです。

毎年、最も頻繁に攻撃対象になった業界を包括的に見るために、X-Force の研究者は、部門ごとに観測された攻撃の量をランク付けしています。最も頻繁に攻撃対象になった業界は、X-Force で管理しているネットワークの攻撃とセキュリティー・インシデントのデータ、IBM のインシデント対応サービスで抽出したデータと洞察、公開インシデントに基づいて決定されます。

図 12:
攻撃対象になった上位 10 の業界
攻撃対象になった上位 10 の業界 – 2019 年と 2018 年の比較(出店: IBM X-Force)

セクター	2019 年度順位	2018 年度順位	変動
金融サービス	1	1	–
小売	2	4	2
運輸	3	2	-1
メディア	4	6	2
専門サービス	5	3	-2
政府	6	7	1
教育	7	9	2
製造	8	5	-3
エネルギー	9	10	1
医療	10	8	-2

図 12 は、2019 年に頻繁に攻撃された上位の業界と 2018 年の順位を比較した図です。

金融サービスについては驚くことはありませんが、小売業界が攻撃者の注目を集めています。メディアおよびエンターテイメント企業、教育、政府機関も同様です。

以降のセクションでは、2019 年の各業界について、さまざまなデータ・ソースや IBM の知見に基づき、攻撃対象になった頻度を他と比較して詳しく説明します。一部の業界の説明では、ここ数年に特に活発に攻撃を仕掛けた脅威アクターを取り上げています。ただし、このリストは網羅的なものではなく、また 2019 年より前のデータも含まれています。X-Force IRIS は、国家の支援を受けた多数のサイバー犯罪グループを追跡し、プロファイリングしています。攻撃者が不明のアクティビティーとキャンペーンは、「HIVE」アクティビティーで追跡しています。TTP、インフラストラクチャー、攻撃対象の絞り込み、攻撃技術の組み合わせに基づいて、厳格な分析しきい値を満たしたアクティビティーは、IBM Threat Group (ITG) に移ります。

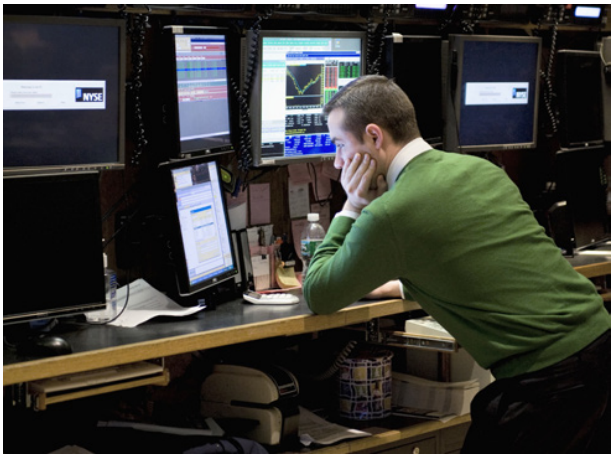
金融と保険

2019 年に最も頻繁に攻撃対象となった業界は、金融と保険部門でした。これは、4 年連続です。この部門に対する攻撃は、最も頻繁に攻撃対象となった上位 10 の業界の全攻撃の 17% を占めていました。

金融機関を攻撃対象にしているサイバー脅威アクターの最大派閥となっているのは金銭目的のサイバー犯罪者でしょう。金融機関の魅力は明らかです。高額な見返りがすぐに得られる可能性があることです。攻撃が成功すると、何百万ドルも手に入ることもあります。

公表されたデータ漏えいの件数は少ないにもかかわらず、X-Force インシデント対応エンゲージメントのデータでは、金融と保険が、最も攻撃対象になった上位業界の 1 位になりました。

これが意味するのは、金融と保険分野の企業は、他の業界よりも多くの攻撃を受けているが、より効果的なツールやプロセスを配備しているため、重大なインシデントになる前に脅威を検知して封じ込めることができることが多いということです。金融機関は、攻撃への対応計画をテストしている傾向が高く、IBM X-Force コマンド・センターを使用している組織の大部分を占めており、サイバー攻撃に対して準備と訓練を積み重ねています。IBM Security が後援し、米調査会社ポネモン・インスティテュートが実施した 2019 年版「情報漏えい時に発生するコストに関する調査（Cost of a Data Breach Report[4]）」によると、関連性の高いシナリオを使ってインシデント対応計画とチームを広い範囲でテストすることが、データ漏えいによる金銭的損害を緩和するのに効果的であることが分かりました。サイバー・レンジ環境などでインシデント対応計画を広くテストしていた組織で漏えいが発生した場合にかかるコストは、すべての組織のデータ漏えいの平均コストの 392 万ドルよりも平均して 32 万ドル低くなっていました。



2019 年に金融部門の組織を攻撃対象にした主な脅威グループは、ITG03 (Lazarus)、ITG14 (FIN7)、さまざまな Magecart 派でした。TrickBot、Ursnif、URLZone などのバンキング型トロイの木馬は、顧客の口座を乗っ取って金銭をだまし取ることで、2019 年に銀行を悩ませた上位の脅威となりました。

[4] 年刊の「Cost of a Data Breach Report」は、米調査会社ポネモン・インスティテュートが作成し、IBM が後援しています。

小売

2019 年の X-Force のデータによると、小売業界は、すべての業界の中で 2 番目に頻繁に攻撃された業界でした。この部門は、上位 10 の業界に対する全攻撃の 16% を占めており、2018 年の 4 位 (11%) から大きく順位を上げています。この業界に対する 2019 年のネットワーク攻撃件数は、2 番目に多いものでした。

小売業界の 2019 年の 2 位という結果は、X-Force IRIS データと、公表されたデータ漏えい情報に基づいています。小売組織を攻撃対象にしている脅威アクターで最もよく見られるタイプは、金銭目的のサイバー犯罪者です。この業界を攻撃対象にして、顧客の個人情報 (PII)、支払カード情報、金融データ、買い物履歴、ポイント・サービス情報を取得しています。サイバー犯罪者は通常、このデータを使用して顧客の口座を乗っ取って顧客の金銭をだまし取り、さらにさまざまな ID 窃盗シナリオでデータを再利用します。

2019 年に小売業者への攻撃でよく使用された攻撃手法は、POS (販売時点情報管理) マルウェアと e-コマース支払カードのスキミングでした。これらは、物理的な支払端末やオンラインでの取引時に支払カード情報を抜き出そうとします。

特に、Magecart と総称されるサイバー犯罪集団が、サード・パーティーの支払プラットフォームや有名なオンライン小売業者を直接攻撃対象にし、悪意のある JavaScript コードを Web サイトのカード支払ページに組み込んでいます。このコードは、精算プロセスの一部として実行され、被害者の支払カード情報を本来のベンダーだけでなく、サイバー犯罪者にも送信します。

X-Force IRIS のインシデント対応者は、2019 年に複数の漏えいで実際にこのようなタイプの攻撃を検知し、次のように述べています。「悪意のあるコード・スニペットは非常に基礎的なものかもしれないが、基盤プラットフォームのバックエンドの侵害は、総合的に大きな被害を及ぼす可能性があります。犯罪者は、同じ手法を使用して何千もの店舗に攻撃を仕掛けることができるのです。」

小売部門を攻撃対象にした目立った脅威グループは以下です。

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

オンラインの e-コマースでスキミングするだけでなく、POS マルウェアは従来から引き続き、サイバー犯罪者が実店舗で小売業者に対してよく使用する手法でもあります。取引時やメモリーへのデータの書き込み時に POS 端末やバックエンド・サーバーから支払カード・データを抜き出すのです。

運輸

運輸部門は、どの国でも、重要なインフラの一部です。この部門の企業は、産業と顧客サービスの両方で、3 つの主要な輸送タイプ (陸上輸送、海上輸送、航空輸送) によって経済を動かします。2019 年、運輸部門は、3 番目に頻度が高い攻撃対象になりました。攻撃頻度の割合は、2018 年の 13% から低下し、2019 年は 10% になりました。

運輸業界が金融と小売に次いで第 3 位に入ったことは、運輸関連企業が運用しているデータとインフラストラクチャーの魅力が高くなっていることを明確に示しています。このような資産は、サイバー犯罪者にとっても国家脅威アクターにとっても魅力的なものです。
運輸企業が保持している情報は、サイバー犯罪者にとって魅力的な攻撃対象になります。PII、略歴、パスポート番号、ポイント・サービス情報、支払カード・データ、旅程などが対象として考えられます。

この部門では、特に航空会社と空港が、サイバー犯罪者や国家アクターの攻撃対象になることが増えています。目的は、対象の旅客を追跡したり、ダーク Web で売ることで、旅客の個人情報を金銭化することです。

運輸業界に対するサイバー脅威は、他の部門よりもリスクが高くなっています。これは、攻撃が物理的な影響を及ぼし、人命をリスクにさらす可能性があることに加え、輸送サービスに依存して、業務を遂行している他の業界に影響が波及する可能性があるためです。

2019 年を通して、運輸部門を攻撃対象にしている脅威アクター・グループは多種多様にわたり、サイバー犯罪グループと国家アクターがともに世界中の組織に攻撃を仕掛けました。

運輸部門を攻撃対象にした目立った脅威グループは以下です。

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

メディアとエンターテイメント

2019 年の X-Force ランキングの攻撃対象になった業界の第 4 位は、メディア部門でした。上位 10 の業界に対する全攻撃の 10% を占めました。メディア部門は 2018 年の 8% から増加し、6 位から 4 位に順位を上げました。

メディア部門には、ニュース・メディアやエンターテイメントを製作、加工、配信する企業や通信会社などの著名な企業があります。メディアとエンターテイメント業界は、世論に影響を及ぼしたり、情報フローを制御したり、組織や国の評判を保護することを目的としているサイバー犯罪者にとって価値の高い攻撃対象です。特に、国家組織は、ネガティブなメディア・コンテンツを国家のセキュリティーに対する重大な脅威であると見なすことがあります。一方、サイバー犯罪者は、放送前のメディアを盗んで身代金を要求できるため、メディアとエンターテイメントに対する攻撃は金銭的に魅力的であると考えています。

2019 年にこの部門を攻撃対象にしたのは、日和見主義的なサイバー犯罪者と国家アクターでした。

メディアとエンターテイメント部門を攻撃対象にした目立った脅威グループは以下です。

ITG03 (Lazarus)
Hive0003 (Newscaster)
Hive0047 (Patchwork)

専門サービス

専門サービス業界には、専門コンサルティング・サービスを他の部門に提供するさまざまな企業が含まれます。例えば、法務、会計、HR、専門顧客サポートを提供する企業などがあります。この部門は、X-Force データによると、上位 10 の業界の全攻撃の 10% を占めました。2018 年の 12% から低下しています。

公表されたデータ漏えい情報によると、専門サービスは、このランキングの全業界の中で、漏えいしたレコード件数が最も多かったということが示されています。このような企業の多くは、法的手続き、会計、税務のためのデータなど、非常に機密性の高いデータを顧客から受け取ります。こうした機密データは、金銭的利益やインサイダー情報を求める攻撃者にとって魅力的な攻撃対象になることがあります。

また、この業界にはテクノロジー企業も含まれており、攻撃対象になることが増えています。こうした企業はサード・パーティーの企業にアクセスできるため、そのサービスの提供先となっているセキュアで大規模な企業を侵害しようとする攻撃者が悪用することがあります。

また、専門サービス企業の日常的なワークフローは、フィッシング・メールや悪意のあるマクロを介した犯罪者の攻撃手口になる傾向があります。多くの専門サービス企業では、Word や Excel 文書の添付ファイルなどのファイルを非常に頻繁に利用して、契約書を作成したり、顧客とやり取りしたり、日常業務を行ったりしています。マクロの使用は、サイバー犯罪者が悪用する最も有名な攻撃手口の 1 つであり、組織が完全にブロックできないタイプのファイルに悪意のあるスクリプトを埋め込みます。

2019 年に専門サービスを攻撃対象にした主な脅威アクター・グループは以下です。ITG01 (APT10、Stone Panda) (攻撃元が中国と思われる、国家の支援を受けたグループ)

政府

政府部門は、このランキングの第 6 位です。上位 10 の業界の全攻撃の 8% を占めていました。これは、去年と変わっていませんが、全体としての順位は 2018 年の 7 位から上がっています。

政府部門は、仮想敵国より優位に立とうとする国家サイバー・アクター、侵害情報の公開や技術的手腕の誇示を目的とするハクティビスト、恐喝や盗んだデータで金銭的利益を得ようとするサイバー犯罪者にとって価値の高い攻撃対象です。

近年、特に地方自治体が攻撃にさらされています。これは、サイバー犯罪者が、民間部門よりもセキュリティーが低いと思われる組織から金銭をゆすり取ろうとしているためです。政府機関は、主に機密情報や国家機密など、脅威アクターにとって価値の高い資産を所有しています。これには、政府職員の PII、金融情報、内部情報、重要なネットワークの機能などがあります。

国家アクターは、政府機関への攻撃に長い間関心を示してきました。
X-Force IRIS では、国家アクターがそうした攻撃を実現する能力を十分に有していると評価しています。2019 年には、サイバー犯罪グループによる政府機関への攻撃も増加しました。目的は、政府の運営に必要な身代金データを暗号化して保有することです。特に、地方自治体、州レベルでの攻撃が頻繁に行われました。

2019 年 1 月から 7 月だけで、70 の政府機関がランサムウェアの攻撃を受けました。また、サイバー犯罪者は、データ (防衛 Web サイトのものなど) を盗み、ダーク Web で公開しました。ハクティビストは政府を格好の攻撃対象として見なすことが知られています。これは、政治・社会的問題について自分たちの主張を広めるためです。多くの場合、政府組織では、民間部門と同様にサイバーセキュリティーの資金が不足しています。それでも市民のために一貫したサービスを維持する必要があります。そのため、脅威アクターがこうした組織に突きつける課題は深刻化しています。

2019 年に政府機関を攻撃目標にした主な脅威アクター・グループは以下です。: さまざまなサイバー犯罪アクターと国家の支援を受けたグループ

教育

教育部門は、上位 10 の業界の全攻撃の 8% を占めました。2018 年の 6% から上昇しており、このランキングで第 7 位になりました。

教育業界は、金銭的な動機を持つアクターと国家アクターにとって高い価値を持つ、さまざまな資産を持っています。知的財産 (IP) から PII に至るまで、教育組織は、さまざまなタイプの脅威アクターにとって豊富なデータを持つ攻撃対象になります。

攻撃アクターはそれぞれ異なる動機を持っており、さまざまな攻撃手口を使用して、学術機関のネットワークを侵害しています。ただし、最もよく観測された方法は、引き続きフィッシング・メールでした。多くの場合、フィッシング・メールは、特定の学術機関や研究分野に合わせてカスタマイズされていました。

教育部門の組織は、多くの場合、多岐にわたる大規模な IT インフラストラクチャーやデジタル・フットプリントを備えています。職員、生徒、請負業者など、多種多数のユーザーにサービスを提供する各種資産を運用しています。この巨大な攻撃範囲を、脅威アクターによるさまざまな悪意のあるアクティビティーから保護するのが非常に困難になっています。2019 年 10 月に発表されたレポートでは、米国だけで、2019 年に少なくとも 500 の学校がサイバー攻撃 (主にランサムウェア) を受けたと報告されています。

この部門における巧妙な攻撃の目立った例として、国家脅威アクターが大学のネットワークを侵害し、それを足掛かりにしてメディア組織や軍事請負企業を感染させた事例があります。また、米国から資金提供を受けている研究を標的にしている攻撃者というのもいますが、彼らは、莫大な価値をもたらす可能性がある知的財産を盗むため、大学のネットワークを侵害する手段を常に探しています。

教育部門を攻撃対象にした目立った脅威グループは以下です。

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS では、この業界は今後も、価値の高い情報にアクセスしようとしている金銭的な動機を持つアクターと国家に関連したアクターの攻撃対象になると確信をもって見ています。

2019 年にこの部門を攻撃対象にした主な脅威アクター・グループとしては、日和見主義的なサイバー犯罪集団や、中国、ロシア、イランの国家アクターが挙げられます。

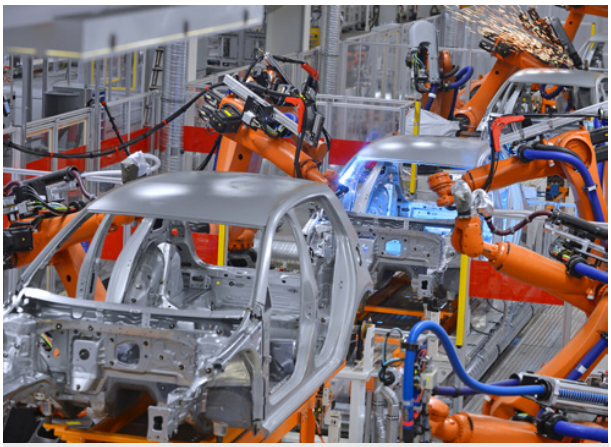
製造

金属、化学、資本財、電機によって経済を動かす製造業も、IT の脅威やネットワークにつながっている OT フロアに影響する脅威から免れることはできません。製造は、頻繁に攻撃を受けた上位 10 の業界の全攻撃の 8% を占めており、このランキングの第 8 位にランクインしました。2018 年の 10% から減少しています。

単に昨年より攻撃が減少している可能性もありますが、この数値の減少を見るとき、製造部門のデータ漏えいでは往々にして、法的な開示や規制が課せられた情報が含まれていないことを考慮する必要があります。つまり、攻撃が常に公表されるわけではないため、製造業者に対する攻撃頻度が実際よりも低いように見えている可能性があります。

製造業者は、IT と OT の両方の環境を運用している組織でもあります。そのため、ICS や SCADA システムに影響を及ぼすものと同じ脅威の影響を受けます。この部門の情報セキュリティーはかつては遅れていましたが、2019 年にノルウェーの製造業者が大規模なランサムウェア攻撃に対する対応を公表して成功したことは、この業界によるサイバーセキュリティーに対するアプローチが変わりつつある証といえるでしょう。

製造部門の企業に対して最大のサイバー脅威となるのは、金銭的利益や知的財産データを求めるサイバー犯罪者または国家アクターであると思われます。2019 年に製造業者に対して使用されたもっとも一般的な攻撃手法は、ビジネス・メール詐欺 (BEC) による不正でした。これは、外国のサプライヤーと頻繁に取引している場合に特に顕著でした。この場合、攻撃者は企業のメール・サーバーやメール・アカウントを侵害します。攻撃者は、既存の通信スレッドに侵入して、最終的に自分が管理している口座に大金を送金します。



製造業を攻撃対象にした目立った脅威グループは以下です。

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

また、製造業者はサプライ・チェーン攻撃も受けやすい傾向にあり、国家アクターが悪用して、製造されている製品にバックドアやマルウェアを埋め込んで他の国に出荷することがあります。

金銭的な動機の側面では、攻撃者は、企業秘密や知的財産を狙って製造業者を攻撃対象にする可能性があります。開発に長年費やされた研究は、サイバー犯罪者にダーク Web で手っ取り早く利益をもたらします。特に防衛や軍備機器の製造業者の場合、そのデータが国家経済や防衛上の優位性を一気に高めたりする可能性もあります。

X-Force データによると、ランサムウェア、フィッシング攻撃、SQLi 注入攻撃も、製造業界に対して頻繁に仕掛けられる傾向にありました。

エネルギー

エネルギー部門は、このランキングの第 9 位です。2019 年、上位 10 の業界のすべての攻撃とインシデントの 6% を占めました。この部門の順位は 2018 年から変動しておらず、攻撃に占める割合も同じ 6% でした。

エネルギー部門の企業は、すべての国の重要なインフラストラクチャーのバックボーンとして重要であるため、サイバー攻撃にとって実りの多い攻撃対象であることがわかっています。エネルギーは、さまざまな形で、経済、国家安全保障、都市や業界の日常の機能にとって非常に重要なものです。

エネルギー部門への攻撃の目的は多種多様です。顧客データ、財務資料、企業秘密、専有テクノロジー情報など、エネルギー企業内の金銭をもたらす資産には、他の業界と同じような価値があります。

エネルギー業界が他の業界と異なるところは、企業を管理している ICS システムや SCADA システムの物理的な中断や破壊の可能性がある点にあります。こうしたシステムは、攻撃対象の施設内の運用を監視、さらには制御しようとしている攻撃者にとって非常に価値の高い攻撃対象になることがあります。例えば、サイバー戦争の状況で、敵国にある各施設に影響を及ぼす場合などです。この業界は、ZeroCleare のような破壊的マルウェアの攻撃対象にもなっています。

運用を中断するための ICS システムへの攻撃が成功すると、エネルギー部門から供給される電力、ガス、石油などのリソースに依存している顧客が壊滅的な影響を受ける可能性があります。過去のこのような攻撃とその悪影響の例として、 ウクライナの発電所を攻撃対象にした一連のインシデントが挙げられます。これは、物理的な破壊を目的とした、ロシアによる攻撃ではないかという見方があります。

この部門を攻撃対象にした目立った脅威グループは以下です。

ITG01 (APT10)	HIVE0006 (APT27)
ITG09 (APT40)	Hive0016 (APT33)
ITG07 (Chafer)	Hive0044 (APT15)
ITG11 (APT29)	Hive0045 (Goblin Panda)
ITG12 (Turla Group)	Hive0047 (Patchwork)
ITG13 (APT34)	Hive0076 (Tick)
ITG15 (Energetic Bear)	Hive0078 (Sea Turtle)
ITG17 (Muddywater)	Hive0081 (APT34)
Hive003 (APT35)	

医療

最も頻繁に攻撃対象になった業界第 10 位は医療であり、上位 10 の業界の全攻撃の 3% を占めました。2018 年の 8 位 (6%) から順位を下げました。

多くの証拠から、医療業界のネットワークや医療機器に対して主に攻撃を仕掛けているのは、金銭的な動機のサイバー犯罪者であることが判明しています。その目的は、医療レコードを盗んでダーク Web で売ること、あるいはネットワーク接続された機器を暗号化して動作しないようにし、企業に身代金を要求することです。

病院や介護施設のネットワークを中断すれば、運用を復元して人命を守るために、ランサムウェア攻撃に金銭を支払うように医療機関にプレッシャーをかけることができます。例えば、2019 年の Ryuk による攻撃後の 1,400 万ドルの要求など、身代金は考えられないほど高額になることもあります。

2020 年に入っても、医療部門は引き続き、データを保護するためのセキュリティー態勢を進化させる必要があります。ランサムウェア攻撃が頻繁に行われているため、病院はインシデント対応機能を強化し、動機を持った攻撃者によって悪用されて簡単に侵害され、踏み台にされてしまいかねない非セキュアな医療機器に対する新たな攻撃を監視する必要があります。

この部門を攻撃対象にした主な脅威アクター・グループとしては、金銭的な動機のサイバー犯罪グループ (Ryuk によるランサムウェアを組織したグループなど) が挙げられます。ランサムウェア攻撃によって病院が影響を受けたときに見舞われる危機は非常に大きなものですが、国家アクターはこの部門に関心を示していません。

地域的に見た洞察

2019 年、脅威アクターは、あらゆる地域を攻撃対象にしました。その活動は、北米、アジア、ヨーロッパで最高レベルでした。

X-Force の研究者は、脅威アクターが 2019 年は中東と南アメリカを積極的に攻撃対象にしていることを突き止めました。中東は、ハクティビストや国家アクターによる攻撃が多く、南アメリカは主に金銭的な動機のアクターの影響を受けました。

このセクションでは、X-Force で判明した攻撃対象の性質、各地域に焦点を合わせた主要な脅威アクター、脅威アクターの活動が活発になる可能性がある 2020 年に注意すべき重要な日付について理解を深められるように、各地域における攻撃について詳細に説明します。一部の地域については、近年にその地域に対して特に活発に攻撃を仕掛けた脅威アクターを取り上げています。ただし、このリストは網羅的なものではなく、また 2019 年より前のデータも含まれています。このセクションでは、前述の IBM Threat Group 体系を使用し、IBM のグローバルなインシデント対応からのデータに加え、公表されている漏えいデータも使用します。

北アメリカ

北アメリカは、すべてのカテゴリーで脅威アクターの最大の攻撃対象であり、2019 年のインシデントの 44% を占めていました。

北アメリカには大量の攻撃対象となる候補があり、大量のインターネット・インフラストラクチャーがあります。そのため、犯罪アクターにとって実りの多い攻撃対象になっています。2019 年、北アメリカでは、50 億件を超えるレコードが侵害されました。

2019 年、IBM は、コモディティー化されたマルウェア (アンダーグラウンド・マーケットで購入できるコードや無料で入手できるコード) を使用した北アメリカの複数のインシデントに対応しました。コモディティー化されたマルウェアは、その帰属を特定するのが困難になることがありますが、犯罪の目的を達成する上では非常に効果的になることがあります。

北アメリカを特に攻撃対象にしている国家アクターには変化はなく、2019 年は重大なインシデントは発生しませんでした。米国と中国間の最近の貿易交渉が原因で、両地域と取引している組織が攻撃対象になることが増加する可能性があります。該当する組織では、この交渉の結論が出るまで、警戒し続ける必要があります。

サイバーセキュリティーにとって歴史的に重要な今後のイベントは以下です。

7 月 13 日
(米国民主党全国委員会)

8 月 24 日
(米国共和党全国大会)

11 月 3 日
(米国大統領選挙)

この地域を攻撃対象にした脅威アクター・グループは以下です。

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

2019 年に X-Force インシデント対応エンゲージメントで観測されたもっとも目立った攻撃アクティビティーは以下です。

ビジネス・メール詐欺 (BEC)、ランサムウェア、国家アクターによる金融部門への攻撃

アジア

アジアは、X-Force 分析で 2 番目にリスクが高い地域であると評価されています。公開されている漏えいインシデント件数は第 2 位であり、2019 年のインシデントの 22% を占めています。2019 年、アジアでは 20 億件のレコードが侵害され、北アメリカに次ぐ第 2 位でした。

多数の脅威アクターが、アジアに関連した組織を攻撃対象にしていました (特に朝鮮半島、日本、中国)。この地域で観測された多くの攻撃は、国家アクターの TTP に従っていました。1 つの例として、ITG01 が挙げられます。これは、韓国のエンティティーを攻撃対象にしている北朝鮮のアクターと思われます。もう 1 つの例として ITG15 が挙げられます。これは、日本を攻撃対象にしている中国のアクターのようです。

最近のアジアにおける政治的な活動の影響で、この地域では国家に関連したアクティビティーの発生確率が高まっています。香港における民主化抗議運動とそれに続く弾圧は、中国をいらだたせています。北朝鮮と周辺国間の緊張の高まりのため、北朝鮮の政権が急進化しています。インドによるカシミール地域の吸収も同様に、地域の緊張を高めています。

2020 年は、こうした潜在的に不安定な政治的な危機状況を監視することが、この地域で活動している企業がさらされるリスクを理解する上で重要になります。

サイバーセキュリティーにとって歴史的に重要な今後のイベントは以下です。

7 月 24 日
(東京 2020 オリンピック)

10 月 10 日
(中華民国国慶日)

アジアを攻撃対象にした主な脅威アクター・グループは以下です。

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049
(Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079
(Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear)

2019 年に X-Force インシデント対応エンゲージメントで観測されたもっとも目立った攻撃アクティビティーは以下です。

PowerShell 攻撃、インサイダー攻撃、ランサムウェア

ヨーロッパ

ヨーロッパは、アジアと同程度に悪意のあるアクティビティーの被害を受けており、インシデントの 21% を占めています。

主に国家間の競争の影響を受けているアジアとは異なり、ヨーロッパは主に、金銭的な動機の脅威アクターの攻撃対象になっているようでした。この違いは、通貨為替レートの影響で、ヨーロッパを拠点としている企業から盗んだ方が大きな見込みがあるということで説明できます。あるいは、犯罪の動機が知的財産を得ることであり、それを競合他社に販売して大きな利益を得ることができるということも考えられます。

英国の欧州連合離脱 (ブレグジット) のため、ハクティビスト・サークルの残り火が 2020 年も継続する可能性がありますが、2019 年には関連したアクティビティーは発生しませんでした。また、主な EU 諸国 (ドイツ、フランス) での今後の選挙が、該当する国の政策に影響を及ぼすことを企てている国家アクターの攻撃対象になる可能性があります。

サイバーセキュリティーにとって歴史的に重要な今後のイベントは以下です。

1 月 31 日
(英国、第 50 条の下に EU 離脱)

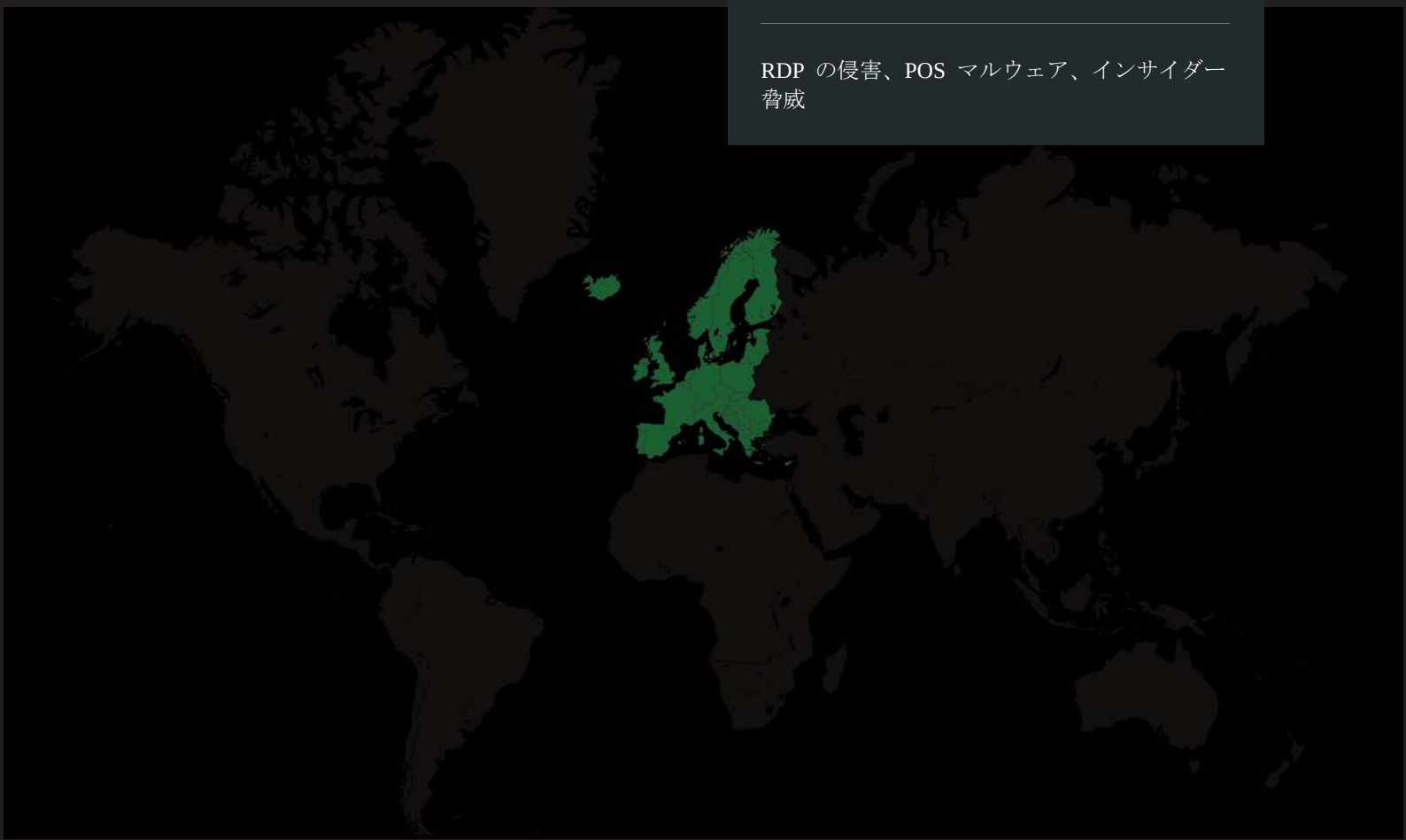
6 月 28 日
(ウクライナ憲法記念日/NotPetya 記念日)

この地域を攻撃対象にした主な脅威アクター・グループは以下です。

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

2019 年に X-Force インシデント対応エンゲージメントで観測されたもっとも目立った攻撃アクティビティーは以下です。

RDP の侵害、POS マルウェア、インサイダー脅威



中東

X-Force IRIS では、2019 年に中東の組織に影響を及ぼした多数の国家関連のインシデントを観測しましたが、2019 年の脅威アクター・アクティビティーの全体的なインデックスは比較的低くなっていました。この地域はインシデントの 7% を占めていました。

他の地域の方がサイバー犯罪アクティビティーの投資収益率が高いことなど、アクティビティーが少なくなった理由の説明はいくつか考えられます。
ただし、他の地域とは異なり、中東では、ハクティビストと国家アクターのアクティビティーの比率が世界の他の地域よりも高くなっていました。

ハクティビストのアクティビティーは、2019 年の地域における政治的不安に関連している可能性があります。イランに関係する複数の重大なインシデントがありました。同様に、ITG13 によるイランの国益を求めるアクティビティーなど、国家アクターのアクティビティーは、国家の目的に沿って行われ、破壊的攻撃によってこの地域のエネルギー部門の組織が攻撃の対象になりました。

イエメンにおける政治的不安と武力衝突により、引き続き、サイバー脅威アクティビティーのリスクが生じます。紛争のすべての当事者のアクターがサイバー攻撃を使用して、自身のメッセージを拡散し、収益を得ようとしています。長引く紛争でさまざまな当事者が公然と脅迫しあう中、このようなリスクは 2020 年も継続する見込みです。

サイバーセキュリティーにとって歴史的に重要な今後のイベントは以下です。

11 月 21 日
(カタール FIFA クラブ・ワールド・カップ 2020)

この地域を攻撃対象にした主な脅威アクター・グループは以下です。

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

2019 年に X-Force インシデント対応エンゲージメントで観測されたもっとも目立った攻撃アクティビティーは以下です。

破壊的マルウェア、DDOS 攻撃、Web スクリプト。

南アメリカ

南アメリカは、2019 年に重大なサイバー犯罪アクティビティーに苦しみましたが、上位 3 地域に比べると攻撃数は少なく、インシデントの占有率はわずか 5% でした。ただし、この地域では、前年と比較してアクティビティーは増加しています。X-Force の観測によると、特に小売り部門と金融サービス部門で、重大なインシデント対応アクティビティーが増加しています。

この地域で観測されたインシデントには、ランサムウェアのアクティビティーがありました。これは、2019 年を通して頻度が上がり続けていました。

サイバーセキュリティーにとって歴史的に重要な今後のイベントは以下です。

6 月 12 日
(コロンビアとアルゼンチンでのコパ・アメリカ 2020 サッカー・トーナメント)

この地域を攻撃対象にした主な脅威アクター・グループは以下です。

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

2019 年に X-Force インシデント対応エンゲージメントで観測されたもっとも目立った攻撃アクティビティーは以下です。

ビジネス・メール詐欺 (BEC)、ランサムウェア、国家アクターによる金融部門への攻撃

2020 年レジリエンスへの備え

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、業界や国にかかわらず、進化している脅威を緩和する効果的な方法です。

IBM では、2020 年のサイバー脅威に対する備えを強化するために、以下のステップを各組織で実行するよう推奨しています。

- 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理解し、セキュリティーのリソースを優先順位付けする。
- 組織内でインシデント対応チームを構築してトレーニングする。これができない場合は、組織外部のインシデント対応機能を有効活用して、影響力の高いインシデントに速やかに対応できるようにしてください。2019 年、IBM Security では、影響を封じ込めることで、関連コストが大幅に削減されることを確認しています。IBM のチームが MegaCortex の感染に、迅速に介入してランサムウェア攻撃を途中で阻止し、何千万ドルもの損害を食い止めました。
- 組織のインシデント対応計画の負荷テストを実施して身につける。机上演習やサイバー・レンジの実体験により、チームで重要な経験を積むことで、漏えい発生時の対応時間やダウン時間を短縮し、最終的にコストを削減できます。
- 多要素認証 (MFA) を実装する。これは、引き続き、組織にとって最も効率的なセキュリティーの優先事項の 1 つです。2019 年に脅威アクターが最もよく使用した攻撃方法は、資格情報の窃盗または再利用でした。MFA を使用すれば、この攻撃を効果的に抑制できます。
- 組織でドメインのなりすましを検知してブロックするためのソリューション (Quad9 など) を配備する。これは、攻撃手口としてフィッシングがよく見られるからです。
- バックアップの実行、バックアップのテスト、バックアップのオフラインでの保管を行う。バックアップが存在していることを確認するだけでなく、実際にテストしてバックアップが有効かどうかを確認することは、組織のセキュリティーを確保する上で非常に重要です。

知っておくべきセキュリティーの脅威 まとめ

2020 年、組織は、従来の脅威と新たな脅威を課題とする必要があります。

- リスクの範囲は 2020 年も広がり続けます。現在の脆弱性は 150,000 件を超えており、絶えず新しい脆弱性が報告されています。
- 2019 年に侵害されたレコードの件数は 2018 年の 4 倍を超えました。2020 年も漏えいや攻撃により失われるレコードの数が増える可能性があります。
- 脅威アクターは引き続き、異なる攻撃手口に照準を移しています。例を挙げると、IoT デバイス、OT (オペレーショナル・テクノロジー)、工業分野や医療分野におけるコネクテッド・システムを攻撃対象にすることが増えています。
- 脅威アクターによるマルウェアの使用は変化し続けます。2019 年は、ランサムウェア、暗号通貨マイニング、ボットネットが、入れ替わり首位になりました。このトレンドは 2020 年も続くと予想され、時間の経過とともに変わりゆく脅威から組織を保護する必要があります。
- ランサムウェアや暗号通貨マイニングのコードの革新が高水準にあることを踏まえると、2020 年もこれらの脅威は引き続き進化する可能性が高く、検知と封じ込めのための能力をさらに強化していく必要があります。
- スパム・アクティビティーは衰えることなく続いています。組織でしっかりとブラックリスティング、脆弱性パッチの適用、脅威の監視を行う必要があります。
- 業界それぞれにおける攻撃状況は前年から移り変わっています。こういった変化に対応できるよう、リスクはすべての業界に存在していると認識し、業界枠を超えて全体が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。
- 組織の地理的なロケーションにおける傾向を把握することで、可能性の高い攻撃者や攻撃の動機を特定し、直面する可能性のあるリスクを予想して緩和できます。

X-Force について

IBM X-Force は、脅威の最新動向の研究と監視に取り組むと同時に、新たに出現した重大な脅威についてお客様や一般ユーザーに助言し、IBM のお客様の保護に役立つセキュリティー・コンテンツを提供しています。

インフラストラクチャー、データ、アプリケーションの保護から、クラウドやマネージド・セキュリティー・サービスまで、IBM Security Services は重要資産の保護を支援する専門知識を備えています。IBM Security は、世界で最も高度なネットワークをいくつも保護しており、業界最高レベルの人材を揃えています。

協力者

ミシェル・アルヴァレズ
デイヴ・ベイルズ
ジョシュア・チャン
スコット・クレイグ
クリスティーン・ダール
チャールズ・デベック
アリ・エイタン (Intezer)
ブレディー・ファビー (Intezer)
ロブ・ゲイツ
ディルク・ハルツ
リモール・ケッセム
チェンタ・リー
デイヴ・マクミレン
スコット・ムーア
ジョージア・プラシノス
カミーユ・シングルトン
マーク・アッシャー
アシュカン・ビラ
フセイン・ビラニ
クレア・ザボエヴァ
ジョン・ゾラベディアン

IBM Security の詳細はこちら →

IBM Security
〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2020 年 2 月

IBM Security