SOPHOS
Cybersecurity delivered.

Active Adversary Playbook 2022

2021年のインシデント対応の最前線で見られたサイバー攻撃者の行動、戦術、ツール

CTO Office、Senior Security Advisor、**John Shier**

ソフォスホワイトペーパー 2022年 6月

はじめに

急速に進化し、ますます複雑化するサイバー脅威から組織を守ることは、相当困難のものとなり得ます。攻撃者は、行動やツールセットを常に適応・進化させます。新しい脆弱性を活用して、日常的に使用している IT ツールを悪用することで、検知を回避し、セキュリティチームの一歩先を行くのです。

組織の IT およびセキュリティ運用の専門家にとって、攻撃者が使用する最新のアプローチに追い付くのは困難な場合があります。特に、初期アクセスブローカー（IAB）が標的を侵害し、そのアクセス権をランサムウェアの犯罪グループに販売して攻撃に使用するなど、複数の実行者が関与する標的を絞ったアクティブな攻撃の場合は困難になります。

Active Adversary Playbook 2022 では、ソフォスの最前線のインシデント対応者が 2021年に目撃した主な攻撃者、ツール、攻撃行動について詳しく説明しています。これは、Active Adversary Playbook 2021 に続き、攻撃の状況がどのように進化し続けるているかを説明しています。

本ドキュメントでは、攻撃者が攻撃時に何をするのかを理解し、ネットワーク上で攻撃活動を見つけて防御する方法を理解できるようにすることを目的としています。

この調査結果は、2021年に Sophos Rapid Response チームが調査したインシデントのデータに基づいています。可能な場合、Active Adversary Playbook 2021 に記載されているインシデント対応の結果とデータを比較します。

インシデント対応統計情報 2021

このレポートは、米国、カナダ、英国、ドイツ、イタリア、スペイン、フランス、スイス、ベルギー、オランダ、オーストリア、アラブ首長国連邦、サウジアラビア、フィリピン、バハマ、アンゴラ、日本に所在するあらゆる規模の組織で、さまざまな業種を対象とした 144件のインシデントに基づいています。

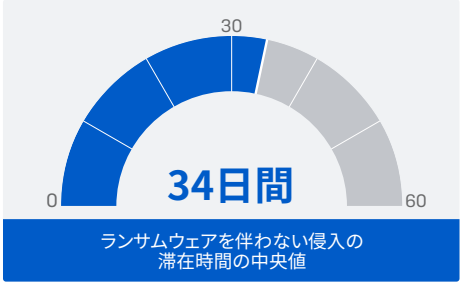
最も代表的な業種は、製造業（インシデント対応ケースの 17% がこのセクター）であり、次いで小売業（14%）、医療機関（13%）、IT（9%）、建設業（8%）、教育（6%）となっています。本レポートの巻末にあるデータテーブルには、追加のプロファイル情報が記載されています。

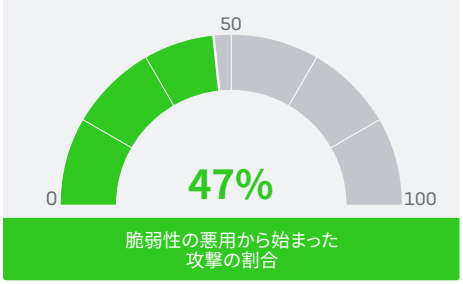
ダッシュボード: 2021 年のアクティブな攻撃手法の分析

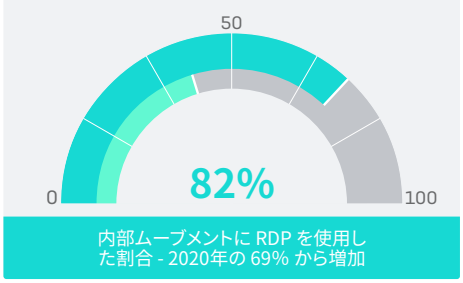
今年の最も影響力のある 2つのサイバー脅威の動きが、2021年 3月と 8月に発生し、Microsoft Exchange サーバーの ProxyLogon および ProxyShell の脆弱性が報告されました。CISA やその他の政府のセキュリティ機関によって最近指摘されているように、ProxyLogon / ProxyShell のバグは攻撃者によって広範囲に悪用されています。予想されるように、これらのバグは 2021年 にソフォスが調査したかなりの数のインシデントに含まれています。

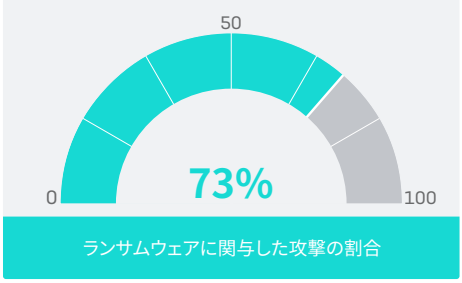
ダッシュボード: 2021 年のアクティブな攻撃手法の分析

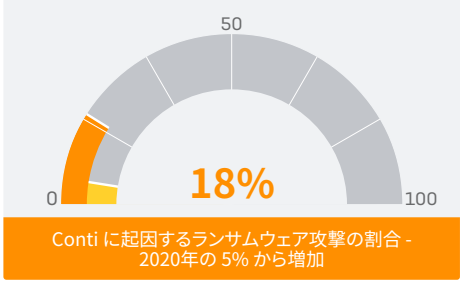
インシデント対応調査から得られた主な調査結果

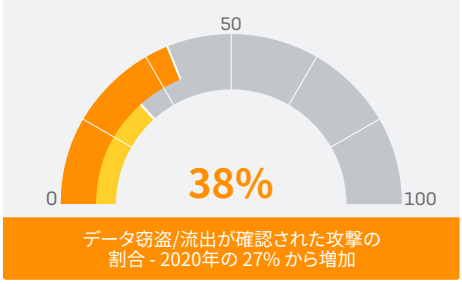












現在知られていない ProxyLogon/ProxyShell の侵害が、さらに多く発生している可能性があります。この場合、Web シェルとバックドアを被害者に埋め込んで、永続的にアクセスを行い、そのアクセスが使用または販売されるまで静かに待機しています。

これは、2021年にサイバー脅威の状況を形成する別の大きな発展につながります。つまり、初期アクセスブローカー（IAB）の影響力と力の増大につながっています。

IAB の成功は、標的を最初に突破し、販売できるアクセスを獲得できるかどうかにかかっています。そのため、IAB は新たに報告されたバグにいち早く反応し、広範囲にパッチが適用される前に標的を攻撃しようとすることがよくあります。彼らの目的は、被害者の中に足がかりを確保し、場合によっては資産の価値を把握するために最初の探索的な動きを実行することです。その後、ランサムウェアの運営側など他の攻撃者にアクセス権を販売します。これには最初の侵入から数か月かかる場合もあります。

2022年版ソフォス脅威レポートで強調されているように、IAB の増加は、専門サービスサプライヤーの数が増加しているサイバー脅威市場において、攻撃の「プロ化」していることが反映しています。RaaS（ランサムウェア・アズ・ア・サービス）業界が繁栄していることも、この傾向の一例です。

最後になりますが、2021年のインシデント対応調査で明らかになったフォレンジックエビデンスでは、IAB、ランサムウェア犯罪グループ、クリプトマイナー、そして時には複数のランサムウェアオペレーターなど、複数の攻撃者が同じ組織を同時に標的にしている事例が明らかになりました。これは、2022年以降もサイバー脅威の状況を形成していくことになります。

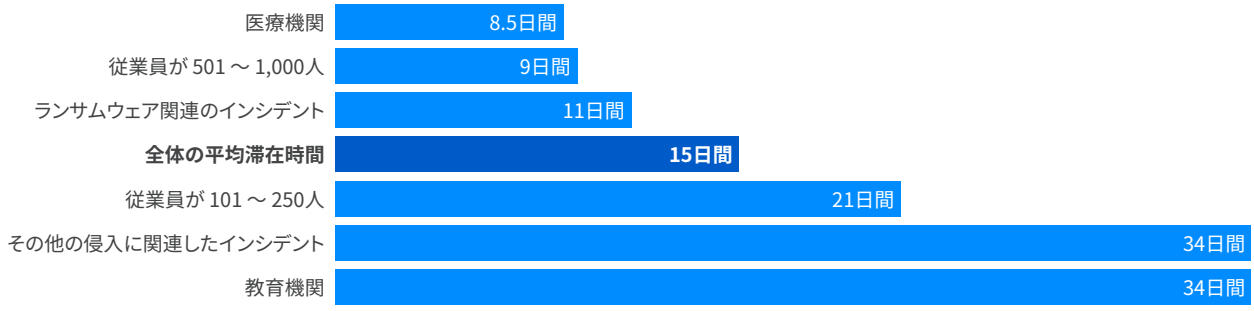
侵入者が被害者のネットワークに滞在する時間が長くなっているのは、このような活動によるものと思われます。長い間、時には同時に被害者のネットワークに存在する他の攻撃者とは、ボンネットビルダーやマルウェア配信プラットフォーム、またはドロッパーなどがあります。

これらの状況の形成については、以下で詳しく説明します。

隠れた侵入者

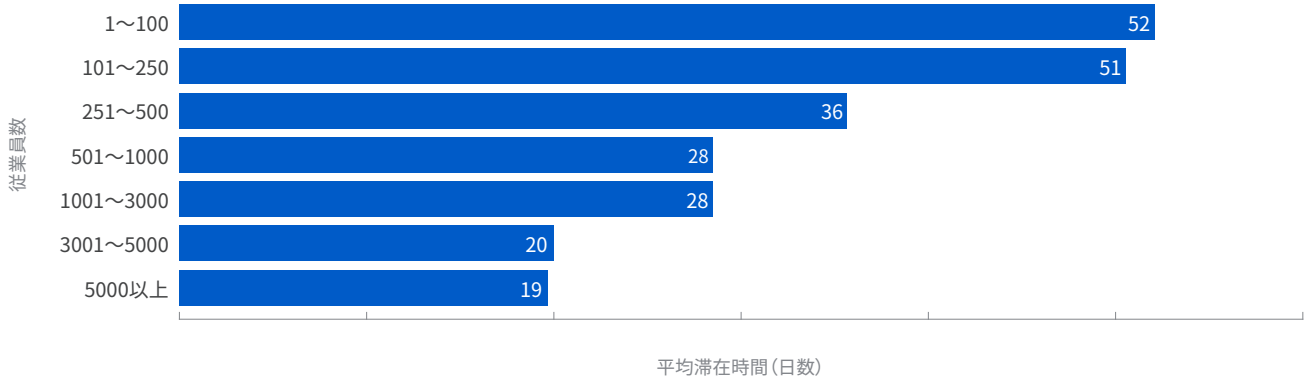
インシデントデータによると、2020年から 2021年にかけて、平均滞留時間の中央値が 11日から 15日と約 3分の 1に増加しています。ランサムウェアでは、滞留時間が平均で約11日（2020年の 18日から減少）と短く、その他の侵入を伴う攻撃は滞留時間の中央値は 34日と大幅に長くなっており、かなりのばらつきがあります。

侵入者の平均滞留時間の変動（中央値）



前述のように、滞留時間が長いのは、IAB の関与を反映している可能性があります。また、小規模企業や教育機関（平均滞留日数 34日）などの業種では、滞留時間が長くなることは、社内の IT セキュリティ担当者が疑わしい警告や潜在的な脅威を積極的に探し、調査し、対応することがいかに困難かを反映しています。

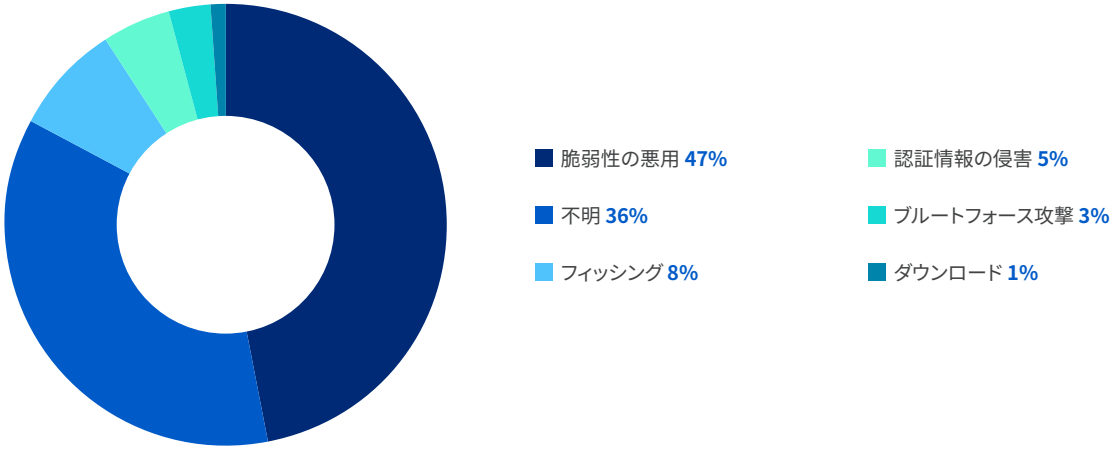
企業規模別の侵入者の滞留時間 (平均値)



攻撃の根本原因

攻撃の根本原因を特定することは、必ずしも可能だと限りませんし、容易でもありません。攻撃者が意図的に自分たちの活動の証拠を削除している場合もあれば、インシデント対応者が証拠にたどり着く前に、IT セキュリティチームが感染したマシンをすでに消去したり、再イメージングしたりしている場合もあります。それにもかかわらず、ソフォスが調査したインシデントの中で、ProxyLogon や ProxyShell などのパッチが適用されていない脆弱性の悪用が、2021年に調査されたサイバーインシデントの約半数（47%）の根本原因であることが明らかになっています。

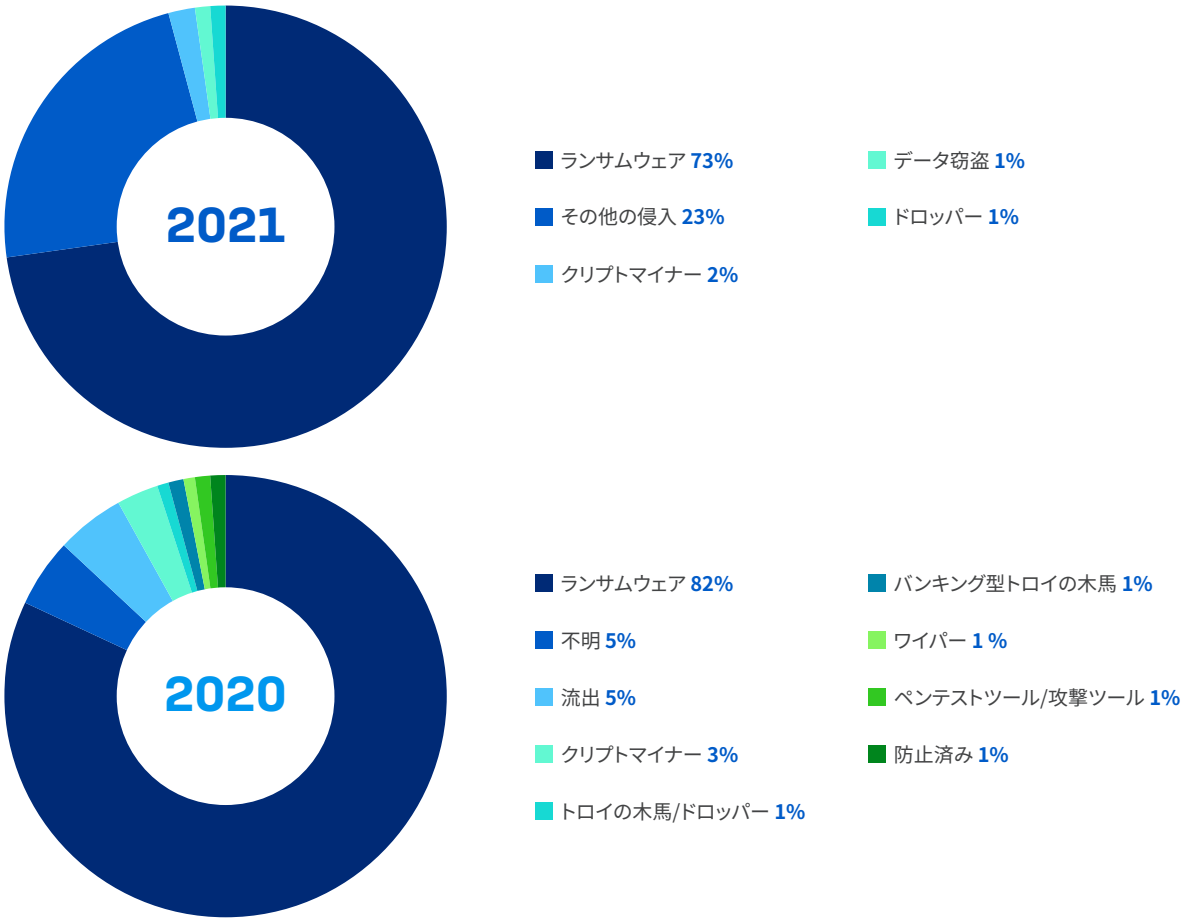
攻撃の根本原因



主な攻撃タイプ

ランサムウェアの展開は、多くの場合、IT セキュリティチームが攻撃を認識できるようになるポイントです。したがって、2021年にソフォスが対応したインシデントの 73% がランサムウェアに関連していたことは驚くべきことではありません。また、ランサムウェアは、2020年に最も普及した攻撃タイプであり、82% (この数値が高いのは、データセットが小さいことを反映している可能性があります) でした。データ窃盗の場合、インシデントの 1% を占めるインシデント対応者は、これらの攻撃がランサムウェア攻撃にまで拡大した可能性があると考えていますが、時間内に捕捉され、無効化されました。

攻撃の種類



インシデント対応調査で明らかになった 2番目に一般的な攻撃は、「その他の侵入」という広範なカテゴリであり、インシデントの 23% を占めていました。このレポートでは、「その他の侵入」とは、ランサムウェアやその他の追跡可能な攻撃タイプではない侵入のことを指します。

侵入は、ProxyLogon や ProxyShell など、パッチが適用されていない脆弱性を悪用した結果であることが多いですが、リモートアクセスサービスや安全でない VPN の悪用、アカウントの認証情報の盗難、セキュリティの見落とし (インターネットへの侵入拠点を公開したままにするなど) も含まれます。

重要なことは、悪意のあるペイロードが標的に配信される前に、侵入を検知し、無力化したことです。これらの侵入の大部分とは言わないまでも、一部は IAB の余剰在庫であったと考えるのが妥当であり、別の攻撃者にまだ販売されていない「バンクされた」アクセスです。もし、侵入が検知されなかったら、かなりの数がランサムウェア攻撃に発展していた可能性があります。

調査したインシデントの 2% で、クリプトマイナーが主な攻撃タイプとなっていました。悪意のあるクリプトマイナーが、不正なコインの採掘によってコンピュータの処理能力を引き出すため、システムパフォーマンスへの影響を受けて検出されることがよくあります。クリプトマイナーは、低レベルで厄介な脅威として排除したくなるかもしれませんが、ネットワーク内に存在するという事実は、どこかに脆弱な侵入拠点が存在することを証明しており、今後発生する深刻な脅威の前触れである可能性があります。

一般的に、同じことが、標的となるシステムに他の悪意のあるペイロードを配信、ロード、インストールするように設計されたドロッパーやマルウェア配信システムについても当てはまります。これらは、バックドアやランサムウェアなどの悪意のあるモジュールを追加するためのプラットフォームを提供し、攻撃を展開するためのイネーブラ(後援者)となります。そのため、防御側は、大規模な攻撃の前兆となることが多いため、Trickbot や Emotet などのドロッパーやマルウェア配信システムの存在を主要なランサムウェアグループと同じ深刻さで処理する必要があります。

混雑した狩場

攻撃タイプは相互に排他的ではない。前述したように、IAB、ランサムウェア犯罪グループ、クリプトマイナーなど、複数の攻撃者が個々のターゲットネットワークで同時に出没することがあります。

たとえば、わずか 2% のインシデント対応の事例では、クリプトマイナーが主な攻撃タイプでしたが、7% のランサムウェアインシデントにもクリプトマイナーは存在していました。クリプトマイナーは、感染したネットワーク内の他のマイナーをスキャンして削除することがよくありますが、ランサムウェアなどの他の脅威と快適に共存することができます。

2021年にソフォスが報告した同時攻撃インシデントには、Atom Silo ランサムウェアや 2つのクリプトマイナーが関与するものや Netwalker と REvil が関与する二重脅迫型ランサムウェア攻撃があります。この傾向は 2022年になっても続いています。

攻撃者のツールボックス

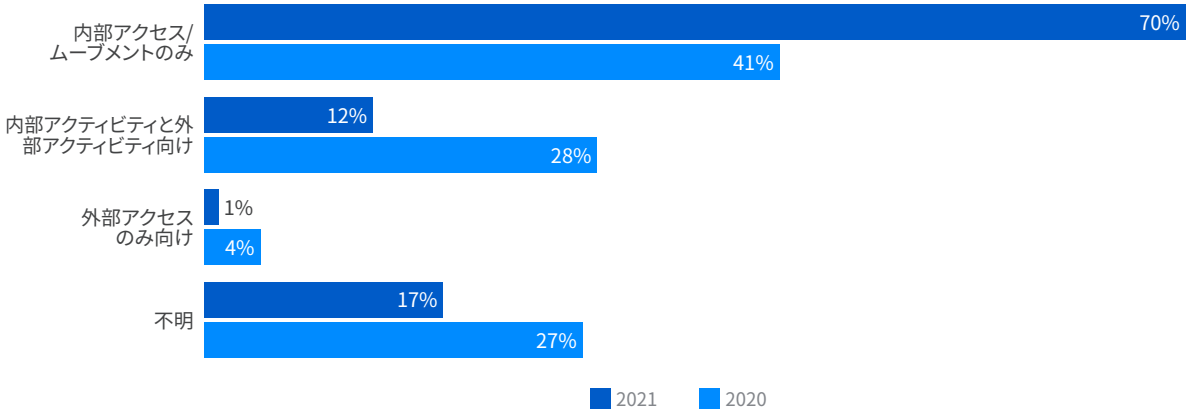
リモート デスクトップ サービスは主な内部脅威

RDP は少なくとも 83% の攻撃に関与しており、2020年（73% の攻撃に関与）から増加しています。事例の 82% では内部使用、13% が外部使用となっていました。これは、2020年のそれぞれ 69%、32% と対照的になっています。

ただし、攻撃者が RDP を使用する方法には注意が必要です。RDP を使用したインシデントの 4分の 3以下（70%）では、このツールは内部アクセスとラテラルムーブメント向けのみに使用されており、2020年の 41% から大幅に増加しました。

RDP が外部アクセスに**のみ** 使用されたケースはわずか 1% で、2020年の 4% から減少しています。攻撃のわずか 12% で、外部アクセスと内部ムーブメントの両方で RDP を使用していることが示されており、これは 2020年（28%）の半分以下の割合となっています。

攻撃者の RDP (リモートデスクトッププロトコル) の使用率



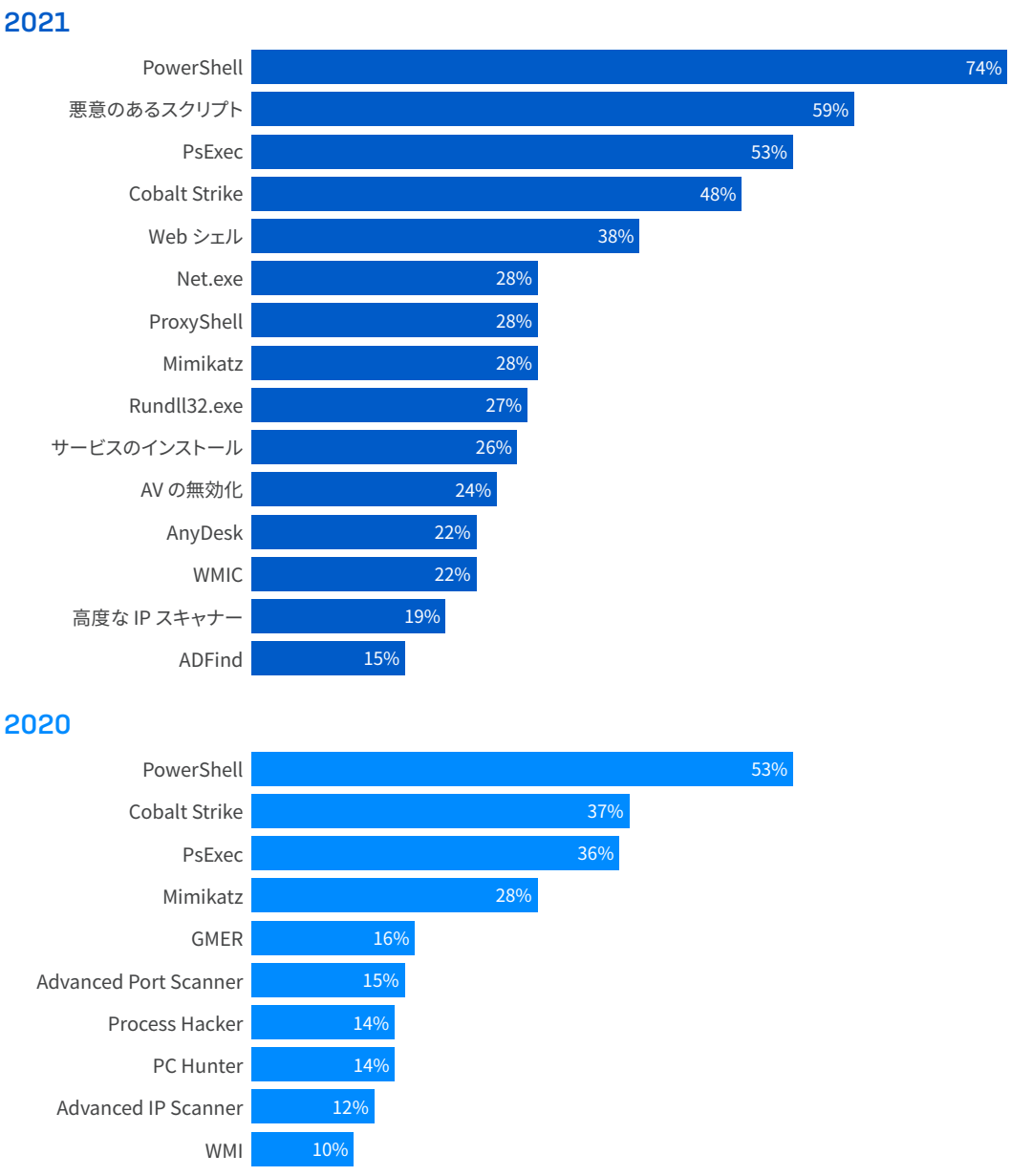
RDP による外部アクセスの減少では、サービスを無効化するなどのセキュリティの向上が反映されていると考えられます。ただし、RDP は境界内で広くアクセス可能であり、このアクセスを強化することはセキュリティチームにとって重要な焦点となります。

2021年の攻撃ツールセット

次のグラフは、2021年の攻撃者のツールセットに含まれた可能性が最も高いツール、テクニック、サービスなどの「アーティファクト」を表示しています。これらの多くは、IT 専門家が正当な行いを目的として使用することもできます。攻撃者に人気がある理由は、認証情報の盗用、発見、ラテラルムーブメント、マルウェアの実行など、日常の IT 活動に害を与えることなく紛れ込むことができるためです。

このアーティファクトの数と性質は、ネットワーク上の悪意のある活動と合法的な活動を区別する際に、防御側が直面する課題を浮き彫りにしています。

攻撃で使用される主なアーティファクト



攻撃で使用される最も一般的な項目を詳しく調べると、2021年のサイバー攻撃の典型的なプレイブックが明らかになります。

ツールセットを構成するアーティファクト

インシデント対応の調査中に特定されたアーティファクトは、合法的なツールとハッキングツール、Microsoft バイナリ、追加アーティファクト（スクリプト、テクニック、サービスなど）の 3つのカテゴリに分類できます。

インシデントレスポンスの調査では、アーティファクトは、2020年の 132種類 (基本サンプルサイズも大きくなっていますが) から増加し、全部で 525種類が見つかりました。この内訳は、209種類の合法的なツールとハッキングツール、107種類の Microsoft バイナリ、209個の追加アーティファクトで構成されています。

合法的なツールとハッキングツール

これらのツールには、攻撃を支援するために使用されたソフトウェアが含まれます。2020年から Cobalt Strike（48%）と Mimikatz（28%）が上位 2位を維持し、その後に AnyDesk（22%）、Advanced IP Scanner（19%）、ADFind（15%）と続きます。2020年と比較すると、Cobalt Strike がシェアを伸ばし（37% から上昇）、Mimikatz は横ばい（28%で維持）で、新たに3つのツールがトップ 5にランクインしました。

Cobalt Strike は、セキュリティチームがさまざまな攻撃シナリオを再現できるように設計された、市販のエクスプロイトツールスイートです。攻撃者は、感染したマシンに Cobalt Strike の「ビーコン」バックドアを確立しようとします。ビーコンは、コマンドの実行、追加ソフトウェアのダウンロードと実行、ターゲットネットワーク全体にインストールされている他のビーコンへのコマンドのリレー、Cobalt Strike サーバーへの通信を行うように設定できます。ネットワーク上で Cobalt Strike が検出された場合は、すぐに調査する必要があります。

2番目に広く普及しているツールである **Mimikatz** は、攻撃的なセキュリティツールとして設計されたもので、パスワードやその他のアカウントの認証情報を盗んで攻撃に活用することができます。

合法的なネットワークスキャナである **Advanced Port Scanner** や **IP Scanner** などを使用して、IP とデバイス名のリストを生成します。これにより、攻撃者は被害者の最も重要なコンピュータやインフラに侵入できます。

合法的な **AnyDesk** IT 管理ツールの悪用は、ますます一般的になっています。これは、マウス/キーボードの制御や画面表示機能など、攻撃者が標的とするコンピュータを直接制御できるからです。また、**TeamViewer**、**Screen Connect**、**Atera RMM**、**Splashtop** などの合法的なリモートアクセスサービスも、2021年に上位となりました。

Process Hacker、**PCHunter** および **GMER** はすべて、カーネルドライバを含む合法的なツールです。攻撃者が適切なカーネルドライバをインストールした場合、セキュリティ製品を無効化することがよくあります。

Microsoft バイナリ

Microsoft ツールを一般的なツールから分離することで、攻撃者がいかにその場所に根ざして生きているかがわかります。これらのツールはすべて、Microsoft によってデジタル署名されています。**PowerShell**（74%）がリストの上位に表示され、続いて **PsExec**（53%）、**net.exe**（28%）、**rundll32.exe**、および **WMIコマンドライン**（WMIC）ツール（22%）が表示されています。PowerShell、PsExec、および WMIC の使用はすべて、2020年に比べて 2021年に増加しました。

このツール「net.exe」は攻撃の多くの段階で使用され、検出ツールとして最も一般的に使用されました。一方、「rundl32.exe」は実行と防御の回避に広く使用されました。

ネットワークに潜む攻撃者を指し示す可能性のあるその他の Microsoft ツールには、「**whoami.exe**」、**タスクスケジューラ**（持続性を維持）、および「**schtasks.exe**」(悪意のあるコードを実行)があります。このようなツールの使用は注意深く監視する必要があります。

追加アーティファクト

このカテゴリには、保護機能を無効にしようとした、ProxyShell などの脆弱性、**Mega.io** などのクラウドサービスの使用、検出された追加のマルウェア、二次感染、使用したトランスポートプロトコルなどのツールとテクニックの両方が含まれています。

調査したインシデントの 59% で、**悪意のあるスクリプト**（PowerShellを除く）が確認されました。悪意のあるスクリプトとは、悪意のあるアクティビティを可能にするソフトウェアコードです。攻撃者に悪用されるスクリプトの例としては、DOS/CM バッチスクリプトやコマンドラインスクリプト、Python スクリプト（プログラムのように実行するコマンドをファイルにまとめたもの）、VBScripts（Windows や Windows Explorer で実行できる Visual Basic スクリプト）などがあります。

Web シェルは、2番目に多い種類の脅威（インシデントの 38%）であり、ProxyShell（28%）と ProxyLogon（11%）も調査で目立っていました。サービスのインストール、保護の無効化、LSASS のダンピング、不正なアカウントの作成、レジストリの変更、ログの消去などが上位 10位を占めています。

データ窃取

2021年、**Rclone** は、窃取に使用される上位のアーティファクトのリストに入りました。Rclone は、Mega などさまざまなクラウドストレージプロバイダーに接続するコマンドラインツールで、2021年にはデータ窃取で最も多く使用されたツールでした。今年のデータに見られる他のクラウドストレージプロバイダーには、**Dropbox**、**DropMeFiles**、**M247**、**pCloud**、**Sendspace** などがあります。

インシデント調査で発見されたデータ窃取を支援するツールには、Rclone の他に、**Megasync**、**FileZilla**、**Handy Backup**、**StealBit**、**WinSCP**、**Ngrok** があります。

2021年の上位リストに窃取ツールが登場したことは、調査したすべてのインシデントの 38% (2020年の 27% から上昇) がデータの窃取に関係していたという事実を考えると、納得がいきます。その他の多くのインシデント（全体で8%）では、データが収集され、削除される可能性があるようにステージングされている形跡が見られました。窃盗が行われた場合、盗難にあった情報がその後インシデントの 46% において漏洩したことが証拠から示唆されています。

攻撃者は通常、ランサムウェアを展開する前の最終段階として情報を削除します。ソフォスのインシデント解析によると、2021年のデータ窃盗とランサムウェアの展開との中央値ギャップは約 44時間でした。平均ギャップは 4日（4.28日）を超え、中央値ギャップは 2日（1.84日）未満でした。

どちらの平均値を使用するかにかかわらず、ここで重要なメッセージは、窃取後に、防御側が攻撃の最終的かつ最も損害を与える段階が展開されるのを防ぐ絶好のチャンスの見込みがあるということです。したがって、データ窃取に使用されることがわかっているツールの検出は、優先的に調査する必要があります。

ツールの組み合わせ

インシデント調査により、IT セキュリティチームに強力な警告信号を提供する被害者ネットワーク上のツールの組み合わせパターンが次のように明らかになりました (一部のケースでは 2020年の比較データが利用可能な場合もありました)

- 2021年には、PowerShell スクリプトと悪意のある非 PS スクリプトが 64% のケースで一緒に見られました
- PowerShell、Cobalt Strike、PsExec は 2020年の 12% に対して、33% でした
- PowerShell と PsExec の組み合わせが 2020年の 49% に対して、51% でした
- PowerShell、悪意のあるスクリプト、Cobalt Strike は 42% でした
- PowerShell、悪意のあるスクリプト、PsExec は 38% でした
- PowerShell、Cobalt Strike、PsExec は、2020年の 12% から 33% になりました
- Cobalt Strike と Mimikatz の組み合わせは 16% でした

このような相関関係は、昨年同様、今年も重要です。検出は差し迫った攻撃の早期警告として機能したり、アクティブな攻撃の存在を確認したできるためです。

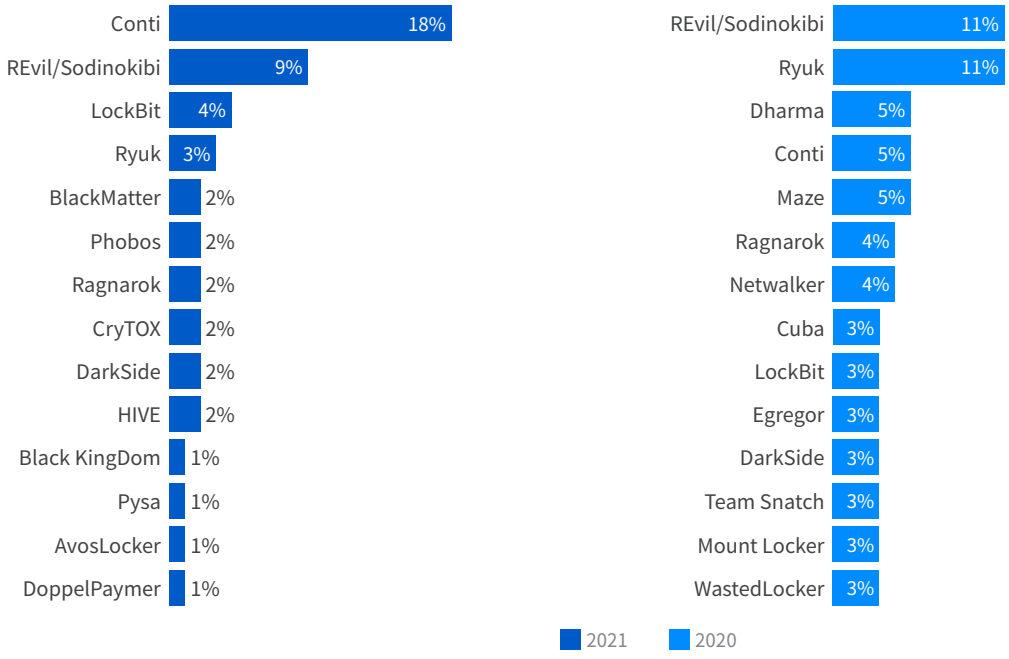
2021年の主要なランサムウェア攻撃

解析に含まれている 144件のインシデント全体で、41種類のランサムウェア攻撃が確認されました。その中で、約 3 分の 2 (28) は 2021年に初めて報告された新しいグループでした。2020年のインシデントで見られた 18 つのランサムウェアグループは、2021年にはリストから消えていました。これは、サイバー脅威の状況が非常に混雑、動的、複雑になっているか、そして防御者にとってどれほど困難になっているかを明確に示しています。

多くの点において、2021年は、ソフォスが調査したインシデントの 5分の 1 (18%) をわずかに下回る、多くの RaaS オペレーターである Conti に「属していた」ことになります。しかし、REvil ランサムウェアは、2021年 7月に明らかに運用を停止したにもかかわらず、全体の 10件中 1件を占めていることは注目すべき点です (2021年 9月に一時的に出現に、そして 2022年に再び出現)。

2021年に流行した他のランサムウェアファミリーとしては、米国のコロニアルパイプラインへの悪名高い攻撃を行った RaaS である DarkSide や、ProxyLogon の脆弱性をきっかけに 2021年 3月に登場した「新しい」ランサムウェアファミリーの 1つである Black KingDom が挙げられます。

属性: 上位のランサムウェア攻撃



2020年には約 25%、2021年には約 4分の 1 (24%) のインシデントが、他のランサムウェアグループに起因していましたが、残りのインシデントは既知のグループに起因していることに確信を持てませんでした。

ソフォスは、Conti ランサムウェアについて詳細に説明しています。Conti や、LockBit、Ryuk などその他に流行したランサムウェアファミリーに関する記事の包括的なリストは、ソフォスのランサムウェア脅威インテリジェンスセンターで確認できます。

まとめ

どの組織もどこかで攻撃者の標的になっており、ますます複数の攻撃者に狙われています。フィッシングや金融詐欺から、ボットネットビルダー、マルウェア配信プラットフォーム、クリプトマイナー、IAB、データ盗難、企業スパイ、ランサムウェアなど、ネットワークへの脆弱なエントリポイントがある場合、攻撃者はそれを探して、いずれはそれを悪用する可能性があります。

公開されたエントリポイントが閉じられ、攻撃者がアクセスを確立して保持するために行ったすべてのことを完全に削除するまでは、ほとんど誰もがアクセスすることができますし、おそらくそうすることでしょう。

セキュリティチームは、疑わしいアクティビティを監視し調査することで、組織を守ることができます。無害のアクティビティか悪意あるアクティビティかの区別は、必ずしも容易ではありません。サイバーテクノロジーであろうと物理的なテクノロジーであろうと、どのような環境でもテクノロジーは大きな力を発揮しますが、それだけでは十分ではありません。セキュリティ対策には、人間の経験とスキル、および対応能力が欠かせません。

2021年のインシデントレスポンスの大きな教訓は、攻撃者がいかに迅速かつ広範囲にわたって脆弱性を悪用し、侵入の長期化と複数の攻撃者に貢献しているかということです。これらの教訓より、防御側は、既知の攻撃者のツールセットとテクニックの危険信号を検出、調査、対応することがこれまで以上に重要であることがわかります。

Sophos Rapid Response

本レポートの調査結果は、専門のインシデント対応担当と脅威の無力化スペシャリストチームである Sophos Rapid Response が調査したインシデントのデータに基づいています。Sophos Rapid Response サービスは、ソフォスの既存のお客様とソフォス以外のお客様の両方が利用できます。

アクティブなインシデントが発生し、Rapid Response チームにお問い合わせされる場合は、次の電話番号にお気軽にお問い合わせください。

米国：+1 4087461064

オーストラリア：+61 272084454

カナダ：+1 7785897255

フランス：+33 186539880

ドイツ：+49 61171186766

英国: +44 1235635329

スウェーデン: +46 858400610

追加のデータテーブル

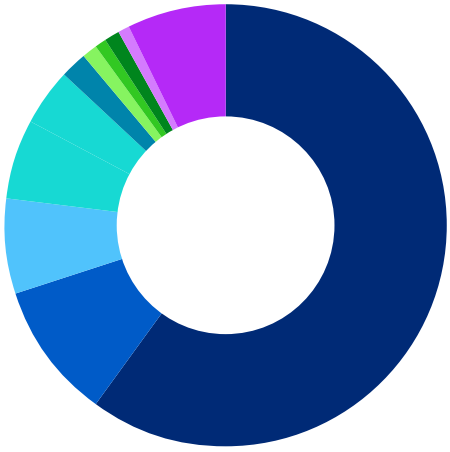
MITRE 攻撃チェーンにマッピングされたインシデント調査のアーティファクト

インシデント調査中に観察されたツール、テクニック、その他のアーティファクトは、MITRE ATT&CK フレームワークと照らし合わせてマッピングされました。詳細については、ソフォスニュースの関連記事で紹介します。

MITRE ATT&CK の段階											
初期アクセス	実行	常駐	権限昇格	防御の回避	認証情報アクセス	探索	ラテラルムーブメント	収集	コマンド&コントロール	データの盗み出し	影響
アーティファクト											
リモートサービス	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	ネットワークブラウジング	Cobalt Strike	Rclone	データ暗号化
エクスプロイト	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	ネットワーク侵害

インシデント対応統計情報 2021

国別のインシデント対応事例



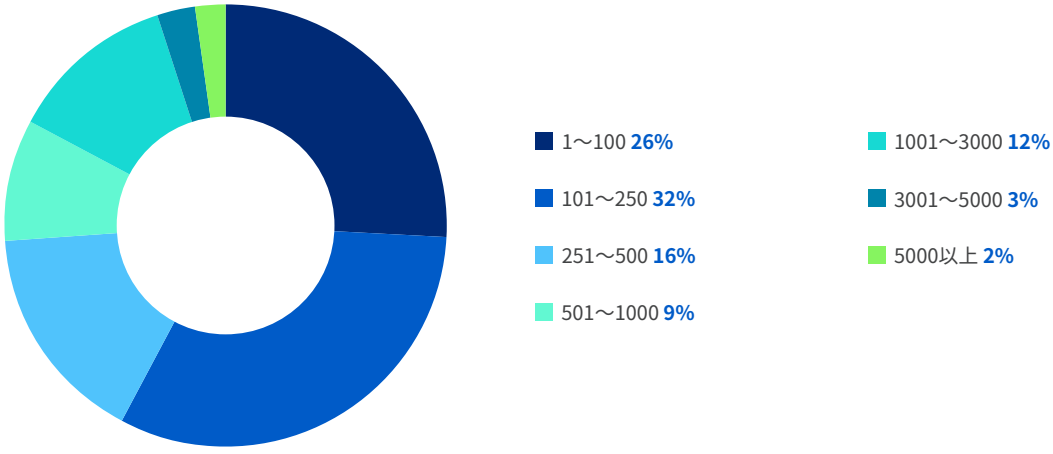
- 米国 **60%**
- ドイツ **10%**
- 英国 **7%**
- カナダ **6%**
- イタリア **4%**
- スペイン **2%**
- フランス **1%**
- スイス **1%**
- ベルギー **1%**
- フィリピン **1%**
- その他 **7%**

(オランダ、オーストリア、アラブ首長国連邦、サウジアラビア、バハマ、アンゴラ、日本)

業界別のインシデント対応事例

- 製造 **17%**
- 小売 **14%**
- 医療機関 **12%**
- IT **9%**
- 建設 **8%**
- 教育 **6%**
- 食品 **4%**
- 物流 **4%**
- 金融 **4%**
- エンターテインメント **3%**
- サービス **3 %**
- ニュースメディア **3%**
- その他 **13%** (運輸、製薬、MSP/ホスティング、非営利、政府、接客業、法務、農業、エネルギー、不動産)

組織の規模（従業員数）別のインシデント対応事例



ソフォス株式会社営業部
Email: sales@sophos.co.jp

2022-05-25 JA (DD)