SOPHOS

ソフォス「アクティブアドバーサリーレポート」2024 年上半期版

2023 年の後半は、攻撃者が攻めあぐねた事例が数多くありました。防御者はこの状況に上手く対応できているのでしょうか。

John Shier および Angela Gunn 著

はじめに

アクティブアドバーサリーーレポートは、Sophos X-Ops のインシデント対応 (IR) チームが世界各国のセキュリティインシデントに対応して得た、現在のアクティブアドバーサリーー (進行中の実際攻撃) の状況を解説しています。本記事は、IR チームの 2023 年の活動から抽出した 150 件以上の事例から得られたデータに基づいています。この分析の対象となった企業や組織の詳細については、レポートの最後のセクションを参照してください。

ソフォスのアクティブアドバーサリーレポートでは通常どおり、2020 年の IR サービス開始までさかのぼり、過去の IR 事例のデータを組み込んでいます。本レポートでは主に 2023 年に IR チームが調査した事例の分析に焦点を当てますが、有意な変化や傾向、あるいは停滞を把握するため、場合に応じて、より長期的な視点でデータを分析します。

秋の初めに公開される第 2 回の報告書には、2024 年前半のデータ、つまり現在対応中の事例と今後発生する事例が盛り込まれる予定です。永遠に続く攻撃側と防御側の戦いには、独自の周期、転換点、流れがあります。事態が静穏に見えるときでも、そのリズムを注視し続けることが、脅威を理解し対応しようとする防御側にとって重要な鍵となります。

重要ポイント

- ランサムウェアのレベルは恒常状態に達している
- タイムラインで見ると攻撃は安定している
- 攻撃に用いられるツールは停滞している
- 真の問題はゼロデイ脆弱性ではない
- それでも防御は追いついていない

分析対象のデータ

本レポートのデータは例年通り、ソフォスの社外向けインシデント対応チームが調査した事例から抽出したものであり、データセットの 88% は従業員数 1,000 人以下の組織から得られたものです。例年と同様に、ソフォスの支援を必要としている組織の 55% 以上が従業員数 250 人以下の組織です。2023 年に IR が関与した組織の 12% が従業員 1,000 人以上の企業であり、2022 年の 19% から減少しました。(ソフォスの IR チームと MDR チームの総力を結集して作成した、従業員数 500 人以下のお客様に関するデータについては、姉妹出版物である 2024 年版ソフォス脅威レポートをご覧ください。)

これらの組織はどのような業務に従事しているのでしょうか。ソフォスに IR サービスを依頼する業種は、4 年連続で製造業 (25%) が最も多く、次いで情報技術 (10%)、小売業 (9%)、サービス業 (9%) となっています。このデータセットには、合計で 26 種の業種が含まれています。本レポートの事例選定に使用したデータと方法に関する詳細は、付録を参照してください。

分析結果の概要

もはや業界全体のインシデント対応レポートにおける恒例となっていますが、攻撃の種類ではランサムウェアが 2023 年もトップであり、調査の 70% がランサムウェアによるものでした。四半期ベースでは 62% から 80% まで多少の変動はあるものの、年間平均では実際のランサムウェア発生率の範囲内に収まっていると考えられます。

攻撃の種類

2023 年に対応した攻撃の種類	件数	%
ランサムウェア	108	70.13%
ネットワーク侵害	29	18.83%
データ恐喝	11	7.14%
データ窃取	2	1.30%
ビジネスメール詐欺 (BEC)*	1	0.65%
Web シェル	1	0.65%
ローダー	1	0.65%
DDoS	1	0.65%
合計	154	100.00%

図 1: 例年と同様、2023 年もインシデント対応チームはランサムウェアに関する調査を他のどの種類の攻撃よりも多く実施しました。ただし、ソフォスのビジネスメール詐欺の定義に合致する対応事例が今回用いたデータセット外に多数存在することがデータから判明しています。完全な調査に至った対応事例は 1 件のみであったため、データセットにはほとんど含まれていませんが、本レポートの作成者が後日、これらの事例に関する調査結果を公表する可能性があります。

ネットワーク侵害は、2023 年には 19% の割合で発生し、前年に引き続き 2 位となりました。すべての事例で共通しているわけではありませんが、多くのネットワーク侵害が実際には失敗に終わったランサムウェア攻撃であることを示す証拠が出てきています。たとえば、5 件のネットワーク侵害 (17%) は、既知のランサムウェアブランドによるネットワーク侵害であることが確認されています。ネットワーク侵害とランサムウェア攻撃を四半期ごとに比較したところ、興味深い数字が浮かび上がりました。ランサムウェアの流行が最も収まっていた四半期 (67% の第 2 四半期および 62% の第 3 四半期) において、ネットワーク侵害は年間平均を大幅に上回っており、第 2 四半期は 21%、第 3 四半期は 28% でした。

ランサムウェアとネットワーク侵害の月別発生件数 (2021 ～ 2023 年)

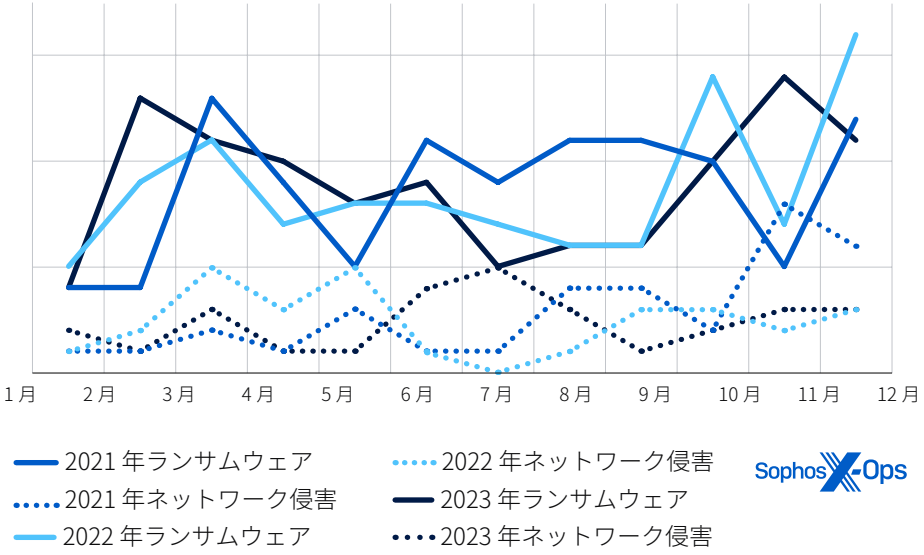

図 2：2021 年から 2022 年にかけて、ランサムウェアの件数とネットワーク侵入の件数には、ランサムウェアが増加しているときは侵入も増加するという緩やかな対応関係があるように見えます。しかし、2023 年半ばには、ネットワーク侵入が急増したのと同時にランサムウェアが減少しました。2021 年 11 月における「大逆転」ほどではありませんが、重要な出来事だと考えられます。

このデータから何が推測できるでしょうか。あまり定かではありませんが、この 2 つの四半期の被害者たちは、ランサムウェアのオペレーターを検知し、実被害が出る前に環境から排除する準備を整えていた可能性があります。 あるいは、攻撃者が一年で最も過ごしやすい時期のソチでのんびり過ごしていたのかもしれません。

ソフォスのデータセットで最も変化が見られた攻撃の種類は、データ恐喝とデータ窃取です。データ恐喝とは、データを窃取し、そのデータの公開の抑止や削除と引き換えに支払いを要求するものと定義します。データ窃取は、身代金の支払いを考慮しないもので、外部に公開されたか、されなかったかにかかわらず、データが盗み出された場合を指します。年末の集計では、データ恐喝攻撃は前年比で倍増した一方、データ窃取攻撃は半減しました。ソフォスが調査したデータ恐喝攻撃の大半は、2023 年 1 月に恐喝に焦点を当てて攻撃戦略を切り替えた BianLian によって、今年の前半に実行されたものです。

2023 年に確認された残りの攻撃の種類は、ビジネスメール詐欺、Web シェル、ローダー、DDoS です。いずれも調査対象事例の 1% 未満でした。

攻撃の影響

2023 年に確認された攻撃の影響	ATT&CK	件数	全事例に占める割合
影響を与えるためのデータ暗号化	T1486	106	68.83%
(影響なし)	該当なし	29	18.83%
システム回復の阻害	T1490	29	18.83%
金融資産の窃取	T1657	12	7.79%
リソースの乗っ取り	T1496	6	3.90%
アカウントへのアクセス権の削除	T1531	2	1.30%
データの破棄	T1485	1	0.65%
ネットワークサービス拒否 (DoS)	T1498	1	0.65%
合計		186	

図 3：2023 年に調査した事例の既知の影響。1 件の事例が最終的に複数の影響をもたらす可能性があるため、合計が全事例数の 154 件を上回っています。

攻撃の結果は、MITRE ATT&CK フレームワークでは「影響 (TA0040)」に属する戦術 (カテゴリ) です。影響を与えるためのデータ暗号化 (T1486) が群を抜いて多いのは驚くことではありません。ランサムウェアが攻撃の種類として最も多いのであれば当然、この戦術が最大の影響になるでしょう。暗号化の補助として、多くの攻撃者は他のタスクを実行したり、他のカテゴリに分類される追加のペイロードを展開したりします。たとえば、システム回復の阻害 (T1490) と影響を与えるためのデータ暗号化が組み合わされているのがしばしば確認されます。

次に多かった影響は、「影響なし」でした。この事実はネットワーク侵害と密接に結び付いています。攻撃者がネットワークに特権アクセスを持っていれば、何らかの影響を与えられることは明らかです。しかし、MITRE のテクニックは広範囲に及びますが、この現象を適切に説明する個別のテクニックはありません。

注目すべきは、MITRE が 2023 年 10 月にフレームワークのアップデートを発表したことです。変更点の 1 つとして、「影響」に属するテクニックとして金融資産の窃取 (T1657) を追加したことが挙げられます。この変更の理由については、「ネットワークそのものには関係しないものの、直接ネットワークのインタラクションやネットワークへの影響に関連する活動をより多く包含するため」と述べられています。従来はラベルが存在しなかったデータ恐喝やデータ窃取攻撃の結果を適切にラベル付けできるようになるため、歓迎すべき変更です。

次にランクインしたのは、「金融資産の窃取」です。この種のデータ恐喝が増加したことで、関係するテクニックも相応に増加し、2023 年のランキングではリソースの乗っ取りを上回った一方で、リソースの乗っ取りが確認された件数は 2022 年と比べて 3 分の 1 にまで減少しています。このテクニックは、SquirrelWaffle への感染事例の多くで見られるように、攻撃者が侵害されたシステムをスパム攻撃に利用した結果でもあります。しかし、ほとんどの場合はネットワーク上にコインマイナーが存在することを意味します。(コインマイナーが減少している理由は、マイニングはそれほど儲かるものではないという事実以外には不明です。)

教育業界の組織に対するネットワークサービス拒否 (DoS) 攻撃 1 件を除き、データセットに含まれる残りのテクニックは、ランサムウェア攻撃に関連する二次的な影響でした。

攻撃の帰属 (アトリビューション)

2023 年に確認された攻撃の帰属	件数	%
LockBit	24	22.22%
Akira	12	11.11%
ALPHV/BlackCat	10	9.26%
Play	7	6.48%
Royal **	6	5.56%
Black Basta	5	4.63%
CryTOX	4	3.70%
BlackByte	3	2.78%
Team Snatch	3	2.78%
Mario	3	2.78%
Rorschach	2	1.85%
Faust	2	1.85%
(不明)	2	1.85%
BitLocker*	2	1.85%
Vice Society	2	1.85%
Phobos	2	1.85%
BlackSuit **	2	1.85%
Rhysida	2	1.85%
Prometheus	1	0.93%
Hunters Intl	1	0.93%
INC	1	0.93%
Cyclops	1	0.93%
Cuba	1	0.93%
8Base	1	0.93%
Money Message	1	0.93%
HIVE	1	0.93%
RA Group	1	0.93%
Mimus	1	0.93%
FuxSocy	1	0.93%
d0nut	1	0.93%
NoEscape	1	0.93%
Qilin	1	0.93%
RansomEXX	1	0.93%
合計	108	100.00%

図 4：2023 年に確認されたランサムウェア事例のファミリごとの分布。アスタリスクが付いた項目では、攻撃者は Windows BitLocker サービスをインストールし、ファイルの暗号化とボリュームシャドウコピーの削除の両方を行いました。また、2 つのアスタリスクが付いた項目については、同一のものである可能性があります。以下で詳述します。

脅威環境の分析には、ほとんどの場合攻撃の帰属に関する議論が必要です。誰がこれらの攻撃を実行したかを長々と論じるつもりはありませんが、ソフォスが見たままの事実を提示することはできます。当然ながら、最も信頼できるのはランサムウェア攻撃から直接取得した帰属情報です。というのも、攻撃者は、ファイル拡張子 (多くの場合)、ランサムノート (常に)、データ漏洩ポータルサイト (時々) を通じて、どのランサムウェアブランドがネットワーク上に展開されたかを教えてくれるからです。多くのテレマーケティング業者と同様に、ほとんどのランサムウェアブランドはサービスとしてのランサムウェア (RaaS) として存在するため、攻撃者は複数のブランドを活用できます。

LockBit は、2 年連続でその年最も多く使われたランサムウェアブランドの首位を維持し、ついに Conti を抜いて歴代ランキングのトップに躍り出ました。2023 年に調査したランサムウェア攻撃の 5 分の 1 以上が LockBit を使用していました。

Sophos X-Ops が対応したインシデントで検出されたランサムウェアの割合 (2020 ～ 2023 年別)

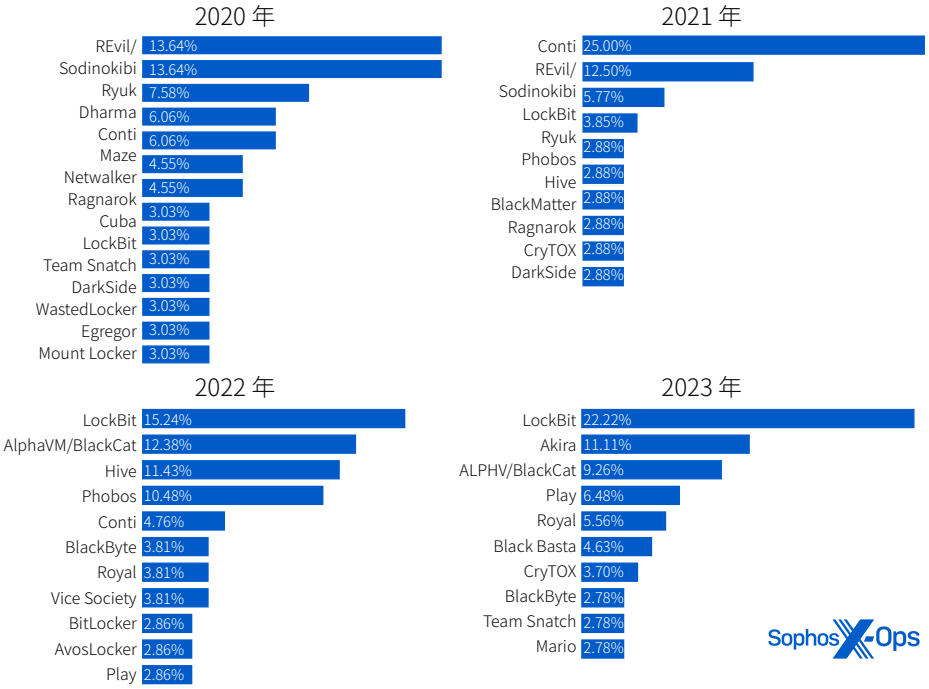

図 5：LockBit は、2021 年の Conti 全盛期以来、どのランサムウェアファミリよりも 2023 年のランキングを支配しています。当時も今も、2 位のランサムウェアファミリは 1 位の半分以下に過ぎません。

ランサムウェア環境に現れた新顔のうち、注目すべきは Akira です。2023 年 3 月に登場したこの新しいランサムウェアブランドは、ALPHV/BlackCat、Royal (2023 年に BlackSuit としてリブランディングされたと考えられる)、Black Basta といった他の注目すべきブランドを押しのけて、2 位にランクインしました。(Royal と BlackSuit を同一のものとして扱った場合、4 位にランクインします。) しかし、この躍進は必ずしもランサムウェアが完全であることを意味するわけではありません。ソフォスがネットワーク侵害として調査した事例の 1 つは、ALPHV、Black Basta、Everest、Vice Society の事例と同様に、失敗した Akira 攻撃であることが判明しました。これらの攻撃が成功していれば、ランサムウェアのシェアは 73% に増加し、それに比例してネットワーク侵害の割合も低下していたことでしょう。

上位 5 件のランサムウェアブランドは、全ランサムウェア攻撃の半分以上 (55%) を占めていますが、これらのブランドの出自を考慮すれば驚くには値しません。Akira と Royal はどちらも、Conti ランサムウェアグループとその多くの亜種を生んだ Ryuk ランサムウェアファミリに関連付けられています。上位 10 件まで広げてみると、Conti から派生したとされる Black Basta (6 位) と BlackByte (8 位) の 2 件が見つかります。データ恐喝グループのうち、Karakurt がこの悪名高いランサムウェアファミリとつながりがある可能性も明らかになりました。LockBit もある意味では関係しています。というのも、このグループは 2022 年の Conti のリーク後、コードの一部を使用していることが確認されているからです。

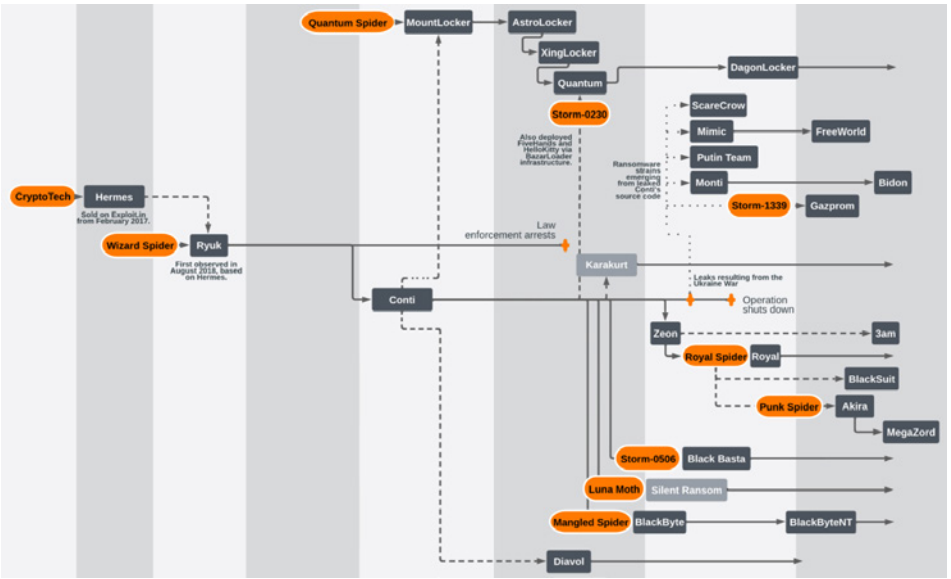

図 6：毒の木の果実：今日のランサムウェアファミリの大半は、2016 年の CryptoTech をはじめとするいくつかの「始祖」に関係しています。Royal が BlackSuit に名称を変更したことに起因する曖昧さは、右下に反映されています。出典：World Watch - Global CERT - Orange Cyberdefense(上図は一部です)

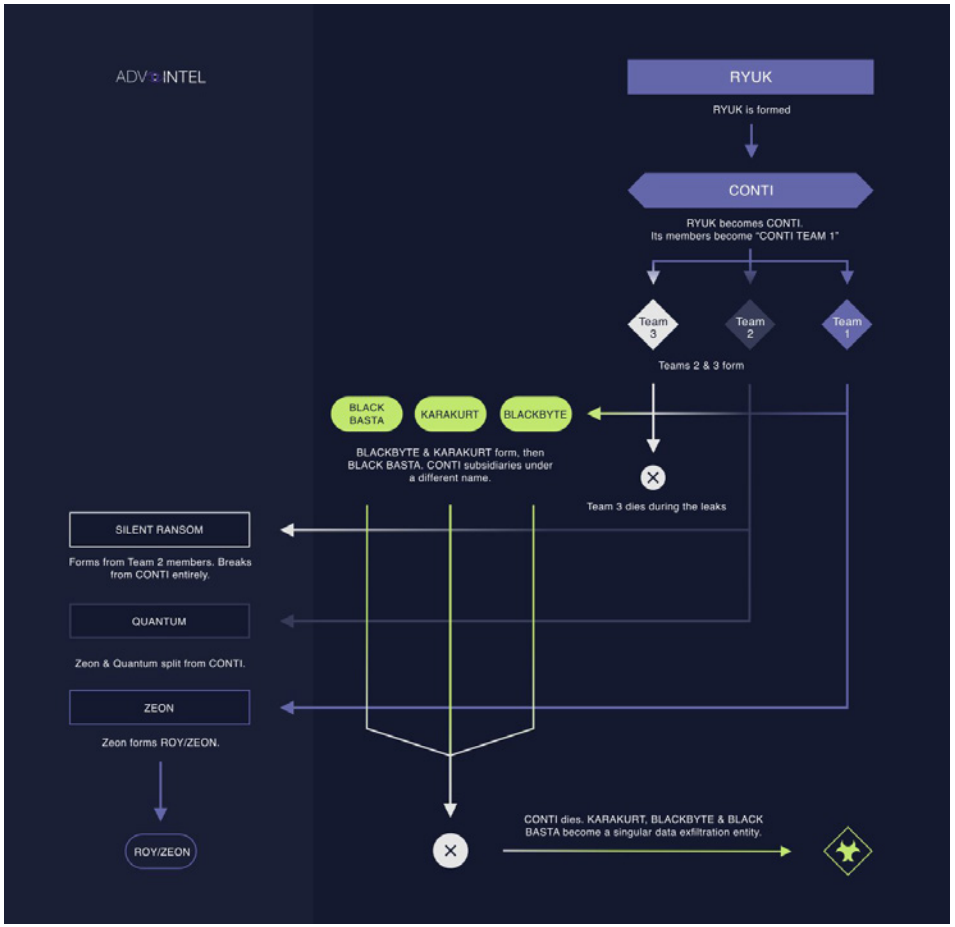

図 7：(やや近親交配的な) Conti ファミリの詳細 (2022 年～)
出典：https://twitter.com/VK_Intel/status/1557003350541242369/photo/1

これらのグループは特異的な発達を遂げたのではないかと考えたくなりますが、そうではありません。今日のランサムウェアは、2023 年 9 月中旬に 10 年目を迎えました。実際には、これらのグループに属する個人の多くは、長期にわたって活動しており、十分な時間と機会を活用してスキルを磨いてきました。さまざまな理由から、ランサムウェアグループは誕生と消滅を繰り返しています。しかし、Cuba、LockBit、Phobos、Snatch といった、最初のアクティブアドバーサリーレポート以来調査され続けているグループもいくつか観測されています。

2023 年の攻撃の帰属 (データ恐喝の事例)	件数	全事例に占める割合
BianLian	8	72.73%
Cl0p	1	9.09%
Hunters Intl	1	9.09%
Karakurt	1	9.09%
合計	11	100.00%

図 8: ソフォスが確認したデータ恐喝事件の大半を BianLian が占めていました。Cl0p は多くの記事の見出しを飾りましたが、ソフォスの IR のお客様に対する実際の影響はごく僅かでした。

データ恐喝グループとしては BianLian がトップであり、Cl0p、Hunters International、Karakurt が続きました。Hunters International による攻撃はランサムウェア攻撃としては失敗しましたが、データの窃取には成功したため、盗んだデータの公開と引き換えに支払いを要求するデータ恐喝に方針を転換しました。

脅威を与え続ける攻撃者

攻撃者の正体を知ることは、気休めにはなるかもしれませんが、それ以上の意味はありません。ただし、例外が 1 つあります。身代金を支払うつもりなのであれば、相手のランサムウェアグループが政府から制裁対象団体に指定されている場合には事前に法律顧問に相談することが絶対に必要です。

いずれにせよ、ランサムウェア攻撃の多くは、ランサムノートに書かれたブランド名にかかわらず、同じ個人またはグループによって実行され、ほとんど同じツールとインフラストラクチャを使用しています。インシデント対応において最も重要なのは、攻撃者がどのように組織に侵入し、なぜ成功したのかということです。この情報を得ることにより、完全な修復と復旧が可能になります。

初期アクセスと根本原因

2023 年の初期アクセス	ATT&CK	2023 年の件数	2023 年の事例に占める割合	全事例に占める割合
外部リモートサービス	T1133	100	64.94%	45.95%
有効なアカウント	T1078	78	50.65%	25.24%
外部向けアプリケーションの悪用	T1190	26	16.88%	25.05%
(不明)	該当なし	15	9.74%	7.34%
フィッシング	T1566	6	3.90%	5.46%
サプライチェーンへの侵入	T1195	4	2.60%	0.75%
信頼関係の悪用	T1199	3	1.95%	1.88%
ドライブバイ攻撃	T1189	2	1.30%	0.75%
合計		234		

図 9：調査の過程で判明した初期アクセスのテクニックは、2023 年には少し種類が増えました。いくつかの事例では、有効な初期アクセスシナリオが複数明らかになりました。最も特徴的だったのは、有効なアカウントが用いられた 78 件の事例のうち、主な手法だったのは 1 件のみであり、残りの 77 件はリモートサービスを主な手法とする事例の一因だったことです。

2023 年の根本原因	2023 年の件数	2023 年の事例に占める割合	全事例に占める割合
認証情報の侵害	86	55.84%	33.33%
脆弱性の悪用	25	16.23%	29.76%
(不明)	20	13.64%	18.27%
ブルートフォース攻撃	6	3.90%	3.01%
フィッシング	5	3.25%	5.65%
サプライチェーンへの侵入	4	2.60%	1.13%
悪意のあるドキュメント	4	2.60%	3.20%
アドウェア	2	1.30%	0.56%
認証トークンの窃取	1	0.65%	0.19%
合計	154	100.00%	

図 10：根本原因については、2023 年に初めて「認証情報の侵害」が通年ランキングのトップに踊り出ました。

攻撃者がどのように標的組織に侵入したかを説明する MITRE の戦術および関連テクニックは「初期アクセス (TA0001)」に分類され、正式な ATT&CK の指定がない Root Causes (根本原因) は、なぜそのテクニックが機能したかを説明しています。たとえば、攻撃者が VPN などの外部リモートサービスを介してネットワークに侵入した場合、「外部リモートサービス」が侵入方法となります。しかし、根本原因、つまりその手法が機能した理由は、おそらく侵害した (窃取した) 認証情報 (MITRE ATT&CK の用語では「有効なアカウント」) が用いられたからだと考えられます。上記のような例では、「外部リモートサービス」および「有効なアカウント」の両方が初期アクセスを提供したとし、根本原因は「認証情報の侵害」とします。初期アクセスと根本原因はしばしば同一視されますが、ソフォスでは、攻撃がどのように成功したかをより詳しく理解し、復旧と防御に役立てるため、この 2 つを分離して考えます。

これまでのアクティブアドバーサリーレポートと同様、「外部リモートサービス (T1133)」が初期アクセス手法のトップでした。65% の事例で、何らかのリモートアクセス技術が侵入に用いられました。VPN デバイスであれ、公開されたリモートデスクトッププロトコル (RDP) サービスであれ、攻撃者にとっては格好の機会です。攻撃者に残された課題は、この機会をどのように利用するかを考えることだけです。

考えられる方法の 1 つは、有効なアカウント (T1078) の使用です。認証情報の侵害は、4 分の 3 以上 (77%) の攻撃で初期アクセスの主な手法であり、半数以上 (56%) の攻撃の根本原因でした。ほとんどの場合、アカウントがどのように侵害されたかはわかりませんが、攻撃者が有効なユーザー名とパスワードを用いて「正面突破」したことはわかっています。

2023 年の大半の事例で、初期アクセスには認証情報の侵害が関連していました。前回のレポートでは、2023 年上半期に認証情報の侵害が根本原因のランキングでトップに急浮上したことを指摘しました。2023 年のデータセットが全て揃った現在でもこの傾向は続いれており、昨年の合計のほぼ 2 倍になっていることがわかります。

主な根本原因、2021 年～ 2023 年および全期間

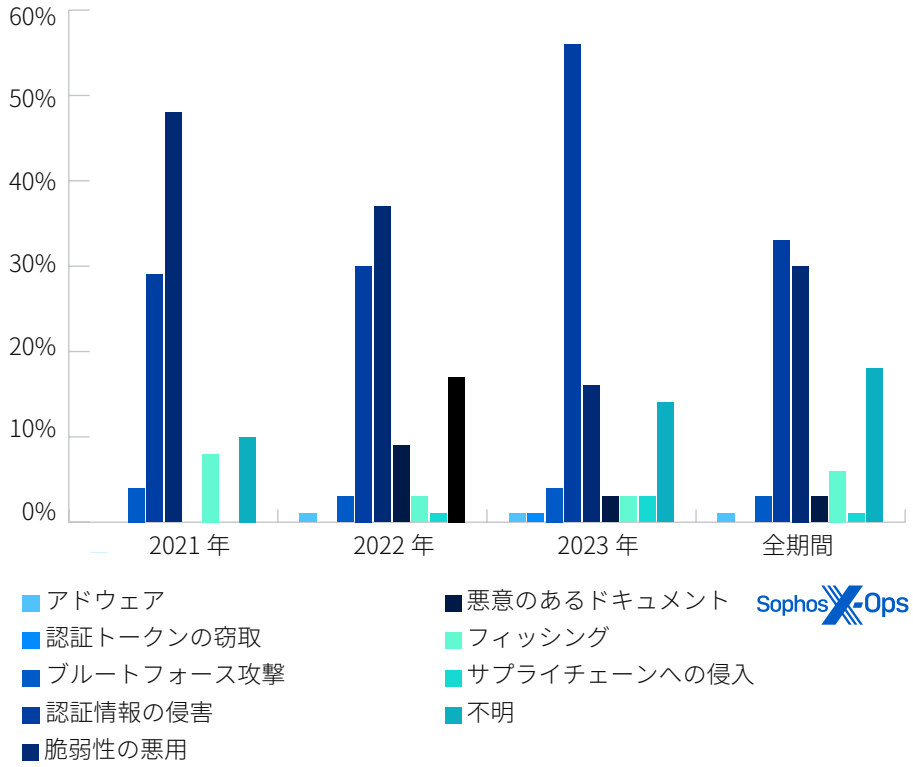

図 11：「認証情報の侵害」は攻撃の根本原因として爆発的に増加しました。(大半は回避可能な) この問題は、2023 年のランキングのみならず歴代ランキングのトップです。

この状況をさらに悪化させているのは、認証情報保護強化の悲惨な現状です。調査された事例の 43% で、多要素認証　(MFA) が設定されていませんでした。(念のため言及しておきますと、MFA は現時点で 30 年近く前のテクノロジーです。公開当時の特許の 1 つには、双方向ポケットベルを含む実装例が示されています。)

リモートサービスに関連する攻撃におけるその他の根本原因はブルートフォース攻撃 (6%)、不明 (3%)、フィッシング (3%)、エクスプロイト (2%) でした。

認証情報の侵害が台頭していることを考えると、従来型の脆弱性の悪用は 2 位に後退したことになります。前述の通り、この事実は攻撃者が脆弱性を利用しなくなったことの確固たる証拠ではありません。もしかすると、以前ほど悪用しやすい脆弱性がなかったのかもしれません。あるいは、初期アクセスブローカー (IAB) が、安く処分したい在庫をたくさん抱えていたのかもしれません。いずれにせよ、攻撃者は最も手を出しやすい手段を選ぶものであり、2023 年においては、その手段が侵害された認証情報の使用だったということです。

上位「3 件」の他に (カテゴリとしての「不明」が、そのカテゴリの主要因が判明している場合でも、調査者にとってどれだけ有用であるかは議論の余地があるため、) 特定された根本原因 (ブルートフォース攻撃、フィッシング、サプライチェーンの侵害、悪意のあるドキュメント、アドウェア、認証トークンの窃取) は、全調査結果のうち 14% を占めました。「不明」カテゴリは、初期アクセスおよび根本原因の両方で 3 番目に多い「理由」であり、どちらの場合でも最大の要因はテレメトリの欠落でした。攻撃者によってログが消去されたのか、あるいはそもそもログへの記録が設定されていなかったのか、ソフォスの調査担当者は攻撃の主要素を特定できませんでした。率直に言って、2023 年は認証情報の侵害と脆弱性の悪用の年でした。

データで見る傾向

本記事執筆時点では、脅威環境は比較的落ち着いています。そこで、アクティブアドバーサリーチームが何度も述べているように、「私たちがいかにして新しい知見を得ているのか」について少し考えてみましょう。本レポートで提供するすべてのデータから最大限の知見を得るために、統計データについて、またそのデータが何を示し、何を隠しているのかについてお話ししましょう。まず、2023 年を通じて取り上げた、滞留時間の顕著な減少を検証し、この数字をもう 1 度確認することで他に何がわかるかを検討します。次に、昨年から監視を開始した Active Directory への到達時間を確認し、その分析がどのように攻撃の変化を捉えるのに役立つかを見ていきます。その後、重要なデータが不足しているために研究が停滞しているトピックを検証します。最後に、昨年半ばにデータセットから予期せず除外され、今なお私たちに疑問を投げかけている統計データについて紹介します。

統計データ #1：攻撃のタイムライン

2021 年に (2020 年のデータに基づいて) 最初のアクティブアドバーサリーレポートを発表した際、滞留時間は多くの人々の関心を呼んだ指標の 1 つでした。当時、滞留時間は週や月単位で考えるのが慣例でしたが、特にインシデント対応事例では滞留時間の中央値は日単位で測定可能であることを示しました。2 番目のレポート (2021 年のデータに基づく) では、滞留時間の増加が見られました。この増加は初期アクセスブローカー (IAB) の出現によるものです。初期アクセスブローカーは、最も初期の侵害と最終的な攻撃の間に空白の時間を生み出します。

「攻撃の検出」について

「攻撃の検出」の定義についての簡単な説明：ランサムウェアの事例では、単にランサムウェアのバイナリが配信された時間を指します。それ以外の事例では、配信、実行、警告の発出、被害者による声明の時間が混在しています。

その後、滞留時間は減少傾向に転じました。2022 年にはわずかに、2023 年には大幅に減少しました。2023 年の第 1 四半期レポート (2022 年末までのデータを含む) では例年通りで、滞留時間は前年同時期と同等の長さでした。2023 年の最終レポート (第 1 四半期から第 3 四半期までのデータを含む) を発表する頃には、滞在時間は半減していました。2023 年末には、状況は安定していました。毎度のことですが、詳細を理解することが重要です。

2023 年のインシデント滞留時間 (四半期ごと)

2023 年	最小	最大	平均値	標準偏差	中央値
第 1 四半期	0	112	18.69	24.06	10.00
第 2 四半期	0	73	12.37	15.66	7.00
第 3 四半期	0	114	16.86	31.18	5.00
第 4 四半期	0	289	23.76	49.33	8.00
通年	0	289	18.18	33.08	6.00

図 12：滞在時間は 2023 年を通じて少し増減しましたが、それでも前年の中央値である 10 日を明らかに下回っています。

滞留時間 (および他の多くの指標) を中央値で比較することにした理由のひとつは、外れ値の影響を減らすためです。たとえば、2022 年に正味で 955 日の滞留時間を記録した事例がありました。この事例をデータセットから除いたものとオリジナルを比較すると、平均値は 6 日強減少しますが、中央値は影響を受けません。

大きな影響を与える外れ値
2022 年の外れ値が滞留時間の統計に与える影響

	最小	最大	平均値	標準偏差	中央値
外れ値あり	0	955	36.99	95.32	10.00
外れ値なし	0	345	30.78	58.11	10.00

図 13：データセットに異常な値 (外れ値) が 1 つあるだけで、数値に大きな歪みが生じます。そのため、本記事では中央値を比較しています。

通常はあまり注目しないものの、ソフォスが注目しているもう一つの値は、データセットの標準偏差です。簡単に言うと、標準偏差はデータの平均からの広がりやばらつきを測るものです。図 13 のデータセットを例にとると、外れ値を除外した場合、滞在時間の標準偏差も 95.32 日から 58.11 日へと劇的に低下します。言い換えると、データを構成する一連の値が平均値に近づいています。

外れ値の問題点は、データの傾向が不明瞭になることです。このことを念頭に置いて、過去 3 年間の滞留時間データを、上図のように 2022 年の外れ値を管理しながら調べてみました。

2021 ～ 2023 年の攻撃者の滞留時間 (2022 年の外れ値を除外)					
滞留時間	最小	最大	平均値	標準偏差	中央値
2021 年 (回答者数 = 144)	0	411	41.69	59.65	13.00
2022 年 (回答者数 = 148)	0	345	30.78	58.11	10.00
2023 年 (回答者数 = 147)	0	289	18.16	33.08	6.00

図 14：2022 年のデータから外れ値の影響を取り除くと、滞留時間が年々減少しているという傾向が明らかになります。

以前のレポートで、滞留時間の減少は検出能力の向上などの要因による可能性が高く、攻撃者はこれらの要因に対応して攻撃を高速化している可能性が高いと指摘しました。

滞留時間の中央値が減少していることに加え、図 14 で見られるように、同等の規模の集団であるにもかかわらず、他の値が減少していることも確認されました。ランサムウェアを他の全攻撃の種類から分離すると、さらに興味深いことがわかります。

2021 ～ 2023 年のランサムウェア攻撃の滞留時間					
	最小	最大	平均値	標準偏差	中央値
2021 年	0	190	29.88	42.29	11.00
2022	0	292	23.80	45.42	9.00
2023	0	146	15.92	25.53	5.00

2021 ～ 2023 年の非ランサムウェアの滞留時間					
	最小	最大	平均値	標準偏差	中央値
2021 年	1	411	72.38	83.58	52.50
2022	0	345	45.79	77.25	10.00
2023	0	289	23.22	45.79	10.00

図 15：データから 2022 年の外れ値を除外した場合、滞留時間の減少傾向はランサムウェア攻撃のみならず、(程度は小さいものの) 他のすべての攻撃の両方に当てはまることがわかります。

ランサムウェア攻撃者がネットワーク内部に滞留する時間が他の種類の攻撃者よりも短いことは、直感的に理解できます。現在、ランサムウェア攻撃者の一部は、個々の支払い要求にあまり依存せず、多くの攻撃を行うことに重点を置いているようです。(この戦略は成功しているようです。Chainalysis 社が今年初めに発表した統計によると、2023 年の支払額は 10 億ドルを超える可能性が高いとのことです。) 攻撃そのものは、特にペイロードがネットワークに持ち込まれる時に多くの活動が行われる傾向があります。対照的に、Web シェルの埋め込みとコインマイナーにはもとよりステルス性と持続性が備わっています。

滞留時間を測定し、その意図についてコメントするのは、本レポート開始以来の恒例行事です。したがって本レポートにも記載しましたが、脅威環境や攻撃者の行動の多くの側面と同様に、滞留時間も停滞期に達していると見られています。これらの滞留時間が短期間で劇的に変化するとはあまり考えられません。ランサムウェアの流行のように、年によって多少の変動はあるかもしれませんが、全体的な傾向は安定しており、当然ながらゼロになることもないでしょう。

滞留時間はラグのある指標です。これは、侵入者が発見された後にしか算出できないためです。滞留時間を短縮させる 1 つの方法は、侵入をより早く検知することですが、ネットワーク内の不審な活動を検知するために防御者が利用できる時間ベースの指標は他にも存在します。もちろん、その指標を監視していれば、の話ですが。

統計データ #2：Active Directory への到達時間攻撃のステージは Active Directory へ

攻撃のタイムラインをより理解するため、ソフォスは 2023 年に AD (Active Directory) への到達時間という指標の収集を開始しました。その結果、すべての攻撃における AD インフラへのアクセスまでの時間の中央値が 2023 年には 0.64 日間だったことを確認しました。最も短い AD 到達時間は –28.90 日、最も長い AD 到達時間は 281.45 日でした。これらの値は、AD サーバーにアクセスしてから攻撃が検知されるまでの時間とは対照的です。攻撃が検知されるまでの時間の中央値は 2.02 日でした。

入手可能な場合には、攻撃を受けた AD サーバーの OS のバージョンも記録しました。Microsoft はその後のリリースで AD のベースラインセキュリティを着実に改善しているため、このデータは重要な意味を持つ可能性があります。AD サーバーの 90% が、2024 年 1 月にメインストリーム サポートが終了した Windows Server 2019 またはそれ以前のバージョンを実行していることがわかりました。(事例のデータセットの中には、Windows Server 2008 を実行していたサーバーも 3 台確認されました。) さらに、攻撃を受けた AD サーバーの 79% は Windows Defender のみで保護されており、少なくとも 2 台のサーバーは全く保護されていませんでした。

小さなデータセットでは重要に思えたことが、大きなデータセットを調べた結果覆されることがあります。ソフォスは念の為、2022 年に調査された 152 件の AD 到達時間データも収集しました。その結果、全体像を把握し、値を比較できるようになりました。滞留時間と同様、2022 年の AD までの到達時間の中央値は 1.34 日で、2023 年の中央値の 2 倍以上でした。最も短かったのは -208.29 日 (またもや負の値です。この事例では、顧客はネットワーク侵害に関連する他のアーティファクトよりもずっと以前に AD の侵害を受けていました) であり、最も長かったのは 140.64 日でした。2022 年には、AD サーバーの 98% が Windows Server 2019 またはそれ以前の OS で稼働しており、69% が Windows Defender で保護されていました。

AD はタイムトラベルが可能？

負の攻撃時間は攻撃の発生以前を意味するものではありません。調査者が攻撃のタイムラインを定義する際には、入手可能な証拠を用いて攻撃の開始時期を特定しようとします。事例によっては、定義された攻撃開始時刻より前にセキュリティ侵害の痕跡 (IoC) が存在する場合があります。この現象は通常、初期アクセスブローカー (IAB) の活動を示しています。

攻撃者が Active Directory サーバーを積極的に狙っていることを知った上で、私たちはいち早く攻撃者を検知する準備をしなければなりません。その準備の一環として、不審な活動を検知するための適切なソリューション、不審なシグナルを調査するための人材、そして何が起こったのかを特定するために必要なテレメトリなどを用いることができます。

大事な統計データを検討した後は、別の項目に視点を移しましょう。

統計データ #3：データの窃取

データの窃取は、侵入者を検知するもう一つの機会です。実際にデータ窃取やデータ恐喝に直面する頃には、すでに手遅れです。しかし、ランサムウェア攻撃を発見した場合は、侵入者を検知し、最終的な攻撃活動に移る前にネットワークから排除するチャンスが残されています。

データ窃取の全事例において各要因の占める割合は、2023 年も 2022 年とほぼ同じでした。2023 年には、40% の事例でデータの窃取が確認され、さらに 14% の事例で窃取の可能性またはデータのステージング (窃取を試みる過程で行われると考えられる活動) が示唆されています。2022 年には、43% でデータ窃取が確認され、さらに 9% がデータ窃取の可能性があると判断されました。

ログの欠落が調査に支障をきたすもう一つの領域は、データの窃取が発生したかどうかの判断です。42% の事例で、インシデント対応者はデータ窃取が発生したかどうかを入手可能な証拠からは判断できませんでした。この主な要因は、インシデント対応者がデータ窃取の発生を肯定または否定できる証拠がなかったためです。さらに細分化すると、十分な証拠がなかった 55 件の事例のうち、29 件 (53%) でログが欠落しており、さらに 6 件 (11%) は攻撃者によってログが消去されていました。

ランサムウェア攻撃については、44% の事例でデータ窃取を確認でき、さらに 18% の事例でデータ窃取またはデータステージングの可能性が示唆されました。残念ながら、30% の事例ではデータが盗まれたかどうかを判断できませんでした。判断ができなかった事例のうち、69% はログの欠落が原因でした。そのうち 56% はそもそもログが記録されておらず、13% はログが消去されていました。

驚くべきことに、調査されたネットワーク侵害の 72% で、データ窃取の証拠が見つかりませんでした。その半数以上は、ログの欠落 (43%) または消去 (14%) によるものでした。

AD への到達時間とデータの窃取には負の相関関係があります。攻撃者が急いで AD にアクセスする事例では、ランサムウェア攻撃のデータ窃取コンポーネントは攻撃の最終段階で出現するようです。たとえば、2023 年のデータでは、攻撃の開始から、侵害が実行されてランサムウェアのペイロードが展開されるまでの時間の中央値は 3.76 日でした。一方、データ窃取からランサムウェア展開までの時間は 0.6 日でした。

AD への到達時間と同様に、この指標は組織がデータ窃取イベントを検知し、対応するために必要な要素を備えている場合にのみ有用です。データの窃取が攻撃者の最終目標である場合、組織は迅速にデータが公開されていることを判断し、規制当局やその他の利害関係者に通知するプロセスを開始できます。各国政府がデータ窃取に関する規則や規制を強化しているため、被害組織はそれぞれに対応する必要があります。データの窃取がランサムウェア攻撃の前兆である場合、データ窃取の検出は、業務上の不幸な出来事で済むか、大々的に報じられる最悪の出来事になるかの分かれ道になり得ます。

統計データ #4：ランサムウェアが展開される時刻

2023 年の中間レポートで行われたデータ分析で最も驚くべき結果の 1 つは、ランサムウェアが展開された時間帯に強い傾向が見られたことです。このレポートのデータセットには、2023 年上半期のすべての事例が含まれています。分析によると、ランサムウェアのペイロードの 91% が一般的な業務時間ではない時間に展開されていました。AD までの到達時間の調査と同様、ソフォスはより大きなデータセットによっても同様の結果が得られるかどうかを確認するために、通年のデータを待ち望んでいました。上述の通り、より大きなデータセットはしばしばデータの偏りを明らかにし、確実な情報を提供するからです。データの集計を待つ間、既存のデータを再調査し、一般的な業務時間が月曜日から金曜日でない国のデータを補正しました。(当初の分析では、「業務時間」を月曜日から金曜日までの 5 日間、午前 8 時から午後 6 時までの標準的な営業日とし、「週末」を金曜日の午後 6 時から月曜日の深夜 0 時までの期間としていました。)

データセットのサイズを 2 倍にすることで若干の補正が加えられたものの、2023 年にはランサムウェアの 90% が業務時間外に展開されていることがわかりました。現地時間での業務時間内に攻撃が開始されたのは合計 11 件でした。

すでに各事例について AD への到達時間を再分析していたため、2022 年のランサムウェアの展開時間も把握しようと試みました。その結果、2022 年のランサムウェア展開の 94% が業務時間外に発生していることがわかりました。業務時間内に発生した事例はわずか 6 件でした。

すべてのランサムウェア攻撃が可視化されているわけではないため、ソフォスはこの結果を確定的なものとは考えていませんが、ランサムウェアの展開が一般的な業務時間ではない時間帯に最も盛んに行われていることは断言できます。2022 年と 2023 年の両方を見ると、ランサムウェア攻撃の 92% がこの結果を裏付けています。

攻撃のタイムライン分析から導き出される結論の 1 つは、攻撃中は時間が防御者の味方になり得るということです。滞留時間が減少したとはいえ、防御者が侵入者を検知するのに要する時間の中央値は 6 日です。しかし、士気の高い攻撃者では、この時間は劇的に変化します。2023 年には、他のすべての種類の攻撃で滞留時間の中央値が 10 日であったのに対し、ランサムウェア攻撃では 5 日でした。

さらに、ネットワークに潜む潜在的な危険を防御側に知らせる指標もあります。Active Directory サーバーへの侵入者を即座に検知することは、24 時間以内に攻撃を阻止することを意味します。データ窃取イベントを発見すれば、壊滅的な結果を防げます。

私たちは、多くのランサムウェア攻撃者が長年の経験を通じてそのスキルを磨いてきたことを知っています。しかし、これは一方通行の戦いではありません。防御者もまた、有効な対応策を実践することによって、またこの項目で述べたように、データが指し示す事柄を正しく理解することによって、スキルを磨けます。

アーティファクト、LOLBin、その他の発見

データから離れ、いつも通りツールや戦術、手法、手順 (TTP) の調査に目を向けると、今年の分析結果は強い既視感を呼び起こします。各ランキングの上位 5 件には、順位は若干異なるものの、前年と同じ項目が並んでいます。上位 10 件を過ぎて初めて、見慣れない名前が登場します。過去 3 年間で攻撃者が悪用したツールほど、停滞が顕著なものはありません。検出されたツールと Microsoft のバイナリの両方において、上位 10 件はほぼ同じです。まるで攻撃者は何の困難にも直面しておらず、同じツールと TTP を無制限に再利用しているかのようです。

アーティファクト

2023 年に最も頻繁に確認されたアーティファクト

2023 年のアーティファクト	2023 年の件数	2023 年の事例に占める割合	全事例に占める割合
SoftPerfect Network Scanner	51	33.12%	22.79%
Cobalt Strike	41	26.62%	38.61%
AnyDesk	40	25.97%	23.16%
Advanced IP Scanner	39	25.32%	20.72%
mimikatz	37	24.03%	26.93%
Impacket	34	22.08%	5.27%
WinSCP	28	18.18%	10.17%
Rclone	24	15.58%	13.37%
PuTTy	23	14.94%	11.30%
7zip	20	12.99%	9.42%
WinRAR	20	12.99%	11.86%

図 16：SoftPerfect Network Scanner は、2023 年の IR 事例で発見されたアーティファクトのランキングで 1 位となり、アクティブアドバーサリーレポートの発行開始以来 1 位だった Cobalt Strike をその座から追いやりました。

ランキング上位のツールは前年比でほぼ同じであるにもかかわらず、攻撃者の行動に変化をもたらす可能性のある傾向が 1 つあります。長年のリーダーであった Cobalt Strike が、過去 3 年間で着実にシェアを落としていることです。絶対数では依然として歴代ランキングの首位を維持しているものの、Cobalt Strike のペイロードを使用した攻撃の割合が大幅に減少しており、2021 年から 2023 年までの期間で、Cobalt Strike のシェアは 48% から 27% に低下しています。この理由として考えられるのは、Cobalt Strike があまりにも悪用されてきたため、防御側がその検知とブロックに熟達してきたことです。

今年の総合トップは、SoftPerfect の Network Scanner でした。このソフトウェアは、攻撃者がネットワークをマッピングし、潜在的な標的を発見するために日常的に悪用されています。このソフトの悪用は何年も前から確認されており、その有用性に攻撃者も気付いていました。Network Scanner の他にも、正規ソフトでありながら悪用されることの多いアプリケーションとして、エンドポイント管理用の一般的なツールである AnyDesk があります。

上位 10 件の興味深い要素の 1 つは、ツールの 50% がデータの窃取に用いられていることです。7zip と WinRAR (これらも正規の用途を持つツールですが、攻撃者に悪用されています) は、データの窃取を補助、あるいは難読化するためのアーカイブの作成に日常的に使用されており、他のツールはこのアーカイブの収集と転送に使われています。残念ながら、多くの組織は正常な状態がどのようなものであるかを十分に把握できていないため、自社のネットワークからの大規模なデータ転送を見逃しています。(たとえば、MEGA クラウドストレージサービスはあまりにも頻繁にデータ窃取のために悪用されています。通常の業務で MEGA を利用していないにもかかわらず、MEGA を出入りするトラフィックがある場合には調査が必要です。)

また、ソフォスのデータセットでは Impacket というツールが確認できることも注目に値します。このプロジェクトの管理者は以下のように説明しています。「Impacket はネットワークプロトコルを扱うための Python クラスの寄せ集めです。」Impacket はツール群であるため、ソフォスではそれぞれが攻撃でどのように使用されるかを詳しく理解する目的で、個々の使用 (Impacket/atexec、Impacket/secretsdump、Impacket/smbproxy など) を記録しています。しかし、個々のツールをすべて「Impacket」という 1 つの項目にまとめると、重要な結果が浮かび上がります。それは、2023 年における Impacket の全使用例を合計すると、アーティファクトランキングの 6 位にランクインすることです。

いくつかの例外を除いて、このカテゴリに属するツールの大半は、監視 / ブロック用ツールの有力候補です。

MS-LOLBin

2023 年に最も頻繁に確認された Microsoft LOLBin

2023 年の MS-LOLBin	件数	2023 年の事例に占める割合	全事例に占める割合
RDP	139	90.26%	83.80%
PowerShell	120	77.92%	71.94%
cmd.exe	83	53.90%	29.94%
net.exe	60	38.96%	26.93%
PsExec	60	38.96%	43.88%
タスクスケジューラ	55	35.71%	25.99%
rundll32.exe	43	27.92%	22.79%
ping.exe	41	26.62%	15.63%
nltest.exe	31	20.13%	10.73%
reg.exe	31	20.13%	12.62%

図 17：RDP は MS-LOLBin でトップに君臨し続けており、PowerShell は常に後塵を拝しています。

リモートデスクトッププロトコル (RDP) は、Microsoft の LOLBin (Living-off-the-Land Binary: 環境寄生型バイナリ) の中で最も悪用されているバイナリです。本記事では、RDP についての解説は簡単なものに留めておきますが (代わりに、RDP に関する統計と推奨事項について解説した特別補足記事をご覧ください)、RDP の悪用は「殿堂入り」しています。RDP の悪用は新たな段階に達しており、攻撃の 90% で内部からのラテラルムーブメントに、20% で外部からのラテラルムーブメントに RDP が使用されています。RDP を未だにインターネットに公開している 18% の企業は、「なんて愚かなことをしているんだ」と自問すべきでしょう。(あるソフォスのお客様に対してどのように RDP が用いられたかについては、本レポート下部の「ケーススタディ」の項をお読みください。) 本レポートの公開時点で、インターネット上に公開されている RDP システムは約 400 万台ありました。

IR チームが担当した事例での RDP の調査結果、2021 年～ 2023 年および全期間

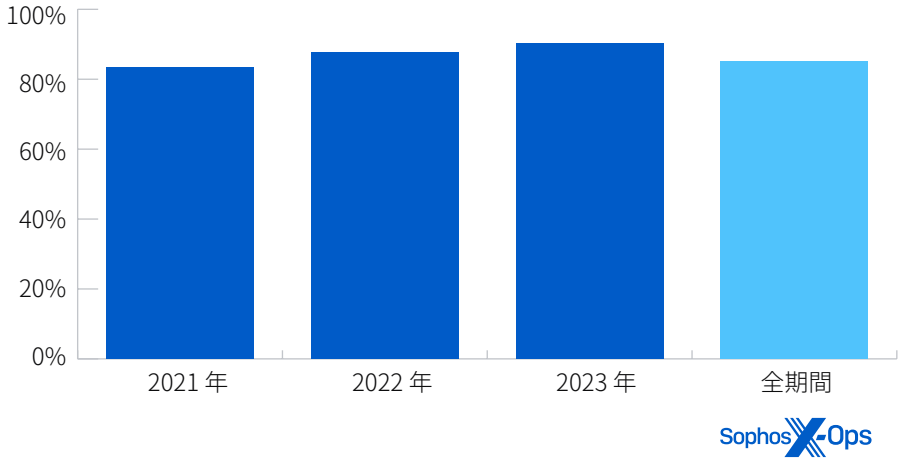

図 18：2023 年に IR チームが対応した攻撃の 10 件に 9 件で RDP 悪用の証拠が確認されました。

RDP の他にも、PowerShell はその汎用性、権限の大きさ、柔軟性、そして有用性から、多くの攻撃に悪用され続けています。PowerShell をネットワークから排除することは難しく、唯一の選択肢は、PowerShell を厳密に監視し、制御することです。PowerShell を安全かつセキュアに使用するための戦略には、PowerShell のすべてのアクティビティをログに記録すること、スクリプトを実行できるアカウントに最小権限の原則を適用すること、最新バージョンを実行すること、制約付き言語モードを有効にすることなどがあります。

ランクインしているその他のバイナリは、攻撃の実行、常駐化、防御回避、ネットワークの探索、ラテラルムーブメントなど、さまざまな目的で使用されます。すべてのデバイスを可視化し、必要なときに行動できる能力を持つことは、今日の防御者にとって必須です。

その他

2023 年に最も頻繁に確認されたその他の発見

2023 年のその他の発見	件数	2023 年の事例に占める割合	全事例に占める割合
有効なアカウント	122	79.22%	44.26%
サービスのインストール	92	59.74%	42.56%
ログの欠落	83	53.90%	17.89%
ネットワークの参照	79	51.30%	28.06%
悪意のあるスクリプト	73	47.40%	50.09%
保護機能の無効化	73	47.40%	30.70%
無効な MFA	66	42.86%	19.96%
アカウントの作成	52	33.77%	20.72%
ログの消去	49	31.82%	22.03%
ローカルグループの改ざん	35	22.73%	9.98%
LSASS のダンプ	35	22.73%	17.33%

図 19：アーティファクトや LOLBin よりも変動の激しいカテゴリである「その他」カテゴリでは、2 年前から「有効なアカウント」が首位を維持しています。2020 年および 2021 年には「悪意のあるスクリプト」が首位でした。

過去 1 年間に観察されたテクニックやその他の指標は、多くの攻撃にとって非常に標準的な攻撃手順でもあります。通常、調査から得られたデータのこの項目は最もばらつきが大きい部分です。たとえば、ソフォスはこのカテゴリを通じて、実環境で使用されているエクスプロイトを追跡しています。エクスプロイトの多くは年ごとに変化しますが、そうした新しいエクスプロイトの大半がデータセットの末尾に (200 件以上も) 連なっています。その前には、多くの調査を必要とする攻撃に関連するテクニックや発見が含まれています。

ログの欠落と消去については、今後のアクティブアドバーサリーレポートで詳しく取り上げる予定です。攻撃者は防御を無効にし、痕跡を消すことに長けています。このような防御側の目をくらませるための協調的努力は通常、検知を回避するためのものです。しかし、防御を無効にすることが、防御側に有利になるという意図しない結果を引き起こすこともあります。テレメトリ信号が停止することは、早急な対応を必要とする何かが環境内で起きていることを示すビーコンであるべきです。

検出を回避しようとする攻撃者も重要ですが、多くの場合、私たち自身が気付こうとしていないのです。

2023 年、ソフォスは一部でテレメトリの欠落が発生しているのを捕捉しました。調査対象となった攻撃の 54% がこれに該当していました。最も驚かされたのは、この新しい指標がかなり広範に確認できることでした。アクティブアドバーサリーレポートの調査を開始した年に、この指標は歴代ランキングの上位 10 件に入りました。ログが取得できない理由はいくつかありますが、多くの場合、組織が重要な場面でログを確実に取得するために必要な措置を講じていなかったことが原因です。

そして、過去の認証情報の侵害で懲りていなかったのか、43% の組織が外部に公開されたサービスの MFA を有効にしていませんでした。残念ながら、攻撃者を足止めできるソリューションが存在するにもかかわらず、実装されていないというのは故意の怠慢であると言わざるを得ません。 本レポートの最後の項目では、ある MDR のお客様の事例を解説します。

ケーススタディ：攻撃は次から次へとやって来る

これまでのアクティブアドバーサリーレポートを通じて、私たちは 3 つの基本的なセキュリティ原則を繰り返しお伝えしてきました。いずれも防御者にとっては基本的なセキュリティハイジーンです。以下に再度強調しておきます。

公開されている RDP ポートを閉じる

MFA を使用する

脆弱なサーバーにパッチを適用する

なぜ何度も繰り返す必要があるのでしょうか。それは、この 3 つのセキュリティ原則が未だに普遍的に導入されていないという事実を目の当たりにしているからです。 昨年、ある MDR のお客様が、半年間に 4 回もセキュリティ侵害の被害に遭い、これらの原則を痛感しました。業務要件が根本原因への対処を妨げていたため、攻撃者は毎回同じ侵入経路、つまり公開された RDP ポートに対するブルートフォース (総当たり) 攻撃で初期アクセスを得ていました。お客様の身元を保護するため詳細を一部変更していますが、同じ轍を踏まないように基本的なセキュリティハイジーンを優先することを読者の皆様に理解していただくために、1 年間のストーリーをご紹介します。

2022 年 12 月 (プロローグ): 初期アクセスが、公開されていた複数の RDP ポートに対するブルートフォース攻撃により成功しました。攻撃者は、複数の PowerSploit モジュールと Rubeus ツールを利用して認証情報を侵害した後、悪意のあるバイナリを多数ドロップし、EDR キラーツールをダウンロードしました。Sophos MDR の対応活動により、脅威は迅速に封じ込められました。しかし、お客様は業務上必要だからという理由で、公開されている RDP ポートへのアクセスを制限すべきだという MDR の提言を拒否しました。

ソフォスの提言：この事例を受け、MDR はインターネットに公開されている各種 RDP ポートを非公開にするよう提言しましたが、お客様は業務上の必要性を理由に拒否しました。(ドメイン全体の認証情報リセットやパッチ適用の提言も同様に拒否されました。)

2023 年 夏：初期アクセスが再度、公開されていた RDP ポートに対するブルートフォース攻撃により成功しました。その後、攻撃者は、オープンソースの PAExec ツールを作成・悪用して Nltest コマンドを実行し、環境内のドメインコントローラーを一覧化しました。その後、攻撃者はラテラルムーブメントを実行してレジストリ値を変更し、リモートデスクトップ接続を有効にし、心当たりのないリモートアシスタンス要求を許可し、RDP のネットワークレイヤ認証を無効にしました。

ソフォスの提言：この事例の後、MDR は公開された RDP ポートを閉じるようお客様に再度提言しました。また、特に RDP ポートの公開がまだ必要な場合は、多要素認証 (MFA) を有効にすることも推奨しました。お客様はこの提言を再度拒否し、MFA については社内で検討中であると述べました。

～ 2023 年 12 月：約 5 か月後、およそ 2 週間間隔で攻撃が相次ぎ、それぞれで個別の対応活動を余儀なくされました。いずれの攻撃でも、初期アクセスは公開された RDP に対するブルートフォース攻撃で獲得されました。以前の攻撃と同様、初期アクセスに続いて、攻撃者はドメインコントローラーの一覧化、ラテラルムーブメント、レジストリ設定の変更、RDP アクセスの制限緩和を行いました。対応措置は迅速に取られましたが、調査担当者は MFA が設定されておらず一般公開された従業員用 Web ポータルを発見しました。一方、前年に初めて確認された 6 個のポートも、依然としてインターネットに公開されていました。MDR の再三の提言にもかかわらず、お客様は社内の業務要件が原因で適切なセキュリティ対策を実践できず、ブルートフォース攻撃の標的として狙われやすい状況が続いていました。

2024 年 1 月：2 週間後、このお客様の新年は、同一のオープンポートを経由した別の攻撃で始まりました。レポートの記録はここまでですが、おそらくこのお客様に対する攻撃が終わったわけではないでしょう。このお客様の業務要件に従うと、公開された RDP へのアクセスを制限することも、MFA を有効にすることもできません。このような状況では、次から次へと押し寄せる攻撃の波に対する防御層は十分ではなく、インシデント対応者が提供できるアドバイスもあまりありません。

リスクを受け入れるかどうかは、それぞれの組織次第であり、リスク管理に万能薬はありません。しかし、リスクを受け入れることで継続的かつ広範囲の対応活動を強いられるのであれば、おそらくは見直しが必要です。 基本的なセキュリティ原則に従わなければ、他の防御をいくら強化しても、最初の防御層でアクセスを阻止できたはずの攻撃者に対して防御し続けることになります。

結論

2023 年のデータを振り返ってみると、組織を危険から守るために十分な対策が取られていないように感じられます。必要な保護措置を講じている企業もあるでしょうが、全体的に脅威に対して十分な注意が払われていません。多くの場合、侵害を受けた組織と受けなかった組織の大きな違いは、1) 適切なツールの選択と配置に伴う準備、2) 必要なときに行動するための知識と準備です。

ランサムウェア攻撃はその流行、使用されるツール、攻撃のタイムラインにおいて停滞期に達しています。残念なことに、防御者が毎年同じ過ちを犯しているのを目の当たりにしています。この事実を踏まえ、組織が緊急に自らの救済に乗り出す必要があるとソフォスは考えます。どの業界も、どの製品も、どのパラダイムも完璧ではありませんが、現在の私たちはいまだに一昨日の武器で昨日の戦いを戦っています。本レポートに記載されているツールやテクニックの大半は、解決策 (少なくとも被害を抑えるための緩和策) にはなり得ますが、それ以前に防御が追いついていません。

認証情報の侵害やパッチが適用されていないシステムは、過去の遺物であるべきです。無防備なシステム、過剰な権限を持ったユーザー、および管理されていないアプリケーションは、解決できる問題です。テレメトリの欠落は、被害者だけの責任ではないかもしれませんが (高度な攻撃者は、今後もテレメトリを妨害することで防御を困難にし続けるでしょう)、不十分なログ機能、あるいはログの未設定は、良く言えば意図しない見落としであり、悪く言えば意図的な失敗行動です。これらはすべて必要のない過ちであり、今すぐ止めるべきです。

本レポートのような遡及的分析は、特に対処中の問題が比較的停滞している時に、過去の失敗から学ぶ機会となります。自身の失敗を目の当たりにし、思うように進歩していないことに腹を立てたくなることもあるでしょう。しかし、怒りに任せてはいけません。より良い明日のために、今日どのようにポジティブな変化を起こせるかを前向きに考えましょう。

謝辞

MDR の Hilary Wood は、本レポートのケーススタディ (「攻撃は次から次へとやって来る」) の項目の執筆に貢献し、Lee Kirkpatrick は、本レポートで何度も言及している RDP に関するアクティブアドバーサリー特別レポート（「Remote Desktop Protocol：記事一覧）を寄稿しました。本レポートでは、その詳細を掲載しています。また、分析において洞察力を発揮した Chester Wisniewski に筆者一同謝意を表します。図 6 は、World Watch - Global CERT - Orange Cyberdefense が 2023 年に公開したデータから抜粋したものです。図 7 は故 Vitali Kremez 氏が作成したものです。御冥福をお祈りします。

付録：回答者の内訳と調査方法

本レポートを作成するにあたって、2023 年末時点での攻撃の状況について有益な情報を得るため、有意義な解析が可能な 154 件の事例に焦点を絞りました。ソフォスでは、お客様の機密を保護することを最優先事項としています。ここに掲載されているデータは、このデータからお客様を特定できないように、また、お客様のデータが不適切に集計を歪めることがないように、複数のプロセスを経て検証されています。問題があると考えられた特定のケースについては、そのお客様のデータをデータセットから除外しています。

業種

2023 年版のアクティブアドバーサリーレポートに使用されたデータセットのデータは以下の業種のものです。

農業	食品	MSP/ ホスティング
アーキテクチャ	政府機関	非営利団体
コミュニケーション	医療機関	製薬
建設業	ホスピタリティ	不動産
教育機関	情報テクノロジー	小売業
エレクトロニクス	法務	サービス
エネルギー	物流	運輸・交通
エンターテイメント	製造業	公益事業
財務データ	鉱業	

各国の現状

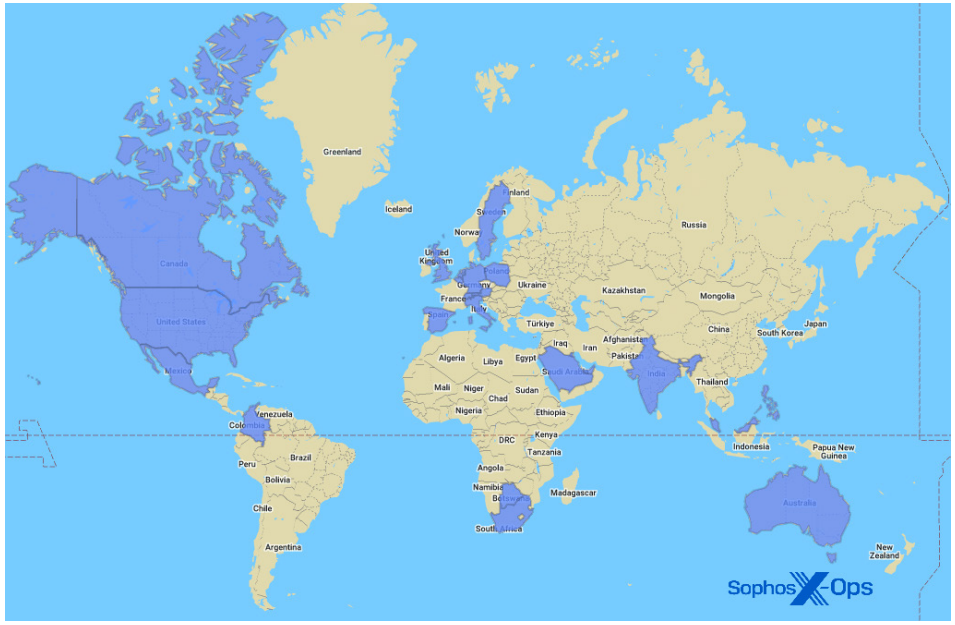

図 A1：Sophos X-Ops の IR チームがサービスを提供した組織の所在地

2023 年版のアクティブアドバーサリーレポートに使用されたデータセットのデータは以下の国・地域のものです。

オーストラリア	イタリア	シンガポール
オーストリア	クウェート	南アフリカ
ベルギー	マレーシア	スペイン
ボツワナ	メキシコ	スウェーデン
カナダ	オランダ	スイス
コロンビア	フィリピン	アラブ首長国連邦
ドイツ	ポーランド	英国
インド	サウジアラビア	米国

調査方法

本レポートのデータは、Sophos X-Ops インシデント対応チームが個別に実施した調査の過程で取得されています。2024 年の初回レポートである本レポートでは、2023 年に同チームが実施したすべての調査に関する事例情報を収集し、43 種の業界にわたって正規化しました。また、使用したデータが、本レポートの目的と照らして集計報告にふさわしい詳細さと範囲を備えていることを確認するために、各事例を調査しました。

データが不明確であったり、入手できなかったりした場合は、筆者たちが各事例の対応者と協力して疑問や混乱を解消しました。レポートの目的と照らして十分な解析ができなかった事例、またはレポートに記載することでソフォスとお客様との関係が公開される、あるいは、その他の損害を被る可能性があると判断された事例は除外されています。その後、初期アクセス、滞留時間、データ窃取などの事項をさらに明確にするため、残りの事例のタイムラインを調査しました。結果として得られた 154 件の事例をもとに本レポートは作成されています。

2024-04-18 (WP-NP)