DARKTRACE

2024年 年間 脅威レポート

サイバーセキュリティーにおける
進化する脅威と新たな戦術

目次

02	はじめに
03	手法と注意事項
04	まえがき
05	攻撃キャンペーンの概要
07	ランサムウェア：持続的な脅威および新種
08	RansomHub
08	ダイヤモンドモデルを使ってRansomHubを理解する
10	ダークトレースの観測した重大な脆弱性エクスプロイト
10	**ダークトレースが2024年に最も広範に観測した脆弱性のエクスプロイト**
12	Eメール脅威
13	LOTLテクニック
14	SOCの視点
15	SOCの月次内訳
16	OT（Operational Technology）およびICS（Industrial Control Systems）に対する脅威
17	エネルギー
18	ヘルスケア
19	国家と関連したスパイ活動の発見
20	ダークトレース脅威調査チームからの推奨策
21	コミュニティ利益のための取り組み
21	2024年のパリ五輪と米国の大統領選挙
22	参考文献

はじめに

ダークトレース脅威調査チームより

ダークトレースの 2024 年度脅威レポートをまとめるにあたり、調査結果は非常に興味深く、また大きな憂慮を抱かせるものでした。 ダークトレースでは、動作の異常を識別することが既知の脅威、新手の脅威どちらの発見においても肝要であるという信念に基づき、従来とは違った視点から脅威インテリジェンスにアプローチしています。

私達は脅威ランドスケープの分析を続ける一方で、ダークトレースの方法論をさまざまなデータ要素、脅威ハンティングテクニック、そしてサイバー業界全体のコミュニティエンゲージメントに適用する、よりプロアクティブなアプローチにもシフトしています。私達はこのタイプのアプローチにより、お客様への早期の警告を強化できるだけでなく、さまざまな重要インフラ分野への考察をコミュニティ全体に対して提供するのに役立つと確信しています。

ますますデジタル化する世界で私達は変化を続けていますが、そこでいくつか強調しておきたい情報や観測結果があります。攻撃者達は、エッジデバイスの脆弱性や、LOTL（Living-off-the-Land）を使った回避に重点を置く一方で、漏えいした SaaS（Software-as-a-Service）認証情報も利用しており、アイデンティティが引き続きデジタルエステート全体でコストのかかる問題であり、エンタープライズおよびビジネスネットワークにおいて根強い悩みの種であることを示しています。

2024 年、年間を通じて CNI（Critical National Infrastructure）に対する多数の脅威トレンドを観測しましたが、1 つの重要な結果はソフトウェア脆弱性を見つけ出そうとする競争が激化していることでした。2020 年、MITRE は約 18,000 件の脆弱性をリストしていましたが、2024 年現在のリストは 29,000 件を超えています [1]。

この増加はいくつかの理由で説明することができます：CNA（CVE Numbering Authorities）の増加、学術研究による脆弱性発見の重要性強調、“バグバウンティ” プログラム（報奨金制度）の成熟、そして現在も進行中の調査です。

世界中の脆弱性の総数は約 240,000 件といわれていますが、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）の KEV（Known Exploited Vulnerability）カタログにおいては、**実際に悪用が行われているものとして 1,200 件あまりの脆弱性**だけがリストされています [2]。脅威アクターはこれまで同様に検知を回避し続けていますが、より小さい範囲のエッジネットワークテクノロジーに対する理解により、リバースエンジニアリングの繰り返しとエクスプロイト方法の特定が可能になり、ゼロデイ脆弱性の発見と初期アクセスを可能にしています [3]。

ランサムウェアグループはその戦術をフィッシング以外にも進化させており、IT チームとのやり取りにより情報を引き出してアクセスすることや、SaaS ベースでの攻撃、そしてエクスプロイトの高速化や二重恐喝のためにファイル転送技術の研究まで行っています。IT 管理者や実務者にとって、組織の脆弱性管理プログラムの優先度を高め、デジタルエステート全体の潜在的攻撃経路を明らかにして不正なアクセスを予防することがきわめて重要です。これには、ビジネス全体、そして IT チーム全体でベストプラクティスを適用することも含まれます。攻撃、防御双方のチームにおいて AI ベースの技術が利用されるようになり、CNI への影響はこれまで以上に深刻な懸念です [4]。

本脅威レポートの以降のセクションでは、脅威ランドスケープレベルでのこれらの広範な問題について取り上げ、ダークトレースの脅威調査チームの調査結果がこれらの問題の数多くを裏付けていることを解説します。

謝辞

本レポートに貴重な考察を提供し協力してくれたダークトレースのアナリストチームおよび社員の皆さんに感謝します：

Adam Potter、Alexandra Sentenac、Anna Gilbertson、Daniela Alvarado、Dylan Hinz、Emma Foulger、Freek Klein、Iris Isac、Justin Frank、Justin Torres、Maria Geronikolou、Min Kim、Nahisha Nobregas、Nathaniel Jones、Nicole Wong、Ryan Traill、Safiy Soel、Sam Lister、Steven Sosa、Vivek Rajan、Weronika Walczak、Zoe Tilsiter

手法と注意事項

ダークトレースの 2024 年度脅威レポートは情報提供の目的のみを意図したものであり、発表の時点で利用可能であったデータ、傾向、分析に基づいたものです。本レポートの内容は、サイバーセキュリティ環境における現在の脅威および新たに生じつつある脅威についての可能な限りの理解を反映したものです。本書で提供される情報はすべてを網羅したものではなく、またサイバーセキュリティ上の脅威は急激に変化する性質を持っています。

データと考察の正確性と信頼性を確保するための努力は行われていますが、ダークトレースは情報の完全性または正確性を保証するものではありません。さらに、ダークトレースは本レポートにおいて提供されている情報の有効性、充足性、あるいは適用可能性について明示的か暗黙的かに関わらず何らの表明あるいは確約も行いません。

本レポートに記載されている調査結果および結論はダークトレースのものであり、第三者の意見や推奨を反映しているわけではありません。読者は自ら独立した評価を行い、特定のセキュリティニーズに対応するにあたってはサイバーセキュリティプロフェッショナルに相談されることをお勧めします。ダークトレースは、本レポートで提供されている情報の使用またはこれに基づくことにより生じた、いかなる直接的、間接的あるいは結果的損害についても責任を負いません。

ダークトレースの脅威調査手法

ダークトレースの脅威調査チームは、顧客の運用環境に対する詳細な調査を行ってアクティブな脅威を識別し、主要な侵害インジケーター（IoC）を特定し、関連する脅威インテリジェンスを提供しています。

この調査はダークトレースの異常ベース検知に基づいたもので、脅威調査チームによる徹底した分析およびコンテキスト化が行われています。検知された脅威は関連する顧客のセキュリティチームに直ちに報告されます。顧客がダークトレースの自律遮断テクノロジーを使用している場合、これらの脅威は速やかに緩和され、エスカレーションが阻止されます。

2024 年 1 月 1 日から 12 月 31 日までの期間、ダークトレースは多種多様なサイバー脅威を調査しました。その多くは複数の顧客を標的とした攻撃作戦的活動であったことが判明しています。ダークトレースの分析による情報はすべて、ダークトレースの AI 駆動アプリケーションおよび異常調査から得られた検知結果および個別のデータに基づいています。

‘ダークトレースの観測した重大な脆弱性エクスプロイト’ の調査手法

‘ダークトレースの観測した重大な脆弱性エクスプロイト’ セクションにリストされている ‘最も広範に観測した脆弱性のエクスプロイト’ は Darktrace / NETWORK を使用している複数の顧客で観測された、エクスプロイトの試みであることが確認された事象に基づいています。2024 年 1 月 1 日から 12 月 31 日までの期間にダークトレースの顧客に最も大きく影響したこれらの脆弱性は、侵害アクティビティをトリアージした後、ダークトレース社内の脅威調査およびオープンソースインテリジェンス（OSINT）を通じて、確認済みの IoC に一致したものです。

‘SOCからの視点’ の調査手法

本レポートの ‘ダークトレース SOC からの視点’ セクションの内容は、ダークトレースの Managed Threat Detection and Security Operations Support サービスを通じて分析された高確度の情報に基づいています。2024 年 1 月 1 日から 12 月 31 日までの期間に実施されたこの分析には、パターン解析とデータ有意性評価の両方が含まれています。これらの考察は主として定性的なものであり、ダークトレース SOC チームによる 2024 年の最も顕著なサイバー脅威の評価を反映したものです。

‘Eメール脅威’ の調査手法

‘E メール脅威’ セクションで紹介されている統計情報は、2023 年 12 月 21 日から 2024 年 12 月 18 日の間にクラウドでホスティングされたすべての顧客環境において監視されていた Darktrace / EMAIL モデルデータの分析結果に基づくものです。世界のダークトレースの顧客の E メール環境の約 90% がクラウドベースです。Darktrace / EMAIL モデルは、顧客の環境に対して 100% 特異であると見なされ “フィッシングインジケーター” が含まれる E メールに対してアラートを生成するよう設計されています。本レポートの目的、とりわけ Darktrace による E メール環境の分析において、“フィッシングインジケーター” とは単に迷惑なスパム E メールではなく、悪意があると確認される E メールを指しています。Darktrace / EMAIL データは現在、1 か月単位ではなく 28 日ごとに収集および処理されています。そのため、この分析には調査期間以外の、具体的には 2023 年 12 月の最後の 10 日間が含まれています。同じ理由により、2024 年 12 月 19 日から 12 月 31 日までのデータも含まれていません。

まえがき

ダークトレースの脅威調査チームは昨年、国家重要インフラ（CNI）セクターの世界中の組織を標的とした、高度な脅威アクターの著しい増加を観測しました。

この傾向は、国の情報機関からの警告の高まり、およびこれらの産業分野の顧客で発見されたアクティビティに対する脅威分析の焦点によって裏付けられています。CNI 組織を標的としていること、そしてアクセス後の行為は、脅威アクター達が紛争において地政学的な力を得るための戦略的道筋を構築しようとしているかもしれないことを示しています。この現実は、2024 年の年間を通じてダークトレースの脅威調査の焦点と内容のどちらにも表れています。

昨年は CNI セクターにおいて、世間の注目を集めた悪意ある行為の公表が複数見られました。ダークトレースの脅威調査チームは、CNI 組織に侵入した APT（Advanced Persistent Threats）を示唆する情報を基に、顧客ベースに対する脅威ハンティング調査を実施しました。

たとえば、ダークトレースのアナリスト達は Salt Typhoon および LiminalPanda グループが ISP（Internet Service Providers）プロバイダーを狙っているという公表された情報に対応し、これらのアクティビティの証拠を捜査しました。さらに、2024 年には Fuxnet や FrostyGoop といった新たな ICS/OT ネイティブなマルウェアが発生し、またヘルスケア等の脆弱な産業を標的とするランサムウェアグループは引き続き幅広く見られました。また、ダークトレースの脅威調査チームは、侵害の兆候が見られた防衛および政府機関の特定の顧客に対し複数件の詳細な調査を実施しました。これらの調査からは、有名な防衛産業および政府機関の顧客のネットワーク内において高度な脅威アクターが活動しているという明確な証拠が見つかり、今後の地政学的紛争において利用される可能性があることを示唆しています。

このような脅威アクターの攻撃手法と長期的な方向性はさまざまであり、CNI 組織にとって難しい問題となります。CNI 侵害の事例の多くは、インターネットに接続されたデバイスに対するゼロデイおよび既知両方のエクスプロイトから発生しています。

CVE エクスプロイトが存在しなくても、脅威アクターは外部リモートサービスを実行する境界デバイスを利用してアクセスしており、今後もそうするでしょう。IoC もまた、こうした攻撃を抑止する効果が弱いことをますます証明しています。VoltTyphoon のようなグループは、パッチの適用されていないシステムを悪用することにより、IoT（Internet of Things）やインターネットに接続したデバイスの膨大なボットネット（KV Botnet）を構築し続けています。これらのボットネットやオペレーショナルリレーネットワークの利用は、ダークトレースの脅威調査チームが調査した個別の事例でも証明されている通り、検知やアトリビューションの回避に役立ちます。一般に、CNI セクターを標的とする APT は、LOTL 戦術を利用して検知を免れる傾向も高まっています。

さらに、CNI ネットワークをエクスプロイトする悪意あるグループ達は、その活動範囲に対応した異なる目的を持っています。一部の APT グループは、CNI ネットワーク内で永続性が得られさえすれば、その後すぐには目標をもたない場合もあります。国家が支援する脅威アクターは、潜伏して待つアプローチをとる場合があります。ビーコニング以外は最小限のアクティビティでネットワーク内に潜むことを選択し、外部の戦略的条件が変化したときにはじめて活動を強化するのです [5]。

また、CNI 組織を狙う脅威アクターはより攻撃的なアプローチをとり、背後にある国家にとっての戦略的目標に役立つような機密性の高い情報を抜き取ろうとする場合もあります。ダークトレースはこのパターンの動作を 2024 年 6 月～ 7 月に観測しています。それはあるアジア太平洋地域の政府機関が Mustang Panda によるエクスプロイトを受け、機密性の高いデータをクラウドストレージプロバイダーに抜き取られようとした事例です。同様に、ダークトレースの調査チームはある製造業の組織において北朝鮮の APT によるデータ抜き取りとみられる証拠を発見しています。これもおそらく地政学的な状況に対する活動と思われます。この傾向の拡大により、ヘルスケア産業のようなセクターまでが標的となっており、ダークトレースのアナリストは従来のランサムウェア攻撃の一環としての暗号化よりもデータ抜き取りへ攻撃がシフトしていることを確認しています。

また、一部の脅威アクターはその目的に応じて、即時の中断を引き起こすようなマルウェアを利用することもあるでしょう。こうした脅威はたとえばエネルギーセクターなどの OT（Operational Technology）および ICS（Industrial Control Systems）環境、そして病院や金融機関など従来ランサムウェアの標的となっていた組織に対して特に大きな影響があります。

ダークトレースの脅威調査アナリストは、エネルギーセクターに混乱を引き起こそうとうする攻撃の増加を確認しています。ダークトレースが観測したこれらの攻撃の手段は、カナダのエネルギープロバイダーにおける変電所のSCADA環境のPLCモーターを狙ったOT専用攻撃や、複数のFogランサムウェア攻撃により暗号化の成功に至った事例などさまざまです。APTグループはまた、金銭目的以外でヘルスケア組織を標的とすることが増えています。OSINTによれば、こうした侵害の多くは公的医療サービスの妨害による社会全体の不安定化を狙ったものと思われます。この傾向は、RaaS（Ransomware-as-a-Service）グループが変化し、ヘルスケア組織と非医療組織の両方をランサムウェアプラットフォームを使って攻撃することにより、背後にある国家の目的を推進しようとしていることにも表れています。

以降のセクションでは、ダークトレースによる個別の産業および脅威に対する調査結果をレビューすることにより、これらの傾向をさらに詳しく解説します。結論として、ダークトレースの脅威調査チームが2024年に実施した調査は、高度なサイバーアクターによるCNI組織へのリスクが2025年に向けてさらに高まることを明らかにしています。

攻撃キャンペーンの概要

2024年に観測された大規模なキャンペーンにおいては、エッジおよび境界ネットワークテクノロジーのゼロデイおよびnデイ脆弱性のエクスプロイトが引き続き見られました。脅威ランドスケープ全体へのこうしたエクスプロイトの蔓延は、ダークトレースが年間を通じて観測した結果と一致していました。

Ivanti Connect Secure (CS) およびIvanti Policy Secure (PS) アプライアンス - CVE-2023-46805およびCVE-2024-21887

- 観測されたアクティビティの中でも、次のものが顕著でした：エクスプロイト検証アクティビティ、システム情報の抜き出し、AWSからのC2インプラントの投下、JavaScript認証情報スティーラーの投下、SimpleHelpの使用、およびポート53に対する暗号化されたC2
- さらに詳しい情報については次をお読みください：ダークトレースのInside the SOCブログ - The Unknown Unknowns:Post-Exploitation Activities of Ivanti CS/PS Appliances

Palo Alo Network (PAN-OS) ファイアウォールデバイス- CVE 2024-3400

- PAN-OSファイアウォールの重大な脆弱性が2021年4月11日に公式に発表されました。異常ベースの検知により、ダークトレースの脅威調査チームはPAN-OSデバイスのエクスプロイトに関連した一連の疑わしい動作を既に3月26日には特定していました。これにはC2アクティビティ、データ抜き出し、およびブルートフォースアクティビティ等が含まれていました
- さらに詳しい情報については次をお読みください：ダークトレースのInside the SOCブログ- Post-Exploitation Activities on PAN-OS Devices:A Network-Based Analysis

Fortinet - FortiManager CVE 2024-47575

- この分析は2024年9月に発生したCVE-2024-47575によるFortiManagerのエクスプロイトならびにこれに関連して6月と9月に観測された悪意あるアクティビティについてまとめたものです
- 攻撃キャンペーンの比較：Mandiantとダークトレースのソースはどちらも6月に起こったエクスプロイトの試みを認識しています。ダークトレースの記事はそれよりも前により大規模なキャンペーンが発生していた可能性を明らかにしより広範なレポートとなっています
- さらに詳しい情報については次をお読みください：ダークトレースのInside the SOCブログ - Post-Exploitation Activities on Fortinet Devices: A Network-Based Analysis

Operation Lunar Peek:Palo Alto Network ファイアウォールデバイス(CVE 2024-0012 and 2024-9474

- PAN-OSファイアウォールのエクスプロイトに関連した2つ目のキャンペーンです。ダークトレースはエクスプロイト検証と初期ペイロード取得、C2接続等のアクティビティを観測しました
- Sliver C2プラットフォームの使用が最新のPAN-OS侵害をさらに差別化するものとなっており、調査されたケースの約半数でSliverアクティビティの証拠が見つかっています
- さらに詳しい情報については次をお読みください：ダークトレースのInside the SOCブログ - Darktrace's view on Operation Lunar Peek: Exploitation of Palo Alto firewall devices (CVE 2024-0012 and 2024-9474)

その他注目の事例：CleoとJet Brains

- 2024年のCleoのMFTソフトウェアにおける脆弱性CVE-2024-50623およびJetBrains TeamCityの脆弱性CVE 2024- 27198
- ランサムウェアグループはCleoのようなファイル転送アプリケーションを好んで狙うことが明らかになりました。これらのアプリケーションに含まれる大量のビジネス情報の抜き出しやこれを使った二重恐喝のためです。一方、JetBrainsのケースでは、組織のサプライチェーンに深く組み込まれたソフトウェアに対してエクスプロイトまでの時間の短期化がかなり一般的になってきたことがわかります
- さらに詳しい情報については次をお読みください：ダークトレースのInside the SOC ブログ - Race Against Time: Detecting JetBrains' TeamCity Exploitation Activity with Darktrace およびCleo File Transfer Vulnerability: Patch Pitfalls 、ならびにDarktrace's Detection of Post-Exploitation Activities

ダークトレースが観測し文書化した特定のキャンペーン以外にも、以下のような手法が普及したことにより攻撃者が引き続き成功を収める要因となっています：

- Mamba 2FA のようなAiTMフィッシング脅威
- Fogランサムウェアを含むランサムウェアキャンペーンにおけるRMM（Remote monitoring and management）ツールの使用（Supremo、AnyDesk、UltraVNC、SplashTop、N-able - 旧Solarwinds MSP、SimpleHelp）
- クリプトマイニング オペレーションCoinLoaderを含めた多くのキャンペーンで見られたDNSトンネリング

PAN-OSエクスプロイトの検知

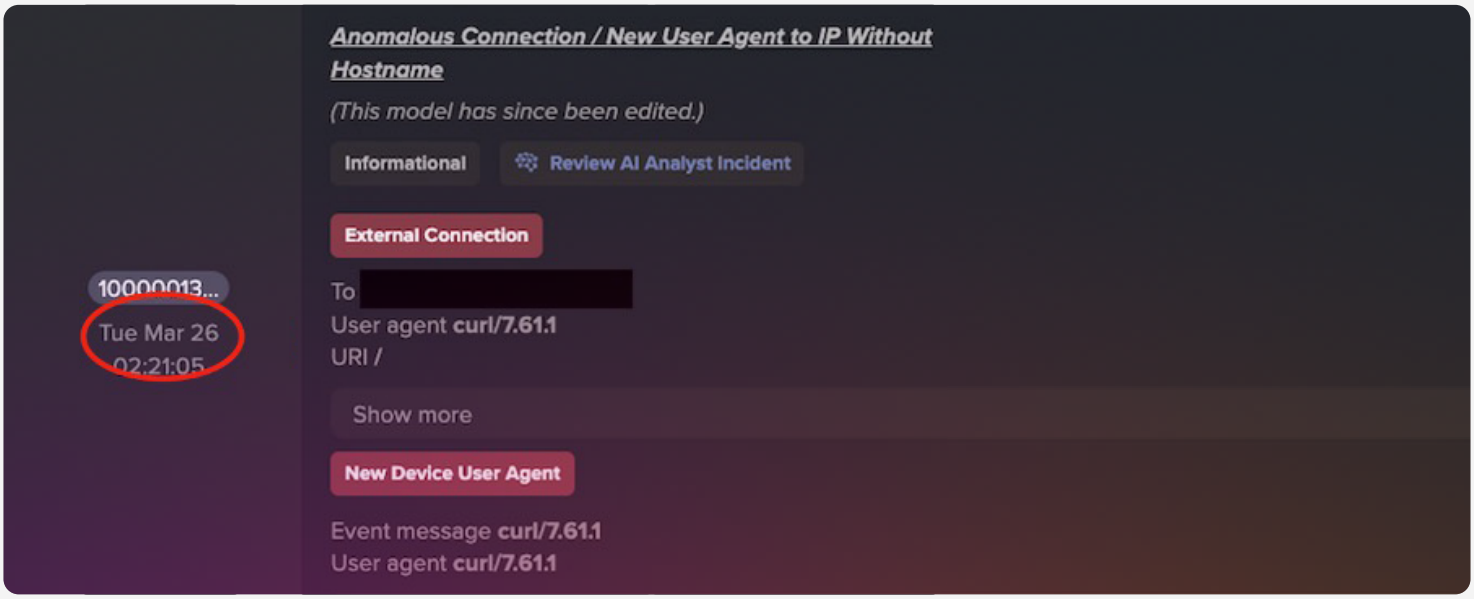


図 01: Darktrace / NETWORKのモデルアラートにより、PAN-OSのエクスプロイトに関連した悪意あるアクティビティが、この脆弱性の公式発表の前に検知されました。

FortiManagerエクスプロイトの検知

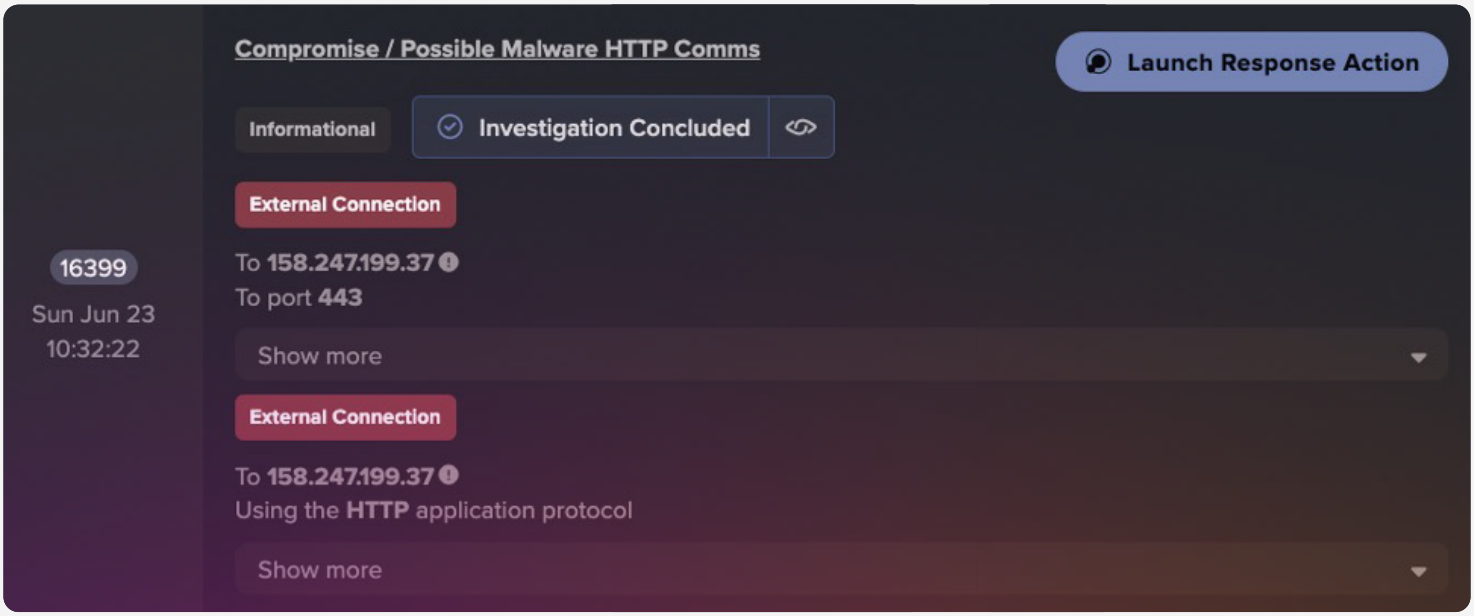


図 02: Darktrace / NETWORKのモデルアラートにより、FortiManagerデバイスに関連した悪意ある接続が2024年6月に検知されました。

2024 年年間を通じて、ダークトレースの脅威調査チームは顧客に対して彼らの運用環境で観測された攻撃キャンペーンの詳細を通知してきました。前半においては、**識別された攻撃キャンペーンの 40%** にインターネットに接続されたデバイスのエクスプロイトが関係していました。

ところが、6月から12月にかけては、インフォスティーラーがダークトレースの脅威調査チームが識別した最も顕著な攻撃キャンペーンタイプとなりました。

リモートアクセス型トロイの木馬（RAT）も 2024 年後半に大幅に増加し、**識別された攻撃キャンペーンの 46%** となりましたが、これは前半ではわずか **12%** でした。

また、2024 年後半にダークトレースの脅威調査チームが特定した攻撃キャンペーンにおいて**サービスとしてのマルウェア（MaaS）は 57%** を占め、1 月から 6 月までの 40% から増加しました。

ランサムウェア：持続的な脅威および新種

2024 年に世界で観測されたランサムウェアの事例は前年を下回りましたが、ランサムウェアの 1 事例あたりの平均支払い額は 273 万米ドルとなり、2023 年と比較すると 100 万ドル上昇しています [6]。

この上昇は RaaS モデルの導入が拡大していることを考えると驚くべきものではありません。RaaS モデルははではより経験の浅い脅威アクターにも破壊的な攻撃を実行するのに必要なツールが与えられ、参入障壁は著しく下がっています。

ダークトレースの脅威調査チームは2024年年間を通じて、さまざまな顧客で発生した複数のランサムウェア脅威を追跡しましたが、Lynxのような新種とともに、Akira、RansomHub、Black Basta、Fog、Qilin（Agenda）等の再発も観測しています。特筆すべき傾向としては、攻撃ベクトルとしてのフィッシングEメールの頻繁な使用、およびAnyDesk、Atera、Splashtop等の正規のツールをC2通信を隠すために利用していることが挙げられます。

Windows Management Instrumentation（WMI）およびPSEXESVCを水平移動に使用するなどのLOTLテクニックが頻繁に使用され、多くの場合、管理者認証情報が権限昇格に使用されていました。

MEGAやRclone等のクラウドストレージサービスへのデータ抜き出しも、もう1つの傾向として挙げられます。これらのサービスも正当な目的で広範に使用されているものです。

このセクションでは、ダークトレースの脅威調査チームが 2024 年に組織に対する重大な脅威として特定した 5 つのランサムウェアアクターを紹介します。これらは今後も引き続き脅威ランドスケープにおいて大きな存在となることが予想されます。

1.Akira ランサムウェア

- **背景：**RaaS型マルウェアであり、2023年に最初に観測され、2024年に再出現した[7]
- **影響を受けた顧客の国：**オーストラリア、カナダ、南アフリカ、英国、米国
- **観測されたTTP：**二重恐喝、リモートデスクトッププロトコル（RDP）サーバーへの受信接続、水平移動時のRDP使用およびVMWare使用、拡張子 “.akira” でのファイル暗号化

2.LockBit ランサムウェア

- **背景：**米国司法省により “世界で最も活発かつ破壊的なランサムウェアグループ” と説明されるRaaSグループであり、120ヶ国以上において2,500以上の被害者に損害を与え身代金の支払いで5億USドル以上を得ている [8]。グループのメンバーおよび開発者の逮捕にもかかわらず[9]、LockBitは根強い脅威として残っておりダークトレースも引き続きそれらを観測している
- **影響を受けた顧客の国：**世界的に影響
- **観測されたTTP：**NetScanを悪用した偵察、VMware ESXi デバイスの脆弱性エクスプロイト

3.Lynx ランサムウェア

- **背景：**INCランサムウェアの後継種として2024年に最初に観測された。不動産、小売り、金融、環境サービスを含む複数の産業セクターの組織を標的とする[10]
- **影響を受けた顧客の国：**英国および米国
- **観測されたTTP：**フィッシングEメールおよび悪意あるペイロードによる初期アクセス、二重恐喝、“.LYNX” 拡張子によるファイル暗号化、再起動マネージャー使用の可能性[10]。暗号化が失敗すると、権限の昇格を試行。管理者認証情報を使ったドメインコントローラーへのRDP接続

4.Fog ランサムウェア

- **背景：**最初に出現が観測されたのは2024年4月から5月にかけてであり、被害者のほとんどは米国内の教育関連セクターに分布。FogランサムウェアのバリアントはLinuxおよびWindowsプラットフォーム上に存在 [11][12][13]
- **影響を受けた顧客の国：**米国
- **観測されたTTP：**VPN認証情報の侵害、デフォルト管理者認証情報の通常とは異なる使用、SMBv1水平移動、AnyDeskへの異常な接続、大量のデータ流出、‘.flocked’ または ‘.flock’ 拡張子

5.RansomHub ランサムウェア

- **背景：**このRaaSグループの活動が最初に観測されたのは2024年2月であり、クラウドストレージバックアップや、Amazon S3インスタンスの設定ミスを狙うことで知られている。BlackCat/ALPHVアフィリエイトを吸収したと見られている[14]。ダークトレースは2024年末に起こった教育、製造、およびソーシャルサービスセクターに対する複数の攻撃でShadowSyndicateによるRansomHubの使用を観測している
- **影響を受けた顧客の国：**世界的に影響があったが、独立国家共同体（CIS）、中国、北朝鮮、キューバ内の組織を避けていた[15]
- **観測されたTTP：**Windows、Linux、ESXI、NAS、 Zerologon (CVE-2020-1472) の脆弱性を利用して初期アクセスを獲得、C2用としてAteraやSplashtopおよび偵察用として NetScan等、正規のツールを利用[16] [17]二重恐喝戦術

■ ランサムウェアの分析：

RansomHub

多くの企業や組織が、RansomHubのような高度なランサムウェアアクターのもたらす問題の深刻化に直面しています。これらの敵対行為をより詳しく理解し分析するために、セキュリティアナリストや研究者の間では、侵入分析のダイヤモンドモデル（Diamond Model of Intrusion Analysis）と呼ばれるサイバーセキュリティフレームワークが幅広く使用されています。

このダイヤモンドモデルを適用しDarktraceの機能を組み合わせることにより、ダークトレースの脅威調査チームはこれらの執拗な攻撃者の行動を理解する能力を強化しています。このアプローチは組織に対して、より深い考察とプロアクティブな防御戦略を提供することができます。

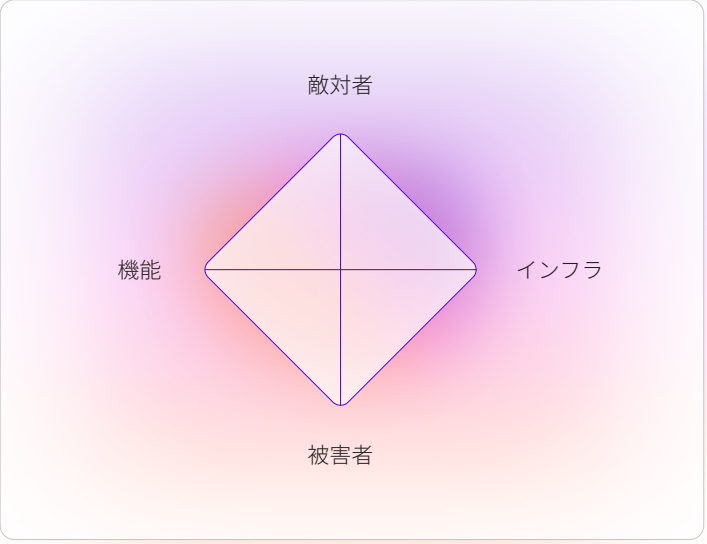


図 03: 侵入分析のダイヤモンドモデル

ダイヤモンドモデルを使ってRansomHubを理解する

敵対者の特定

比較的新しいランサムウェアグループであるにも関わらず、RansomHub はそのアグレッシブな戦術と世間の注目を集めた攻撃事例により、短期間に世界で知られるようになりました。彼らのアプローチは先行グループである LockBit や ALPHV（BlackCat）のものとよく似ており、これらのグループの元メンバーが RansomHub 下で活動しているという報告もあります [14]。

RansomHubはRaaSモデルで活動しており、攻撃を実行させるアフィリエイトを集め、彼らに必要なツール、インフラ、そしてサポートを提供します。

ほとんどのランサムウェアアクター同様、彼らの動機は金銭であり、主な目標は二重恐喝テクニックを使って、機密性の高いデータを暗号化し、身代金が払われなければデータを公開すると相手を脅すことです [15]。

ダークトレースの脅威調査チームは 2024 年、RansomHub によって影響を受けた複数の顧客ネットワークを調査しました。攻撃は 2025 年初めまで続き、ダークトレースのセキュリティオペレーションセンター（SOC）チームは少なくともさらに 3 件のケースを調査中です。

インフラ分析

RansomHub は HTTPS および DNS ベースの通信プロトコルを用いて侵害されたシステムと C2 サーバー間のデータフローを暗号化し、これらの通信を監視または傍受しようとする防御者の作業を困難にしています [17]。さらに、RansomHub は Tor などの匿名サービスを使用して多数のドメインを頻繁に登録し所有者情報を隠蔽しており、アトリビューションがますます難しくなっています [17]。

たいていの場合、脅迫状には、被害者とのやりとりと支払いに使用される固有の “.onion” URL へ誘導する情報だけが含まれています [17]。

盗み出したデータは、専用のサーバーとクラウドストレージサービスを使用して一時的に保管し、これを二重恐喝戦術のてことして利用して、支払いがなければデータを公開すると被害者を脅します。被害者が支払いに同意した場合、RansomHub は暗号通貨しか受け付けないため、支払いは Bitcoin または Monero で行わねばなりません [18]。

被害者プロファイリング

RansomHub は約 500 の組織および企業を攻撃したと報告されていますが、これにはメキシコ大統領の法律顧問 [19] やスコットランド住宅協会 [20] に対する攻撃など有名な事例も含まれています。RansomHub は北米、ヨーロッパ、アジア地域の組織を標的としており、特に政府機関、金融機関、ヘルスケアプロバイダーなどを重点目標としています。これらの組織の持つデータの重要性と金銭的潜在力の大きさによるものと思われます [21] [22]。

ただし、これ以外のセクター、たとえば情報技術、緊急対応サービス、食品および農業、通信などのセクターも標的になっています [23]。重要インフラに加えて、このグループは最高責任者レベルのエクゼクティブや IT 管理者も標的としていました。これはネットワークへのフルアクセスが可能な特権資格情報の取得を狙ったものです [15]。

このグループは非営利団体を攻撃せず、またすでに支払った被害者を再び標的としないルールを持っています。さらに、RansomHub は、アフィリエイトが独立国家共同体（CIS）、キューバ、北朝鮮、中国を標的とすることも許可しておらず [15]、このグループの所在地または提携関係を示唆している可能性があります。

能力分析

初期アクセスにおいては、RansomHubはインターネットに接続するアプリケーションの既知の脆弱性をエクスプロイトし、フィッシングやスピアフィッシング攻撃により侵入します。これに加えてクレデンシャルスタッフィングやブルートフォース攻撃による認証メカニズムの弱点のエクスプロイトも行います[17]。
侵入後、RansomHubはZeroLogon（CVE-2020-1472）の使用や、エンドポイント検知および対処（EDR）防御を無効にするために設計されたツール、EDRKillShifterの使用など高度なエクスプロイトテクニックを駆使します[16] [24]。

彼らはPowerShellスクリプトを利用して悪意あるコマンドの実行や、ネットワーク偵察、既存のアカウントの操作や無効化されたアカウントの再有効化により権限昇格などを行います。
さらに、RansomHubはMimikatz等のツールを使用して侵害されたシステムから認証情報を抽出し、SMBExec、AnyDesk、Cobalt Strike等の脆弱性をエクスプロイトして水平移動します。

暗号化には多くの場合 “Curve 25519” と呼ばれる楕円曲線暗号化アルゴリズムを使用し、暗号化されたファイルに一意の6桁の英数字コード拡張子を追加します[17]。データの抜き出しにおいては、BITSAdmin、HTTP POSTリクエスト、WinSCP等のツールを使用してWebサービスを介したデータの転送を行うことが確認されています[17]。

RansomHubに対するダークトレースのカバレッジ

ダークトレースが観測した3つの攻撃ケースにおいては、侵害されたデバイスは外部C2インフラとの通信が観測され、Darktrace / NETWORKにおいて複数のC2関連のモデルが発動していました。
さらに調査を行うとこれらのデバイスは通常とは異なるTCPポートでの通信も行っていました。これらの通信が検知されたのは、対象のドメインの珍しさ、および使用されたTCPポートが通常とは異なることを識別するDarktraceの能力によるものです。

これらの顧客のうち1社はダークトレースのマネージド脅威検知（Managed Threat Detection）サービスを契約していたため、SOCチームは侵害の最初の兆候がネットワーク上で検知されると、即座に確認されたアクティビティについて顧客に警告しました。

このケースでは、ダークトレースの SOC アナリストは顧客に対して、1 台のデバイスが AnyDesk を使った接続を受信し、ネットワークスキャニングを行い、ネットワーク上を水平移動していると伝えました。

この最初の警告後、攻撃がネットワーク上を急速に伝播するのに対応してダークトレースの SOC はさらに複数のアラートを送信しています。攻撃全体を通じて、ダークトレースは侵害された複数のデバイスが大量のデータを外部エンドポイントにアップロードしていることを観測しました。これには MEGA や Atera 等の正規のクラウドサービスも含まれていました。こうしたアクティビティはこの脅威アクターが二重恐喝の一環としてデータを抜き出す手法と一致しています。

この悪意あるアクティビティは、デバイスが大量のデータを外部に転送していることの異常な特徴により検知されたものです。ここで確認すべき重要な点は、Darktrace においては外部ドメインの珍しさが外部データ転送に関連したモデルの発動における主要なパラメーターなのではないということです。このケースでは MEGA や Atera が使用されたように、正規のサービスも攻撃者に悪用されることがあります。

対照的に、他の 2 社の顧客はマネージド脅威検知サービスを契約していなかったため、攻撃者が彼らのネットワークに対するアクセスを獲得したときに通知を受け取ることはできませんでした。しかし、ダークトレースの SOC チームはセキュリティオペレーションサポート（Security Operations Support）サービスを通じてサポートし、エキスパートアナリストへの直接アクセスを提供することができました。SOC のアナリストは攻撃がどのように始まったか、感染したデバイスのリスト、攻撃がどのように伝播したかの詳細、そして攻撃者により “.b2202a” のコード拡張子で暗号化されたファイルについての情報を提供しました。

さらに詳しい情報については、2024年のShadowSyndicate脅威アクターによるRansomHubの展開に対するダークトレースの詳細な調査レポートをお読みください。これには観測されたIoCおよびTTPの内訳や、関連するDarktrace / NETWORKモデルの詳細が掲載されています。

ダークトレースが観測した重大な脆弱性エクスプロイト

幅広く使用されているサービスやアプリケーションに新たに発見された脆弱性を脅威アクター達が特定し悪用することはますます一般的になっています。攻撃者は深刻かつ世界的に影響のある CVE に対するエクスプロイトの開発に注力することも多いですが、たいていの場合最もよく成功するのは、既知の脆弱性に対する公式発表後 1-2 年以内の攻撃です。

一部のケースでは、公式発表後数時間でエクスプロイト検証が発生します。

2024年、ダークトレースの脅威調査チームは前述のようなインターネットに接続されたシステム、たとえばIvanti CS/PSアプライアンス、Palo Alto製ファイアウォール、Fortinet製アプライアンス、Cleo製ソフトウェア、ScreenConnectサーバー、そしてTeamCityオンプレミス等の脆弱性を狙った複数の攻撃キャンペーンを観測しました。これらのエクスプロイトされた脆弱性は、Spark、WARPWIRE、Spectre RAT、CACTUS等のマルウェア、および悪意ある暗号通貨関連アクティビティとの強い関連性があります。

これらの脆弱性にタイムリーに対処することで攻撃の有効性は低くなり、悪意あるオペレーションの進行が遅れることで、攻撃者はゼロデイエクスプロイトやソフトウェアサプライチェーン攻撃等、よりコストと時間のかかる手法を使わざるを得なくなります。脅威アクター達はさまざまな脆弱性を狙ったツールを開発していますが、重大で公開されている既知の脆弱性に対するエクスプロイトは、インパクトの大きい、低コストかつ広範に使える手段を彼らに提供します。

ダークトレースが2024年に最も広範に観測した脆弱性のエクスプロイト

CVE-2024-3400

- **脆弱な製品：**PAN-OSを実行するPalo Alto Networks製ファイアウォール機器
- **脆弱性のタイプ：**コマンドインジェクションおよび不十分な入力検証
- **関連するマルウェア：**Spark（バックドア）
- **確認されたアクティビティ：**エクスプロイト検証アクティビティ、バイナリおよびシェルスクリプトの取得、HTTP POSTを介したデータ抜き出し、未知の外部エンドポイントとの継続的C2通信
- 技術的詳細およびIoC

CVE-2023-46805およびCVE-2024-21887

- **脆弱な製品：**Ivanti Connect Secure（CS）およびIvanti Policy Secure（PS）
- **脆弱性のタイプ：**不十分な認証による認証バイパスおよびコマンドインジェクション
- **関連するマルウェア：**WARPWIRE、Monero暗号通貨マイニング
- **確認されたアクティビティ：**エクスプロイト検証への帯域外アプリケーションセキュリティテスティング（OAST）サービスの使用、システム情報の抜き出し、AWSでホストされるC2インプラントの投下、JavaScript認証情報スティーラーの投下、SimpleHelp（リモートサポートソフト）の使用、SSLベースのC2の使用、暗号通貨マイニングマルウェアの投下
- 技術的詳細およびIoC

CVE 2024-23113およびCVE-2024-47575

- **脆弱な製品：**FortiGate および FortiManager
- **脆弱性のタイプ：**外部からコントロールされたフォーマット文字列の使用ならびに重要機能に対する認証の欠如
- **確認されたアクティビティ：**ホスト上でのコマンド実行、ペイロード取得、
機密性の高いデータの抜き出し
- 技術的詳細およびIoC

CVE-2024-0012およびCVE-2024-9474

- **脆弱な製品：**Palo Alto Networks製ファイアウォール
およびPAN-OS（Web管理インターフェイス）
- **脆弱性のタイプ：**重要な機能に対する認証の欠如による認証バイパス、およびOSコマンドインジェクション
- **関連するマルウェア：**Spectre RAT
- **確認されたアクティビティ：**エクスプロイト検証、初期ペイロード取得、C2接続およびさらなるバイナリダウンロードの可能性、偵察および暗号通貨マイニングの可能性
- 技術的詳細およびIoC

CVE-2023-48788

- **脆弱な製品：**FortiClient EMS
- **脆弱性のタイプ：**SQLインジェクション
- **確認されたアクティビティ：**エクスプロイト検証、Silver C2フレームワークの使用、Splashtop、Atera、AnyDesk等の各種RMMツールの使用、内部偵察、権限昇格、水平移動、機密性の高いデータの抜き出し
- 技術的詳細およびIoC

CVE-2024-1708およびCVE-2024-1709

- **脆弱な製品：**ConnectWise Screen Connect
- **脆弱性のタイプ：**制限付きディレクトリへのパス名の制限の不備（パストラバーサル）および認証バイパスに対する脆弱性
- **確認されたアクティビティ：**疑わしいエンドポイントへのアウトバウンド接続、PowerShellの使用、実行形式ファイルのダウンロード
- 技術的詳細およびIoC

CVE-2024-50623

- **脆弱な製品：**Cleo製Managed File Transfer
(MFT) ソフトウェア
- **脆弱性のタイプ：**危険なタイプのファイルに対する無制限のアップロード
- **確認されたアクティビティ：**疑わしいエンドポイントへのアウトバウンド接続、データ抜き出し、PowerShellを使ったコマンド実行
- 技術的詳細およびIoC

CVE-2024-27198

- **脆弱な製品：**JetBrains TeamCity
- **脆弱性のタイプ：**代替パスまたはチャネルを使った認証バイパス
- **関連するマルウェア：**暗号通貨マイニング（XMRig）
- **確認されたアクティビティ：**公開されているエクスプロイト実証コードの使用、悪意あるファイルのダウンロード、C2接続、暗号通貨マイニングマルウェアの投下
- 技術的詳細およびIoC

CVE-2023-41266、CVE-2023-41265、CVE-2023-48365

- **脆弱な製品：**Qlik Sense Enterprise
- **脆弱性のタイプ：**パストラバーサル、HTTPリクエストトンネリング
- **関連するマルウェア：**CACTUSランサムウェア
- **確認されたアクティビティ：**疑わしいエンドポイントへのビーコニング、PowerShellを使った悪意ある実行形式ファイルのダウンロード、RDP、SMB、 LDAPプロトコルを使用したネットワークスキャニングと水平移動、Qlik、Kerberosブルートフォース攻撃、ランサムウェア暗号化、暗号化されたファイルの隠蔽の試行
- 技術的詳細およびIoC

Eメール脅威

2023 年 12 月 21 日から 2024 年 12 月 18 日までの間に、Darktrace/EMAIL は顧客ベース全体で **3040 万通のフィッシング E メール**を検知しました。

正当なサービスや送信者の悪用は2024年年間を通じて脅威アクターがさかんに使用した手法でした。

少なくとも

270万の

- **マルチステージペイロードが**
  発見されました

940,000+

- **有害なQRコードが**
  これらのEメールで検知されました

信頼されるプラットフォームやドメインを利用することで、悪意のあるアクターは従来のセキュリティ対策を回避しフィッシングの成功率を高めることができます。

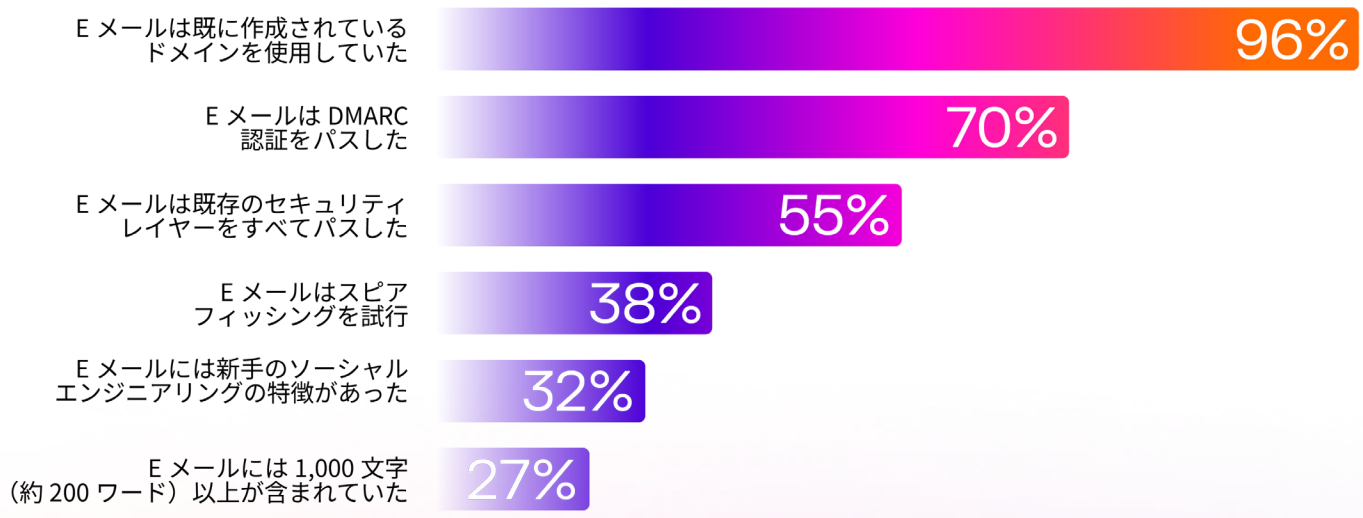
2024 年の後半 6 ヶ月間にダークトレースの脅威調査チームが E メールベースのサイバーインシデントで送信者アドレスやペイロードのリンク内で正当なドメインが悪用される著しい傾向を観測しています。

この傾向は、年間を通じてダークトレースが観測したフィッシング E メール全体のパターンとも一致しています。すなわち、正規に認証された送信者および確立済みのドメインがかなりの割合で使用されており、Darktrace / EMAIL が検知した**フィッシング E メールの 96%** は、新しく登録したものではなく既存のドメインを使用していました。

年間を通じて、ダークトレースは脅威アクター達が Zoom Docs、QuickBooks、HelloSign、Adobe、Microsoft Sharepoint を含む信頼されるサービスを悪用し、正当な送信者アドレスを使ってフィッシング E メールを送信している様子を確認しました。これらの E メールは多くの場合本物らしさが増しており、受信者が反応する可能性は高まっています。

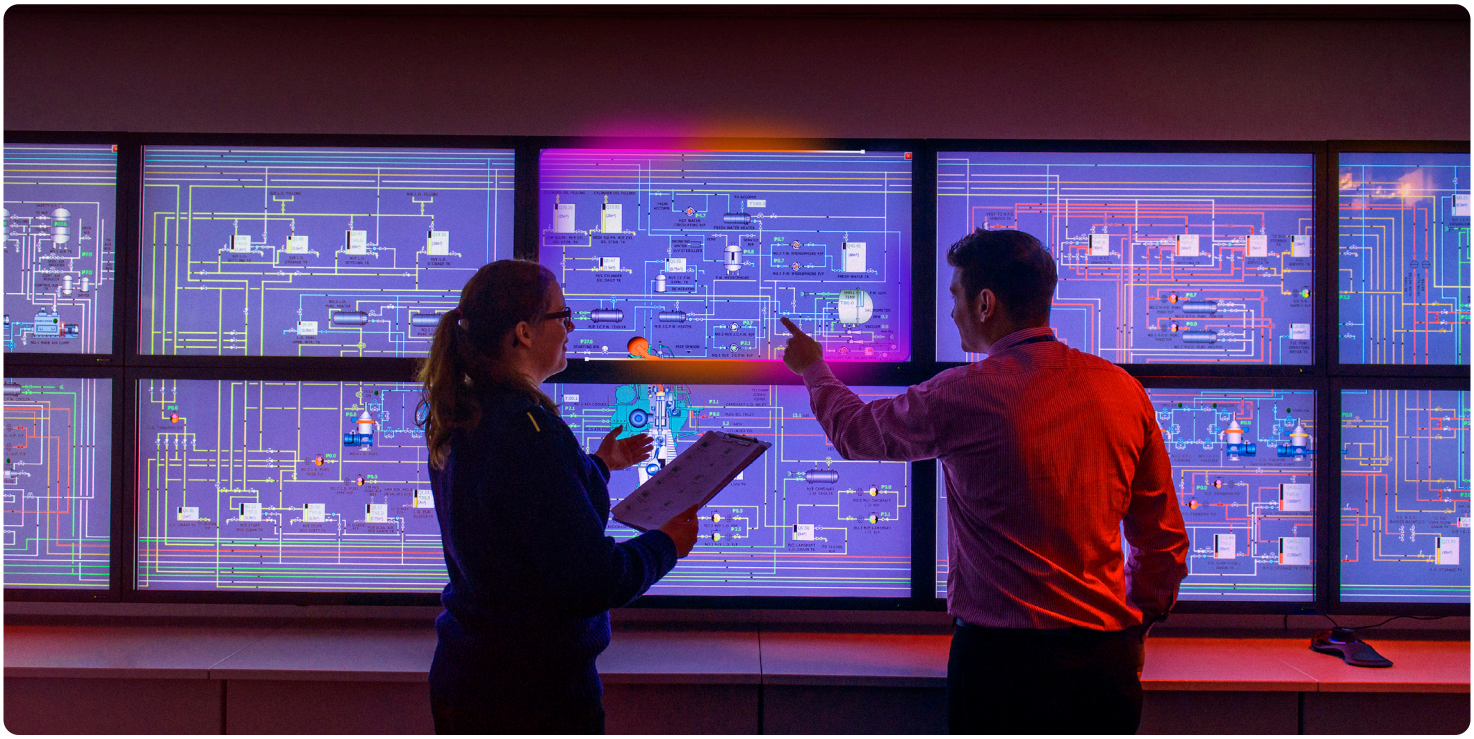
脅威アクター達はしばしば Google 等の正規のサービスを介したリダイレクトを使って悪意あるペイロードを投下し、検知を免れていました。さらにダークトレースは、ビジネスパートナーや信頼されるベンダー等、正当な第三者が所有する Amazon Simple Email Service（SES）を含む E メールアカウントを攻撃者が乗っ取るケースも確認しています。

この戦術は、以前にやりとりしたことのある信頼される相手先からの E メールであるため、従来の E メールツールの検知プロセスをさらに困難にしました。



■ ネイティブツールのエクスプロイト：

LOTLテクニック



年間を通じて、LOTL テクニックはダークトレースの脅威調査チームが観測した脅威の中で一貫して見られ、数多くのインシデントにおいて攻撃者はネイティブプロトコルおよびサービスを悪用することにより、標的ネットワーク内で検知されないままに目的を達成しようとしていました。

年初、チームは TA577 Initial Access Broker (IAB) グループと関連した認証情報窃盗キャンペーンを調査しました。このキャンペーンは SMB プロトコルプロトコルおよび NTLMv2 チャレンジ / レスポンスを悪用して NTML 認証ハッシュを盗むものでした。ダークトレースは複数の顧客ネットワーク内のデバイスが、攻撃者がコントロールする外部 SMB サーバーからテキストファイルを取得しようとしていることを発見しました。これらのサーバーは NTLM を介した SMB セッション認証を必要とし、それが完了すると NTLM ハッシュを攻撃者に露出させていました。暗号化されたチャレンジ文字列は、その後パスザハッシュ（pass-the-hash）攻撃や、ブルートフォースにより元の認証情報を取得するのに使用することができます。

4 月および 5 月にかけて、PAN-OS コマンドインジェクション脆弱性エクスプロイト（CVE-2024-3400）の調査を行う中で、ダークトレースの脅威調査チームは複数の顧客環境において、デバイスが珍しい外部エンドポイントに対して HTTP リクエストを送信していることを確認し、これらは多くの場合 “cURL” または “wget” ユーティリティを使っていました。多くの場合開発者やシステム管理者が使用するこれらのユーティリティを、攻撃者はペイロードの取得や、機密性の高い設定情報を攻撃者がコントロールする IP に抜き出すために利用していたと思われます。

ほぼ同じ時期に、脅威調査チームは正規の Windows プロセスを使って Raspberry Robin ワームを拡散させるキャンペーンを調査しています。感染すると、“cmd.exe” および “msiexec.exe” 実行形式を使って悪意あるファイルを外部ドライブから実行し、Raspberry Robin C2 サーバーに接続してメインのマルウェアコンポーネントをダウンロードします。

さらに、ダークトレースは ShadowPad による複数の感染例を調査しました。これは以前、API41 を含む、国家の支援を受けたアクティビティと関連づけられていたモジュール型のマルウェアプラットフォームです [25]。感染したデバイスとドメインコントローラ間の異常な SMB および RDP アクティビティにより、ドメインコントローラが TShadowPad の DNS C2 インフラと関連した、長い、エンコードされたサブドメインに対して XT DNS リクエストを開始し、これは DNS トンネリングアクティビティの兆候と思われます。

管理者による正しい使用と攻撃者による不正な使用を区別することは、ユーザーの動作についての確立されたベースラインなしには困難です。LOTL テクニックは攻撃者が通常のトラフィックに紛れ込むことを可能にし、スパイ活動や情報収集キャンペーンなど、気づかれない状態でいることが重要な攻撃には理想的です。APT はこれらのテクニックを使用することにより、シグネチャや IoC に基づくアトリビューションの取り組みを阻害しようとします。しかし、より小規模な犯罪組織であっても、ネイティブツールの悪用にはカスタムマルウェア開発の必要性を回避することで時間と費用を節約できるという利点があります。またカスタムマルウェアを開発しても、一旦 IoC と TTP が公開されれば従来型のセキュリティツールでブロックされる可能性もあります。

SOCの視点

ダークトレースの SOC による以下の考察は、2024 年に多くの組織が直面し、2025 年以降も継続することが予測される最も重大なサイバー脅威を紹介するものです。

リモートネットワークアクセスソリューションの悪用

リモートネットワークアクセスソリューション、たとえば VPN ソリューション、VDI（Virtual Desktop Infrastructure）ソリューション、そして Microsoft の RDS（Remote Desktop Services）等を使うことにより、組織はユーザーに対してネットワークへのリモートアクセスを提供することができます。2024 年、ダークトレースの SOC は、悪意あるアクター達が組織のネットワークに侵入するためにこれらのリモートネットワークアクセスソリューション、特に VPN を頻繁に悪用する事例を観測してきました。盗んだ認証情報を使って VPN、VDI、RDS 環境にログインした後、悪意あるアクター達は広範なネットワーク偵察活動を行い、攻撃の次のフェーズの準備を行っていました。

AiTM フィッシング

AITM フィッシングは SaaS アカウントの多要素認証（MFA）保護を回避できる方法として脅威アクター達に人気のあるテクニックです。このテクニックはダークトレースの SOC が 2024 年に調査した SaaS 侵害において幅広く観測され、Mamba 2FA および Tycoon 2FA フィッシングキットが脅威アクター達の間では特に人気がありました。AiTM フィッシングによりユーザーの SaaS アカウントへのアクセスを獲得すると、脅威アクター達は HideMyAss (HMA) VPN、Private Internet Access (PIA) VPN、ExpressVPN、Cloudflare WARP VPN 等の VPN サービスを使って接続元を隠蔽しました。

データ抜き出し

データ抜き出しは 2024 年においても悪意あるアクター達のよくある目的であり、恐喝とスパイ活動オペレーションのどちらにおいても確認されています。Ransom-Hub のような二重恐喝ランサムウェア攻撃で使用されたステルス型のデータ抜き出しや、Clop 恐喝ギャングにより仕組まれた最近の Cleo 関連侵害で見られたようなランサムウェアレスの恐喝など、恐喝の方法はさまざまです。Darktrace の SOC が観測したあるスパイ活動オペレーションでは、国家が支援したアクターが、侵害された複数の合法なサイトのネットワークを使用して標的ネットワークから機密性のデータをひそかに抜き出していました。

SOCの月次内訳

以下の表は、ダークトレースのSOCによって追跡された、ダークトレースの顧客に最も大きく影響した特筆すべき脅威の一部を2024年の月毎にまとめたものです。

1月	2月	3月
Ivantiのエクスプロイト	Dropboxの不正使用	トンネリングツールの不正使用（Cloudflare Tunnel、Ngrok）
データ抜き出し（MEGA、Put.io）	ブルートフォースアクティビティ	Teamsフィッシング
Microsoft Customer Voiceサービスの不正使用	Ivantiのエクスプロイト	JetBrains TeamCityのエクスプロイト
Amadeyインフォスティーラー	RMMツールの使用（AnyDesk）	SSHベースのC2
RMMツールの使用（AnyDesk、ConnectWise Control）	ランサムウェア（LockBit、Akira、8Base）	ランサムウェア（Akira、Phobos）

4月	5月	6月
セッションクッキーの不正使用	eM Clientの不正使用によるメールボックス偵察	VPNを使った初期アクセス
FortiClient EMSおよびPalo Alto Pan-OSのエクスプロイト	プロキシボットネットアクティビティ	AiTMフィッシング
RMMツールの使用（AnyDesk、Atera、DWService）	内部関係者からの脅威	VPSエクスプロイト
プロキシツールの使用（Stowaway、SystemBC、ProxyScrape）	データ抜き出し（OneDrive、Vultr）	XMRigクリプトマイニング
PowerShellの使用	MFA操作	Akiraランサムウェア（Medusa、Akira）

7月	8月	9月
DNSトンネリング	LDAP偵察	SSHの使用
VPNを使った初期アクセス	VPNを使った初期アクセス	VPNおよびVDIインフラを使った初期アクセス
SharePointの不正使用	Purple Fox	Cobalt Strike
メールボックス偵察	支払先変更詐欺	データ抜き出し（MEGA）
ランサムウェア（Medusa、Fog）	ランサムウェア（LockBit、Akira、Fog）	ランサムウェア（LockBit、Akira、RansomHub）

10月	11月	12月
ステルスC2	AiTMフィッシング	Chrome拡張機能サプライチェーン侵害
ExchangeおよびFortinetのエクスプロイト	支払先変更詐欺	AiTMフィッシング
LOTL （comsvcs.dll、drsuapi）	Palo Alto Pan-OSのエクスプロイト	Cleoのエクスプロイト
データ抜き出し（Easyupload.io）	RMMツールの使用（Splashtop、Supremo、NetSupport Manager）	RMMツールの使用（Supremo、AnyDesk、UltraVNC、SplashTop、N-able、SimpleHelp）
ランサムウェア（Black Basta、Crytox、RansomHub、Fog）	ランサムウェア（Play、Brain Cipher）	ランサムウェア（Lynx、Medusa、RansomHub）

OT（Operational Technology）およびICS（Industrial Control Systems）に対する脅威

2024年、ダークトレースの脅威調査チームは多数のOT攻撃を調査し、その数は前年のOT攻撃調査数の2倍以上になりました。

チームは新しいICS専用マルウェア、政府機関からの警告、そしてDarktrace / OTユーザーで発生した侵害の可能性について調査を行いました。この調査では、OTシステムのハッキングはますます達成可能な目標となっており、この傾向は続くと見られることが明らかになりました。

2024年5月、NCSCおよびCISAを含む複数のセキュリティ組織が、国家を背後に持つグループによる西側の国家重要インフラを狙った脅威の高まりについて警告を発しました。NCSCは「2024年初め、親ロシアのハクティビストが北米とヨーロッパに所在する脆弱な小規模のICSシステムを狙っていることが確認されている」と警告しました[26]。NCSCはすべてのOT所有者および運用者に対して防御の強化を促しました。CNIには“多層防御”アプローチが最も大きな保護をもたらします。実際、この警告の数か月後には、北米に所在するダークトレースの顧客2社がOT関連のインシデントを経験し、どちらも7月から8月後半の間に発生していました。どちらのインシデントも、国家重要インフラにリンクされているOTデバイスで発生した予期しないアクティビティが関係しており、片方のケースでは後に顧客の物理的な重要インフラに影響が発生していたことが判明しています。

その際、1社で発生した疑わしいアクティビティには次が含まれます：

- 顧客のITネットワーク内のデバイスからHMIやSCADAサーバーを含むOTデバイスまで、さまざまなデバイスからの異常なRDPの使用
- HMIデバイスからの予期しないNmapスキャニングおよびSMBv1セッションの試行
- SCADAサーバーからの通常とは異なるDNSリクエスト

これは、NCSC および CISA からの[27] CNI ネットワーク内で必要なリスク緩和策についての警告と一致しています。つまり、HMI リモートアクセスのセキュリティ強化、インターネットアクセスの制限、および内部のコンポーネントからの接続を必要な IP リスト内からの接続だけに制限することです。

Darktrace / OT ユーザーが経験したインシデントの調査とともに、脅威調査チームは OT 環境に対する新種の脅威、たとえば FrostyGoop ICS マルウェア等についても調査し、Darktrace での検知の可能性を研究しました。

このマルウェアが最初に発見されたのは 2024 年 4 月であり、ウクライナのエネルギーインフラに対するサイバー攻撃に使われていた可能性があります[28]。これは ICS 専用のマルウェアとして識別されたものとしてはまだ 9 番目であり、こうした攻撃の珍しさを示すとともに、脅威アクター達の OT 空間での能力の拡大を示しています[28]。FrostyGoop に対する外部の調査によれば、この攻撃者は、適切にセグメント化されていなかった外部に接続されたルーターの何らかの脆弱性を利用してネットワークに侵入した可能性があるということです[28]。

ダークトレースの顧客ベースにおいては FrostyGoop の兆候は見られていませんが、外部研究者により報告されたルーター脆弱性エクスプロイトの可能性は、エッジデバイスのもたらすリスクを示しています。このセクターに対する様々な予測は、エッジデバイス、特に IoT デバイスに対する攻撃の増加を示唆しています[29]。IoT デバイスやセンサーは多くの場合セキュリティが弱い傾向にあり、OT ネットワークへのアクセスを狙う攻撃者にとっては主要な標的となります。

Darktrace / OT ユーザーに対する脅威調査チームの調査では、OT ネットワークにおいて、その設計そのものがセキュアでないケースがいかに多いかが明らかになりました。これらのセキュリティギャップには、セキュアでないプロトコルおよびシステム、セグメント化されていないネットワーク、不十分なアセットインベントリなどが含まれます。

OT と IT システムの統合が進むにつれ、これは攻撃者にとっての機会が拡大することを意味します。OT セキュリティは堅牢な IT セキュリティのサポートにより最も強力なものとなります。これにはネットワーク全体の防御を目的とした IT チームと OT チーム間での調整が必要となります。

■ セクターの分析：

エネルギー

2024 年、ダークトレースの脅威調査チームはエネルギーセクターを含む業界別の調査に重点を置きました。エネルギーセクターは経済のあらゆる部分の原動力であり、大きなテクノロジー転換を経験しています。こうした変化がこのセクターのサイバーアタックサーフェスおよびリスクを拡大させました。

2023 年の Rockwell Automation による OT/ICS セキュリティインシデントに関するレポートでは、脅威アクターがエネルギーセクターに狙いを集中させ、インシデントの件数は 2 位となったセクター（重要製造業および運輸）の 3 倍に上ったことが報告されています[30]。

エネルギーセクターに対するダークトレースの調査は、英国および米国におけるエネルギーセクターの脅威ランドスケープについて理解するために次の点に焦点を当てて行われました：

- どのAPTおよび攻撃ベクトルがエネルギー関連組織を狙ったか？
- AIを含めテクノロジーはこの脅威ランドスケープをどのように変貌させたか？
- AIはこのセクターのサイバー防御の性質を変化させたか？
- こうした脅威ランドスケープの変化は政策に反映されているか？そして企業と政府が検討すべき主要な項目は何か？

主な調査結果

- 技術の進歩はサイバーリスクをもたらします。変動性発電である太陽光や風力発電セクターにおけるIoTの導入と制御自動化は、アタックサーフェスの拡大につながり、IT/OT統合はサイバーインシデント発生時の分離を難しくします。
- 少数のベンダーやシステムへの過度な依存や、クラウド運用への動きはさらなる単一障害点を作り出し、また複雑に絡み合ったサプライチェーンがアセットの可視性と管理を難しくしています。
- ダークトレースの調査ではエネルギーセクターにおいてAI駆動の攻撃はまだ確認されていません。
- エネルギーセクターにおいては既に長い間AIが使用されている部分もありますが、データ品質の準備の欠如、データリスク、そしてこのセクターに対する厳しい規制により、セクター全体での導入には至っていません。
- このセクターのステークホルダー達は、内製のAIシステムを開発するためにデータ駆動型に転換する、という課題に直面しています。

意味

- 組織はサプライチェーンに渡る包括的なアセット管理を行い、定期的なリスク評価を実施し、対処計画シナリオの演習をおこなわなければなりません。これらの取り組みはサイロ型であってはならず、セクター全体でのコラボレーションが欠かせません。
- Eメールセキュリティの強化は初期アクセスを減らすためにきわめて重要であり、MFAポリシーの徹底や、インターネットに接続されたデバイスのセキュリティ強化による脆弱性対策が肝要です。
- 政府は国家による攻撃に対する準備と対処を強化し、エネルギーセクター内のサイバー検知と防御のイノベーションに対して資金援助するべきです。

詳細な調査結果は、エネルギーセクターの状況に的を絞った当社のホワイトペーパーで以後報告します。

■ セクターの分析：

ヘルスケア

ヘルスケアセクターでは歴史的にサイバーセキュリティへの投資が欠如していたことから、サイバー攻撃に対してより脆弱であると従来考えられていました。しかし、近年では患者の安全を確保するために、サイバー意識、防御、基準の向上に対して多大な投資が行われています。2024年、英国、米国、ブラジル等の政府はさらなるデジタル変革を支援するための投資を約束しており、その中でも特にサイバーセキュリティは優先分野として挙げられています。

これら3カ国のヘルスケア事業モデルは対照的であり、デジタル変革と政策の拡大レベルも異なっているため、ダークトレースの持つ専門知識を適用する上で理想的なサンプルとなりました。

ヘルスケアセクターに対するダークトレースの調査は、英国、米国、ブラジルにおけるヘルスケアセクターの脅威ランドスケープについて理解するために次の点に焦点を当てて行われました：

- どのAPTおよび攻撃ベクトルがヘルスケア関連組織を狙ったか？
- 2017年のWannaCryランサムウェア攻撃後にこのセクターに対して行われた主要なレビュー以降、脅威ランドスケープはどのように変化したか？
- AIの進化と医療用IoTデバイスの導入拡大が脅威ランドスケープを変化させたか？

主な調査結果

- ランサムウェアは引き続きヘルスケア産業に対する主要な脅威ですが、脅威アクター達はデータ抜き出しを、暗号化よりも直接恐喝に使用することを好む傾向にあります
- ビジネスEメール侵害（BEC）、クラウドアカウント乗っ取り、およびその他の方法のネットワーク侵入が広範に見られます
- 米国の脅威アクターにおいては詐欺が多く見られ、ソーシャルエンジニアリング手法を使って給与システムや会計担当者にアクセスし、銀行口座情報の変更を行おうとします。他の地域におけるBEC攻撃の目的との違い、またデータ収集および第二段階攻撃が伴うことは、米国におけるヘルスケア提供のビジネス指向モデルが反映されていると言えます。そこでは、支払い先情報の交換はよくあることであり、ヘルスケア組織文化としての親切さ、そして支払いできなかった場合の組織運営上、金銭上の影響の大きさなどが、この地域での支払い詐欺の有効性を強化していると思われます。このことは、組織が現在の脅威ランドスケープの状況に加えて運用面およびシステム面のリスクを考慮しなければならないことを表しています。
- 他の地域では機密性の高いデータへのアクセス（おそらく第二段階攻撃への準備として）が観測されました。
- 攻撃者はしばしばサプライチェーンの信頼される関係を悪用しており、これはサプライヤーに対する直接的侵害またはサプライヤーのドメインの「タイポスクワッティング」（似たドメイン名を使用）により行われていました。
- ヘルスケアサプライヤーに対するサイバー攻撃と、ヘルスケアプロバイダーに対する攻撃の数に著しい違いはありませんでした。

詳細な調査結果は、英国、米国、ブラジルのヘルスケアサイバーセキュリティの状況に的を絞った当社の産業別ホワイトペーパーで以後報告します。

■ ダークトレースの行った調査で2024年に最も注目すべき事例：

国家と関連したスパイ活動の発見

2024 年 10 月、ヨーロッパに所在する製造業の顧客のネットワーク内で、国家が背後にあると思われるスパイ活動が展開していました。このオペレーションは非常に的を絞った、かつステルス性の高いものでした。脅威アクターはデータ抜き出しフェーズを開始する前に、数週間あるいは数か月間も休眠状態で潜んでいたものと思われます。データ抜き出しフェーズにおいては、SMB および WMI を介した、高度に偽装した実行形式ファイルのネットワーク内拡散、内部サーバーからの機密情報の的を絞った収集、そして侵害された複数の正当なサイトへの収集した情報の抜き出し、等が行われました。

このオペレーションのデータ抜き出しフェーズで見られた数々の動作が、Darktrace のリアルタイム検知アラート、および Cyber AI Analyst のインシデントイベント発生につながりました。

Cyber AI Analyst はこの疑わしいアクティビティに対して自律的な調査を開始し、個別のイベントをつなぎ合わせました。複数のエンドポイントに対する C2 接続、水平移動、疑わしい SMB 書き込みなど、これらを単独のイベントとして見るのではなく、より大きな侵害インシデントを組み立てます。

これにより、顧客とアナリストの双方が、攻撃の全体像を把握することができます。

このインシデントが終結した後、ダークトレースの脅威調査チームはこのオペレーショの背後にいる脅威アクターについての理解を深めるための調査を継続しました。その証拠の一部は公開することのできない性質のものですが、2 つの違った方向を示していました。中国（PRC）との関係の可能性があるアクターと、北朝鮮（DRPK）との関係の可能性があるアクターです。

DPRK と PRC についての仮説は、標的となった顧客のネットワーク内で観測された証拠に基づいて比較されました。データ窃盗アクティビティの数か月前に標的となった顧客のネットワーク内で観測された ShadowPad 侵入アクティビティは、PRC とのつながりを示す仮説を裏付ける可能性がある証拠と思われましたが、7 月の ShadowPad 侵入アクティビティと 10 月のデータ窃盗アクティビティの間に明確なつながりの証拠は見つかりませんでした。さらに、これらのアクティビティの間のつながりが見つかったとしても、ShadowPad アクティビティの観測から PRC とのつながりを推測することは不確かであった可能性もあります。公開されている証拠はないものの、ShadowPad は PRC 以外の国家に関係したアクターまたは国家以外のアクターによって使用される可能性もあるからです。

顧客ネットワーク内で観測された、DPRK の特徴を持つ動作は、DPRK とのつながりを裏付けるより強い証拠を示していました。このオペレーションのデータ窃盗フェーズで観測された動作には、過去に DPRK が関連した侵入事例で見られた TTP、アーチファクト、C2 インフラと類似した TTP、アーチファクト、C2 インフラが含まれていました [31] [32] [33] [34] [35]。

ダークトレースは、このオペレーションに適用されたリソース、根気、難読化方法、回避策を、外部の報告書、サイバーコミュニティとのコラボレーション、世界の地政学的状況および攻撃者の動機の評価を組み合わせることにより、中程度から高度の確信を持って、おそらく DPRK の可能性の高い国家が関与したものと査定しています [36]。この評価は 10 月のデータ抜き出しアクティビティと 7 月の ShadowPad アクティビティの間のつながりについて疑問を残すものですが、このアトリビューションは大変な作業であると考えられます。

国家と関係のあるアクターはアトリビューションを回避するため、誤認を導くテクニックを使うことが知られており [37] [38] [39] [40]、偽旗作戦の可能性も検討されました。このインシデントをさらに調査するため、ダークトレースの脅威調査チームは世界最先端のサイバーインテリジェンス企業および著名な政府機関とも協調して作業を行い、彼らの専門知識によりさらなる考察も提供されましたが、確定的なアトリビューションには至っていません。

ダークトレース脅威調査チームからの推奨策

変化し続ける脅威ランドスケープの性質、および本レポートでも紹介されている脅威アクターの能力の拡大を鑑み、ダークトレースの脅威調査チームは御社のサイバーセキュリティ体制強化のために以下のアクションを推奨します：

01 **最新情報の取得：**進化する脅威ランドスケープに遅れをとらないこと

02 **リスクベースのアプローチ：**重要データを損失した場合のビジネスへの影響を理解し、リスクベースのアプローチを取り入れること

03 **AIの統合：**ビジネスのさまざまなレベルに対して、どのようにAIが導入されるかを理解し、それに備えること

04 **露出したアセットの識別：**露出したアセットについて定期的な識別と評価を行うこと

05 **エッジデバイスの優先付け：**脆弱性管理プロセスにおいてエッジデバイスに重点を置くこと

06 **サプライチェーンのリスク：**内部、外部の準備度およびクリティカルな攻撃経路を評価することによって、サプライチェーンを理解すること

07 **インシデント対処計画：**インシデント対応計画を定期的に見直しテストすること

08 **ゼロトラストの方針：**ゼロトラストの方針および原則を導入すること

09 **アイデンティティアクセス管理：**堅牢なアイデンティティアクセス管理方針およびテクノロジーの適用を確認すること

10 **早期異常検知：**大きな影響が出る前に、より低レベルの異常をキルチェーンの早い段階で調査すること

組織は、良いサイバー衛生習慣を取り入れ、デジタルエステートをプロアクティブに保護し、エクスプロイトされる前に脆弱性に対処することにより、ますます機会便乗性を強めている脅威アクターからネットワークをより効果的に防御できるようになるでしょう。

コミュニティ利益のための取り組み

サイバーセキュリティプロフェッショナルはしばしば、脅威アクターの動機や戦略的目標を抽象的に説明します。しかしこれらの目的の作戦上、戦術上の現実は常にサイバーセキュリティの範囲を超えたイベントにより形作られます。なかでも、スポーツ、政治、文化などの世界での大きな出来事が、脅威アクターが作戦を展開する機会を作り出しているのです。

2024 年にはこのようなイベントが 2 つありました。パリの夏季五輪と米国の大統領選挙です。

サイバーセキュリティエコシステム内のステークホルダーとして、ダークトレースは知識とスキルを社会のために使用する責任を認識しています。ダークトレース脅威調査チームはこうしたコミュニティ利益の増進を目指すプロジェクトをサポートしています。これらのプロジェクトにはアナリストによる調査と監視により、これらのイベントの参加者と運営者を標的とした悪意の可能性のあるアクティビティを特定する取り組みが含まれていました。

2024 年のパリ五輪と米国の大統領選挙

オリンピックのようなスポーツイベントは脅威アクターが大きな攻撃を仕掛ける格好の機会となります。ダークトレースの脅威調査チームはオリンピックの前および後に分析を行い悪意の可能性のあるアクティビティおよび脅威アクターの活動を調べました。
チームは、APT を含むパリ五輪を標的とした手段と同期を持つすべての潜在的な攻撃者を特定しました。
同様に、2024 年の米国大統領選挙も、国家の支援を受けたグループとサイバー犯罪ギャングの両方にとって特別な機会でした。

ダークトレースの脅威調査チームは、部外秘情報の漏えいや投票データの完全性の毀損につながった攻撃活動は、APT グループを支援しているいくつかの敵対国家の戦略的目的のためであったとみています。アナリストは米国の選挙の混乱を狙ったと思われる APT に関する既存の情報や過去の調査データを集約しました。また、国家安全保障関係機関、およびサイバー脅威インテリジェンス（CTI）企業と協力して関連情報の収集と共有を行いました。

今後も、ダークトレースは引き続き Inside the SOC ブログや英国国家サイバーセキュリティセンター等の政府機関との協力を通じてコミュニティへ貢献してまいります。さらに、セクター別やプロジェクトベースの調査も強化します。

2025 年には、セクター別に的を絞ったレポートを発表する計画で、ヘルスケアとエネルギーセクターから始めます。このレポートには、ダークトレースの脅威調査チームとさまざまな国家機関、CTI 企業、シンクタンク、政府、そして当社の顧客との協力した取り組みが反映されます。

その結果生じる脅威調査とコミュニティプロジェクト間のサイクルが、ダークトレースの専門知識をさらに強化し、他のプロバイダーとのさらなるコラボレーションの実現につながることを期待しています。このモデルは、今後コミュニティパートナーとの関係のひな形として利用できる可能性もあります。ダークトレースの脅威調査チームは 2025 年、そしてそれ以降も引き続き、サイバーコミュニティと社会一般の両方のステークホルダーとの協力関係を維持してまいります。

今後のコミュニティプロジェクトへの参加にご興味がありますか？是非 threatintelligence@darktrace.com までご連絡ください。

参考文献

01 CVE Metrics: https://www.cve.org/about/Metrics

02 CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

03 Pacific Rim:Neutralizing China-Based Threat: https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/

04 Adversarial Misuse of Generative AI: https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

05 CISA Cybersecurity Advisory AA21-201A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

06 Ransomware Statistics: https://www.varonis.com/blog/ransomware-statistics

07 CISA Cybersecurity Advisory AA24-109A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

08 Two Foreign Nationals Plead Guilty in LockBit Ransomware Group: https://www.justice.gov/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group

09 US Charges Dual Russian and Israeli National in LockBit Ransomware Group: https://www.justice.gov/usao-nj/pr/us-charges-dual-russian-and-israeli-national-developer-lockbit-ransomware-group

10 Ransomware Rebrand to Lynx: https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

11 Arctic Wolf:Fog Ransomware: https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/

12 Darktrace Inside the SOC - Lifting the Fog: https://darktrace.com/blog/lifting-the-fog-darktraces-investigation-into-fog-ransomware

13 SentinelOne - Fog Ransomware: https://www.sentinelone.com/anthology/fog/

14 ESET Threat Report H2 2024: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf

15 RansomHub Ransomware: https://blackpointcyber.com/resources/threat-profile/ransomhub-ransomware/

16 RansomHub Actors Exploit Zerologon Vulnerability: https://www.darkreading.com/cyberattacks-data-breaches/ransomhub-actors-exploit-zerologon-vuln-in-recent-ransomware-attacks

17 CISA Cybersecurity Advisory AA24-242A: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

18 Meet RansomHub: https://www.s-rminform.com/latest-thinking/meet-ransomhub

19 Mexico President Hacking Attack: https://apnews.com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f-71d2af3d67c8

20 Russian Gang Hacks Scottish Housing Charity: https://www.thetimes.com/uk/scotland/article/russian-gang-hacks-one-of-scotlands-largest-housing-charities-j7spkmmrv

21 Ransomware Groups: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-groups

22 Ransomware on the Move:BlackBasta, Fog, KillSec, RansomHub: https://www.halcyon.ai/attacks-news/ransomware-on-the-move-blackbasta-fog-killsec-ransomhub

23 RansomHub: https://www.sentinelone.com/anthology/ransomhub/

24 Ransomware Spotlight:RansomHub: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub

25 ShadowPad:A Masterpiece of Privately Sold Malware in Chinese Espionage: https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

26 Heightened Threat of State-Aligned Groups: https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

27 Defending OT Operations Against Pro-Russia Hacktivist Activity: https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity

28 Dragos FrostyGoop ICS Malware Intel Brief: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf

29 Top 25 Security Predictions for 2025 (Part 2): https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-25-security-predictions-for-2025-part-2

30 Cyberattacks Against Critical Infrastructure on the Rise: https://www.rockwellautomation.com/en-us/company/news/press-releases/New-Research-Finds-Cyberattacks-Against-Critical-Infrastructure-on-the-Rise-State-affiliated-Groups-Responsible-for-Nearly-60.html

31 Lazarus Luring Employees with Trojanized Coding Challenges: https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

32 ZINC Attacks Against Security Researchers: https://www.microsoft.com/en-us/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

33 Lazarus Initial Access Tradecraft Using Social Media: https://www.nccgroup.com/es/research-blog/north-korea-s-lazarus-their-initial-access-trade-craft-using-social-media-and-social-engineering/

34 ZINC Weaponizing Open Source Software: https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

35 Lazarus Malware: https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

36 Joint Cyber Security Advisory: https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/1/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF

37 Frequent Freeloader Part I:Secret Blizzard Compromising Storm-0156 Infrastructure: https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

38 Frequent Freeloader Part II:Russian Actor Secret Blizzard Using Tools of Other Groups: https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/

39 ChamelGang Attacking Critical Infrastructure with Ransomware: https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/

40 State-Backed Hackers Using Ransomware: https://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html

■ **ダークトレースについて**

ダークトレースはAIサイバーセキュリティのグローバルリーダーであり、日々変化する脅威ランドスケープに立ち向かう組織を支援しています。2013年に英国ケンブリッジで設立されたダークトレースは、それぞれのビジネスからリアルタイムに学習するAIを使用して未知の脅威から組織を保護する、必要不可欠なサイバーセキュリティプラットフォームを提供しています。ダークトレースのプラットフォームおよびサービスは2,400名を超える従業員により支えられ、世界でおよそ10,000社の組織を保護しています。より詳しい情報については、http://www.darktrace.com/jaをご覧ください。

北米：+1 (415) 229 9100　ヨーロッパ： +44 (0) 1223 394 100　日本： (03) 5456 5537　ラテンアメリカ：+55 11 4949 7696

darktrace.com/ja | japan@darktrace.com