OTセキュリティに関する調査レポート2023

～リアルな脅威を理解して、効果的な対策を打つために～

この資料は Dragos 社による OT サイバーセキュリティの 2023 年レビュー (原文：OT Cybersecurity THE 2023 YEAR IN REVIEW) であり、OT サイバーの最新動向を伝えるため極力原文通りに翻訳しています。OT サイバーセキュリティ対策の参考になれば幸いです。

株式会社マクニカ　OT サイバーセキュリティ技術チーム

MACNICA

FEBRUARY 2024

DRAGOS

目次

イントロダクション
INTRODUCTION

2023年、国際情勢の緊張により世界中のサイバー脅威活動が増加し、重要インフラの混乱が起きました。ウクライナとロシア、イスラエルとハマス、南シナ海の国々など、衝突がエスカレートする中、サイバー攻撃グループやハクティビストによる新たな攻撃法の開発、古い手法の再利用が盛んになりました。ランサムウェア攻撃は多くの産業組織に影響を与え、報告されたインシデント数は年間で約50%増加しました。(企業など組織の)アセットオーナーは、これらの脅威の犠牲者とならないよう、必要な予防措置をとらなければなりません。

組織が考慮すべき脅威には、紛争地域で開発された能力が含まれます。ロシアによるウクライナ侵攻以降、周辺国でのサイバー脅威活動はエスカレートしています。Dragos社とコミュニティは、ウクライナの重要インフラに対するサイバー作戦を担う脅威グループ**ELECTRUM**による、新たな破壊型マルウェアの存在を確認しました。物理戦とサイバーをミックスした軍事活動は、増加する世界の脅威の新たな試験場となっています。

中東で勃発した紛争には、重要インフラへのサイバー攻撃も含まれていました。親イスラエルのハクティビストは、イランにあるガソリンスタンドへの攻撃を担い、その70%以上を混乱させたと主張、一方、親ハマスのハクティビストは、イスラエル製OT[1]ハードウェアとソフトウェアを標的にしました。これら産業機器への攻撃がもたらす影響は、紛争地域を超えて世界中の製造業や水道事業など様々なセクターに及びました。

年間を通じて、Dragosは脅威グループ群の能力開発とアクセス権獲得の状況を追跡してきました。中国と台湾の緊張が高まる中、脅威グループ**VOLTZITE**がアジア太平洋地域、アフリカ、北米にある複数の産業組織を標的にしたことが観測されました。電力、衛星通信、電気通信、緊急管理、防衛産業基盤セクターの事業者に対し、長期的なスパイ活動を目的としたサイバー攻撃が行われています。**VOLTZITE**の活動は米国の電力事業者、電気通信、GIS(地理情報システム)にも向けられており、将来的に破壊的あるいは混乱をもたらすサイバー攻撃で利用可能な、国家の重要インフラに関する脆弱性の特定を明確な目的としています。Dragosは、新しい3つの脅威グループを含め、産業組織を狙う21の脅威グループを追跡しています。

脅威グループとハクティビストは2023年の重大リスクですが、多くの組織にとって一番の懸念はランサムウェアでした。これは、ランサムウェア攻撃そのものが増加したことに加え、Dragosが実際のインシデントで観測した産業への影響からも明らかです。さらに、(ランサムウェア被害に関する)新たな報告要件により、多くの組織がインシデント対応に焦点を当てるようになりました。米国、ヨーロッパ、オーストラリア、アジア、中東での規制の変更により、組織は報告義務を満足するためのケイパビリティ獲得が必要となりました。2023年においてDragosは多くの演習をより幅広い参加者と産業に対して提供しました。

組織にとってもう一つの主要な焦点は、報告された脆弱性がどんなリスクをもたらすのか、最善の対応は何かを理解することでした。2023年には、脆弱性情報(アドバイザリ)が14%増加しましたが、Dragosが分析したアドバイザリの31%に誤ったデータが含まれていました。また2023年は、Rockwell AutomationのControlLogix通信モジュールに影響を与える重大な脆弱性が発見されました。これは脅威グループ**XENOTIME**がTRISIS攻撃で悪用したゼロデイと類似しています。一方この発見と対応は、ベンダー、政府、Dragosコミュニティの連携によるリスクベースの対応の良い例となりました。

OTサイバーセキュリティ・コミュニティの主要トレンドを伝えるため、Dragosは本レビューを開始しました。今年のレポートは、最新のデータ、現場からの視点を実務家やリーダーに提供することにより、より良い形で世界の重要インフラを守ることを目指しています。産業に対するサイバー脅威に対し、組織が効果的に防御を行い対応できるよう、実証済みの洞察を提供することに主眼を置いています。

[1] OT: Operational Technology - 運用制御技術。物理的な装置や工程を監視・制御・運転するハードやソフトのテクノロジー。

産業に対するサイバー脅威活動の高まり

THE RISING TIDE OF INDUSTRIALCYBER THREAT ACTIVITY

Dragos Platform[2]は、**OT Watch**[3]と**Neighborhood Keeper**[4]のデータを通じて可視性と洞察を提供します。Dragosの脅威インテリジェンスチームは、脆弱性を調査・評価し、OTに影響を与える攻撃者を積極的に追跡しています。またDragosのコンサルタントやレスポンダーは、アセスメント、演習、インシデント対応などから得られる最前線の視点を提供しています。Dragosが2017年に初めて年次レビューのためのデータ収集を開始して以来のトレンド、そのマイルストーンが明確になっています。このレポートで提示されているデータと視点は、Dragosがサポートするグローバルな産業に焦点を当てています。

2016年 – CRASHOVERRIDE

CRASHOVERRIDEマルウェアは、2016年に初めて電力変電所を攻撃する最初の悪意のあるコードとして使用されました。大規模な電力システムを保護するよう設計された施設と設備に対し、保護とは逆の作用を与えるよう改変されていました。**CRASHOVERRIDE**の実績は、2022年10月まで観測されていた**INDUSTROYER2**マルウェアによる一連のサイバー攻撃に引き継がれています。

2017年 - TRISIS

脅威グループ**XENOTIME**は、サウジアラビアの石油化学プラントの安全計装システム（SIS）に対して**TRISIS**マルウェアを展開しました。**TRISIS**は、マルウェアの実行ターゲットと実行方法を拡張可能であり、システムの安全機能を狙って直接侵害します。

2018年 - 脅威グループの拡大

2018年、Dragosは追跡する脅威グループの数を3から8に広げました。この傾向は続いており、現在までに、OT環境へのアクセスを取得し、それらを混乱させることを目的とした21のDragos指定脅威グループがあります。

2019年 - OTにおけるランサムウェアの増加

2019年、OT領域でのランサムウェア被害が50%増加したことを確認しました。Dragosが対応した電力セクターにおける最初のランサムウェア・インシデントも2019年に発生しています。

2020年 - EKANSランサムウェア

Dragosは**EKANS**マルウェアの亜種を分析しました。これは暗号化を開始する前にICS関連のWindowsプロセスを停止する能力を持ち、懸念すべき結果を引き起こします。ランサムウェア・グループにとって、ビジネス妨害は身代金が支払われる可能性を高めます。

2021年 - ランサムウェア攻撃がOTに影響を与える

2021年、コロニアルパイプラインはランサムウェアの影響を受け、予防的観点からOTの運用が停止しました。その後ランサムウェアの事案は膨れ上がり、2023年は905件と前年比でほぼ50%増加しました。

2022年 - CHERNOVITEの登場

2022年、Dragosは**CHERNOVITE**脅威グループを発見しました。このグループは、高い動機と豊富な資金を持ち、ソフトウェア開発手法を熟知し、産業制御システム（ICS）の侵入技術に精通した高度なスキルを持つ存在です。彼らは**PIPEDREAM**マルウェアの開発者でもあります。

2023年 - 脅威動向の変化

高まる緊張と経済機会は、ハクティビスト、犯罪組織、新たにDragosに指定された3つの脅威グループを含むさまざまなアクターが産業環境を標的にする原動力となりました。

[2] Dragos Platform：OT向けのセキュリティ監視ソリューション。OTネットワークにセンサーを導入して通信を監視し、脅威を検出する。
[3] OT Watch：Dragos Platformの検知情報を遠隔で監視するサービス。
[4] Neighborhood Keeper：Dragos Platform利用組織における検出情報を匿名集約し、解析結果を業界への攻撃動向や対策情報として再共有する集団防衛サービス。

重要なポイント：行動を促す

KEY HIGHLIGHTS: INSPIRING ACTION

2024年は、重要システムの外部公開インフラに対してアセスメントを実施すべきタイミングです。これには、インターネットへルーティング可能なネットブロックやIPスペースを特定することや、請負業者やベンダーが設定していったものも含まれます。公開スペースをネットワークスキャンし、Shodan、Whois、およびドキュメントと比較します。インターネットからは、重要なアセットやプロセス環境に接続されたアセットが発見できないようにすべきです。10-11ページに掲載した、CyberAv3ngersによるUnitronics（ユニトロニクス）製PLCデバイスへの2023年の攻撃に関する詳細が参考になります。

ネットワークのセグメント化をしていない場合、最適な時期は2000年代でしたが、次に最適な時期は今です。ネットワークセグメンテーションには、デバイスの機能に応じたネットワーク分離、ホストベースのファイアウォールによる分離が含まれます。インターネットからの分離だけでなく、システム同士や重要プロセスからも分離します。IPv4にだけ焦点を当てるのではなく、システムがIPv6も使用しているか注意してください。オペレーターが仮想プライベートネットワーク（VPN）、リモートデスクトッププロトコル（RDP）、または他のリモートアクセスツールを使用してログインしネットワークゾーンを横断する場合は、別個の認証を利用するべきです。2023年におけるOT環境へのランサムウェアの増加により、この古くても依然として有用なガイダンスの必要性が強調されました。ランサムウェアに関する詳細は22ページを参照してください。

セグメンテーションに加えて、外向き通信の制限と監視も重要です。これには、デフォルトルート、ゲートウェイ、外部ネットワークやプロキシ設定のファイアウォールルールの評価が含まれます。2023年には、**VOLTZITE**、**GANANITE**、ランサムウェア・グループなどの複数の攻撃者が、コマンド&コントロール（C2）のために外部ネットワークとの通信を利用することで、データの流出やネットワークアセットのリモート制御を実現しました。これに関しては、このレポートの「OTサイバー脅威動向 OT CYBER THREAT LANDSCAPE」セクションを参照してください（9ページ）。

既に標準ガイドに沿って定期監査（セグメンテーションのルールや設定の評価など）を実施している場合、更にやるべき仕事があります。防御アーキテクチャが成熟するにつれて、攻撃者のテクニックも変化します。Dragos最前線の視点セクションでは、OTアセスメントでDragosのペンテスターが活用する技術を学び（21ページ）、ランサムウェア・グループ（22ページ）や脅威グループ（12ページ）では、どのような技術がまだ機能しているかを学んでください。アタックサーフェースの理解は、対応の優先度付けや、ネットワーク内に侵入した攻撃者を識別するために不可欠です。これらの知識を用いモニタリングシステム上で証拠を探すことは、OT環境に潜む望まれざるオペレーターを特定する最善の方法です。

最後に、OTプロセスで使用される脆弱な機器のリスク軽減を、体系的な手法で行うことです。2023年、Dragosは531件のOT関連の脆弱性アドバイザリ、2010件の脆弱性に対する優先順位付けと緩和ガイダンスを作成しました。脆弱性からの主な洞察、トレンド、緩和策については、27ページで詳しく読んでください。

ロックウェル・オートメーションの脆弱性から学ぶ

LEARNING FROM ROCKWELL AUTOMATION VULNERABILITIES

2023年、米国政府は、ControlLogix通信モジュールの一部に影響を与える2つの脆弱性について、ロックウェル・オートメーションに通知しました。これらの通信モジュールは、ロックウェル・オートメーションの重要な製品ラインの一部であり、多くの産業分野でプロセス制御を担っています。ロックウェル・オートメーションは、政府パートナーと協力して、Dragosを含むさまざまなベンダーから成る防御的なワーキンググループを組織しました。ワーキンググループの目標は、これらの脆弱性の検出方法を開発し、攻撃の証拠を探すことでした。

ワーキンググループの一環として、Dragosのアナリストは脆弱性と影響を受けた通信モジュールを調査しました。ロックウェル・オートメーションや他のコミュニティメンバーと共に、悪用可能な各手法と関係するアーティファクトに対して警告を発する検知シグネチャを開発しました。Dragosの脆弱性アナリストは、これらのシグネチャをNeighborhood KeeperとOT Watchに展開して、悪意のある活動の兆候を見つけました。アラートをトリアージし、誤検知に注意を払い、シグネチャを適切に調整しました。

Dragosのアナリストは、検出結果をワーキンググループに渡し、コミュニティの他のメンバーがそれぞれのプラットフォームに対してシグネチャを調整できるようにしました。このようにして、Neighborhood Keeperは、検出と脆弱性が公になった後に不必要な警告を避けるのに役立ちました。シグネチャの調整以外にも、Neighborhood Keeperは、脆弱なデバイスの数や、それらが異なる産業や地域でどれだけ広く使用されているかを示す可視性を提供します。Dragosはこの情報をワーキンググループに返し、彼らが脆弱性のリスクと潜在的な影響を評価できるようにしました。

米国政府とロックウェル・オートメーションが、セキュリティベンダーとワーキンググループを作り、公開前に防御戦線を構築できたこと、そして脆弱性情報の公開をコーディネートできたことは、産業制御システム（ICS）コミュニティにとって重要な成果です。ロックウェル・オートメーションの事例は、製品のオーナーや製造元（OEM）にとって、防御に向けた実践とコミュニティの優れた参考例であり、脆弱性公開までの道筋として検討に値します。米国政府の情報、セキュリティ業界の専門知識、OEMの知識を融合するこの新しいアプローチは、この先、重要インフラに対するサイバー攻撃者の脅威と戦うためにとるべき道です。

Dragos最前線の視点：脆弱性

ロックウェル・オートメーションと米国政府は、以下の2つの脆弱性を公表しました：

CVE-2023-3595:
この脆弱性は1756 EN2および1756 EN3製品に存在し、悪意のあるユーザーが改ざんしたCIPメッセージを用いることで、ターゲットシステム上での持続的なリモートコード実行を可能にします。

CVE-2023-3596:
この脆弱性は1756-EN4*製品に存在し、悪意のあるユーザーが改ざんしたCIPメッセージを用いることで、サービス停止を引き起こすことを可能にします。

Dragos最前線の視点

DragosのOT Watchの顧客とNeighborhood Keeperの参加組織は、この脅威が公表される前から、モニタリングによって防御されました。このような状況が再び起こった場合でも、Dragosのコミュニティディフェンスプログラムに参加するメンバーは、最新の脅威モニタリングによる恩恵を得られます。

13%

ロックウェル・オートメーションのアセットの**13%**は、製造、製紙・パルプ、自動車、鉱業、化学、食品飲料、電気、石油・ガスなどの分野で使用されているControlLogix通信モジュールでした。

数字で見るハイライト

KEY HIGHLIGHTS: BY THE NUMBERS

Threat Group Highlights – 2023

21 Total Threat Groups

10 Active Threat Groups

3 New Threat Groups

Key Vulnerabilities Findings

80%

of vulnerabilities **reside deep within the ICS network.**

16%

of advisories were **network exploitable and perimeter facing** in 2023.

53%

of the advisories that Dragos analyzed **could cause both a loss of view and loss of control,** up from 51% last year.

31%

of advisories **contained errors** in 2023.

49%

Dragos provided mitigations for 49% of the advisories that had none.

DRAGOS
SAFEGUARDING CIVILIZATION

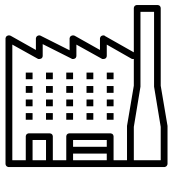
Key Ransomware Findings

↑ **50%**

Ransomware attacks against industrial organizations **increased 50 percent** over last year.

28%

Dragos tracked **28% more ransomware groups** impacting ICS/OT in 2023.



70%

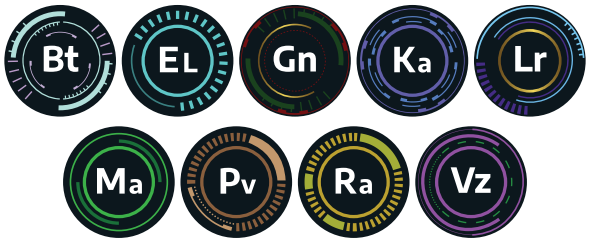
of all ransomware attacks targeted **638 manufacturing entities** in **33 unique manufacturing subsectors**.

2023 Dragos Threat Groups Summary

Three new threat groups: **GANANITE, LAURIONITE** and **VOLTZITE**

10 active threat groups: **BENTONITE, ELECTRUM, GANANITE, KAMACITE, LAURIONITE, MAGNALLIUM, PETROVITE, RASPITE, TALONITE** and **VOLTZITE**

ELECTRUM demonstrates Stage 1 & 2 aspects of the ICS Cyber Kill Chain



9 threat groups demonstrate at least Stage 1 of the ICS Cyber Kill Chain: **BENTONITE, ELECTRUM, GANANITE, KAMACITE, LAURIONITE, MAGNALLIUM, PETROVITE, RASPITE,** and **VOLTZITE**

2 threat groups, **ERYTHRITE** and **COVELLITE**, were retired in 2023. **11 threat groups** were dormant

Threat Group Statistics from 2022 Year in Review:

2 new threat groups: **BENTONITE** and **CHERNOVITE**

8 active threat groups: **BENTONITE, CHERNOVITE, ELECTRUM, ERYTHRITE, KAMACITE, KOSTOVITE, WASSONITE** and **XENOTIME**

OTサイバー脅威動向

OT CYBER THREAT LANDSCAPE

OTサイバー脅威の様相は2023年も進化を続けました。グローバルで生じた衝突によって、追跡対象の脅威グループの数、ランサムウェア被害、その他の脅威活動が増加しました。これらの活動に関与する攻撃者は、その洗練度合い、行使可能な能力、狙う対象などが広く異なっています。広がりの一端では、一部の脅威グループが高度な技術を使用し、偵察活動や情報収集のためにLOTL[5]（環境寄生型）テクニックを含む環境ネイティブな機能を活用しました。一方、一部の攻撃者は、インターネットにアクセス可能で且つ適切なハードニングが施されていないデバイスなど、低い場所にぶら下がる果実を標的とし、これらのデバイスに容易に被害を与え運用停止を引き起こすことが可能でした。

脅威グループは、公開された脆弱性を利用し続け、また、独自の能力を見出し開発しています。観測された脅威活動の大半において、Sierra WirelessモデムやCitrixなど広くOT環境で利用されるIT寄りの機器が標的にされました。2023年、Dragosは戦略的パートナーの1つロックウェル・オートメーションと協力し、OTデバイスを標的として攻撃者が仕込んだ一連の脆弱性について、コミュニティによる対応を行いました。特定された脆弱性により、視認性の喪失/拒否（T0829、T0815）、制御の拒否/操作（T0813、T0831）、運用情報の盗難（T0882）、生産性と収益の損失（T0828）が発生する可能性があります。

紛争に関連する脅威活動

CONFLICT-DRIVEN THREAT ACTIVITY

2023年におけるOTサイバーセキュリティの脅威は、これまで以上に世界や地域で起こる活動と重なっていることが明らかになりました。幅広い能力を有するサイバー攻撃者が、ウクライナ-ロシア間、イスラエル-ハマス間の衝突を利用して重要インフラを狙う作戦を主導しました。また、より未熟なハクティビストの場合、同じ紛争を利用してパニックを引き起こし、重要サービスのレジリエンスについて公衆の認識にネガティブな影響を与えました。アジアやアフリカなど世界中の地政学的な緊張も、情報収集やサイバー攻撃力の建付けが進む要因となりました。

ウクライナ・ロシアの紛争は、**ELECTRUM**など成熟度が高い脅威グループの活動を促進し、ウクライナの重要インフラ機関に対する標的型サイバー作戦につながりました。**ELECTRUM**に帰属する新種の破壊型ワイパーマルウェアが2023年6月にフィールドで観測されました。2023年9月、Dragosは**ELECTRUM**および**KAMACITE**が関与する、ウクライナの重要インフラ機関に対するスピアフィッシングキャンペーンについて報告しました。更に2023年11月には、サイバーセキュリティベンダーが2022年10月に発生したウクライナの電力関連施設を標的とした破壊型マルウェアの活動の証拠を提供する報告書を公表しました。Dragosは、**ELECTRUM**が2022年10月の破壊型マルウェア活動を実施したと見積もりましたが、信頼度は中程度でした。

複数の情報源によると、中国と台湾の緊張が高まる中、アジア太平洋地域とアメリカ合衆国の複数の産業組織に対する標的型サイバー諜報攻撃が増加しています。特に**VOLTZITE**という脅威グループは、少なくとも2021年

[5] LOTL：Living off the Land – 不正アプリなどを使わず、対象環境が備えているツール、コマンド、機能を利用して偵察や攻撃を行う手法。自給自足型、環境寄生型、とも呼ばれる。

以降、グアム、アメリカ合衆国、および他の国々の数多くの重要インフラ機関を標的としています。**VOLTZITE**は、米国政府が中華人民共和国との関係性を公言したVolt Typhoonと重なっています。**VOLTZITE**はLOTLテクニックを積極的に使用し、実例として、被害者のネットワーク内で「手の込んだ」攻撃行動を行っていることが観測されています。

VOLTZITEは、米国の電力および通信セクターに関心を持ち続けており、複数の電力機関における長期に及ぶ偵察活動からもそのことが裏付けられます。**VOLTZITE**が一旦ターゲットのネットワーク境界に初期の足場を築くと、その後、被害者の情報技術（IT）ネットワークにさらに侵入し、その後被害者のOTネットワークに横展開する可能性があります。Dragosの観測では、**VOLTZITE**の行為はICSサイバーキルチェーンの第1段階達成に留まっています。ICS/OTのアセットや運用に対する妨害や破壊などの行動や能力は確認されていません。

Dragosは保有するインテリジェンスを活用し、顧客環境およびコミュニティ内をハンティングしています。これは、**VOLTZITE**脅威グループに関係する侵害インジケーター（IOC）、行動戦術（タクティクス）、技術（テクニック）、および手順（プロシージャ）の追跡と分析にも活用されました。その重要な成果として、Dragosプラットフォームを利用する顧客環境において、信頼性の高いインジケーターを発見できたこと、顧客のインシデントレスポンスをOT Watchが効果的に支援したこと、**VOLTZITE**の侵害インジケーターおよび関係する実際の振る舞い（リモートデスクトッププロトコル（RDP）の使用やサーバーメッセージブロック（SMB）ディレクトリトラバーサルの兆候）をDragosインテリジェンスとして提供できたことが挙げられます。別の興味深い発見として、**VOLTZITE**はMiraiボットネットに関連する攻撃インフラとも重なります。**VOLTZITE**とは別の活動集団も存在し、これらは運用上連携している可能性があります。

Dragos最前線の視点

LOTL（環境寄生型）とは、被害者のホストやネットワークが備えている正規の機能を悪用することを指します。情報技術（IT）の世界では、これはPowerShellやサーバーメッセージブロック（SMB）などのネイティブなシステム機能を攻撃の一部として使用することを意味します。OTの世界では、これはPLCや制御システムのネイティブ機能を使用して制御コマンドを発行することを意味します。

Dragos最前線の視点

Dragosは、Volt TyphoonとDragosが追跡する脅威グループ**VOLTZITE**の間で複数の運用上の重複を観測しています。Electric Information Sharing and Analysis Center（E-ISAC）[6]との共同作業により、2023年11月から12月、北米の電力セクター組織への**VOLTZITE**によるスキャン活動が確認されました。重要インフラ分野に対し**VOLTZITE**が持続的な関心を持って活動しており、ICS/OT組織による監視と備え重要です。

Dragosによる分析から、**VOLTZITE**の活動はグローバル電力セクターのネットワークに対して継続して高い関心を示すものであり、そこで操業を行う組織を横断した警戒の必要性を示しています。さらに**VOLTZITE**が実行する長期間の監視とデータ収集活動は、Volt Typhoonの目的であるアジア太平洋地域における偵察と地政学的優位性の獲得とも一致しています。

2023 年を通じて、ハクティビスト、その他の洗練されていない日和見主義的な脅威グループは、さまざまな業界組織や重要インフラに対して広範囲にわたる分散型サービス拒否 (DDoS) 攻撃を実施しました。「CyberArmyofRussia_Reborn」など親ロシア派グループは、2023 年 5 月にヨーロッパの産業組織を攻撃しました。
「NoName057(16)」は、ヨーロッパおよび北大西洋条約機構 (NATO) 加盟国とその製造および輸送組織を攻撃しました。さらに、「Anonymous Sudan」による米国や他のNATO加盟国への攻撃も観察されました。
「CyberAv3ngers」や「Team Insane Pakistan」などの親ハマス系ハクティビスト集団でも同様の活動が観察されており、スラエルの鉄道、イスラエルの町の送電網システム、イスラエルの水力発電所に対する破壊的攻撃を主張しています。

[6] E-ISAC 米国の電力ISAC https://www.eisac.com/s/

2023年12月下旬、ハクティビスト集団「Predatory Sparrow」が不特定のサイバー攻撃でイランのガソリンスタンドを混乱させたとされています。

これらの作戦には、11月下旬のユニトロニクス製デバイスへの攻撃で観測されたように、公開されたOTデバイスに対する侵害の成功も含まれていました。「CyberAv3ngers」（サイバーアベンジャーズ）は、インターネットからアクセス可能なユニトロニクス製PLCデバイスを使用し、多数の米国、ヨーロッパ、オーストラリアの産業組織を侵害しました。Dragosは、この攻撃者がオープンインターネットをスキャンし、公開されているユニトロニクス製デバイスを特定、その後、ユニトロニクス製デバイスのデフォルトパスワードを使用してログインを試みる、と見積もっています。この攻撃者はOTを処理する能力を持っていないようですが、この攻撃は視認性と制御の損失をもたらしました。

Dragos最前線の視点

ハクティビストのDDoS攻撃は最小限の影響しかなく、主に組織のウェブサイトを妨害しました。多くの場合、重要インフラに対する妨害攻撃の主張が大げさにされているか、完全に捏造されていることをDragosは発見しました。ほとんどのハクティビストグループは、悪名を得たり、誤情報を広めたり、恐怖、不安、疑念（FUD）を引き起こしたり、地政学的および社会的な問題に国際メディアの注意を引き付けることを目指しています。

Dragos最前線の視点

Dragosはインターネットに公開されている1,800以上のユニトロニクス製デバイスを特定しましたが、Neighborhood Keeperが監視しているアセットのうちユニトロニクスのものは0.0001%しかありませんでした。Dragosは、ユニトロニクス製デバイスが、例えば遠隔地や小規模な組織といった視認性の限られた環境でよく用いられる、と中程度の自信を持って評価しています。この種のデバイスは、適切な視認性やハードニングなしに展開されることがよくあります。攻撃活動を阻止するためには、アクセス可能な公開アセットを把握することも含めた、基本的なハイジーンとデバイス管理が重要でです。

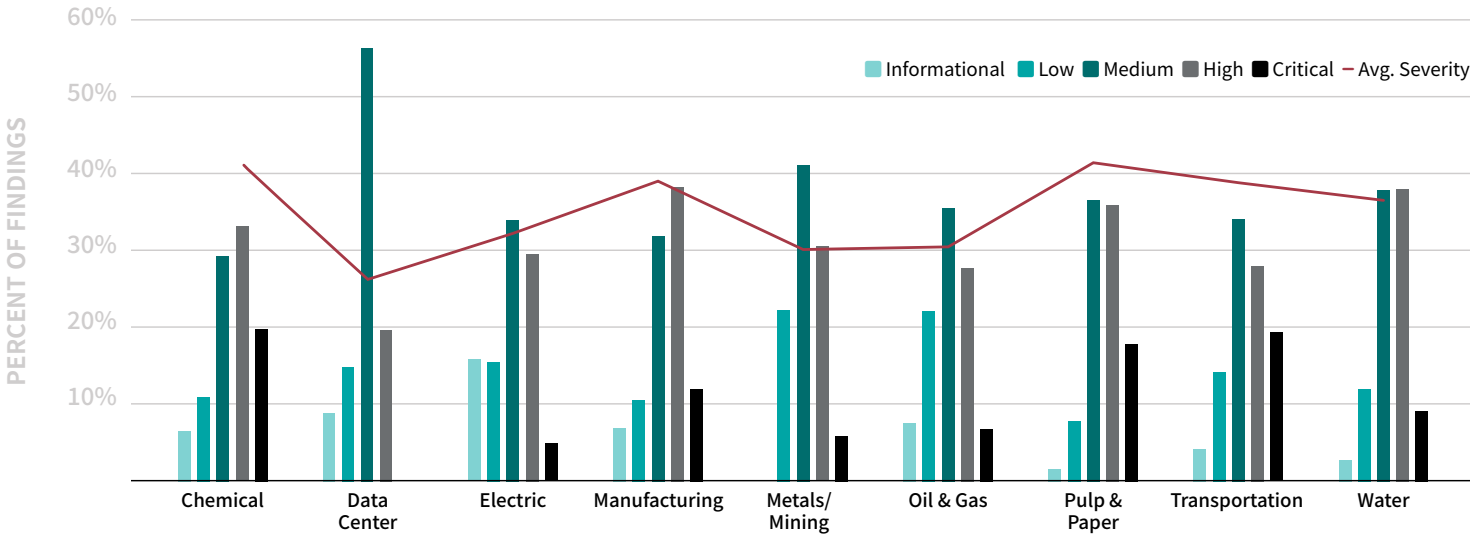


Figure 1: Findings Severity per Vertical

新しい脅威グループの活動
NEW THREAT GROUP ACTIVITY

2023年には、Dragosは10の活発な脅威グループを観測しました。これには、Dragosが新たに特定した3つの脅威グループ**GANANITE**、**VOLTZITE**、**LAURIONITE**が含まれます。これらの新しい脅威グループは、主に長期の偵察と知的財産の窃盗作戦を行っています。この3つのうち、**VOLTZITE**が重要インフラ組織を標的にして最も活発でした。Dragosは、**VOLTZITE**、**GANANITE**、**LAURIONITE**がICSに特化した能力を利用していることを特定していませんが、重要インフラセクターに持続的な関心と活動を示しており、ICS/OT組織による監視と準備が必要です。

Dragosは、これらの3つの脅威グループが、サイバーセキュリティ調査企業、政府および軍事防衛機関、鉄道、製造業、自動車業界、公益事業など、さまざまな組織に対して多様な作戦を実施していることを観測しました。**GANANITE**と**LAURIONITE**は、初期アクセスの実行において日和見主義的なアプローチを示しますが、**VOLTZITE**の活動は、アジア太平洋地域と米国、特に電力セクターにおけるスパイ活動と偵察の目的を強く示しています。

これら新しく特定された3つの脅威グループは、被害組織が使用または所有する公開インフラを標的とし侵害する能力を持っています。標的となるのは、公開インターネット向けのSierra Wireless Airlinkデバイス、Fortinet FortiGate、VPNインフラストラクチャ、およびOracle eBusiness Suite iSupplier Web Servicesなどです。

Dragos最前線の視点

GANANITEや**LAURIONITE**を含む脅威グループは、成熟度が低い環境を有するセクターを標的としています（運輸、製造、水道公益事業など）。Dragosはアセスメントにおいて、発見した所見の数と重大度（セベリティ）に基づきセクターの成熟度を評価します。そのセクターの組織は、示されるリスク上昇について理解すべきです。脅威グループは、特定のMITRE ATT&CKテクニックを使用していることが観測されています。DragosはこれらのTTP（Tactics, Techniques, and Procedures）を使用し、脅威アクターの行動と現場の観測を相関させます。

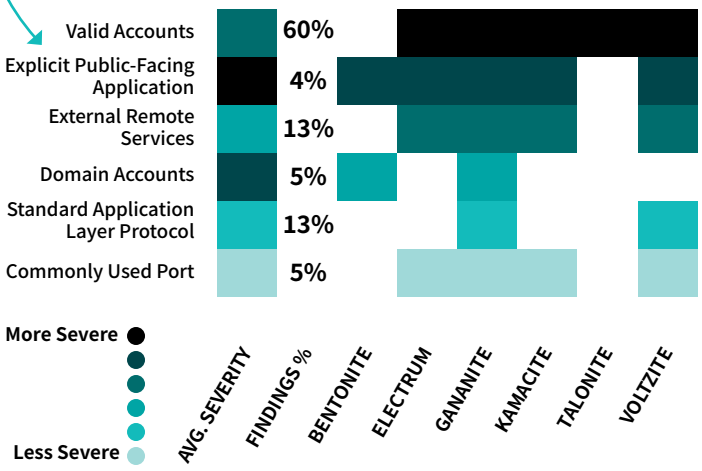


Figure 2: Findings and MITRE TTPs by Threat Groups Using Public Exploits

Dragos最前線の視点

Dragosが2023年に観測した4つの脅威グループに共通する攻撃手法は、外部公開されているデバイスや外部サービスを悪用することです。この手法に対する防御可能なアーキテクチャには、多層防御、MFA（Multi-Factor Authentication）による安全なリモートアクセス設定、およびセキュリティ監視が含まれます。

20%

Dragos issued findings related to externally facing networks such as the internet in 20 percent of engagement reports.

28%

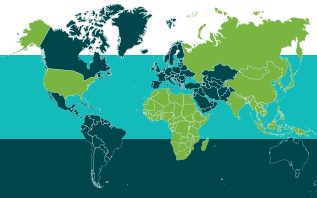
Dragos found inadequately configured firewalls protecting OT environments in 28 percent of engagements in 2023.

VOLTZITE

VOLTZITEは、Dragosが追跡する脅威グループであり、米国CISA（U.S. Cybersecurity and Infrastructure Security Agency）とMicrosoftが2023年5月に最初に報告したVolt Typhoonと運用上の重なりを持つ脅威グループです。米国の複数の電力会社に対する偵察や探索活動を行い、電力送電・配電、緊急サービス、通信、防衛産業基地、および衛星サービスを標的にしていることが観測されました。**VOLTZITE**の行動は、米国の電力施設、通信、およびGISシステムに対する明確な目的を示しており、将来的に破壊的または混乱をもたらすサイバー攻撃で利用できる国の重要インフラ内の脆弱性を特定することを意味しています。**VOLTZITE**は従来、米国の施設を標的にしてきましたが、アフリカや東南アジアの組織を標的にするという情報もあります。
このグループは、検知と対応が困難なLOTLテクニックを頻繁に活用します。この戦略は、ゆっくりと着実な偵察と組み合わされ、**VOLTZITE**がセキュリティチームによる検知を回避することを可能にしています。

被害と影響 Impact and Implications
VOLTZITEは、被害者のインターネットに面したアセットに対して、検知される可能性を減らすためにゆっくりと持続的に探索活動を行います。一度被害者のインターネットに面したアセットを悪用すると、彼らはLOTLテクニックを一貫して使用するため、防衛者にとって検知がより困難になります。**VOLTZITE**の2023年の行動は、スパイ活動と情報収集という作戦上の目標を示唆しています。OTネットワークから盗まれたデータは、重要な工業プロセスの意図しない中断をもたらす可能性があるか、あるいは後続の攻撃ツールの開発やICSネットワークへの攻撃を支援するための重要な情報を攻撃者に提供する可能性があります。

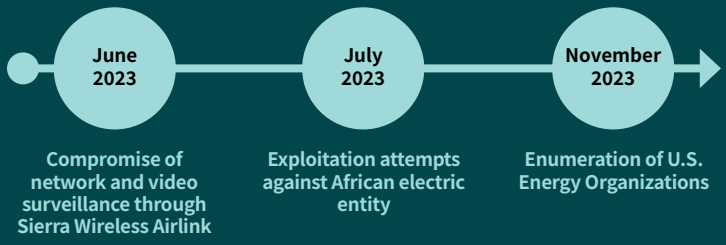
TARGETS: UNITED STATES, ASIA, AFRICA



主なポイント

- LOTLテクニックを頻繁に活用することで、悪意のある活動が特定される可能性を無くす。
- 検知回避およびスパイ活動に必要なセキュリティ技術に高度に集中した、攻めの作戦を実行する。
- 対象に対しゆっくり着実な偵察を行い、資格情報の詐取、ラテラル移動、長期スパイ活動に焦点を当てる。
- インターネットにアクセス可能なSOHOルーターを悪用し、それらを仲介ホップとして、攻撃者が制御するインフラストラクチャに接続する。

特筆すべき活動



- 2023年6月のキャンペーンで、VOLTZITEは米国の危機管理機関および交通監視機関の公共インターネット向けSierra Wireless Airlinkデバイスを悪用した。
- 2023年7月、アフリカの電力送配電および小売業者の企業に対し悪用試行が行われた。
- VOLTZITEは、2023年11月、米国のエネルギー機関に対し包括的な偵察を実施した。

このケーススタディでは、米国の電力公益事業を対象に実施されたDragos OT WatchによるVOLTZITE持続的な脅威ハントを、プラットフォーム、脅威インテリジェンス、Neighborhood Keeperを利用して分析しています。

OT Watch Threat HuntingによるVOLTZITEの発見

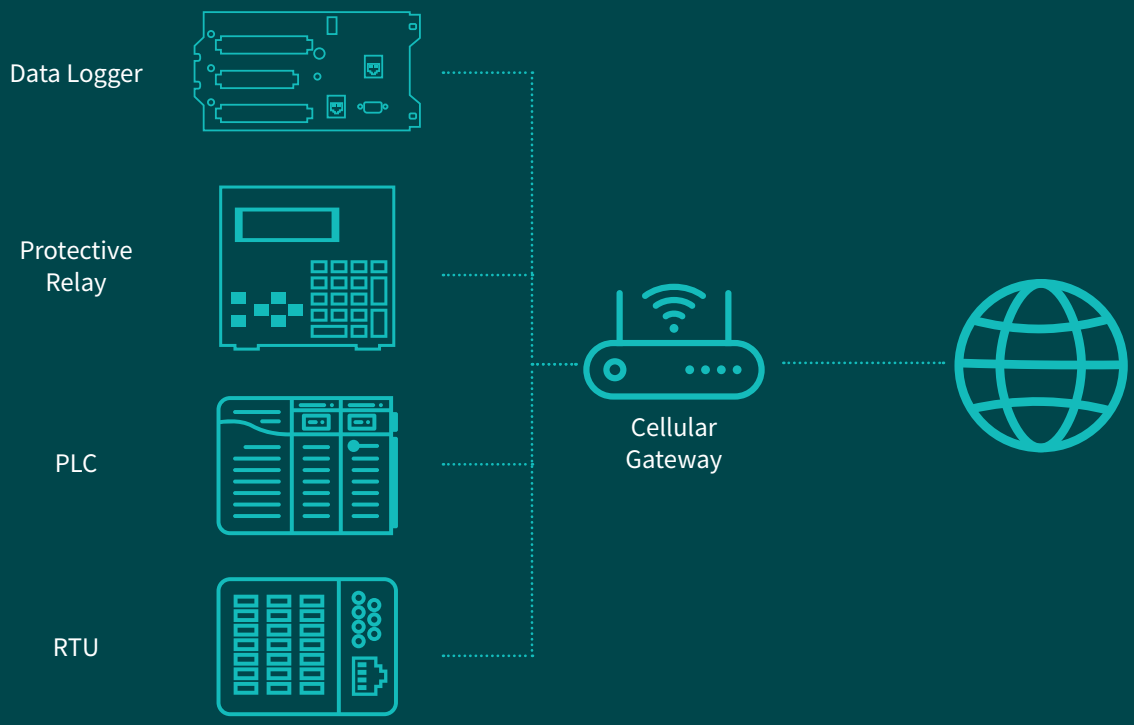
OT Watch Threat Hunting Uncovers VOLTZITE

- Dragosのインテリジェンスチームは2023年初めから**VOLTZITE**の活動を追跡し始めました。
- 公益事業の新たな顧客が、ICS/OTへの影響が懸念される既設ネットワーク侵害に対応すべくDragos Platformを展開しました。プラットフォームは、IT-OTインターフェース（レベル3-4）およびOT-OT通信（レベル2）を監視するように配置されました。
- 展開後、Dragos OT WatchはDragos Platformを活用し、Dragosインテリジェンスによる攻撃の戦術（tactics）、技法（Technique）、手順（Procedure）および脅威ハントの分析によって、環境内の悪意ある活動を特定しました。
- 脅威ハントではOTネットワークに隣接した攻撃の痕跡を確認、インシデント対応分析ではSCADA関連の情報に特化した探索活動の痕跡が見つかりました。これは、Dragos Platform上では、環境内でのピボットを伴うサーバーメッセージブロック（SMB）トラバーサルとして観測され、おそらく、さらなる持続手段として環境に関する情報を探索していたことを示しています。
- OT Watchによって、発見はすみやかに顧客にエスカレートされ、また、調査の完了後に全ての脅威ハントの結果の完全な要約とともに報告されました。環境から攻撃者を排除すべく、インシデント解決のための対応強化が提言されました。環境はDragos PlatformとOT Watchによって引き続き監視されています。
- 脅威ハントの成功、およびDragosインテリジェンスチームが提供した脅威グループの戦術に関する詳細理解を踏まえ、関係する全てのOT Watch顧客に対してハントを拡大しました。
- DragosインテリジェンスチームはNeighborhood Keeperデータの分析を活かして**VOLTZITE**の行動の兆候をとらえ、影響を受ける対象に対して匿名で通知しました。これらの調査結果に基づき、Dragosの脅威検出エンジニアは信頼性の高い検出法を開発、持続的モニタリングのために配備されているDragos Platformに実装されました。

VOLTZITE脅威へ対応を通じて、協調した取り組みの重要性とDragos固有のICS/OT対応力の利点が示されました。この組み合わせは、複雑な脅威に対処するだけでなく、重要インフラ顧客全体に対する予防的な保護対策の強化につながりました。

Dragos Frontline Perspective

有線接続が現実的ではないか経済的ではない遠隔地に対し、しばしばアセットオーナーはSierra Wirelessなどの携帯ゲートウェイを展開します。これらゲートウェイは通常OTデバイスに直接接続され、これがOTデバイスをゲートウェイの誤設定や脆弱性にさらすことになります。ゲートウェイおよび接続デバイスが侵害された場合、可視性の制限および防御レイヤーが単一であることから攻撃者の長期滞在が可能になります。



Dragosは、これらのデバイスが公益事業の中で使用される様子を見てきました。これらは、(訳注：電力における)柱上設置によるキャパシタバンクやリクローザーへの接続、(訳注：上下水道における)遠隔地のポンプステーション、貯蔵タンク、リフトステーションで使用されています。さらに、Dragosは、(訳注：発電の)METタワーや小規模水力発電、分散型太陽光、発電環境のストレージでの使用も見てきました。最も懸念されるのは、携帯ゲートウェイがDCSやPLCプロセス制御ネットワーク(PCN)などの大規模な制御システムに接続されている場合です。これは、標準のセキュリティコントロールをバイパスするリモートアクセスメカニズムとして機能します。組織は、これらのタイプのデバイスが産業環境に導入するリスクに対処するために、正確なアセットインベントリと可視性を持っている必要があります。

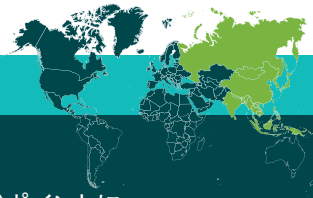
GANANITE

GANANITEは、ドラゴス指定の脅威グループであり、独立国家共同体および中央アジア諸国の重要インフラストラクチャおよび政府機関を標的としています。**GANANITE**はスパイ活動とデータ窃盗に焦点を当てており、初期アクセスを他の脅威グループに引き渡す可能性があります。**GANANITE**は、ターゲットへの持続的侵入セットとして、既知のツールを組み合わせに焦点を当てています。StinkRATを利用し、インターネットに晒されたエンドポイントに対し、広く利用可能なPOCエクスプロイトを使います。**GANANITE**はTELEMIRISやJLORATなどのツールも使用します。Kasperkyは、TURLAと協業する脅威グループが排他的に使用しているツールと見なしています。

被害と影響 Impact and Implications

GANANITEは、ヨーロッパの著名な石油・ガス会社、トルコとアゼルバイジャンの鉄道組織、複数の運送会社や物流会社、自動車機械会社、少なくとも1つのヨーロッパ政府機関が監督する公共水道事業について、ICS運用管理上の重要人物に対する複数の攻撃を行っていることが観測されています。**GANANITE**はまだOTネットワーク内への移動やStage 2に相当する高度な能力は確認されませんが、評価済の能力としてICSサイバーキルチェーンのStage 1にまたがる複数のフェーズを効率的に使用していることが示されています。

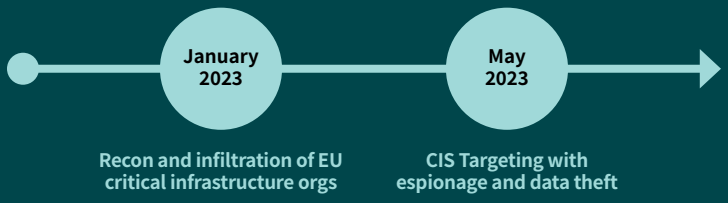
TARGETS: ASIA



主なポイント

- インターネットに晒されているエンドポイントに対し、POCエクスプロイトを活用。併せてStink Rat、LodaRAT、WarzoneRAT、JLORATなどの多くのリモートアクセスTrojans（RAT）を使用する。
- エネルギーに特化したフィッシングルアーを使用。
- 従来のHTTPおよびHTTPSによるC2に加え、Telegramも使用して被害者のマシンからウェブブラウザの情報を外部に持ち出す。
- ShodanやFOFAを通じてターゲット組織を詳細に偵察し、ターゲットのプロファイルと公開アセットの潜在的脆弱性を獲得する。

特筆すべき活動



- 2023年1月13日、TR-2023-01[7]では、ヨーロッパのさまざまな重要インフラ組織 に対する偵察と侵入が掲載された。マスカレード・ドメイン型フィッシングページによる資格情報のキャプチャに加えて、攻撃者はオープンソースのPython RATであるStinkを利用する。
- 2023年5月、引き続き**GANANITE**は独立国家共同体の政府および産業組織をスパイ活動とデータ窃盗のターゲットとし、初期アクセスを他の脅威グループに引き渡す可能性があった。

Dragos最前線の視点

ICS攻撃は2つの部分から成り立つ：企業のIT環境への侵入（ステージ1）によりICSネットワークへの侵入が可能となり、最終的な偵察と制御システムリソースへの侵入（ステージ2）が実行される。ステージ1が必ずしも被害者のIT環境で行われるわけではなく、OT環境へのアクセス権を持つベンダーの環境が侵害される場合もある。

[7] 社発行 Technical Report “Known Adversary Targeting European Critical Infrastructure and Governments”

Dragos最前線の視点

脅威グループはコマンド&コントロール（C2）を使用し、コミュニケーションチャネルとしてHTTP、HTTPS、DNSなど標準プロトコルを利用して侵害されたシステムへの通信と制御を行います。C2の能力は進化しており、C2トラフィックを隠蔽しつつ容易にするために、一部のフレームワークではサードパーティ・アプリケーションや一般的ではないネットワークプロトコルを統合するに至っています。Dragosは、脅威グループがどのように共通のOTプロトコルをC2操作に使用しPOCとして能力開発するか調査しています。

Dragosは、幅広い重要産業の環境で普及していること、および、各プロトコル向けの堅牢なオープンソースライブラリの入手性を考慮し、OPC UA[8]とDNP3[9]に焦点をあてました。Dragosのペネトレーションテスト・チームは、これらのOT C2の能力によって、通常のOTネットワークトラフィックに紛れ込んで産業環境での秘密裏の操作が可能となりました。

さらに**GANANITE**の活動では、ターゲットの外部境界に対し、既知の脆弱性を広範に調査し利用することが示されています。**GANANITE**は、ShodanやFOFAなどの検索エンジンを利用してインターネットに面するアセットのデータを収集し、ターゲットのプロファイルを作成します。ターゲットのIPネットブロックを特定した後、ShodanやFOFAのデータを使用して、既知の脆弱性を有するデバイスを特定します。その後、**GANANITE**は、公開されているエクスプロイトを使用して、これらの脆弱性を悪用します。初期侵入の能力、侵害後のスパイ手法、知的財産の詐取は、被害組織への追加攻撃に活用される懸念があり、特にヨーロッパや中央アジアの産業組織は、**GANANITE**による重大なリスクに直面しています。

[8] OPC-UA1の説明
[9] DNP3の説明

LAURIONITE

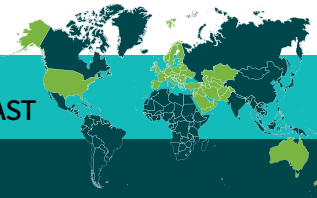
LAURIONITEは、航空、自動車、製造業、政府など複数産業のアセット、およびOracle E-Business Suite iSupplierウェブサービスを積極的に標的とし侵害していることが発見された最初のグループです。このグループは、既知の脆弱性を悪用するPOCコードとオープンソースの攻撃的セキュリティツールを組み合わせて使用しています。

LAURIONITEは、偵察から目的の実行まで を含むICSサイバーキルチェーンのうち、ステージ1を達成する攻撃サイクルの実行能力を示しています。攻撃者のオペレータは、ターゲットシステムの操作、脆弱性の悪用、持続性の維持、ラテラル移動、内部偵察、防御回避、情報の流出など、さまざまな攻撃的サイバーオペレーション技術に精通しています。

Oracle E-Business Suiteは、包括的なビジネスプロセスのための最も広く使用されている企業向けソリューションの1つであり、US Steel社、Unifi Textile Manufucturing社などの多くの産業組織で利用されています。

LAURIONITEは、侵害済インフラを利用することで既知の信頼性のある組織と区別できないようにして、検出されない／無視される状態を保ちます。

TARGETS: UNITED STATES, AUSTRALIA, EUROPE, MIDDLE EAST



主な特徴

- Oracle iSupplierインスタンスを攻撃するためにCVE-2022-21587およびCVE-2022-21589を利用。
- LOLBin（LOTL Binary）を使用してよりステルス性の高いプロファイルを維持。これらのツールを使用してシステムの脆弱性を悪用し、持続性を確立、ラテラル移動、内部偵察を実施し、被害者のデータを外部に持ち出す。
- BehinderとGodzilla Webシェル、および、netcat、proxychains、NeoreGeorg、Pwncat-csなどのオープンソース・セキュリティツールが利用される。
- 侵害した被害者インフラを起点として、他のターゲットへの攻撃を実行する。

特筆すべき活動

- 2023年3月5日以降、**LAURIONITE**はOracle E-Business Suite iSupplier Webサービスを標的として攻撃した。

被害と影響ImpactandImplications
現在観測されている**LAURIONITE**の活動から、OTネットワーク侵入のための探索は見られませんが、攻撃者がそのような行動を取る将来の可能性についてDragosは排除していません。**LAURIONITE**は、製造業のような産業系組織が多く属する業界に対し、重要な存在であるiSupplierインスタンスを積極的に探索しています。

OracleのE-Suite iSupplierテクノロジーを使用する企業を標的にすることは、本質的にOTアセットに影響を与えるものではありません。ただし、iSupplierなどの企業リソースプランニングソフトウェアの性質上、LAURIONITEなどの攻撃者が3rdパーティベンダーとしての可視性を得ることを可能にし、後続の侵入操作につながる可能性があります。

Dragos最前線の視点

OTプロセスがビジネスシステムにどのように依存しているか完全には理解していない組織を、Dragosは机上演習の提供を通じてしばしば発見しています。アセットオーナーがこれらの依存関係を理解して十分な緩和策を講じない限り、重要なビジネスシステムに対する侵害が運用に影響を与える可能性があります。このリスクは、2021年のコロニアルパイプラインに対するランサムウェア攻撃で浮き彫りになりました。企業のビジネスアプリケーションに対するサイバー攻撃が、産業運用に重大な影響を与えました。

その他の活発な脅威グループ
UPDATES ON SOME OF THE MOST ACTIVE THREAT GROUPS

ELECTRUM

ELECTRUMは、Dragosが追跡する脅威グループであり、Sandwormとオーバーラップし、2023年を通じて非常に活発であり、ウクライナ-ロシアの紛争がその活動に大きく影響を与えました。たとえば、2023年6月に特定された新種のワイパーマルウェアはRoarBatと類似した特性を持ち、Windowsオペレーティングシステムを狙うために使われました。**ELECTRUM**は以前にも NDUSTROYER2 イベントの一部として AcidRainやCaddyWiperなどワイパーマルウェアを使用しています。また、**ELECTRUM**に関わるワイパーマルウェア関連の特筆すべき観測として、2022年10月に行われたウクライナの電力サブステーションに対する破壊的サイバー攻撃があり、Mandiant が2023年11月に発行したレポートで言及しています。その攻撃では、**ELECTRUM**はOT環境にありEnd of Life（EOL）を迎えたMicroSCADAソフトウェアを実行する脆弱なハイパーバイザーを悪用し、(当時の)新バージョンのCaddyWiperマルウェアを使用しました。

RASPITE & MAGNALLIUM

Dragosは、**RASPITE**や**MAGNALLIUM**などの脅威グループが、脆弱なSMBデバイスをスキャンし、防衛および鉱業などのさまざまな産業部門に対してパスワードスプレー技術を使用した広範なキャンペーンを実施していることも観測しました。**MAGNALLIUM**はDragosが追跡する脅威グループですが、興味深いことに、ほぼ1年間姿を消していましたが、2023年7月に複数の防衛および鉱業機関に対して再びパスワードスプレー攻撃を開始したことがわかりました。以前の**MAGNALLIUM**のサイバー作戦には、破壊的なワイパーマルウェアを被害者のITネットワークに展開する前に、初期アクセスおよび偵察行動が含まれていました。

Dragos最前線の視点

Dragosが追跡する脅威グループは、関係する活動のクラスター（評価された能力、意図、被害者特性、インフラ）に基づいています。我々の視点では、Dragosが追跡する脅威グループが休眠期間に入ることは普通です。この休眠期間は、彼らの作戦目標の変更、産業組織のカテゴリに属しない広範囲の組織に対するIT志向のサイバー攻撃の実行、またはセキュリティ研究者や法執行機関に先んじて新しいツールの開発や、新しいインフラを立ち上げているためかもしれません。

KAMACITE

ELECTRUMの活動に加えて、**KAMACITE**は、2023年初頭までウクライナの通信企業を標的とし、スピアフィッシングやDarkCrystalリモートアクセストロイの利用しつつ、被害者ネットワーク内ではLOTLテクニックを利用しました。これは複数年に及ぶ**KAMACITE**の活動傾向であり、ウクライナの組織に対する初期侵入作戦、更には、**ELECTRUM**のような脅威グループがグローバル産業企業に対する後続の侵入作戦を可能にするような偵察活動を実施しています。

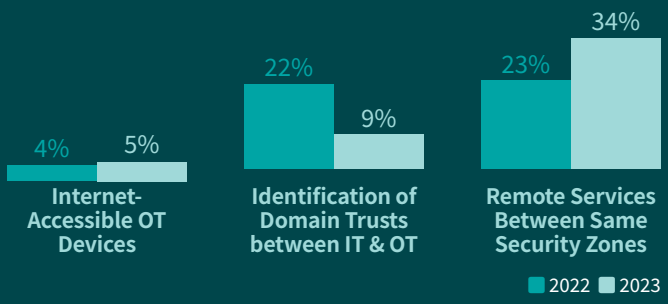
Dragos最前線の視点

DarkCrystal（別名、DCRat）は、2018年に初めて観測されたリモートアクセストロイであり、入手性が高く、様々なレベルの洗練度と能力を持つ多くの攻撃者によって使用されています。DarkCrystal RATはダークネット上の犯罪フォーラムやマーケットプレイスを通じて入手可能であり、侵害されたネットワークにリモートアクセスしたり、ユーザーの資格情報などを盗み出したり、ネットワーク情報を収集したりすることができます。

Dragos最前線の視点

Dragosは（訳注：Dragos PlatformやOTWatchによる）視認性を活用し、ペネトレーションテストの実施に際して、攻撃者が頻繁に用いる戦術、技術、手法（TTP）を反映しています。これには、公に利用可能な偵察行為とオープンソースインテリジェンス（OSINT）を使用した環境への侵入経路把握が含まれます。初期アクセスが確立されると、焦点は持続性の確立、アクセスの拡大、およびOTをターゲットとした侵害に移ります。

2023年を通じて、Dragosは、潜在的に悪用される可能性のあるアカウントやアセットを特定するために、Reconnaissance（TA0043）、Discovery（TA0102）、およびInitial Access（TA0108）を含む一般的なMITRE ATT&CK情報収集タクティクスを活用しました。これには、インターネット経由でアクセス可能なOTアセットの発見（2023年には4%からわずかに上昇した5%）、ITとOTの間のドメイントラストの特定（2023年には22%から13%減少した9%）、同一セキュリティゾーン内でのリモートサービスの特定（2023年には23%からわずかに増加した34%）が含まれます。



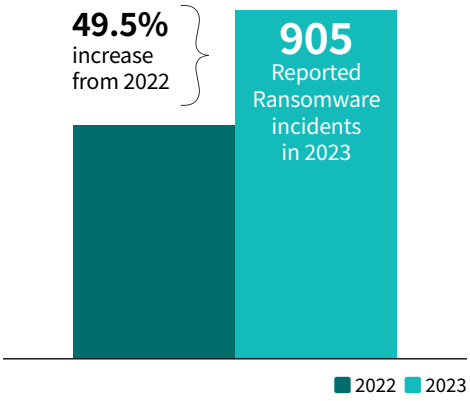
Dragosチームが初期アクセスを獲得した後、優先事項は、適切な場所での持続性（TA0110）獲得であり、ターゲット環境を通してのラテラル移動（TA0109）であり、OT Crown Jewelsに近づくことです。Dragosチームは、2023年に多くのラテラル移動テクニックを特定しましたが、そこでは、IT-OT間のセキュリティ・ギャップとして示される公知の経路がしばしば用いられていました。

2023年、ネットワーク侵入テストのほぼ5%で、Dragosチームはデフォルトの資格情報（T0812）を使用してOT環境全体をラテラル移動しました。また、ハードコードされた資格情報（T0891）も同様の結果をもたらし、更にアクセス権の増加さえももたらすことがわかりました。Dragosは複数のアセスメントにおいて、ドメイン、ネットワーク、アセットを横断して機能を自動実行するためのカスタムPythonスクリプトとPowerShellスクリプトを特定しました。クリアテキストおよびデフォルトの資格情報が集められ、象範囲内のアセット全体に対し、資格情報の再利用が可能か不可能か確認のためテストされます。

2023年 産業界におけるランサムウェアの分析
2023 INDUSTRIAL RANSOMWARE ANALYSIS

ランサムウェア・アクティビティは増加
INCREASE IN RANSOMWARE ACTIVITY

Dragosは、産業組織およびインフラに攻撃を仕掛けてきた77のランサムウェア・グループのうち、50のアクティブなグループが2023年においても産業組織に影響を与えていることを観測しました。これは昨年比で28%の増加です。Dragosが追跡した、産業組織に影響を与えたランサムウェア・インシデント報告は905件であり、2022年から49.5%増加しました。産業組織にとって、操業中断によって失う経済被害と評判の代償は甚大です。更に、連鎖的に下流の企業にも様々な影響が生じる可能性があります。このように（ランサムウェア攻撃が）高い効果をもたらす状況となっています。



ランサムウェアの攻撃者およびその活動は、使用される技術や洗練度を見ても広範囲であり、2023年もさまざまな産業標的に影響を与えました。LockBit、ALPHV、Hunters International、Rhysida、およびNoEscapeなど、世界中には数百ものランサムウェア・バリアントが存在します。2023年に活動したランサムウェア・グループの数より更に多くのグループが世界中に存在しますが、犯罪エコシステム内に広がる特徴に沿って、グループが再ブランド化し、分派のランサムウェア・バリアントが作り出されます。

Dragos最前線の視点

ALPHV、BlackCat、およびDarkside（Colonial Pipeline攻撃の実行者）が、この種のランサムウェアの再ブランディングとコード共有の根拠です。これらの3つのグループは、コード、インフラストラクチャ、およびTTPs（戦術、手順、手法）に共通点を持ち、一部は古いグループであるREvilにまで遡ることができます。

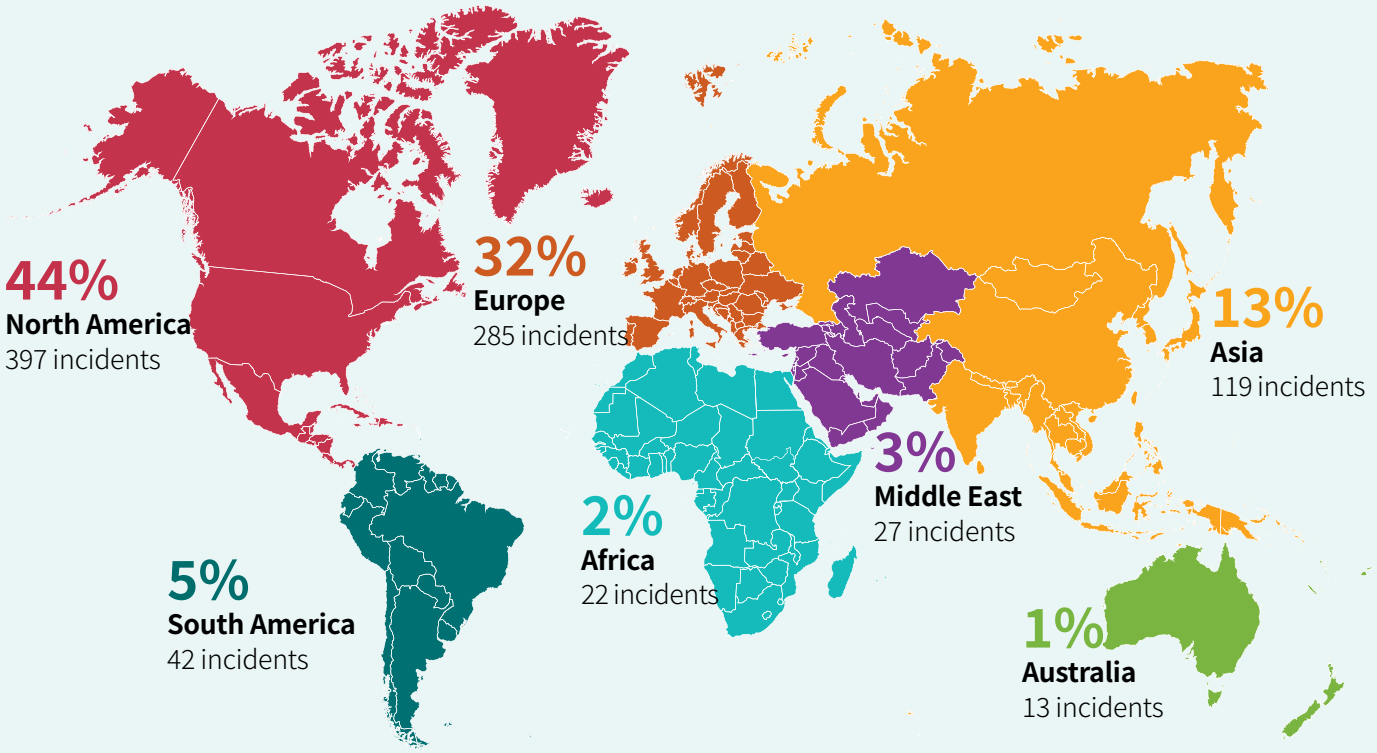
産業向けランサムウェア攻撃
INDUSTRIAL RANSOMWARE ATTACKS

2023年全体を通じて、LockBitランサムウェアが産業組織に対する最も頻繁に使用されたランサムウェア・バリアントでした。具体的には、LockBitの活動が2023年における産業組織へのランサムウェア事件の25%を占め、ALPHVとBlackBastaがそれぞれ9%を占めました。LockBitは、多くのランサムウェア・グループと同様に、ランサムウェア・アズ・ア・サービス（RaaS）プロバイダーとして機能しています。

Dragos最前線の視点

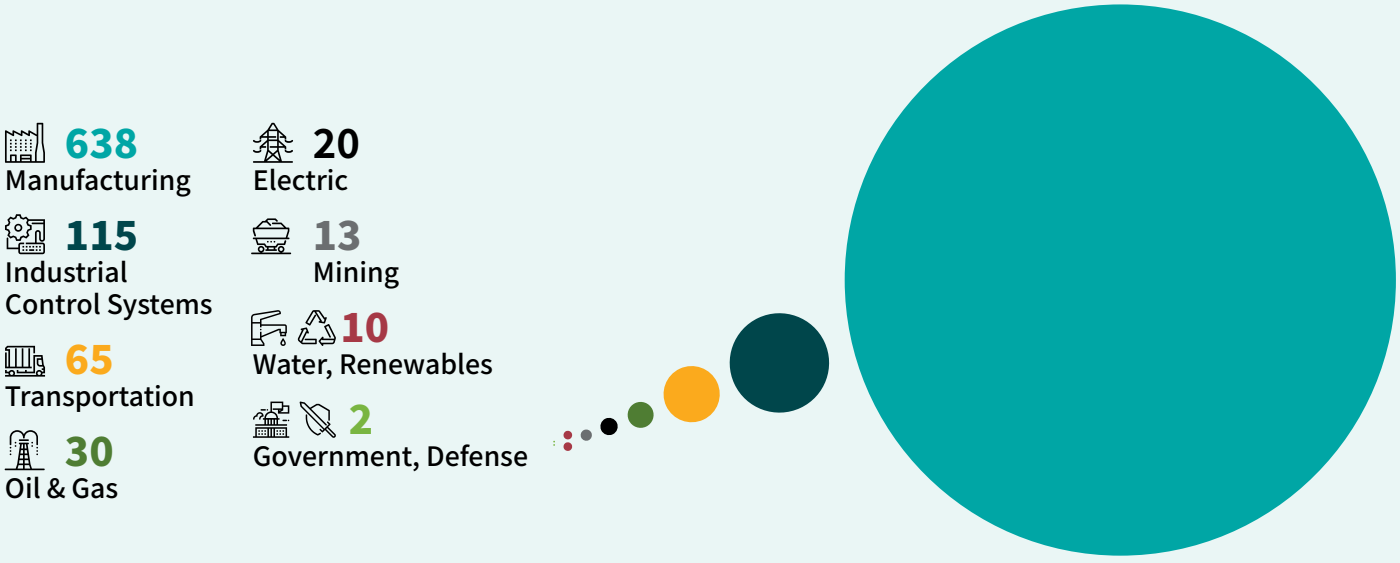
Ransomware-as-a-Service（ランサムウェア・アズ・ア・サービス）は、ランサムウェア提供者が独自のランサムウェア・インフラストラクチャへのアクセスを「貸し出す」モデルであり、これにより、ランサムウェア活動から利益を得ようとするスキルの低い攻撃者にとって、参入障壁の低い選択肢が生まれます。ランサムウェア提供者は、ランサムウェア・アフィリエイトにインフラストラクチャをレンタルすることで利益を得るほか、ランサムウェア活動が成功すれば一定の割合の報酬も受け取ります。アフィリエイトは、ランサムウェア提供者のインフラストラクチャへのアクセスをレンタルことで、独自のカスタム・ランサムウェア・ツールを開発する必要がないというメリットがあります。

LockBitのオペレーターは、被害者が身代金を支払う可能性を高めるために、脅迫的な戦術を活用しています。そうした戦術の 1 つは、LockBit 開発者が作成した情報窃盗ツールである StealBit を使用して、被害者の組織から産業データなどの機密データを盗むことです。StealBit は通常、LockBit が侵害されたシステムを暗号化する前に展開されます。被害者が身代金を支払わない場合、盗まれたデータは LockBit のダークウェブリソースに投稿され、他の攻撃者により利用されます。



Ransomware is a global threat; however, the majority of ransomware attacks impacted organizations in North America with 44 percent of incidents, with Europe being the second most common target with 32 percent.

Figure 4: Ransomware Incidents by Continent • 2023



The most common sector impacted in 2023 was manufacturing, with 71 percent of ransomware incidents.
The industrial control systems sector, which is made up of companies that develop OT equipment and applications, was the second most impacted sector with 13 percent.

Figure 5: Ransomware Incidents by Sector • 2023

産業向けランサムウェアのトレンド
INDUSTRIAL RANSOMWARE TRENDS

既知の脆弱性を悪用する
EXPLOITING KNOWN VULNERABILITIES

2023年も、ランサムウェア運営者による犯罪行為の主な手法は、イニシャル・アクセス・ブローカー[10]との協力、フィッシング、VPNやRDPサーバーなどの公開ネットワークアセットの悪用など、一貫しています。Dragosは、Citrix Bleed[11]の脆弱性を利用した公開サービスの悪用を含む、ランサムウェアキャンペーンも観測しています。これらのランサムウェア・グループには、Lockbit、BlackBasta、およびALPHVが含まれます。ランサムウェア運営者は、Citrix Bleedのような最近公開された脆弱性を巧みに利用しています。多くの場合、攻撃者は、脆弱なテクノロジーに対する利用可能なエクスプロイト機能を迅速に開発または使用し、そのエクスプロイト コードをランサムウェアの運用フレームワークに統合します。多数の産業組織に影響を与えた Citrix Bleed 活動の急速な拡大のタイムラインを以下に示します。

Dragos最前線の視点

Dragosのインシデント対応者は、この攻撃が産業顧客に影響を与えているのを観測しました。あるケースでは、Dragosの対応者が、被害者の外部インフラがスキャンされた後の偵察フェーズの後、Citrix Bleedの脆弱性が初期攻撃ベクトルであることを特定しました。

Date	Event
10 October	Citrix discloses CVE-2023-4966 and CVE-2023-4967
17 October	Mandiant reports in-the-wild zero-day exploitation since at least late August 2023
23 October	Proof-of-Concept (PoC) code to exploit the vulnerability published to GitHub
24 October	GreyNoise starts detecting in-the-wild exploitation exploits
27 October	Mass exploitation of vulneratility underway. Suspected exploitation by Ransomware group. Boeing added to LockBit 3.0 leak site.
10 November	LockBit 3.0 ransomware attack against the Industrial and Commercial Bank of China (ICBC) and DP World
11 November	Evidence of Lockbit 3.0 victim running vulnerable Citrix appliances
16 November	Medusa ransomware attack against Toyota Financial Services — suspected access via German office running a vulnerable Citrux appliance
21 November	Joint Cybersecurity Advisory released

この種の活動のもう1つの例は、2023年5月にMOVEitのゼロデイ脆弱性[12]が公開された後に見ることが出来ます。Cl0pランサムウェア・グループはこの脆弱性を活用して初期アクセスを獲得し、多数の被害者を出しました。これらの被害者の一部には、重要なインフラ組織、重要なインフラに関連する政府機関、および重要なインフラ運用を支援する組織が含まれます。ベンダーやサービスプロバイダーの影響は、制御システムをサポートするという役割を考えると特に問題となり得ます。

Dragos最前線の視点

Dragos による調査と分析により、Cl0p の活動に関する重要な洞察が得られました。特に Dragos は、Cl0p サンプルに埋め込まれた特定のハッシュ値に関連付けられたターゲットプロセス名を復元できました。これらのほとんどは IT 関連のプロセスですが、Cl0p ランサムウェアは Windows オペレーティング システムにある OT 関連のプロセスをターゲットにしています。ただし、OT 固有のプロトコルを使用したり、ターゲットにしたりすることはありません。Cl0p には、Honeywell、IBM、Mitsubishi Electric、Rockwell、Schneider Electric、Siemens などの OT ベンダーに関連する多くの実行中のコンピューター・プログラムを停止する機能があります。

[10] イニシャル・アクセス・ブローカー（IAB）は、可能な限り企業を攻撃し、脆弱な認証情報、フィッシング、水飲み場型攻撃などを活用してネットワーク侵入口を獲得する攻撃グループであり、獲得した侵入情報をダークネットの取引所を通じて他のサイバー脅威グループに販売している。
[11] Citrix Bleedの脆弱性　CVE-2023-4966
[12] MOVEit Transferにおけるクリティカルなゼロデイ脆弱性　CVE-2023-34362

適切なセキュリティの欠如
LACK OF SUFFICIENT SECURITY CONTROLS

攻撃者が被害者の環境へのアクセスを獲得する方法に関わらず、ランサムウェア・グループが産業システムに影響を与える力は、ネットワークの防御側が実施しているセキュリティコントロールの種類に大きく依存しています。Dragosが取り組んでいるほとんどの環境では、アセットが公開ネットワークに直接接続されているのではなく、ファイアウォールやプロキシなどの少なくとも単一の防御レイヤーの背後にあります。これらのセキュリティコントロールの効果は大きく異なり、単一のレイヤーが十分な保護であると想定すべきではありません。

Dragosは、2023年の28%のエンゲージメントでセグメンテーションの問題や適切に構成されていないファイアウォールに関する調査結果を発表しました。多くの観測と同様に、これは業界によって大きく異なります。例えば、交通や製造業におけるネットワークのセグメンテーションの問題を、Dragosは他の業界よりも頻繁に観測しています。

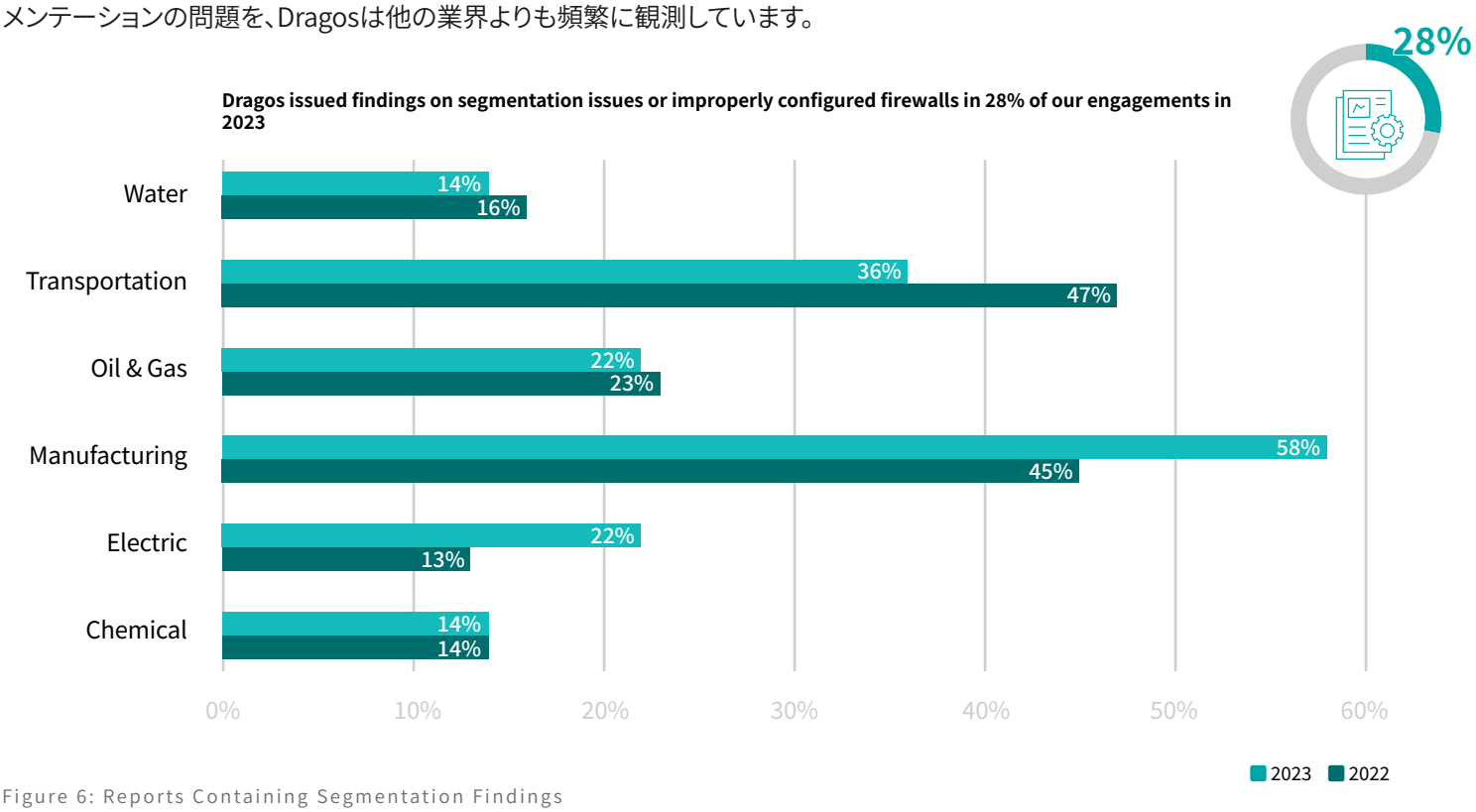


Figure 6: Reports Containing Segmentation Findings

Dragos最前線の視点

2023年、Dragosは、OTに関連するインシデントの約70%がIT環境内から発生していることを観測しました。これらのインシデントの緩和策として、ネットワークのセグメンテーションと独立したドメインが重要なアーキテクチャの変更として推奨されています。

LOTL（環境寄生型）テクニックを活用したアクセス拡大

LEVERAGING LIVING OFF THE LAND TECHNIQUES TO FURTHER ACCESS

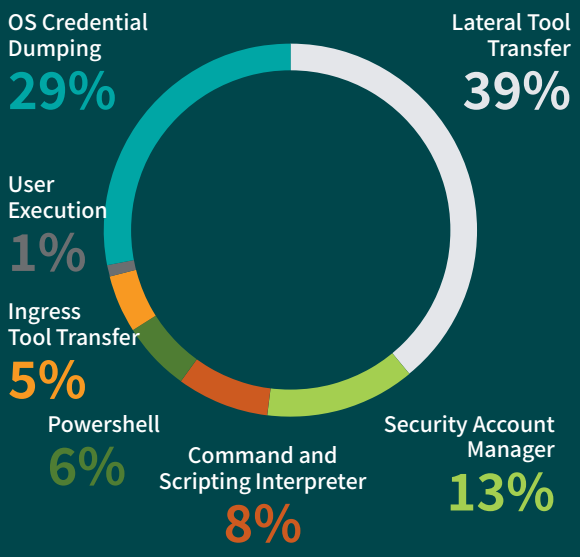
侵害後のTTP（戦術、技術、手順）は、ランサムウェア・グループとその提携先でわずかに異なりますが、ほとんどがLOTL（環境寄生型）テクニックを利用しています。これには、PsExecやPowerShellなどのネイティブツールを使用して被害者のネットワーク内をラテラル移動し、特別に望ましいターゲットを発見することが含まれます。これらのターゲットのうちの1つにリモートアクセスを確立した後、脅威グループは引き続きLOTLツールを活用することで、権限を昇格し（タスクマネージャ、BitsAdmin、およびWMIC）、永続性を確立し（定期的なタスク）、コマンド&コントロール（SSHおよびRundll32）チャネルを確立します。

右の図には、さまざまなペンテストチームが使用したLOTL TTPが示されています。LOTLを使用するだけでなく、攻撃者はノンネイティブツールも使用します。Dragos OT Watchの脅威ハンターは、お客様のOT環境の約10%以上で予期しないリモートアクセスツールが実行されていることを見つけました。ランサムウェア・グループは、これらのツールと関連するTTPを使用して環境全体を移動し、システムを侵害します。Microsoft Active Directoryはしばしば主要なターゲットとなります。ランサムウェア・グループは、LOTLテクニックの利用に加えて、有効なアカウントへのアクセスを獲得するためにActive Directoryを侵害するツールを使うことが観測されています。

Dragos最前線の視点

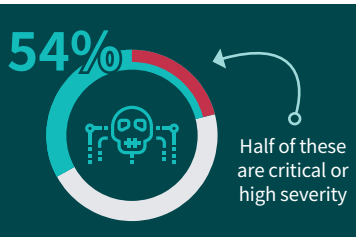
Dragosが提供したペンテストの63%において、ICSサイバーキルチェーンのStage 1およびStage 2の両方でこれらと同一のLOTLテクニックが有効に機能しました。Dragosがペネトレーションテストで使用したLOTLテクニックのうち、Lateral Tool Transfer（T0867）が39%を占め、次にOS Credential Dumping（T1003）が29%、Security Account Manager（T1047）が13%でした。残りの19%は、他の4つのLOTL TTPは：Command and Scripting Interpreter（T1059）、PowerShell（T1086）、Ingress Tool Transfer（T1105）、およびUser Execution（T1204）でした。

LOTL TTPs Used by PenTest Team



Dragos最前線の視点

有効なアカウントを侵害する共通 TTP (T1078)に対抗するには、防御者は、特権アカウント管理 (M0926、M1026)、ユーザーアカウント管理、多要素認証、パスワードポリシーなど、予防的なセキュリティコントロールを実装する必要があります。しかし、最も重要なのは、IT 環境と OT 環境が認証ドメインを共有しないことです。



Dragos found remote access security issues in 54 percent of penetration tests.

Dragos found that 1 in 10 industrial environments have a shared domain architecture.

OTの脆弱性
OT VULNERABILITIES

脆弱性アセスメントの概況
VULNERABILITY ASSESSMENT OVERVIEW

脆弱性アドバイザリは、ハードウェアとソフトウェアに関する共通脆弱性識別子（CVE）に関する情報を提供します。Dragos は、ICS/OT 環境に関連する脆弱性アドバイザリを分析し、それらを優先順位付けして、産業組織のアセットオーナーが行う手間を省きます。

Dragos最前線の視点

Dragosは、次の5年間で工業運用に関連する脆弱性アドバイザリの数が倍増すると予測しています。この急速な脆弱性の増加は、ベンダーや研究者がOTにより焦点を当てていること、およびDragosが追跡している情報源の数が増加していることに起因しています。

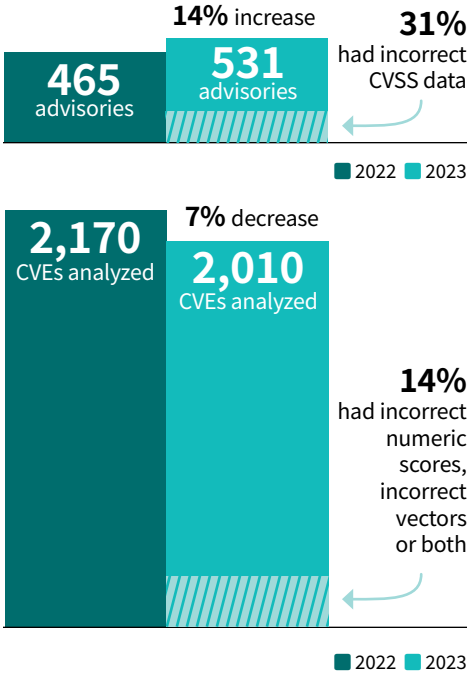
IT環境とOT環境の違いは、脆弱性の評価時に顕著です。OT環境内で使用されるデバイス、システム、プロトコルの種類、典型的なOTネットワークのアーキテクチャ、および脆弱性が通常の運用および物理世界に与える影響が（IT環境との）違いを生み出します。OTの脆弱性は、ITの脆弱性とは異なる方法で、OTシステムの厳格な運用要件（例：システムの稼働時間やベンダーの認証プロセスなど）に基づいて緩和および対処されるべきです。

多くの脆弱性管理プログラムは、CVSSが9.0以上の「重要な」脆弱性に対する是正に焦点を当てています。つまり、これらの脆弱性は緊急性を持って緩和されるべきであるとプログラムが指定しています。このアプローチには3つの問題があります。

• **第一に:** 研究者は公開アドバイザリの最終版に意見を述べないことが多く、共通脆弱性評価システム (CVSS) のスコアが不正確になる可能性があります。産業システムのOEM に依存しているが、それぞれ成熟度が異なるため、業界コミュニティが一貫したスコアリングと重大度のガイダンスを持つことは困難です。このため、ベンダーやその他の CVE 採番機関 (CNA) が発行する脆弱性アドバイザリは、不正確で曖昧な場合が多くあります。

• **第二に:** CVSSは、典型的なOTネットワークアーキテクチャを考慮していません。ネットワーク経由で悪用可能な脆弱性は、ネットワークが適切に設計されサービスを直ちに攻撃できない場合でも、しばしば重大なスコアが付けられます。

• **第三:** アドバイザリには、パッチを適用する以外の実用的な手順がしばしば欠けています。特にファームウェアのようなOTソフトウェアのパッチ適用は、多くの組織にとって困難または不可能である場合があります。時折、アドバイザリはパッチも他の緩和策もないまま公開されますが、それは防御者にとって無価値な文書になります。

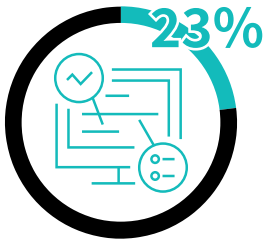


In 2023, Dragos analyzed 2010 CVEs contained in 531 advisories. This is a 14 percent increase in advisories and a 7 percent decrease in CVEs from 2022. As a reminder, Dragos tracked 465 advisories and 2170 CVEs in 2022.

代わりに、OT 環境と要件を考慮したアプローチの方が、より良い結果をもたらします。これは、毎年末のデータ分析で実証されています。

脆弱性の精度
VULNERABILITY ACCURACY

16% of advisories were network exploitable and perimeter facing



Dragos identifies and makes recommendations on vulnerabilities in **23% of its engagements.**

Advisories with no patch when announced

28%

Advisories that had a patch

72%

Advisories that had no mitigation at all

74%

Advisories with no vendor mitigation

73%

Advisories with no alternate mitigation

99%

Advisories with a patch and no mitigation

54%

Advisories with no patch and no mitigation

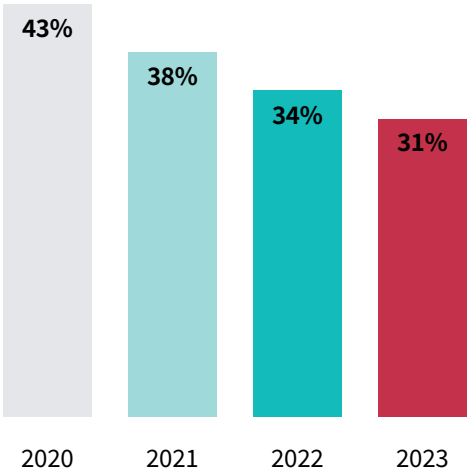
19%

Advisories for which Dragos provided missing mitigation advice

49%

Figure 7: Advisories with Errors and Lacking in Actionable Guidance

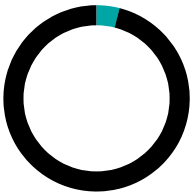
Errors could cause asset owners and operators to waste resources on low-risk vulnerabilities over more severe ones



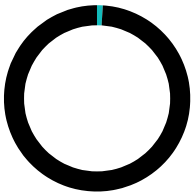
Dragos analyzed 531 advisories
31% had incorrect data

14% of the 2010 CVEs analyzed by Dragos had errors associated with the advisories with incorrect data. Dragos assessed these CVEs to correct the CVSS scores with the below results.

9%
Dragos found to be **MORE SEVERE** than the CVSS score



4%
Dragos found to be **LESS SEVERE**



1%
were the same

Figure 8: The State of ICS/OT Vulnerabilities

脆弱性アドバイザリにおいて遭遇する間違いの代表例は、CVSSの誤適用です。DragosはCVSSスコアを修正し、しばしばベンダーや研究者に直接連絡して、特定の脆弱性がどのように悪用される可能性があるかについての明確化を求めます。

Dragosの確認では、セキュリティアドバイザリに記載されたCVEのち9%が、元の報告と比べてCVSS Calculator[13]の結果のほうが深刻になることを発見しました。CVSSは産業制御システムを念頭に置いて設計されていないため、スコアの上昇がアセットオーナーに対する警鐘とは言えません。後ほど詳しく述べますが、適切な緊急性は「Now、Next、Never」の優先順位で定義できます。修正後も同じスコアだったアドバイザリは、わずか1%でした。

Dragos最前線の視点

Dragosは、次の5年間で工業運用に関連する脆弱性アドバイザリの数が倍増すると予測しています。この急速な脆弱性の増加は、ベンダーや研究者がOTにより焦点を当てていること、およびDragosが追跡している情報源の数が増加していることに起因しています。

[13] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

脆弱性リスクの緩和
VULNERABILITY RISK MITIGATION

OT環境でのすべての脆弱性のパッチ適用は困難であり、OTネットワークのセキュリティを向上させるとは限りません。実際、不必要なパッチ適用は独自のリスクをもたらす可能性があります。パッチの適用に失敗すると、望ましくないダウンタイムが発生する場合があります。さらに、OTデバイスやOTソフトウェアの多くには「"foreverday vulnerabilities" - 永遠の脆弱性（訳注：恒久的に是正困難なセキュリティ的欠陥）」が存在します。これは、脆弱性を閉じるためにシステムにパッチ適用しても、影響を受けるコンポーネントのセキュリティが向上しない可能性があることを意味します。より良いアプローチは、工業プロセス全体のハイジーンにポジティブな影響を与える項目への対策と緩和に焦点を当てることです。

脆弱性の対処とは、通常、アップデートの配布やセキュリティコントロールの適用を意味します。OT環境内でのパッチ適用は、通常、正常かつ安全なオペレーションが維持されるように行われなければなりません。そのため、パッチ適用はメンテナンスウィンドウまで遅延されることがよくあります。従って、アドバイザリ内の脆弱性を緩和するための代替手段を持っていることが重要です。

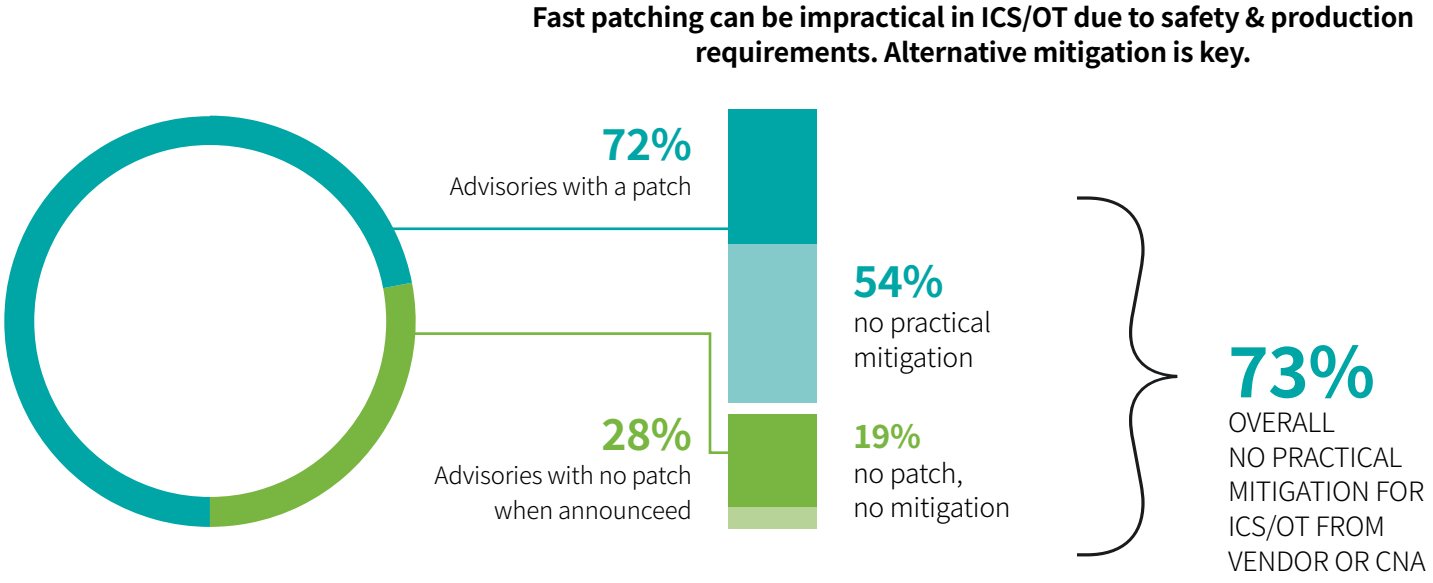


Figure 9: Practical Risk Mitigation in ICS/OT

2023年、Dragosが分析したアドバイザリの72%にはパッチが付属していましたが、そのうちの54%には緩和策のアドバイスが含まれていませんでした。パッチに関して前年比で+1%、緩和アドバイスも+1%の変化です。緩和策のないアドバイザリの49%に対し、Dragosは、他のソースからの緩和策を提供しました。発表時にパッチがないアドバイザリは、2023年の全アドバイザリの28%を占め、そのうち約19%は緩和策もありませんでした。これにより、OTネットワークの防御者が持つ選択肢は多くありませんが、しばしば最も簡単な行動やツールの変更が最も大きな影響を与えることができます。

「NOW、NEXT、NEVER」の優先順位付け

脆弱性をアクション可能なカテゴリに優先順位付けすることで、アセットオーナーや運用者は、自社の運用に殆ど／全く影響を与えない脆弱性に対して時間とリソースを浪費することを防ぎます。2010年の脆弱性のノイズから、対処すべきものに関するシグナルに到達するために、DragosはComputer Emergency Response Coordination Center（CERT/CC）の**Now、Next、Never**方法論に従います。

この方法論は、防御者が即座に緩和すべき脆弱性を優先し、それらを**「Now」**のカテゴリに配置します。**「Next」**のカテゴリには、ファイアウォールルールと良好なネットワーク衛生状態によって緩和できる脆弱性が含まれます。この2番目のグループは、次のメンテナンスサイクルでパッチを適用できますが、異常なネットワークアクティビティや攻撃を監視する必要があります。最後に、デバイスの固有のリスクを増加させない脆弱性は、**「Never」**のカテゴリに属します。

この優先順位付けでは、VPN迂回、ピボットポイントとして使用される可能性のあるデータヒストリアン、リモートアクセスサービスのその他の弱点など、脆弱性が境界に面していて簡単に悪用できるかどうか考慮します。これらの問題は、攻撃者がネットワークへのアクセスを取得することを可能にします。また優先順位付けでは、今日の脅威グループが積極的に悪用している脆弱性に焦点を当てています。Dragosは公開POCを持つアドバイザリを探し、悪用のハードルを下げる入口に対策を講じます。

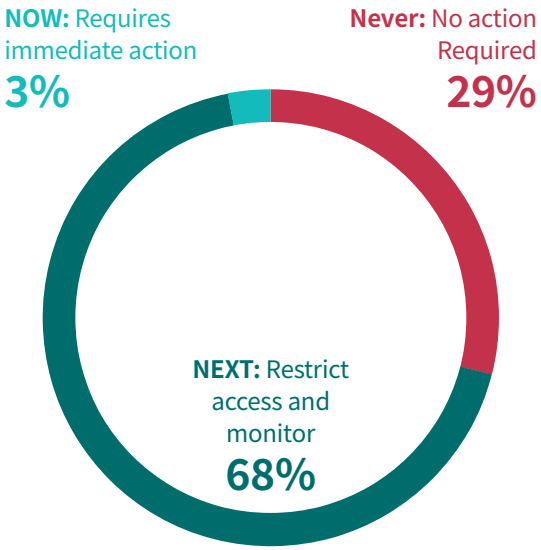
また、ライフセーフティシステム（訳注：建物の非常装置など）も優先すべき対象です。もし、ある脆弱性によって安全システムのロジックを変更できる可能性が生じる場合、それは**「Now」**のカテゴリに属するでしょう。

2023年の脆弱性分析では、上記を主な基準とした**「Now」**のカテゴリに属する脆弱性は全体の3%に過ぎませんでした。この3%のうち、17%はネットワークの端にあるため、そして83%は脆弱性の機能によって、この評価を受けています。

2022年、DragosはCNA（CVE番号機関）となりました。CNAであることの利点は、正確なCVSSスコアリング、適切な緩和策、およびブランド名を付けずに脆弱性に優先順位を付けるためにベンダーやOEMと密接に連携できることです。CNAはまた、ベンダーがシステムを再設計して欠陥を修正するのに数年かかる場合、エンドユーザーへのタイムリーな情報提供を可能にも出来ます。CNAになることで、研究者に対し緩和情報公開の自由を与えます。

2023年、Dragosが発見したCVEのうち、35件が公開されました。このうち18件は、DragosがCNAとして管理しました。これらは主にネットワークに面した脆弱性で、かつ、通常は企業ネットワークやインターネットに露出すべきではない複数のファイル形式の脆弱性であり、資格情報の取得やファイルの上書きが可能です。いくつかの脆弱性は「Critical」のCVSSスコアを持ちながら、それでも**「Now」**レベルの脆弱性とは見なされていませんでした。

2023年の2010件の脆弱性のうち、Dragosは、3%が即座の対応を必要とすると判断しました。68%はネットワークの監視、ネットワークのセグメンテーション、またはMFA（多要素認証）によって対処できます。そして、29%は即時の対応は必要ありませんが、潜在的な攻撃の兆候を監視する必要があります。



脆弱性のセベリティ
VULNERABILITY SEVERITY

工業プロセスにおける制御の喪失と表示の喪失は、ICS環境における最悪のシナリオの1つです。システムを安全かつ確実に運転する能力は、工業プロセスの正確な表示と制御に依存します。組織が最も影響のあるものに集中できるよう、Dragosは、脆弱性によって考え得る影響を調査しています。

2023年、Dragosが分析したアドバイザリのうち、53%の脆弱性がプロセスの表示と制御の両方を失う要因になる可能性を示しています。これは、2022年からの+3%の変化です。全体の脆弱性の46%は、工業プロセスの制御または表示に影響を与えることはありません。これらの脆弱性の1%は、制御の損失に影響を与えることなく、表示の損失のみを引き起こす可能性があります。

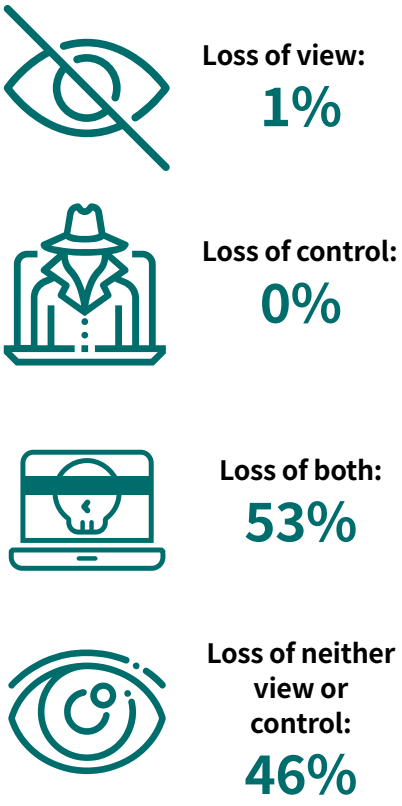


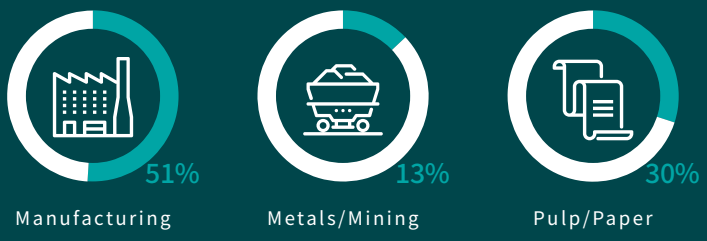
FIgure 10: Loss of view, loss of control, or both

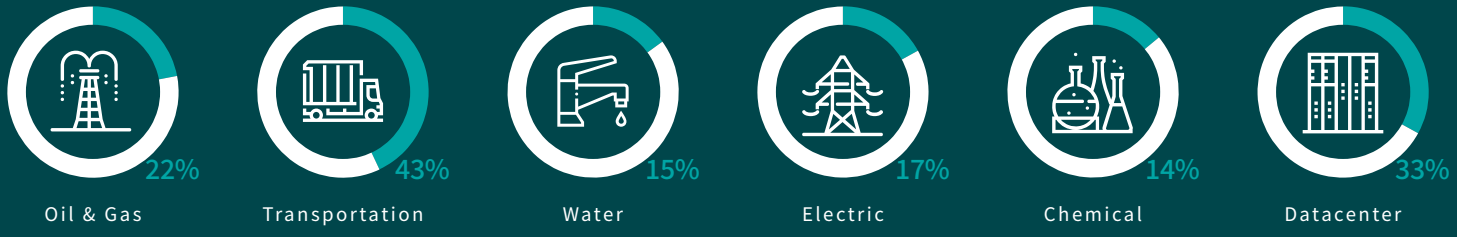
ネットワーク内の脆弱性が存在する場所
WHERE THE VULNERABILITIES RESIDE IN THE NETWORK

ICSネットワークの奥深くにある脆弱なアセットには、企業の境界にあるアセットとは異なる脅威プロファイルがあります。ファイアウォールで保護されたPLCは、インターネットに直接接続されたものよりもリスクが低いです。脆弱性の緩和を優先する際には、組織はネットワークの状況と、アーキテクチャ内の脆弱なシステムが存在する場所を考慮する必要があります。

Dragos最前線の視点

Dragosは、多くのセクターが防御可能なアーキテクチャ（訳注：SANS “The Five ICS critical control”の第2要素）に関して引き続き課題を抱えていることを発見しました。今年のレポートの結果によると、製造業は防御可能なアーキテクチャの核であるセグメンテーションに最も苦労しています。以下は、セグメンテーションに苦労した業界別のエンゲージメントの割合です。





Dragosは、各アドバイザリの評価ひとつひとつに対し、適切に設計された環境における一般的な配置に基づく想定Purdueレベルを提示しています。よく設計されたネットワークでは、工業プロセスに影響を与える前に、攻撃者は複数のレイヤーを侵害する必要があります。この攻撃経路には、企業ネットワークへの初期アクセスを取得してから、OTネットワークにピボットしてICSネットワーク内部のシステムを侵害するというものが含まれます。これにより、ネットワークの奥深くにある脆弱性を悪用する機会はより難しくなります。

2023年、これらの脆弱性のうち、19%は企業と接続されるリモートアクセスの脆弱性であり、80%はICSネットワークの奥深くに存在していました。62%はPurdueモデルのレベル0から3で見つかった脆弱性に関連しており、これらのレベルでは強固な構成に囲まれアクセスが制限されているはずです。そこには工業プロセスに影響を与える可能性のあるエンジニアリングワークステーション、PLC、センサーに対する、アクセス制限が含まれます。

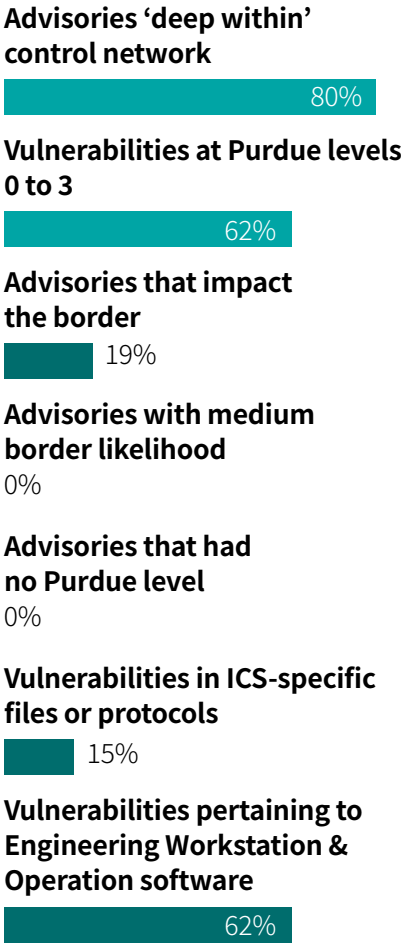


Figure 11: Where do vulnerabilities reside?

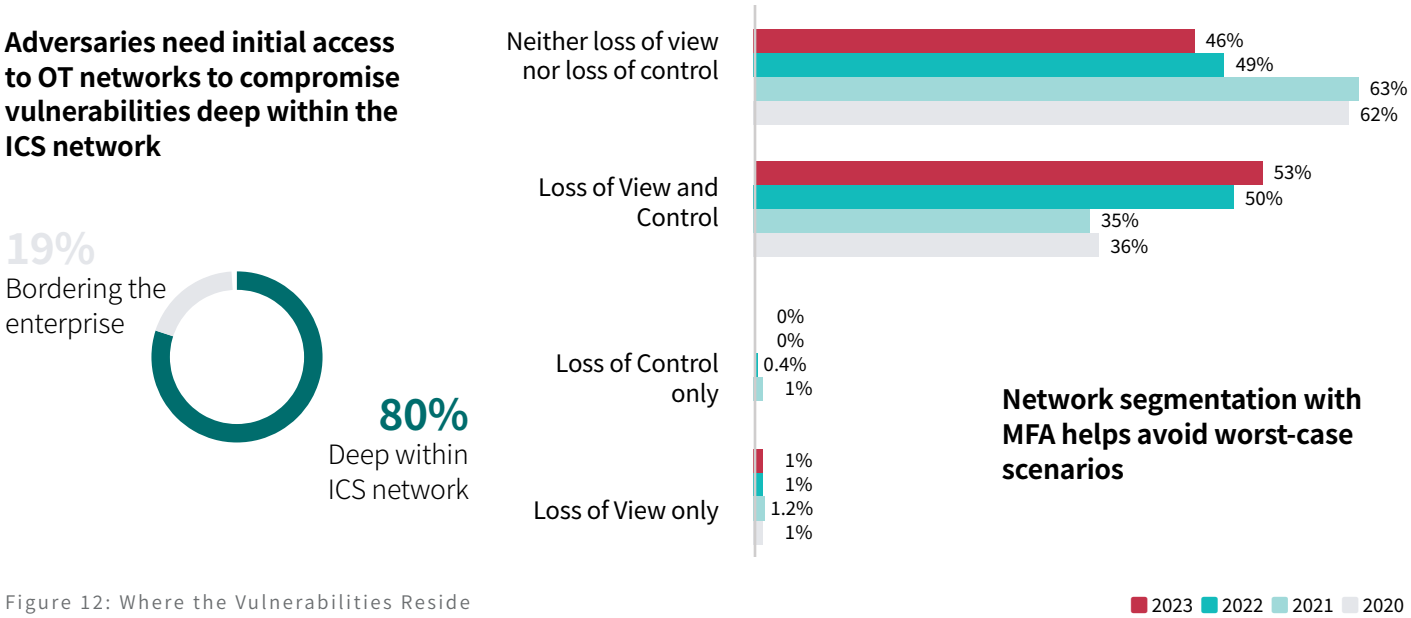


Figure 12: Where the Vulnerabilities Reside

脆弱性悪用の可能性
VULNERABILITY EXPLOITABILITY

Dragosは、実際に悪用されている証拠を継続的に探しています。攻撃者によって実際に悪用されている、またはペネトレーションテストによって証明されている脆弱なアセットを持つアセットオーナーは、緊急性を高めて対処する必要があります。そのため、悪用は**「Now、Next、Never」**の優先順位付けにおいて考慮されます。

2023年には、アドバイザリの5%が積極的に悪用されている脆弱性を含んでいました。すべてのアドバイザリのうち、防御者が即座に緩和すべき脆弱性として、最優先される**「Now」**は3%だけであることを思い出してください。活発な攻撃キャンペーンが、防御者が即座に緩和すべき最高優先度の脆弱性の大部分を占めています。

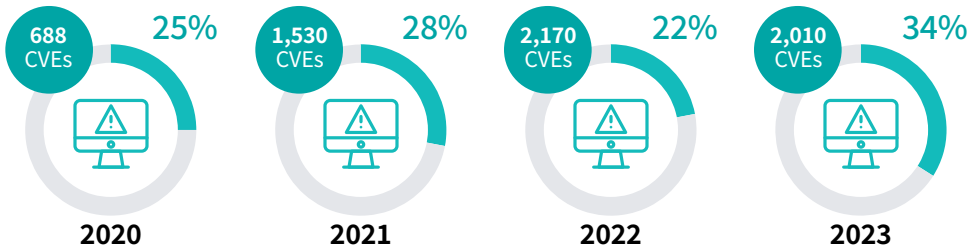
公開された概念実証（PoC）は、広く利用が可能なエクスプロイトコードの例です。PoCは製品の実装と構成に特化している場合があるものの、脆弱性の存在を証明するものです。PoCは、単独のエクスプロイトとして武器化されるか、エクスプロイトフレームワークに組み込まれます。PoCの存在により、攻撃者が脆弱性を悪用するための障壁が低くなります。2023年にDragosが評価したアドバイザリの23%は、公開時点でPoCが利用可能でした。

脆弱性のトレンド
VULNERABILITY TRENDS

認証が必要な脆弱性の増加
THE RISE OF AUTHENTICATION-REQUIRED VULNERABILITIES

2023年、侵害のために認証を必要とする脆弱性の数が大幅に増加しました。多数の記事になった一連の有名な脆弱性について、Dragosは最初に警告を出しました。これらの脆弱性はいずれも興味深い側面を持っています – すなわち、攻撃者が被害者のデバイスにアクセスし効果を実現するために、管理者権限アクセスなど、既存のアクセス権を要求します。

2023年のデータおよび過去のデータによると、認証が必要な脆弱性に関して明確な急増が報告されています。件数および比率（パーセンテージ）ともに著しい増加を示しています。



そのような急増の正確な原因を特定するのは難しいですが*、いくつかの要因が考えられます：

- 調査対象となった多くのデバイスやプロトコルが認証を組み込んでいます。これは良い兆候です。
- 認証を要求するルートキットの悪用が増加しています。例えばCiscoその他のリモート可用性サービスに対するものです。
- レガシープロトコルが持つ、悪用が簡単な脆弱性や常に存在する脆弱性（訳注：”everyday vulnerabilities”-前出の“foreverday vulnerabilities”の誤記か）はすでに発見されてCVEが割り当てられています（場合によっては複数回）。それゆえ、脆弱性研究者は他の場所を探す必要があります。

Dragos最前線の視点

Dragosは、この傾向が今後も続くと予想しています。セキュア・バイ・デザイン開発プロセス[14]を推奨するCISAの勧告は、ベンダーにとって、デフォルトで認証を提供する圧力になるはずです。新規インストールの要件定義および調達段階で、エンドユーザーがそうした報告書を引用することが重要です。

[14]セキュア・バイ・デザイン　https://www.cisa.gov/

重要なのは、脆弱性に特権が必要なことは防御側にとって良いことですが、パスワードが設定されているデバイスを安全と見なす理由にはならないということです。攻撃者はしばしば、総当たり攻撃、ソーシャルエンジニアリング、または製品のデフォルトの資格情報を知っているなど、さまざまな方法で資格情報を入手できます。一部のシステムでは、ユーザーが認証を完全に無効にすることがあり、そのような決定はCVSSスコアに反映されません。

脆弱性の種類別のトレンド分析
TREND ANALYSIS BY VULNERABILITY TYPE

Common Weakness Enumeration（CWE）識別子は、脆弱性を分類し、コミュニティが共通の言語で脆弱性を伝達できるようにする重要な役割を果たしています。これらは、CVE に割り当てられ、脆弱性の根本的な原因を説明するために使用されます。2023 年、Dragos は ICS に影響を与える各脆弱性を評価し、現実世界での使用に基づいていくつかの注目すべき CWE を見つけました。

領域外の読み取り/書き込み - CWE-787/CWE-125
OUT-OF-BOUND READ/WRITE - CWE-787/CWE-125

領域外の読み取りおよび書き込みの脆弱性は、毎年、最も悪用され公開されるCWEとして常に高い位置にランクされています。この傾向は、数万種類のデータ構造と数百のサードパーティ依存を有する複雑なシステムとその開発の複雑さに起因しています。

このような脆弱性は、データ構造の実装方法とアクセス方法を悪用します。開発者は、情報を体系化して保存するため一般的にデータ構造を使用します。その最も基本的な例が配列であり、複数のピースからなる情報を格納し、位置を指定することで任意のデータに簡単にアクセスできるようにする番号付きリストです。問題は、コードがこれらの構造の事前に定義された境界を超えて読み取るまたは書き込むことができる場合に発生します。

ベンダーがプロプライエタリな産業制御システム（ICS）プロトコルを採用し、エンジニアリングワークステーション（EWS）ソフトウェアがPLCに名前を割り当てるシナリオを考えてみましょう。内部では、PLCはそのメモリ内の配列にこのデータを格納し、この目的のために明示的に予約された領域があります。プロトコルコードが配列のサイズ内で文字の制限を課さない場合、攻撃者はこの脆弱性を悪用して、配列の意図したメモリスペースを超えて情報を書き込むことができます。例えば、攻撃者は、配列がサポートするサイズを超える名前を含むリクエストを送信し、結果として表示と制御の喪失を引き起こす可能性があります。すべてのデータアクセスに対するセキュアな境界チェックの確保、セキュアなプログラミング慣行の採用、包括的なコードセキュリティレビューが、バッファオーバーフローを防ぐために重要です。現代のソフトウェアではサードパーティライブラリが広く使用されており、開発者に気付かれない追加の潜在的な脆弱性の通り道になります。したがって、ベンダーがすべてのソフトウェア依存関係を追跡することが重要です。これは、手動での追跡やソフトウェア部品表（Software bill of materials - SBOM）サービスの利用によって実現でき、サードパーティのコンポーネン

STATISTICS

CWE-787 and CWE-125 consistently rank at the top with the most CVEs, the most public proof of concepts, and the most actively exploited vulnerabilities reported year over year. In 2023 alone, advisories reported twelve CVEs related to CWE-787 that have been exploited. This figure surpasses the CWE-787 and CWE-125 CVEs reported over the preceding three years of ten.

Advisories containing CVEs with CWE-787/CWE-125 (combined)

2022	2023	% of advisories
54	**67**	**12.6%**

Number of CVEs with CWE-787/CWE-125

Year	CWE-787	CWE-125	Combined
2022	180	94	274
2023	187	134	321
16% OF ALL CVEs			

Number of CVEs with CWE-787/CWE-125 and a public proof of concept (+ exploits)

Year	CWE-787	CWE-125	Combined
2022	40 of 180	27 of 94	67 of 274
2023	60 of 187	51 of 134	111 of 321

Notable impacted products in 2023

- CODESYS Runtime
- PHOENIX CONTACT PLCnext Firmware
- Hitachi Energy's SDM600
- Rockwell Automation 1756-EN2T

トに関連する潜在的なセキュリティリスクを特定し、管理するための積極的なアプローチを確保します。

悪用 EXPLOITATION

領域外の読み書きコマンドは、脅威グループによって頻繁に悪用されます。注目すべきケースとして、TRISISマルウェアが挙げられます。このマルウェアは、領域外の書き込みを利用してTriconex Safety Instrumented Systemを侵害しました。また、今年は、ある脅威グループがCVE-2023-3595に関する能力を開発していることが発見されました。この特定のCVEは、Rockwell Automation 1756 Ethernetモジュールに影響を与え、領域外の書き込みの脆弱性として分類されています。

OSコマンドインジェクション - CWE-78

OS COMMAND INJECTION - CWE-78

コマンド使用における特定要素の不適切な無効化（訳注：「中和、無害化」とも言う）はコマンドインジェクションとして知られており、アプリケーションがコマンドを実行するの際にユーザーから受け取ったデータを適切に扱えない時に発生するセキュリティ上の脆弱性です。この脆弱性の最も単純な形式では、攻撃者は入力を操作して、アプリケーションが意図しないコマンドをシステム上で無自覚に実行するようにします。攻撃者は、特別な文字を使用して元のコマンドから抜け出し、追加のコマンドを実行します。

このような問題は、特にpingなどのネットワークトラブルシューティングツールを備えたネットワーク機器で一般的です。通常、これらのツールはユーザー提供のIPアドレスを受け取り、それを下位のオペレーティングシステム上のpingコマンドに挿入します。もしデバイスがこの入力を適切にチェックまたは検証しない場合、悪意のあるユーザーは8.8.8.8;cat /etc/passwdのようなものを入力することができます。適切な検証がない場合、pingツールは操作システムでping 8.8.8.8;cat /etc/passwdというコマンドを実行し、誤ってパスワードファイルなどの機密情報をユーザーにさらすことになります。

コマンドインジェクションの脆弱性を防ぐためには、ベンダーは、強固な入力検証とサニタイズ、パラメータ化されたクエリの使用、およびユーザー入力からの直接的なシステムコマンドの構築を避けるなどの安全なコーディング慣行を採用する必要があります。

悪用 EXPLOITATION

Palo Alto Networksの報告では、CVE-2022-29303がMiraiボットネットのさまざまなバリエーションの拡散に使用されました。この特定のCVEは、CONTEC SolarView Compact電力モニタリングシステムに影響を与えました。このデバイスには電子メールサービスを含むWEBサーバーが含まれ、ユーザーが提供した電子メールアドレスを適切に検証していませんでした。脅威グループは、悪意のあるコマンドインジェクションリクエストを作成し、Mirai[15]の亜種をデバイスにダウンロードできました。

STATISTICS

2023年、OSコマンドインジェクションが最も積極的に悪用されたCWEの2番目に浮上し、また過去4年間、最も悪用された脆弱性のトップ3に常にランクされています。この持続的普及は重要な要因にひもづいています：過去4年間のOSコマンドインジェクションのCVEのうちの3分の1には、公開されたPoCがあります。これらの公開されたPoCの利用可能性により、悪用のハードルが下がり、OSコマンドインジェクションは攻撃者にとって魅力的な標的となります。このように簡単に利用できる手法の利用可能性は、悪用に必要な労力を減らします。そのため、DragosはDragosが開発したPoCの公開を禁止し、他のセキュリティベンダーにも同様の措置をとるよう奨励しています。

Number of advisories containing CVEs with CWE-78

2023	2022	2021	2020
17	9	10	4

Number of CVEs with CWE-78

2023	2022
47	23

Number of CVEs with CWE-78 and a public proof of concept (+ exploits)

2023	2022
13 of 47	3 of 23

Notable impacted products in 2023

- Siemens RUGGEDCOM ROX
- Delta Electronics DVW-W02W2-E2
- PHOENIX CONTACT WP
- Multiple WAGO controllers and HMI

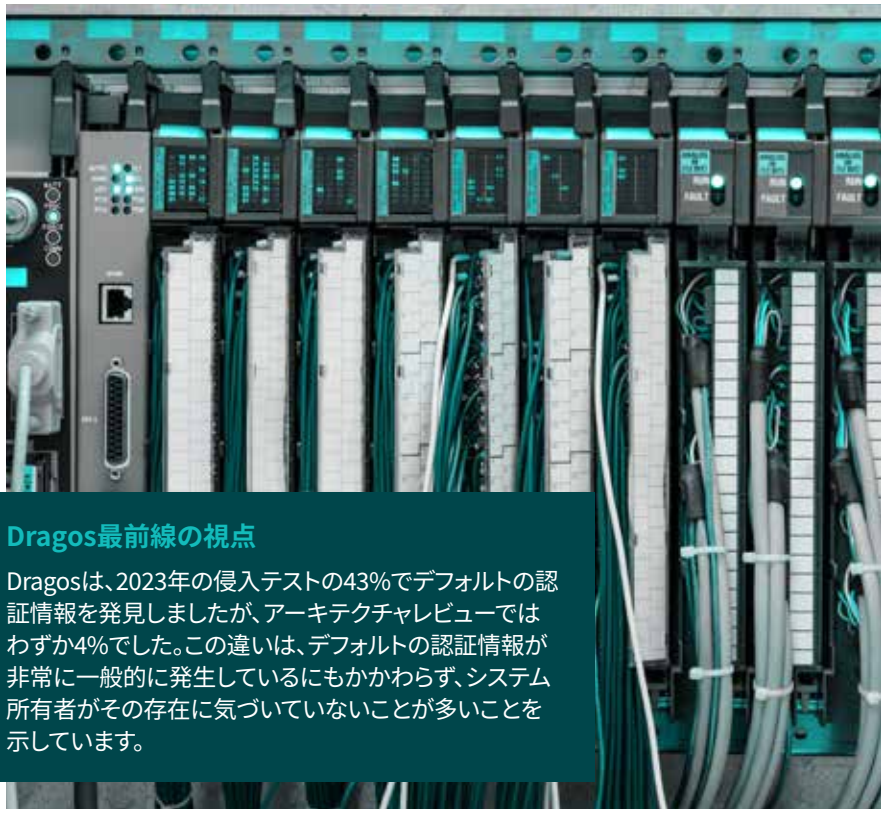
[15]Mirai - https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits

ハードコードされたクレデンシャル情報の利用 – CWE-798
USE OF HARD-CODED CREDENTIALS – CWE-798

ベンダーは、しばしば製品のソースコードに直接認証情報を埋め込んだり、製品のファイルシステムに静的なアクセスアカウントを含めたりします。これらのアカウントは通常変更できず、製品所有者はそれらを変更する手段を持ちません。攻撃者はこれらのパスワードを発見または解析し、特権アクセスを得るために使用します。ICS/OTでは、多くのベンダーが製品をメンテナンスインターフェース付きで出荷しており、これらはアセットオーナーに明示されていないため、これが一般的な問題となっています。

悪用 EXPLOITATION

BADOMENというPIPEDREAMマルウェアモジュールは、Omron PLCを標的とするために設計され、CVE-2022-34151を悪用しました。このCVEは、Omron NX/NJ PLCと通信するためにSysmac Studio EWSソフトウェアに静的にプログラムされた、ハードコードされた認証情報* と暗号化キーに関連しています。おそらくSysmac Studioをリバースエンジニアリングしたことで、CHERNOVITEという脅威グループがこれらの認証情報を発見し、BADOMENの開発に利用しました。その後、同じ認証情報が公開されました。これは、MicrosoftのCyberx研究チームによってGitHubにアップロードされ、Black Hat Europeで発表されたICS Forensics Toolsと呼ばれるプロジェクトでした。幸いなことに、プロジェクトがアップロードされた直後に、CVE-2022-34151を含むモジュールは削除されました。



Dragos最前線の視点

Dragosは、2023年の侵入テストの43%でデフォルトの認証情報を発見しましたが、アーキテクチャレビューではわずか4%でした。この違いは、デフォルトの認証情報が非常に一般的に発生しているにもかかわらず、システム所有者がその存在に気づいていないことが多いことを示しています。

STATISTICS

2019年以来、ハードコードされた認証情報のCVEの発生件数は、年間平均で133%増加しています。しかし、2023年に重大な変化が起こり、新たなハードコードされた認証情報のCVEが初めて減少しました。この年、Dragosはハードコードされた認証情報に関連するCVEを23件特定しましたが、これは2020年以来の最低件数であり、前年の40件から大幅に減少しています。この減少は、これらの脆弱性に対するセキュリティ意識が高まっていることに起因する可能性があります。さらに、ハードコードされた認証情報を持つ多くの一般的なシステムが既に発見され、開示されています。比較的防ぎやすいですが、ハードコードされた認証情報の脆弱性の影響は大きく、しばしば高度な特権アクセスをもたらします。

Number of advisories containing CVEs with Hard-Coded Credentials

2023	2022
17	23

CVEs with Hard-Coded Credentials

2023	2022
23	40

Number of CVEs with Hard-Coded Credentials and a public proof of concept that had exploits

2023	2022
3 of 23	1 of 40

Notable impacted products in 2023

- Moxa NPort IAW5000A-I/O Series
- Siemens SICAM A8000
- Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator
- PHOENIX CONTACT WP 6xxx

パス・トラバーサル – CWE-22

PATH TRAVERSAL – CWE-22

パス・トラバーサルの脆弱性は、Dragosが2023年に分析した中で最も蔓延している脆弱性のタイプの1つでした。一般的に、これらの脆弱性は、デバイス、ホスト、またはサーバーのローカルファイルシステムとやり取りするWebサーバーやその他のアプリケーションに影響します。また、プロジェクトファイルがアーカイブの一部としてファイルパスを含むエンジニアリングソフトウェアにも頻繁に影響します。

この脆弱性を悪用すると、多くの場合、ファイルシステム上の制限された領域または意図しない領域に対し、攻撃者が不正アクセスを獲得します。これらの問題は、一般的に、ファイルパスの構築やファイルシステム上のファイルへアクセスする際、ユーザー入力が適切に検証またはサニタイズされていない場合に発生します。

例えば、画像を提供するウェブサーバーが次のようなURLで画像を提供しているとします：https://x.y.z/images/johndoe.jpeg。攻撃者はエスケープ文字を使用することで、機密ファイルにアクセスするための悪意のあるURLを作成できます。この手の攻撃のベクトルはURLパスだけでないことに注意が必要です。ファイルアクセスのためにユーザー入力を使用するプロセスは、パス・トラバーサル攻撃に対して潜在的に脆弱である可能性があります。これに加えて、zipslips[15]などのさまざまなテクニックやユニバーサルネーミングコンベンション（UNC）パスインジェクションも、パス・トラバーサルの脆弱性を悪用するために使用されることがあります。

悪用 EXPLOITATION

CVE-2018-13379は、FortinetのFortiGateファイアウォールで使用されているFortiOSに影響を与えるパス・トラバーサルの脆弱性です。Dragosは、PARISITEやVANADINITEを含む攻撃者が、Fortinetのデバイスを使用している産業組織やICS組織に対してCVE-2018-13379に対するエクスプロイトを実行していることを確認しています。

CVE-2022-33971は、組み込みWebアプリケーションのパストラバーサルの脆弱性を含む、オムロンPLCの複数の個別の問題を対象とする未解決のCVEです。BADOMENツールを使用すると、ファイルAPIを介してPLCファームウェア上でのファイルのリスト化、取り出し、および上書きが可能です。

STATISTICS

パス・トラバーサルは、年々一貫して、最も一般的な脆弱性の一つです。過去3年間の平均で、年間54件のCVEを記録し、最も一般的な脆弱性のトップ5に位置しています。特に懸念されるのは、この CWE-22 が、2022 年の PIPEDREAMでこのテクニックが使用され、2019 年の PARISITE と 2020 年の VANADINITE による FortiOS に対する使用に次いで、2023 年に 2 番目に活発に悪用されており、常にトップ 5 にランクされていることです。とはいえ、パス・トラバーサルの脆弱性は比較的簡単に防止することができます。適切なユーザー入力の検証を実装することで、これらの問題を完全に回避することができます。今後の数年間で、この脆弱性タイプに対処し、緩和する取り組みが逆方向のポジティブなトレンドにつながることを期待しています。

Number of advisories containing CVEs with Path Traversal

2023	2022
23	**26**
4% OF ALL ADVISORIES	

Number of CVEs with Path Traversal

2023	2022
55	**53**
3% OF ALL CVEs	

Number of CVEs with Path Traversal and a public proof of concept that had exploits

2023	2022
10 of 55	**10 of 53**

Notable impacted products in 2023

- Omron Sysmac Studio and NX-IO Configurator (EWS Software)
- Schweitzer Engineering Laboratories SEL-5033 and SEL-5036 (EWS Software)
- Fortinet FortiOS (networking devices)
- Siemens SICAM A8000 Devices (Remote Terminal Unit)

[15]Zip Slip - https://security.snyk.io/research/zip-slip-vulnerability

NEIGHBORHOOD KEEPER の脆弱性データ

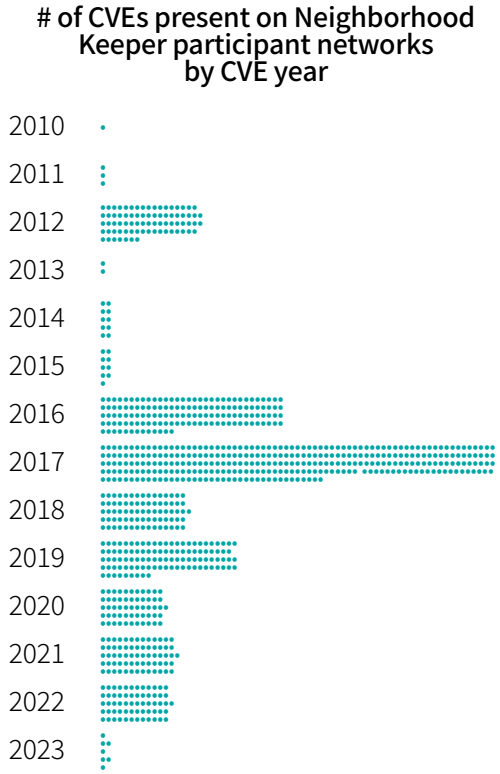
NEIGHBORHOOD KEEPER VULNERABILITY DATA

2023年、DragosはNeighborhood Keeperプログラムに脆弱性タグ付けを追加しました。これにより、Neighborhood KeeperのユーザーとDragosのアナリストの両方が、Neighborhood Keeper参加組織のネットワーク上の脆弱性に関するデータを取得できるようになりました。

このデータは、産業ネットワーク上でどの製品が最もパッチが適用されずに放置されているか、興味深い一端を提供しています。

おそらく驚くことではありませんが、PLC、HMIとしてマーケティングされている産業用コンピュータ、産業用ネットワークスイッチ、およびリモートIOデバイスが、脆弱なコンポーネントの大部分を占めています。

脆弱なコンポーネントに関して驚くべき点は、装置がしばしばパッチを適用されないまま放置されていることです。現在のNeighborhood Keeper参加の匿名性のため、脆弱性のあるコンポーネントの完全な数を収集することはできませんが、データはCVE yearごとに分類できます。特定のCVEがネットワーク上で発生した回数だけを数えた場合、年ごとのデータは以下のようになります。



Neighborhood Keeperデータを過度に解釈すると誤解を招く可能性があります。Neighborhood Keeperセンサーが配置されている場所、センサーによって識別できる脆弱性の両方の観点から、データには見え方のバイアスが存在します。後者の例として、ファイル形式の問題を含むエンジニアリングソフトウェアの脆弱性は、ほぼ確実にNeighborhood Keeperによって観察されません...ソフトウェアが自身を識別するためネットワークに対し非常に明確にブロードキャストでもしない限り、これらの脆弱性は個別のホストファイルシステムの検査を含めた徹底した評価によってのみ発見が可能です。

一方、データはいくつかの興味深い特徴を示しています。具体的には、多くの制御システムネットワークが長期間パッチを適用されない状態にあることが挙げられます。特定された脆弱性の半数以上が、2016年から2017年に日付が付いたCVEであり、つまり、6〜7年前に修正された脆弱性が2023年のネットワークで非常に一般的であったことを意味しています。

この分析からの得られる重要なポイントは、アドバイザリには代替緩和策が含まれることが絶対的に必要だということです。多くのエンドユーザーは、パッチが利用可能になってから何年も経っても適用しない場合があります。実際、それらのパッチが重要であると見なされた場合でも、多くのエンドユーザーは決してパッチを適用しないかもしれません。幸いなことに、これらのエンドユーザーは、脆弱なコンポーネントを守るための他の手段を講じています。

Neighborhood Keeperのデータをさまざまな角度から見てみると、Neighborhood Keeperのデータセットで最も頻繁に発生した脆弱性のうち、すぐに重要と分類された脆弱性はありませんでした。Dragosが Now (所有者が脆弱性を修正するために直ちに行動を起こす必要があることを意味する) として追跡した493件のCVEのうち、Neighborhood Keeperの参加組織のネットワークで確認されたのは86件だけです。これら86件の脆弱性の一部は、Neighborhood Keeperの参加組織全体に広がっています。

コミュニティ内でのある脆弱性の広がり具合は、侵害検知の開発優先度に関する分析でもあります。一部の脆弱性はパッチを適用せずに何年も何十年も経過する可能性があります。既知の脅威グループがそのコンポーネントをターゲットとしたり、また公開PoCエクスプロイトが利用可能になるなど、その脆弱性がクリティカルとなり、且つ、殆どのユーザーがパッチを適用しないことが観測される

場合、その脆弱性に対する侵害検知が非常に重要になります。

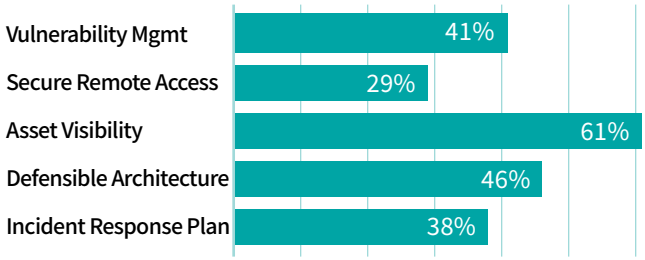
サイバー対策準備状況の評価
ASSESSING CYBER READINESS

2023年、重要インフラのアセットオーナー向けの規制が大きく変化し、組織はサイバーセキュリティイベントの備えに多くの時間とリソースを注ぐようになりました。そこには、北米の米国パイプライン事業者向け「TSA Pipeline-2021-02D (SD-02D) [16]」の更改”が含まれます。ヨーロッパでは「改正ネットワーク及び情報システム指令 (NIS2)[17] 」、オーストラリアでは「重要インフラ安全保障法 (SOCI Act)[18] 」、サウジアラビア王国では「Essential Cybersecurity Controls (ECC) [19]」があります。さらに大きな変化の1つは、対象を重要インフラに限定せず、米国で公開取引されている企業に対する、新しい「証券取引委員会 (SEC) サイバーセキュリティリスク管理規則」です。この規則は投資家が所有する公益事業や製造企業を含む、多くのOTアセットオーナーに適用されます。

Dragosは、組織がサイバーセキュリティ対応能力を向上させ、プロセスを定義または洗練し、計画を実施していることを観測しました。この分野をリードする組織は、ブレークグラス・リテーナー (訳注：break-glass retainer – ガラスブレーク型の緊急保護スイッチ) を活用する事後対応的な考え方から、検出能力、トレーニング、外部の専門家など組織内の各階層を含む総合的なインシデント対応アプローチに移行しています。

レジリエンスの向上は、OTサイバーセキュリティの重要対策5項目 (5 Critical Controls) [20]の中心となる観点です。2023年にDragosが提供したサービス契約のうち94%において、これら対策項目のいずれかに関連する発見がありました。ICSネットワークの可視性向上が、報告書の半数以上に現れ、トップを占めています。限られたログ記録とモニタリング、弱いセグメンテーション、アセットインベントリの不足など、他の上位項目もDragosが発表した5 Critical Controlsに関連する発見です。

2023 Service Engagements with 5CC Findings



Dragosは、顧客との机上演習で明らかになった知見を通じて、この変化を観察しました。2023年には、Dragosが支援した演習の量、種類、範囲が変化しました。2023年の机上演習の数は2022年から倍増し、役員および取締役会レベルの机上演習* は三倍になりました。これは、経営幹部がサイバーセキュリティイベントへの備えに注目している企業の増加を示しています。

この変化は業界全体で同じように認識されたわけではありませんが、ほぼすべての業界で机上演習への注目が高まっています。最も顕著な増加が見られたのは電力業界で、この業界の報告に占める机上演習の割合は、前年比で104%増加しました。産業界

Dragos最前線の視点

2023年、Dragosは長年の顧客と協力して、これまでで最大規模の演習を実施しました。この演習には、ビジネスの様々な部署とレベルを横断した350人以上の参加者が含まれていました。そこでは、レスポンダー、オペレーター、関連するビジネスユニット、パートナー、リーダーが、インシデント対応、事業継続、危機管理計画を用って大規模サイバーセキュリティイベントに対応する訓練を行いました。この演習は、2023年に観測された脅威グループの活動と能力をモデルにしています。

[16] https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf
[17] https://www.nis-2-directive.com/
[18] https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018
[19] https://nca.gov.sa/ar/ecc-en.pdf
[20] https://hub.dragos.com/guide/5-critical-controls

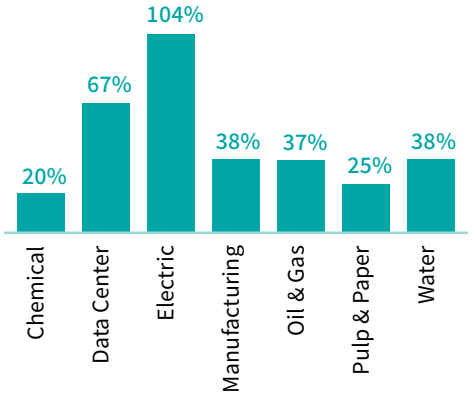
全体を通して、チームは机上演習に焦点を移しています。

規制が演習実施を組織に対して要求していない場合でも、多くの組織は意識と準備を高めるために、意欲的に演習を実施しています。これは、今年の最も重要な規制変更*の1つであるSECサイバーセキュリティリスク管理規則の場合も同様です。SECの規則では、登録事業者は、サイバーセキュリティインシデントが重大であると判断した後、4営業日以内にそのイベントを開示することを要求しています。また、組織がどのようにしてサイバーセキュリティの脅威からの重大なリスクを評価/特定/管理し、取締役会が監督を行うか説明することも求めています。

机上演習の結果と関連する推奨事項は、ICS/OTサイバーセキュリティの準備とインシデント対応に関するコア機能別に整理されています（検知、通知、アクティブ化、対応、封じ込め、文書化、回復）。米国国立標準技術研究所 (NIST) プロセスの4つのステップ、SANSの準備-識別-封じ込め-根絶-回復-教訓 (PICERL)や他のバリエーションのどれを用いる場合であっても、コア機能は、標準的インシデント対応プロセスに対応します。インシデント対応計画がどのように構成されているかに関わらず、サイバーセキュリティイベントを正常に処理するために必要な機能です。

最も低い総合スコアを持つコア機能は「通知」であり、また、2023年にはすべての機能のスコアが低下しました。特に、「封じ込め」の能力は前年比19%減少しました。「封じ込め」のコア機能では、適切な行動を取る前にイベントの範囲と影響を理解する必要があります。

2023 Tabletop Exercise Share Growth per Industry (2022–23)



Dragos最前線の視点

米国で活動する公開企業が参加するほとんどの演習において、SEC 8Kの規制要件は主要なテーマになりました。経営層と取締役会は、サイバーセキュリティリスクの管理と統治について積極的な役割を担っています。

Core Capability	2022 Score	2023 Score	Change
Detect	73%	65%	-8
Activate/Elevate	81%	67%	-14
Respond	76%	62%	-14
Contain	81%	64%	-17
Communicate	76%	57%	-19
Document	73%	65%	-8
Remediate/Recover	81%	61%	-20

Metrics are as follows

- Performed without Challenges **80-100**
- Performed with Some Challenges **66–79**
- Performed with Major Challenges **50–65**
- Unable to Perform **0–49**

Figure 13: Average Tabletop Exercise Scores (All OT)

Dragos最前線の視点

Dragosの机上演習のファシリテーターは、充分に発達した検出能力とプロセスを有する成熟した組織でさえ、システムオペレーターやエンジニアが提供し得る専門知識について見落としていることに気付きました。サイバーセキュリティの意識を日常の活動、特にトラブルシューティングに統合することで、貴重な人的検出能力を実現できます。

すべての業界が同じように機能するわけではありません。2023年において、電力業界は全てのコア能力を総合したスコアで59%と最も低い評価を受けました。

Core Capability	Electric	Oil & Gas	Manufacturing	Pharma
Detect	61%	68%	63%	69%
Activate/Elevate	63%	65%	69%	69%
Respond	60%	70%	60%	56%
Contain	61%	65%	60%	69%
Communicate	51%	68%	52%	56%
Document	58%	63%	69%	69%
Remediate/Recover	61%	70%	63%	50%

Performed without Challenges **80-100**
Performed with Some Challenges **66–79**
Performed with Major Challenges **50–65**
Unable to Perform **0-49**

Figure 14: Average Tabletop Exercise Scores by Industry

2023年、ランサムウェアが最も共通したシナリオであり、全体の50%を占めています。ランサムウェアに対するスコアは、いずれのコア機能においても、すべてのシナリオを含む平均スコアよりも低くなっています。

Core Capability	Score
Detect	61%
Activate/Elevate	72%
Respond	67%
Contain	59%
Communicate	60%
Document	66%
Remediate/Recover	67%

Dragos最前線の視点

Dragosの観察では、OTに特化したインシデント対応計画とランサムウェア対応プレイブックを開発し活用している組織はパフォーマンスが高いです。残念ながら、これらを実装している組織はまだ非常に少ないです。Dragosによると、エンゲージメントの27%に組織のインシデント対応計画に弱点があり、12%はOTインシデント対応計画が完全に欠如していました。これは業界全体で均等に分布しているわけではなく、エンゲージメントに占める割合のうち、インシデント対応計画に関する（訳注：弱点などの）所見が多いのは製造業や化学業界でした。

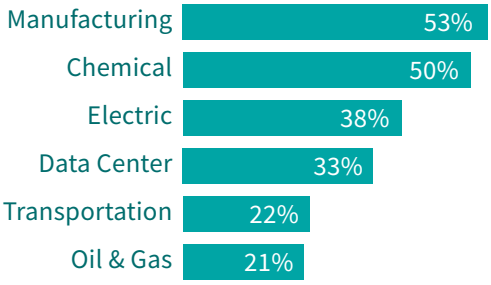


Figure 15: Incident response planning findings by industry

Dragos is an industrial (ICS/OT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Dragos.com

株式会社マクニカ
Dragos担当
dragos-sales@macnica.co.jp