NOZOMI NETWORKS LABS

エグゼクティブサマリー

OT/IoTセキュリティレポート

サイバー戦争に関する洞察、脅威とトレンド、推奨事項

2022年上半期レビュー | 2022年8月

エグゼクティブサマリー

絶えず変化するサイバー脅威の状況下において、それが組織にどのように影響を与えているかを理解することがこれまで以上に重要になっています。過去6か月間で、攻撃者による新たな戦術の使用に加え、攻撃の頻度と複雑さが急上昇しています。過去には可能性が低いと思われていた脅威が、突然ありふれたものになりました。

例えば、以前はランサムウェアの標的ではなかった企業が、現在はその攻撃の被害を受けています。このような変化に加え、攻撃者は、セキュリティソリューションによる攻撃活動の検出を巧妙に妨げる行動を続けています。

セキュリティを強化し、将来の脅威を最小化するために、企業はサイバーリスクへの全容をリアルタイムに把握し、充分な情報に基づいて自社を保護する最善の方法を決定できなければなりません。

本レポートは以下の内容で構成されます：

- **サイバーセキュリティ**の状況をまとめます。
- **現在の脅威**における主要な動きを特定し、それらに対抗するためのソリューションを提案します。
- **ロシア/ウクライナ**危機を振り返り、この紛争を通じて得られた攻撃者の能力に関する洞察、また新しい攻撃ツールとマルウェアがどうやって侵入するかをご紹介します。
- **モノのインターネット**（IoT）のボットネット、対応するセキュリティ侵害インジケーター（IoC）、攻撃者の戦術/テクニック/手順（TTP）に関する知見を提供します。
- **推奨事項**と予測分析を行います。

2022年上半期における脅威の状況

2月に起こったロシアによるウクライナ侵攻開始以来、以下のようなことが起こっています：

ハクティビストの活動

国家の支援を受けたAPTとサイバー犯罪

ワイパー型マルウェア

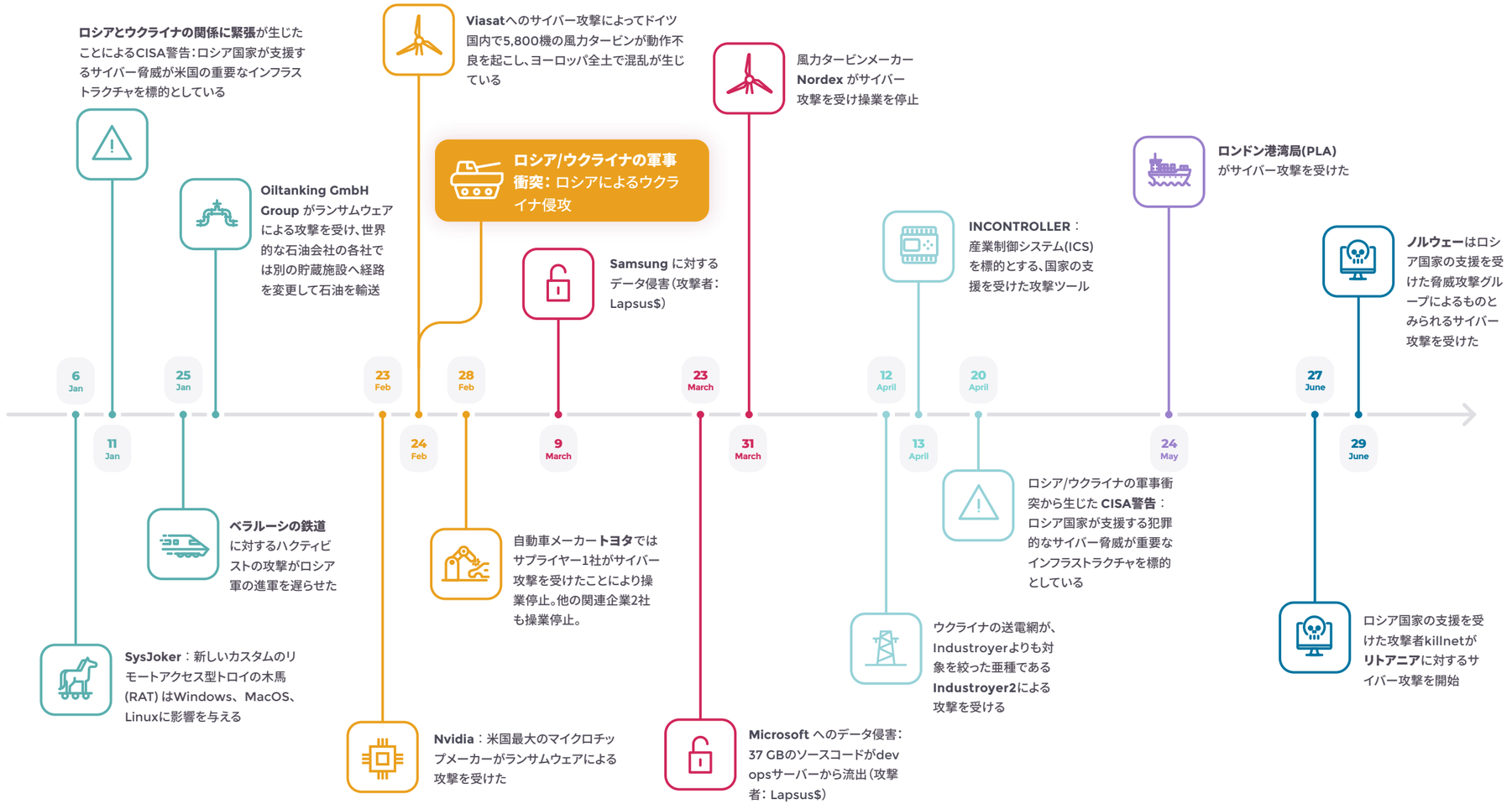
Industroyer2

2022年上半期で注目を集めたサイバー事件のタイムライン

このページでは、現在の脅威を取り巻く状況を形成してきた、2022年1月～6月の重要なサイバー事件の一部をタイムラインで紹介していきます。

2022年2月にロシアがウクライナへの侵攻を開始して以来、ハクティビスト、国家が支援するAPT、サイバー犯罪者など、さまざまな種類の攻撃者による活動が見られてきました。

また、ワイパー型マルウェアの使用も着実に普及しており、Industroyer2と呼ばれるIndustroyerの亜種が、産業環境で広く使用されているIEC-104プロトコルを悪用する目的で開発されました。



IoTボットネットの状況

Nozomi Networks Labsのハニーポットはデータを収集、分析して攻撃者の活動に関する重要な知見を提供しています。2022年上半期は、以下のようなトレンドが見られました：

- **攻撃者が最も多い国：**サイバー活動は、中国と米国のIPアドレスに由来するものが最も多くなっています。両国は高度なハイテク産業と製造業を抱えるため、攻撃対象が増加したと考えられます。
- **ハードコードされた認証情報を含むプロトコル：**Miraiは、もともとTelnetを悪用する有名なボットネットでしたが、攻撃者がソースコードを公開したため、SSHやその他のプロトコルを標的とする亜種が作られてきました。
- **最も多く使用される認証：**「root」と「admin」の認証は、攻撃者がすべてのシステムコマンドとユーザアカウントにアクセスできる可能性があるため、明らかに魅力的な標的となっており、複数の亜種で使用されています。
- **最多の個別攻撃者IPアドレス：**当社のハニーポットが悪意のある活動に関連したIPアドレスを収集したところ、月別では4月における活動が最も盛んであり、5,000件近くの個別攻撃者IPアドレスが判明しました。
- **最も多く実行されたコマンド：**当社では上位10個のコマンドを特定しており、enable, shell, system,which lsが名を連ねています。約12,500のボットがこれらのコマンドを実行しました。

4月
はボットネットが最も盛んに活動していた月で、およそ

5,000
に上る個別攻撃者のIPアドレスが判明しました。

2022年上半期におけるIoTボットネットの詳細な活動については、**レポートの完全版**をご参照ください。

脆弱性を取り巻く状況

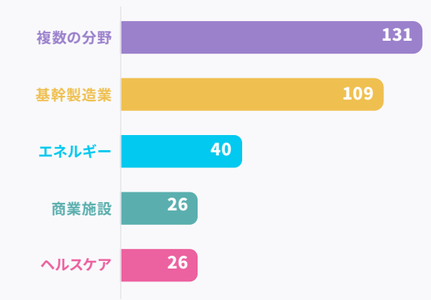
多くのICSソフトウェアおよびハードウェア製品のセキュリティ体制は、主にセキュリティ研究者が発見した脆弱性を通じて開示されています。2022年上半期には、ICS-CERTによって560件の共通脆弱性識別子（CVE）が発表され、そのうち303件が2022年に新しく見つかったものでした。2021年下半期と比較して、報告されたCVEの件数は14%減少しました。

報告されたCVEのうち、131件が複数の分野に影響を及ぼしました。最も直接的な影響を受けた分野は基幹製造業で、109件のCVEが報告されました。次に多かったのがエネルギー業界の40件で、ヘルスケアと商業施設がいずれも26件で第3位となりました。さらに、60社ものベンダーがCVEアドバイザリに記載され、172の製品が関連しています。影響を受けたベンダー数は27%増加し、影響を受けた製品数は2021年下半期から19%の増加となりました。

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560件
の公表されたCVE

最も大きな影響を受けた業界



推奨事項

組織内でどの関係者でも実装できる、予防的なセキュリティ対策を講じる必要性が高まっています。これには、セキュリティの問題について視点が異なるであろうIT部門、コンプライアンス担当者、リスク管理者が含まれます。最優先のセキュリティ対策には以下があげられます：

- 資産目録を正確に維持する
- VPNテクノロジーに関する最新版のパッチを実装する
- 特権アクセスを管理する
- ビッシングやSIMスワッピングの被害を受けにくい強力な多要素認証（MFA）を使用する
- パスワードを頻繁に変更する
- ビッシングやソーシャルエンジニアリング全般に関する従業員の研修を増やす

追加の軽減策：

- **バックアップ：** ランサムウェアやワイパー型マルウェアの攻撃によってデータが完全に消失しないよう、定期的にデータをバックアップし、バックアップシステムをテストし、運用中のサーバーとは異なるネットワークでオフサイトの場所にバックアップを格納してください。
- **脅威インテリジェンス：** サイバー脅威インテリジェンスとは、組織がシステムとデータを保護するのに役立てるために、サイバー脅威に関する情報を収集、分析、配布する手法です。この情報に含まれる内容として、マルウェアの特徴、攻撃対象の領域、セキュリティ侵害インジケーター（IoC）が挙げられます。
- **クラウドのセキュリティ：** クラウドプロバイダーが定評を得ていること、ISO27001やSOC1/2/3認定などの業界標準に準拠していること、データの保存または転送時に暗号化していること、多要素認証（2FA）とID管理ツールを使用していることを確認します。
- **脅威の検出：** 脅威の検出は、将来の事象に対する警告となるのに加え、潜在的な脅威をリアルタイムで検出して対抗するために使用します。脅威の検出では、1つのIPアドレスから送られる異常な量のトラフィックや、特定のサービスへの多数の接続など、疑わしい活動がないか、システムがネットワークを監視します。これは、長い期間にわたって異常なアクティビティを監視したり、既知の脆弱性についてネットワークをスキャンすることによって実施できます。
- **ソフトウェア部品表（SBOM）：** SBOMには、各コンポーネントの異なるバージョンがいくつ存在し、それらが使用されている場所についての情報が記載されているため、時間の経過に伴う変更を追跡し、他のコンポーネントでの問題発生を防止するのに役立ちます。また、どのコンポーネントが他のコンポーネントよりも露出度が高く、脆弱であるかを理解し、それらの脆弱性を軽減する方法を理解するのにも役立ちます。SBOMはまだ広く使用されていませんが、このテクノロジーの開発動向を見守ることには意義があります。

より強力なセキュリティを目指した重要な脅威の軽減

予測

この最新の分析に基づいて、2022年末までの期間で予測される主要なサイバーセキュリティのトレンドのいくつかを以下に示します：

- ICS関連の攻撃の増加
- ランサムウェアによる攻撃者は、引き続き重要なインフラ企業を攻撃
- 大企業を標的とした攻撃の増加
- 技術ソースコードの盗難
- 今年初頭に確立された民間/政府のイニシアチブに伴い、 サイバーポリシーとガバナンスが強化

OT/IoTセキュリティレポートをダウンロードする

Nozomi Networks Labsは、脅威の現状を分析し、以下の情報を提供します：

- 最近のランサムウェアとIoTボットネット攻撃
- ICS、OT/IoTデバイスの脆弱性と悪用のトレンド
- サイバー脅威に対する復旧戦略を改善するための手順

ダウンロードする

Nozomi Networks

OTとIoTのセキュリティと可視化を実現する業界最先端ソリューション

Nozomi Networksは、世界の重要なインフラストラクチャ、産業、政府組織をサイバー脅威から保護することで、デジタルトランスフォーメーションを加速します。当社のソリューションは、OTおよびIoT環境向けに、ネットワークと資産の可視化、脅威の検知、洞察を最高水準で提供します。顧客からの信頼を受け、当社は運用の回復力を最大限に向上しつつ、リスクと複雑さを最小限に抑えます。

NN-SEC-RP-ES-JA-2022-1H-001

nozominetworks.com