Secureworks®

2022年年次レビュー
インシデント対応で得られた教訓

Secureworks® カウンター・スレット・ユニット™ リサーチチーム

目次

概要

Secureworks® は2022年1月から12月までの1年間で、500件を超えるセキュリティインシデントの封じ込めおよび修復対応を支援してきました。こうした現場での体験をもとに、当社カウンター・スレット・ユニット™ (CTU) のリサーチャーが新たな脅威や最新動向に関する知見を取りまとめました。リスク管理における意思決定、ベストプラクティスの共有、リソース配分の優先順位付けの指針としてお役立てください。

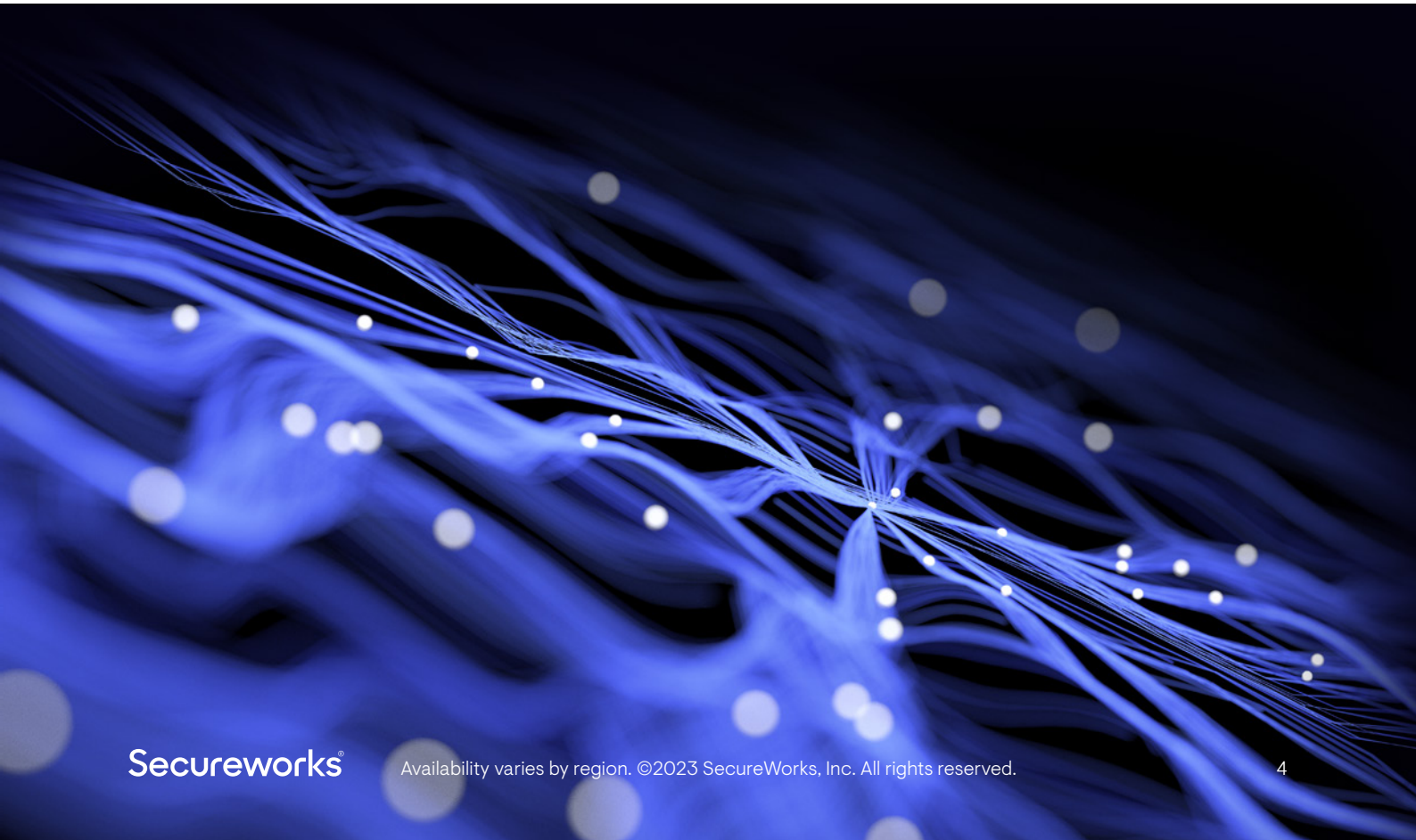
お客様が当社にインシデント対応を委託される経緯やその内容は様々です。たとえば、社内リソースの多寡やインシデントに関する報道を受けて、もしくは社内のセキュリティオペレーションに細心の注意を払うべき局面を迎えた、などのきっかけがあります。そのため、当社が観測した脅威の種類には、大局的な脅威動向が必ずしも反映されていない可能性があります。このような制限はあるものの、インシデント対応で得られたデータを解析することにより、「攻撃者がいかにしてネットワークを侵害するのか」、「攻撃者の活動が標的組織にどのような影響を及ぼすのか」、さらには「こうしたインシデントをどのようにすれば防げるのか」という点において有益な情報が得られます。

主なポイント：

侵入型ランサムウェアは、その影響の大きさから2022年も引き続き組織にとって重大な脅威でした。しかしながら、セキュアワークスが2022年に対応したインシデント事案のうち、金銭目的の攻撃活動で最も多かったのは、侵入型ランサムウェアを抜いてビジネスメール詐欺（BEC）攻撃となりました。

侵入手法（IAV）で最も多かった経路は依然としてインターネット接続システムの脆弱性でした。ただしBEC攻撃の増加を受けてか、2022年に当社が対応したインシデントのうちフィッシングがIAVとして使用されたケースが2021年の13%から33%に増えています。

多要素認証（MFA）とクラウドベースのホスティングにより攻撃対象領域に変化が生じました。このため、攻撃者はセキュリティ対策をすり抜けて目的を達成するための新たな方法を見出そうとしています。



観測された脅威の傾向

2022年に当社が対応したインシデントの79%は金銭目的のサイバー犯罪者によるものであり、当社のお客様にとっての最大の脅威は依然としてサイバー犯罪でした。一方、政府を後ろ盾とする敵対的なサイバー活動の割合は、セキュアワークスのインシデント対応全体の9%でした。残りは、被害組織の従業員による意図的な／過失による行為でした。金銭目的の侵害は過去2年（図1：2021年は85%、2020年は92%）と比べて減少していますが、ロシアによるウクライナ侵攻がその一因であると見られます。ウクライナやロシアのサイバー犯罪者らが、敵国を支持する組織を標的に活動するハクティビストに転向した可能性があるためです。

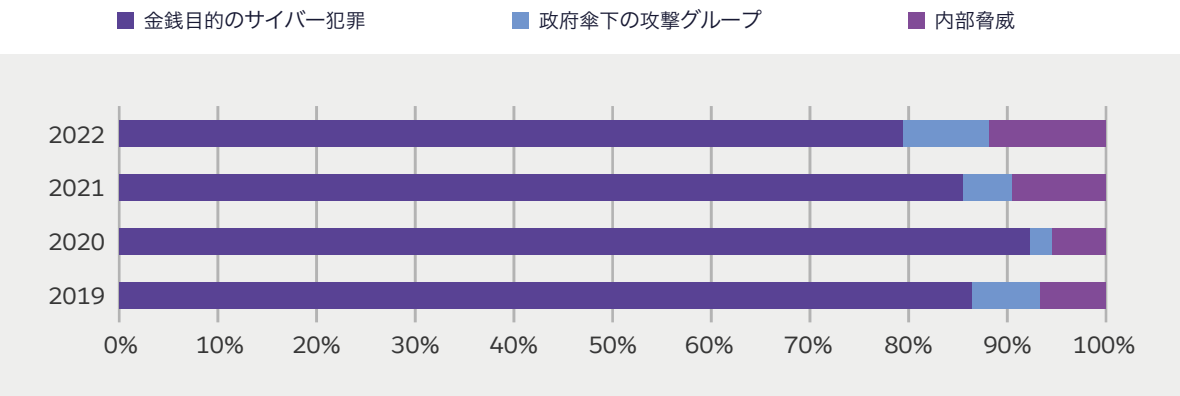


図1：2019年～2022年にかけてセキュアワークスのインシデント対応を攻撃者のタイプ別に分類（出典：SECUREWORKS）

2022年に当社が対応した金銭目的のインシデントには、ランサムウェア、BEC、暗号通貨マイニングなどの脅威が含まれています。サイバー犯罪者の活動は広範囲にわたり、脆弱なネットワークへの不正アクセスを通じてできるだけ多くの金銭的利益を得るという動機があります。そのため、ランサムウェアなど脅迫ベースの攻撃が依然として主流でした。

侵入に用いる攻撃手法（IAV：Initial Access Vector）

2022年にセキュアワークスが対応したインシデントで最も多用されたIAVは「インターネット接続デバイスの脆弱性の悪用」および「フィッシング」でした。両者はそれぞれ、IAVが判明しているインシデントの1/3を占めています（図2）。

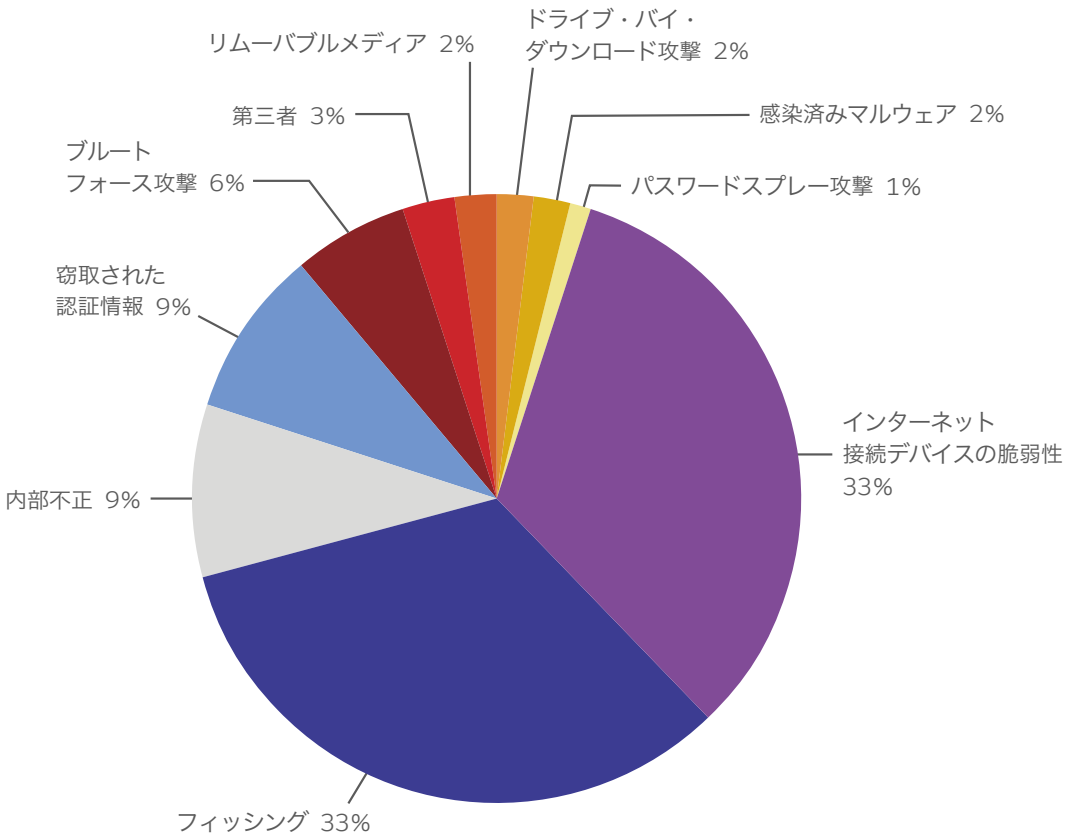
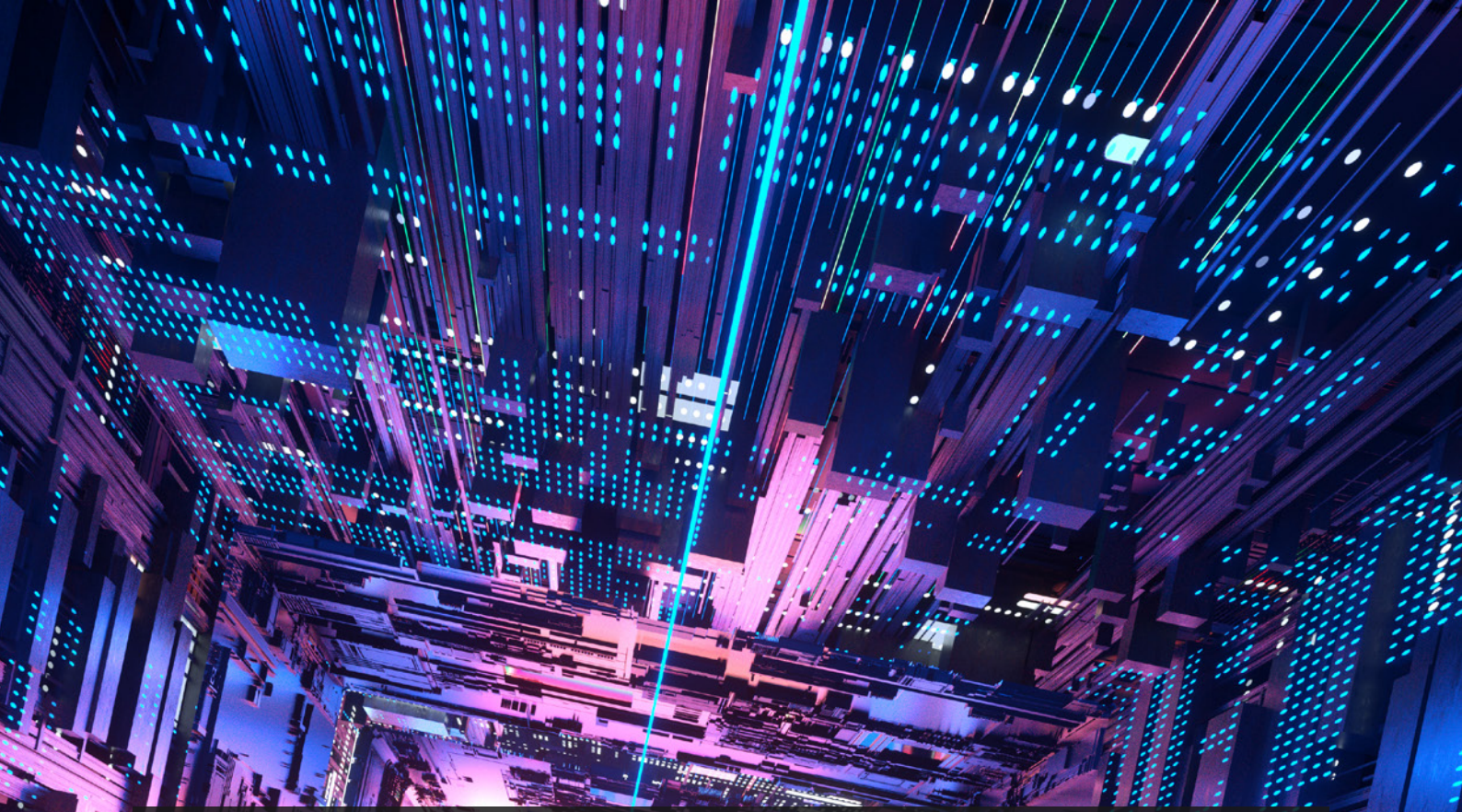


図2：2022年に当社が対応したインシデントで観測されたIAVの内訳（出典：SECUREWORKS）



観測されたIAVのMITRE ATT&CKへのマッピング

下表は、前述のIAVをMITRE ATT&CK®の各カテゴリにマッピングしたものです。このナレッジベースの情報をもとに脅威インテリジェンスデータを整理・分類し、実際の業務にお役立てください。

IAV	該当するMITRE ATT&CKカテゴリ
インターネット接続デバイスの脆弱性	Exploitation of Remote Services（リモートサービスの悪用） Exploit Public-Facing Application（外部公開されたアプリケーションの悪用）
認証情報（ブルートフォース攻撃、パスワードスプレー攻撃、窃取された認証情報）	Valid Accounts（正当なアカウント） Brute Force（ブルートフォース）
フィッシング	Phishing（フィッシング） Spearphishing Attachment（添付ファイル型スピアフィッシング） Spearphishing Link（リンク型スピアフィッシング） Spearphishing via Service（サービスを利用したスピアフィッシング）
第三者	Supply Chain Compromise（サプライチェーンの侵害） Trusted Relationship（信頼関係）
感染済みマルウェア	Develop Capabilities（攻撃能力の開発）
ドライブ・バイ・ダウンロード攻撃	Drive-by Compromise（ドライブ・バイ攻撃）

セキュアワークスが対応したインシデント全体で、「フィッシング」がIAVとして用いられたインシデントの割合は、2021年に比べて大幅に増加しています（図3）。その主な要因は、観測されたビジネスメール詐欺（BEC）インシデントの総数が2021年比で2倍以上に増えたためです。2022年に観測されたBECインシデントの85%で、フィッシングがIAVとして使われているため、これに比例した格好です。大半のケースでは、何千人もの受信者宛にフィッシングメールが送りつけられており、複数の組織にまたがる場合もありました。

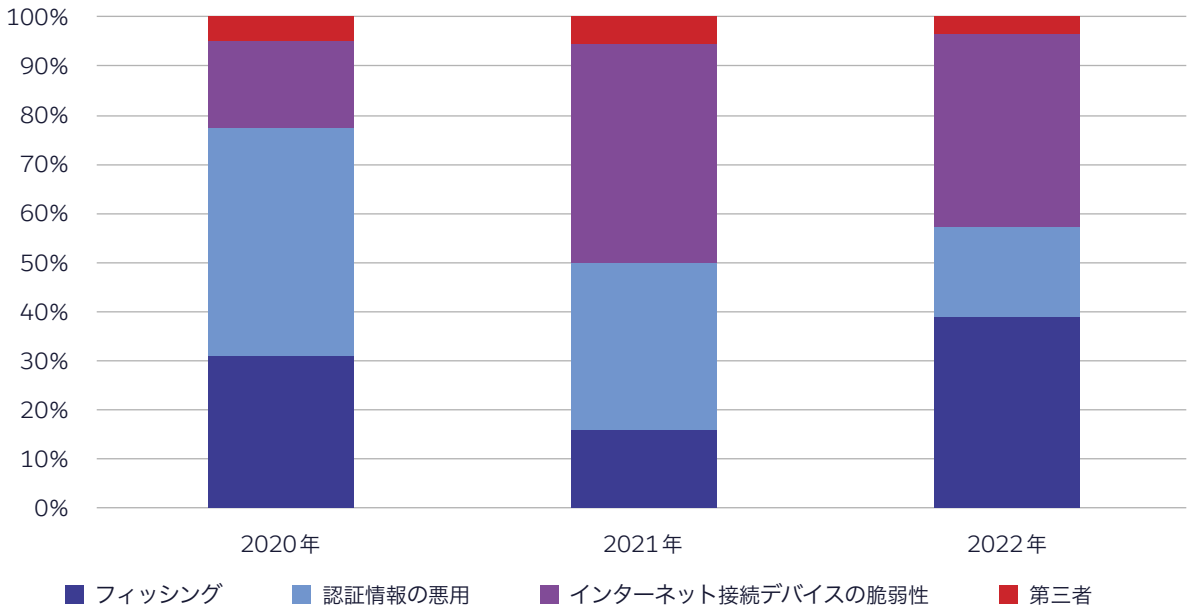


図2：2020年～2022にかけて観測されたIAVの推移。「認証情報の悪用」には、窃取された認証情報、ブルートフォース攻撃、パスワードスプレー攻撃が含まれます。（出典：SECUREWORKS）

本レポートの公表日現在、組織にとってBECは最大の金銭的脅威となっています。米国連邦捜査局（FBI）のインターネット犯罪苦情センター（IC3）は2022年、「世界全域で明らかになったBEC攻撃の被害額が2019年7月から2021年12月までの間に65%増加した」という報告を公表しました。被害額は増えているように見えますが、BECスキームの技術的な側面はこれまで同様、比較的単純です。報道などで目にする多額の儲けへの期待感や参入障壁の低さから、技術力が乏しい、またはほぼ皆無の攻撃グループもBEC攻撃に手を染め始めています。

2022年にセキュアワークスが対応したインシデントで「インターネット接続デバイスの脆弱性」が悪用されたインシデントの割合は前年比で微減したものの、2020年と比べると大幅に高い状況です。当社の観測によると、金銭目的の攻撃者および政府系の攻撃グループのいずれも、インターネット接続デバイスの脆弱性をIAVとして使用しています。多くのインシデントでは、攻撃者自らが脆弱性を見つけ出してエクスプロイトコードを開発するのではなく、公開されている脆弱性情報をもとに攻撃が実行されています。具体的には、脆弱性情報の公開を受けてセキュリティ研究者が開発・公表した脆弱性実証用のエクスプロイトコードが攻撃者によって武器化されていました。これを使って一斉スキャンを実行すれば、脆弱なデバイスを特定し、広範囲に攻撃を仕掛けることができます。中には、脆弱性が長年放置されていたデバイスが攻撃を受けることもあります。2022年もこれまで同様、大きく報道された脆弱性（2021年以降パッチが提供されているProxyLogon、ProxyShell、Log4Shellなど）が存在するサードパーティ製ソフトウェアが悪用された事例が当社CTU™のリサーチャーによって確認されています。

中国：脆弱性を発見しても共有せずに独占する政府

当社のお客様に影響を及ぼすサイバースパイ活動が最も活発な国々は中国、北朝鮮、イラン、ロシアです。なかでも中国は、その標的の幅広さで群を抜いています。2022年に当社のインシデント対応コンサルタントが調査した政府系攻撃グループの活動のうち、90%以上が中国の攻撃グループによるものでした。中国の攻撃グループは、中央政府による政治・軍事・経済的な優先政策を支援する目的でサイバースパイ活動を行っています。また、自国の経済成長目標の達成を後押しするために、様々な組織の知的財産や営業機密を窃取するという攻撃も、その活動の大半を占めています。

彼等の常套手段は、インターネット接続デバイスの脆弱性を悪用してネットワークを侵害することです。当社が2022年に観測した事例では、Zoho ManageEngine、Microsoft Exchange、Pulse Secureなどのサードパーティ製品やデバイス、およびカスタムアプリケーションなどが中国の攻撃グループの標的となっていました。ほとんどの攻撃は、パッチが提供されている既知の脆弱性を狙ったものでしたが、2021年3月にMicrosoft Exchange Serverが大規模な悪用攻撃を受けたことで、ゼロデイ脆弱性を熟知した中国の攻撃グループがもたらす脅威が浮き彫りになりました。

中国で活動する脆弱性対策の研究者らはこれまで、未知の脆弱性を発見して侵害できるかを競う国際コンテストの上位を占めてきました。しかし中国政府は2017年、中国籍の研究者にこうしたセキュリティ関連コンテストへの参加を禁じる規制を発令しました。さらに中国国内の個人や企業も、脆弱性を発見した場合は2日以内に中国政府に報告することが義務付けられています。一連の規制により、中国政府はゼロデイ脆弱性を独占的に入手できる立場となり、この情報が政府傘下の攻撃グループに悪用される恐れがあります。

多層防御型のネットワークセキュリティ対策では、自組織のネットワーク境界および攻撃対象領域を把握し、既知の脆弱性へのパッチ適用に関する厳格なプロセスを確立することが不可欠な要素となります。エンドポイント検知・対応（EDR）ソリューションを導入することで、ゼロデイ脆弱性の悪用が疑われる活動（通常と異なる親プロセス・子プロセスの関係や、横展開など）を効果的に特定できる可能性があります。

脅威動向に関する考察

2022年にセキュアワークスが対応したインシデントをもとに、脅威動向に関する考察を以下のとおり取りまとめました。

ランサムウェア攻撃は減少傾向か

2022年にセキュアワークスが対応したインシデントのうち、ランサムウェアに関連するものは前年比で57%減少しました。ランサムウェア攻撃活動が一見して減少傾向にある要因としては、ロシアのウクライナ侵攻に伴うサイバー犯罪の影響も考えられますが、他にもいくつか理由が考えられます。

- ランサムウェアグループは最大の儲けを得ようとするのと同時に、政府や法執行機関の目に留まらないよう影響度や注目度が大きい侵害を避けようとします。2021年に大きく報道されたColonial Pipeline、JBS、Kaseya各社へのサイバー攻撃を受け、米国政府が対抗措置を講じたことで、実行犯であるランサムウェアグループは多額の代償を支払うことになりました。世界各国の法執行機関および捜査当局は、こうしたランサムウェアグループをはじめとする犯罪集団の検挙に乗り出しており、悪質な活動に関与した個人の逮捕につながった事例もあります。こうした運命を辿らぬよう、一部のグループは既存の攻撃スキームを素早く停止し、名前を変えて活動しています。
- ランサムウェアグループの標的がこれまでのような大企業ではなく、侵害を受けてもインシデント対応を外部委託しないような知名度の低い組織に移っている可能性もあります。標的がシフトしているのであれば、「2022年にランサムウェア被害に遭った組織が支払った身代金の総額は減少している」とする外部機関のレポートにも納得がいきます。被害組織は、たとえ身代金要求に応じてもこれまでより低い金額を支払っていると見られます。
- ランサムウェアの前兆となる活動を検知可能なEDRソリューションの導入が進んでいる可能性があります。EDRソリューションがあれば、多くのランサムウェア攻撃グループがよく用いるペネトレーションテストツールCobalt Strikeや各種TTPs（Tactics（戦術）、Techniques（技術）、Procedures（手順））を検知し、後に発生するランサムウェアの展開を阻止できます。

ただし、Ransomware-as-a-Service（RaaS）型の運営モデルは間もなく破綻するだろう、という予測が2022年中に的中することはありませでした。当社CTUリサーチャーはランサムウェアグループの暴露サイトを監視していますが、これらのサイトに掲載されている被害組織の数は、月によって波はあるものの、2021年比で大きく低下していません（図4）。

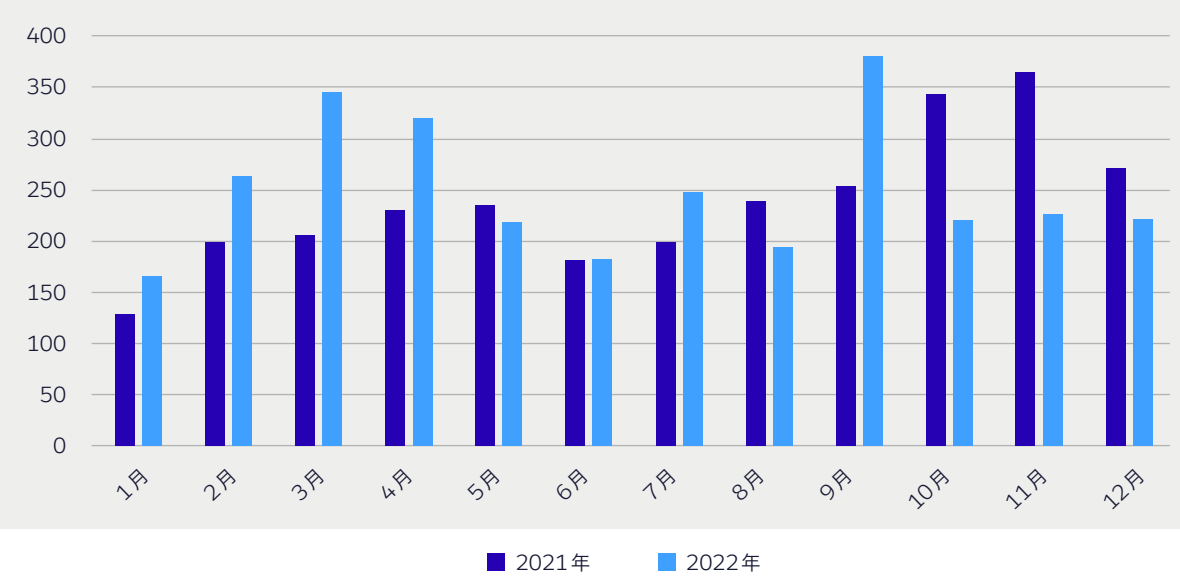


図4：2021年～2022年にかけてランサムウェアの暴露サイトに新規掲載された被害組織の数（出典：SECUREWORKS）

暴露型ランサムウェアの動向を当社CTUで分析した結果、多くの組織に被害を与え続けるRaaS型ランサムウェアの運営実態が明らかになりました。金銭目的で活動する攻撃グループGOLD MYSTICが運営するLockBitの暴露サイトには2022年1年間で920社の名前が公開されましたが、この数は2022年1年間にすべての暴露サイトに掲載された組織の33%近くにのぼります。LockBitサイトには9月だけでも228社が新たに掲載されています。GOLD MYSTICの代表者とされる人物による「LockBit 3.0では機能が強化され、インフラも拡張した」という主張も、同グループの活動が活発化している一因かもしれません。

このほか、ALPHV（別名BlackCat）、Conti、Black Bastaなどのランサムウェアも活発でした。当社は11月、マルウェアQakbotをきっかけにBlack Bastaが展開された複数の侵害事案を調査しました。Black Bastaの運営元である攻撃グループGOLD REBELLIONは4月に、最初の被害組織の名前を自らの暴露サイトに掲載しています。インシデントを分析した結果、侵入後24時間以内にデータが窃取され、ランサムウェアが展開されていました。各組織の皆様は、こうしたインシデントで用いられたTTPsに目を通し、現行のセキュリティ対策で同様の脅威を軽減できるか否かを確認されることを当社CTUリサーチャーより推奨します。とくにセキュリティ担当者の皆様は、Qakbotの検知・阻止が可能な対策を講じるようにしてください。

MFAは「一度導入すれば安泰」ではない

多要素認証（MFA）は、認証情報ベースの攻撃を軽減し、ネットワーク侵害の発生確率を抑制するうえで最も効果的な手段のひとつです。当社インシデント対応コンサルタントが観測した2022年1年間のIAVの構成比をみると「窃取された認証情報」が減少していますが、その理由は多くの組織がMFAを導入するようになったためかもしれません。ただし、MFAの普及が進むにつれ、攻撃者側も手を替え品を替えMFAの迂回を試みる、または別のIAVに乗り換える、などの動きを見せています。

セキュアワークスが2022年に対応したインシデントで、ビジネスメール詐欺の攻撃者が様々な手法を駆使してMFAの迂回を試みていたケースがありました。攻撃者は認証要求を送信し、被害者本人が確認せず承認したことで、MFAのバイパスに成功していました。このように、窃取した認証情報を使って同一アカウントへのログインを何度も試みる「MFA疲労攻撃」が攻撃者の間で広まっている可能性があります。MFA疲労攻撃は、MFAのプッシュ通知をアカウント保有者のモバイル端末宛に立て続けに送信し、本人がうっかり認証要求を承認するよう誘導するという手口です。

あるインシデントでは、フィッシングに成功した攻撃者が企業のOffice 365のユーザー名とパスワードを入手し、ユーザーらにMFA疲労攻撃を仕掛けた後、複数のアカウントにアクセスしていました。当該企業はこの活動を検知し、すぐに侵入を食い止めました。この事例による教訓は、たとえMFAなどの基本的セキュリティ対策を実施していても、社内の基幹リソースへのアクセス状況の監視を怠ってはならない、ということです。MFA疲労攻撃のリスクを軽減する手段のひとつは、「確認」や「承認」ボタンの代わりに、ユーザー本人にコードを入力させるタイプのMFA通知を導入することです。幸い、こうした攻撃者の認証要求はユーザーによって適切に拒否されている、または所属組織にインシデントとして報告されているため、多くの攻撃が失敗に終わっています。

このインシデントは社用デバイスで発生しましたが、情報窃取マルウェアで個人デバイスから企業データが盗み取られるという事案も、組織にとって大きな脅威になりつつあります。個人デバイスは社用デバイスに比べて全体的にセキュリティ対策が甘く、業務で使う認証情報が保存されていることもあるため、MFA疲労攻撃を仕掛けられたり、企業ネットワークに侵入するためのIAVとして使用されたりする恐れがあります。また、正規の企業サイトに偽装したウェブサイトにユーザーを誘導し、本人のデバイス上で認証情報および二要素認証コードを入力させるフィッシングキャンペーンなどを見れば、攻撃者がMFAの認証情報を盗み取れるということもわかります。セキュリティ担当者の皆様はフィッシング耐性の高いMFA（物理トークンなど）の導入を検討し、こうした攻撃に備えてください。

クラウド技術に適した最新の活動ノウハウを身に付ける攻撃者

コロナ禍により、多くの組織でクラウドベースのマネージドソリューションへの移行が加速しました。これらのソリューションは通常、セキュリティ面の影響が充分考慮されないまま短期間で導入されます。クラウドサービスに付随するセキュリティ対策も利用できますが、正しい形で導入しなければなりません。当社のインシデント対応コンサルタントが調査する侵害事案の多くは、基本的なセキュリティ対策の欠如や設定不備が原因です。きちんと対策していても、クラウド環境には依然として攻撃者の足掛かりとなるような脆弱性が存在します。

クラウド型サービスの普及に伴い、攻撃者は標的組織に侵入した後に目的を達成するための新たな活動ノウハウを考案せざるを得なくなっています。当社のインシデント対応コンサルタントが関わった事案にて、標的組織に侵入した中国のサイバースパイグループと思われる攻撃者が、侵害済のオンプレミスネットワークからアカウントが同期されているAzure Active Directory（AD）テナントに横展開したケースがありました。この攻撃グループは、インターネット公開されたMicrosoft Exchange Serverの脆弱性ProxyShellを悪用してオンプレミスネットワークに侵入し、Azure ADテナントにアクセスした後に、Exchange Webサービス（EWS）APIのアクセス許可を使ってシングルテナントアプリケーションを登録していました。これにより、Exchange Onlineを介して標的組織のメールボックスにアクセスできる状態になりました。

自社環境がオンプレミスであっても、クラウドやハイブリッドソリューションの環境であっても「鎖の強さは最も弱い輪によって決まる」という言葉のとおり、最も脆弱な部分が狙われます。前述の事例を見ると、攻撃対象領域の変化に合わせたリスク軽減策が不可欠であることが改めてわかります。セキュリティ担当者の皆様は、自社のクラウド環境からログとして収集しているデータの種類、および収集したデータの保管方法について把握しておくことを推奨します。適切にログ収集ができれば（一元管理されたログ収集プラットフォームが理想）、クラウド環境および自組織のIT資産全体にわたるユーザーの活動状況を可視化できます。ログデータを見ると、通常と異なる活動を特定でき、効果的な軽減策に不可欠な情報（侵入範囲やその影響）に関する洞察を得られます。

インシデント防止に向けた推奨策

当社ではインシデント対応の完了後、発生したインシデントの影響を最小限に抑えるためのセキュリティ対策を丁寧にご説明し、再発防止に向けた対策の優先順位についてお客様にアドバイスしています。侵害されたお客様環境のセキュリティ対策では、EDRソリューションの包括的な展開（ホスト、ネットワーク、クラウドリソース全体にまたがるログ保管・分析の一元的サービス）や不審なドメインやIPアドレスに対するレピュテーションベースのWebフィルタリングやネットワーク検知が徹底されていないケースが目立ちました。

まとめ

当社のCTUリサーチャーは、インシデント対応で明らかになった脅威および攻撃者の振る舞いを追跡し、様々な脅威の特性および発展動向の把握に役立てています。当社のCTUリサーチャーおよびインシデント対応コンサルタントは、脅威への対策プログラムの開発、定期的な脅威動向の分析、インシデント対応を通じて観測された攻撃活動に関するレポート（実務者向けに随時発行）を通じて、お客様を常に保護し、実際のインシデント対応から得られた知見とガイダンスを提供します。

Secureworks®

Secureworksのインシデント対応について

広範囲な専門知識、サイバー脅威に関するインテリジェンス、目的に応じたテクノロジーを擁するセキュアワークスのインシデント対応チームが、サイバーインシデントの予防対策および発生後の対応を支援します。当社のインシデント対応コンサルタント（コマンダー）が、オンサイト*またはリモート形式で皆様のインシデント対応を支援します（*パンデミックによる渡航制限の影響を受ける可能性あり）。緊急インシデント対応サービス、脅威ハンティングによるアセスメント、机上演習、その他様々なインシデント事前準備サービスを通じ、当社の専門家がお客様の社内チームと密接に協力します。これらはすべて、お客様組織におけるインシデント対応プログラムの策定、大規模インシデントの効果的・効率的な解決を目的としたサービスです。

Secureworksについて

Secureworks（セキュアワークス、NASDAQ: SCWX）は、Secureworks® Taegis™を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。

www.secureworks.jp

出典

Abrams, Lawrence. "MFA Fatigue: Hackers' new favorite tactic in high-profile breaches." Bleeping Computer." September 20, 2022.

Asokan, Akshaya. "Microsoft Exchange Flaw: Attacks Surge After Code Published." GovInfoSecurity.March 20, 2021.

Chainanalysis. "Ransomware Revenue Down As More Victims Refuse to Pay." January 19, 2023.

Dignan, Larry. "Colonial Pipeline cyberattack shuts down pipeline that supplies 45% of East Coast's fuel." ZDNET.May 8, 2021.

Hageman, Mitchell. "Secureworks CTU identifies increase in stolen credential sales." SecurityBrief Asia.December 5, 2022.

Makortoff, Kalyeena. "World' s biggest meat producer JBS pays $11m cybercrime ransom." The Guardian.June 10, 2021.

Microsoft. "HAFNIUM targeting Exchange Servers with 0-day exploits." March 2, 2021.

Red Hot Cyber. "RHC interviews LockBit 3.0. 'The main thing is not to start a nuclear war'." July 26, 2022.

Secureworks. "Azure Active Directory Flaw Allows SAML Persistence." January 18, 2023.

Secureworks. "BRONZE STARLIGHT Ransomware Operations Use HUI Loader." June 23, 2022.

Secureworks. "How to Prevent Multi-factor Authentication Bypass." June 7, 2022.

Secureworks. "Kaseya VSA Software Under Active Attack." July 3, 2021.

Secureworks. "Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?" December 17, 2021.

Secureworks. "Secureworks FAQ: Russian Activity in Ukraine." February 24, 2022.

Secureworks. "Think MFA is Hack-Proof? Think Again." April 30, 2020.

Tsai, Orange. "From Pwn2Own 2021: A New Attack Surface on Microsoft Exchange - ProxyShell!" Zero Day Initiative.August 18, 2021.

U.S.Cybersecurity & Infrastructure Security Agency (CISA). "Implementing Phishing-Resistant MFA." October 2022.

U.S.Federal Bureau of Investigation. "Business Email Compromise: The $43 Billion Scam." May 4, 2022.