【報道関係各位】

2023 年 11 月 22 日

【Zscaler ThreatLabz 調査結果】IoT/OT マルウェア攻撃が前年比で 400%増加 重要インフラを保護するゼロトラスト セキュリティの強化が急務

2023 年版 Zscaler ThreatLabz エンタープライズ IoT および OT の脅威レポートを発表 最も標的にされた製造業と教育業界、特に教育業界では IoT マルウェア攻撃が 1000%近く増加

※本資料は、米カリフォルニア州にて 2023 年 10 月 24 日(現地時間)に発表したプレス リリースの日本語抄訳版です。

主な所見

- **最も標的にされた業界は IoT と OT に大きく依存する製造業**で、ブロックされた IoT マルウェア攻撃の 54.5%を占め、週に平均 6,000 件の攻撃が発生
- **教育業界に対する IoT マルウェア攻撃が急増**し、前年比 961%増を記録
- **最も標的にされた国はメキシコと米国で**、攻撃全体の 69.3%を占める結果に
- **OT 分野で懸念が高まっている IoT ボットネットの活動は引き続き活発で**、攻撃ペイロードの 66%が Mirai と Gafgyt のマルウェア ファミリーに由来

カリフォルニア州サンノゼ、2023 年 10 月 24 日 – クラウド セキュリティ業界を牽引する Zscaler (NASDAQ: ZS、以下ゼットスケーラー)は本日、2023 年版 Zscaler ThreatLabz エンタープライズ IoT および OT の脅威レポートを発表しました。本年度のレポートでは、Zscaler Zero Trust Exchange™プラットフォームが保護する IoT デバイスに対して行われた約 30 万件のブロックされた攻撃を分析し、6 か月にわたるマルウェアの動向を詳細に調査しました。本調査結果から、IoT マルウェア攻撃の増加率が前年比 400%以上となったことが明らかになっています。異なるネットワーク間を移動するマルウェアは重要な OT インフラを危険にさらす可能性があるため、OT セキュリティ対策を喫緊の課題として取り組む必要があります。

ゼットスケーラーの調査チームである ThreatLabz はデバイス フィンガープリンティングを通じて IoT デバイスの属性とアクティビティーを把握し、IoT マルウェアの脅威状況を分析することに焦点を当てました。これまで以上に多くの業界、組織、個人がインターネットに接続されたデバイスを利用する中で、マルウェアや古い脆弱性に起因する脅威が増大しています。組織はゼロトラスト アーキテクチャーを採用することで、IoT デバイスのトラフィックを可視化し、IoT セキュリティのリスクを最小限に抑えられます。

ゼットスケーラーのグローバル CISO 兼セキュリティ　リサーチ担当責任者であるディーペン・デサイ(Deepen Desai)は次のように述べています。「IoT デバイス メーカーが十分なセキュリテ

ィ対策を講じていない現状は、企業のシャドーIoT デバイスが急激に増加しているという事実と相まって、グローバル組織に大きな脅威をもたらしています。脅威アクターの多くは、『パッチが適用されていない管理対象外のデバイス』を標的にして、ネット環境への最初の足掛かりを得ます。こうした課題に対処するには、決して信頼せず、常に検証し、侵害を想定するゼロトラストの原則を適用して、IoT や OT デバイスを保護する必要があります。これらのデバイスをセグメント化するために検知と監視を継続的に行うことで、ラテラル ムーブメントのリスクを排除できます」

◇依然として増加傾向にあるマルウェア攻撃

IoT や個人向けコネクテッド デバイスが着実に普及しつつある中、IoT マルウェア攻撃が前年比で400%以上増加していることが本レポートで明らかになりました。この極めて高い増加率からも、IoT マルウェア攻撃を仕掛けるサイバー犯罪者がいかに執拗で、変化する状況への適応能力が高いかをうかがい知ることができます。

また、サイバー犯罪者は古い脆弱性を主な標的にしており、最も一般的な IoT 攻撃の 39 件のうち 34 件は、特に 3 年以上前から存在する脆弱性を狙ったものであることがわかりました。Mirai や Gafgyt のマルウェア ファミリーが依然として攻撃ペイロードの 66%を占めており、感染した IoT デバイスでボットネットを作成して収益力のある企業にサービス拒否(DDoS)攻撃を仕掛けています。ボットネットを利用した分散型 DDoS 攻撃は、あらゆる国や業界で数十億ドルの経済的損失を引き起こすだけでなく、重要な産業プロセスを混乱させ、ひいては人命を危険にさらしかねないことから、OT の大きなリスクとなっています。

◇最も狙われた製造業 – 驚異的な増加率をみせた教育業界

製造業と小売業が IoT デバイス トラフィックの 52%近くを占め、3D プリンター、ジオロケーション トラッカー、産業用制御機器、自動車用マルチメディア システム、データ収集端末、決済端末がデジタル ネットワーク経由で信号の大部分を送信しています。しかし、サイバー犯罪者にとって絶好の標的となるのが、この膨大な量のデバイス トラフィックです。現在、製造業では週に平均 6,000 件の IoT マルウェア攻撃が発生しています。こうした攻撃は、自動車、重工業、プラスチックやゴムなどの工業製造プラントで不可欠な OT プロセスを中断させる恐れもあるため、製造業のセキュリティ部門にとって長期的な課題となっています。また、産業用 IoT は独自の IoT デバイスを最も多く採用しており、その数は他の業界の 3 倍以上と大きく差を付けたことからも、製造業がレガシー インフラの自動化とデジタル化に向けた IoT ツールの導入を継続的に推進していることがわかります。

教育業界もまた、2023 年にサイバー犯罪者から特に狙われた業界の 1 つとなりました。これは、学校のネットワーク内に保護されていないシャドーIoT デバイスが急増したことで、攻撃者がより簡単に侵入できるようになったためと考えられます。教育機関はネットワーク上に豊富な個人データを保存しているため特に魅力的な標的となり、学生や運営組織は被害を受けやすくなっています。本レポートによると、教育業界での IoT マルウェア攻撃は 1000%近い増加をみせています。

◇最大の標的となった米国とメキシコ

調査結果によると、米国は IoT マルウェア作成者にとっての最大の標的であり、IoT マルウェアの 96%が米国内の侵害された IoT デバイスから配布されています。

IoT マルウェアの感染の 46%を占めるメキシコは、最も感染数の多い国となりました。感染数上位 4 か国のうち 3 か国(メキシコ、ブラジル、コロンビア)は、いずれも中南米諸国となっています。

◇IoT および OT 攻撃から保護する Zscaler Zero Trust Exchange™

Zscaler Zero Trust Exchange プラットフォームはゼロトラスト セキュリティへの包括的なアプローチです。Zero Trust Exchang はアイデンティティーとコンテキストを検証し、制御を適用し、ポリシーを施行してから、任意のネットワークを介してデバイスとアプリケーション間に安全な接続を確立します。

Zscaler Internet Access™ (ZIA™)は、アイデンティティーベースのアクセスとリスクに基づく包括的なセキュリティで、IoT デバイスと企業ネットワーク間のテレメトリーのやり取りを保護します。

Zscaler Privileged Remote Access は、リモート ワーカーやサードパーティー ベンダーに機密性の高い RDP、SSH、VNC のプロダクション システムへのクライアントレス リモート デスクトップ アクセスを提供するため、管理対象外デバイスにクライアントをインストールしたり、ジャンプ ホストや VPN にログインしたりする必要がありません。この機能により、リモート ワーカーやサードパーティー ベンダーは、ネットワークや重要インフラの安全性を損なわずに OT デバイスにアクセスし、サービスを提供できるようになります。ゼットスケーラーは ZIA や Zscaler Privileged Remote Access を備えたゼロトラスト プラットフォームで企業ネットワークのセキュリティを確保します。

2023 年版 Zscaler ThreatLabz エンタープライズ IoT および OT の脅威レポートは、こちらからダウンロードして確認できます。

◇調査方法

本レポートの調査には、2023 年 1 月～6 月までの多数のソースと各業界からのデバイス ログの分析が使用されました。

本レポートは、それぞれ 1 日あたり 500 兆を超えるシグナルを処理し、90 億の脅威とポリシー違反をブロックし、25 万件以上のセキュリティ アップデートを提供する、ゼットスケーラーのグローバル セキュリティ クラウドに接続する顧客のデプロイメントから得られたデータに基づいています。

◇ゼットスケーラーについて

ゼットスケーラー(NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™は、世界最大のインライン型クラウド セキュリティ プラットフォームです。

Zscaler ホームページ　:https://www.zscaler.jp/

Zscaler Zero Trust Exchange :https://www.zscaler.jp/platform/zero-trust-exchange

2023 年版 Zscaler ThreatLabz エンタープライズ IoT および OT の脅威レポート:
https://www.zscaler.jp/resources/2023-threatlabz-enterprise-iot-ot-threat-report