プレスリリース

2023 年 2 月9日

# Nozomi Networks Labs レポート: 破壊とランサムが 2022 年の脅威の大半を占める

## 重要インフラへの破壊的な攻撃は、運輸産業、医療と公衆衛生産業、基幹製造業とエネルギー産業などを標的とし *2022* 年後半まで継続

OT および IoT セキュリティのリーダーである Nozomi Networks, Inc.は、Nozomi Networks Labs の 2022 年下半期 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、ワイパーマルウェア、IoT ボットネット活動、ロシア/ウクライナ戦争が 2022 年の脅威状況に大きな影響を及ぼしたことが明らかになりました。Nozomi Networks Labs の研究者は、2022 年前半に見られた傾向が継続し、ハクティビストがデータの盗難や DDoS 攻撃から、より破壊的なワイパーマルウェアを利用した戦術にシフトし、ロシア/ウクライナ戦争における政治力をさらに強めるために重要インフラを不安定にしようしていることを確認しました。

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。
「過去 6 ヶ月間、サイバー攻撃は著しく増加し、輸送から医療まで幅広い産業に大きな混乱をもたらしています。特に鉄道は攻撃の対象となり、鉄道事業者とその資産を保護するための対策が実施されています。サイバー脅威が進化・激化する中、脅威者がどのように OT/IoT をターゲットにしているか、脅威者から重要な資産を守るために必要な行動を理解することは、組織にとって重要です。」

Nozomi Networks Labs が過去 6 ヶ月間に顧客から寄せられた侵入警告を分析した結果、重要インフラ環境へのアクセス脅威のトップは「クリアテキストパスワード」と「弱いパスワード」であることが判明しました。次いで、ブルートフォース攻撃（総当り攻撃）、DDoS 攻撃の試みが上位を占めています。また、企業の IT ネットワークを狙うマルウェアとして、トロイの木馬が最も多く検出され、リモートアクセスツール (RAT) は OT を標的とし、 DDoS マルウェアは IoT デバイスを標的としていました。

悪質なIoTボットネットの活動は高水準で推移し、2022年後半も上昇を続けています。Nozomi Networks Labsは、ボットネットがIoTデバイスへのアクセスを試みる際にデフォルトの認証情報を使用し続けていることから、セキュリティ上の懸念が高まっていることを指摘しました。

Nozomi Networks の IoT ハニーポットから 得られた独自の知見(2022 年 7 月～ 12 月):

- 7 月から 11 月にかけて攻撃が急増し、各月で 5,000 以上のユニークな攻撃が行われました
- 攻撃者の IP アドレスの上位は、中国、米国、韓国、台湾に関連するものでした
- 「root」と「admin」の認証情報は、脅威者がネットワークに初期アクセスし、権限をエスカレートさせる方法として、今でも最も頻繁に使用されています

脆弱性の面では、基幹製造業とエネルギー産業が引き続き最も脆弱であり、次いで上下水道システム産業、医療と公衆衛生産業、運輸産業となっています。

2022 年の過去 6 ヶ月間で:

- CISA が公表した「共通脆弱性識別子（CVE）」は 218 件で、上半期から 61%減少しました
- 影響を受けたベンダーは 70 社で、前回の報告期間から 16%増加しました
- 影響を受けた製品も 2022 年下期から 6%増加しました

Nozomi Networks の「OT/IoT セキュリティレポート: ICS 脅威の現状に関する詳細」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インサイトと、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。

**関連資料:**

- Nozomi Networks Labs OT/IOT セキュリティレポート 2022 年下期レビュー
- **ウェビナーにご登録ください:** ICS 脅威の現状に関する詳細
- 英文ブログ記事

**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・神谷
Nozomi Networks 広報事務局
e-mail: nozomi@jspin.co.jp