2022 年 9 月 7 日

プレスリリース

Nozomi Networks Labs レポート: ワイパー型マルウェアと IoT ボットネットが脅威の主流に製造業とエネルギー業界が最も高いリスクに直面する産業分野に

2022 年上半期、ロシア/ウクライナ戦争、接続デバイスの増加、脅威攻撃者の *IoT* ボットネットが、*ICS* の脅威状況に最大の影響をもたらす

OT/IoT セキュリティのリーダーである Nozomi Networks Inc.は本日、Nozomi Networks Labs の 2022 年上半期 OT/IoT セキュリティ動向レポートを発表しました。本レポートでは、、ワイパー型マルウェア、IoT ボットネットの活動、ロシア/ウクライナ戦争が 2022 年上半期の脅威状況に影響を及ぼした事が明らかにされています。

ロシアが 2022 年 2 月にウクライナへの侵攻を開始して以来、Nozomi Networks Labs の研究者は、ハクティビスト、国家的 APT、サイバー犯罪者など、複数のタイプの脅威攻撃者の活動を検知しています。また、ワイパー型マルウェアが活発に利用されていることが判明し、インダストリアル環境で一般的に使用されている IEC-104 プロトコルを悪用するために開発された「Industroyer」の亜種である「Industroyer2」が出現していることも確認されています。

さらに 2022 年上半期において、悪意のある IoT ボットネットの活動の増加や、巧妙さの進化が確認されました。Nozomi Networks Labs は、脅威攻撃者がどのように IoT を標的にするかについてより詳細なインサイトを得るため、これらの悪質なボットネットを引き付け、その活動を捕捉するハニーポットを設置しました。本調査では、ハードコードされたパスワードとエンドユーザー認証のためのインターネットインターフェースの両方について、セキュリティ上の懸念が高まっていることが明らかになりました。2022 年 1 月から 6 月にかけて、Nozomi Networks のハニーポットで以下のものが発見されました。

- 3 月が最も活発な月で、5,000 近いユニークな攻撃者 IP アドレスを収集
- 攻撃者の IP アドレスの上位が、中国と米国に関連
- 脅威攻撃者がすべてのシステムコマンドとユーザーアカウントにアクセスする手段として、「root」と「admin」の認証情報が最も頻繁に標的とされ、複数のバリエーションで使用

脆弱性の面では、**製造業**と**エネルギー業界**が引き続き最も脆弱であり、**ヘルスケア**と**商業施設**がそれに続いています。2022 年 1 月～6 月の脆弱性トレンドは以下の通りです。

- CISA は 560 の共通脆弱性識別子（CVE）をリリース - 2021 年下半期から 14%減
- 影響を受けたベンダー数が 27%上昇
- 影響を受ける製品も 2021 年下半期から 19%増加

Nozomi Networks OT/IoT セキュリティリサーチ エバンジェリストである Roya Gordon は、次のように述べています。
「今年のサイバー脅威の状況は複雑です。接続機器の増加、悪意のある行為者の高度化、攻撃動機の変化など多くの要因が、侵入やサイバーフィジカル攻撃のリスクを高めています。それと同時に、セキュリティの防御策も進化しています。リスクを最小限に抑え、回復力を最大限に高めるために必要なネットワークの可視化、動的な脅威の検知、実用的なインテリジェンスを重要インフラ組織に提供するソリューションが、現在提供されています。」

Nozomi Networks の「OT/IoT セキュリティレポート」は、セキュリティ専門家に、下記に記載されたリスクモデルとセキュリティ対策の再評価に必要な最新の洞察と、重要インフラの安全確保に向けた実用的な推奨事項を提供します。

- サイバーセキュリティの現状の振り返り
- 脅威の動向とその解決策
- ロシア/ウクライナ危機の総括と、関連する新たな悪意あるツールやマルウェアのハイライト
- IoT ボットネットおよびそれに対応する IoC、脅威アクターの TTP に関するインサイト
- 推奨 ・ 予測分析

関連資料:

- OT/IoT セキュリティレポート。サイバー戦争の洞察、脅威と傾向、改善策
- **ウェビナーにご登録ください:** Nozomi Networks 2022 年上半期の OT/IoT セキュリティレビュー：重要インフラへの教訓

Nozomi Networks について

Nozomi ネットワークスは、世界の重要インフラ、産業、政府機関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/IoT 環境に対して、優れたネット

ワークと資産の可視性、脅威検出、インサイトを提供します。お客様は、リスクと複雑さを最小限に抑えると共に、運用弾力性を最大限に高めることができます。 www.nozominetworks.com

お問い合わせ先：
担当：清水
Nozomi Networks 広報事務局
e-mail: nozomi@jspin.co.jp