2022 年 3 月 30 日

プレスリリース

Nozomi Networks Labs レポート: 法執行機関の反撃が加速する中、ランサムウェア集団とサプライチェーンの脆弱性がリスクとして浮き彫りに

2021 年下半期に脆弱性が *21%*増加し、巧妙化する犯罪攻撃が定期的ニュースになる中、組織によるターゲットを絞った改善の取り組みによって反撃

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 の最新 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、2021 年後半もランサムウェアと Ransomware as a Service（RaaS）攻撃がサイバー犯罪の中心となる一方で、ステートスポンサード攻撃の増加が明らかにされています。

医療、交通、食料生産などの重要インフラは非常に脆弱で、攻撃された場合に社会の混乱を招く可能性があるため、攻撃者にとって儲かる標的とされてきました。7 月から 12 月までに脆弱性は 651 件報告され、過去 6 カ月間に比べて 21%増加しました。サプライチェーンの脆弱性は、製品、サービスプロバイダー、エンドユーザーなど広範囲に渡って被害を拡大させます。

Nozomi Networks が年 2 回のレポートを発行して以降はじめて、防御側がセキュリティとレジリエンスに関する戦略を向上させ、優位に立つ兆候が見られました。2021 年の後半には、国際的な法執行機関が一丸となってランサムウェアの集団を取り締まり、ビットコインによる身代金を押収し、犯罪者を逮捕するという取り組みが行われました。また、Apache Log4j の脆弱性がこれまでで最も広く悪用されたセキュリティ侵害になるという予測に反して、予測されたような壊滅的な損失には至りませんでした。

Nozomi Networks の共同創業者兼 CTO である Moreno Carullo は、次のように述べています。「セキュリティ組織と法執行機関は反撃しています。より多くのセキュリティ専門家が防御とレジリエンスの両方の対策を最新のものにし、侵害後の対応において成果を上げていることを示す良い兆候が見られます。脅威は増加傾向にありますが、脆弱性や攻撃の本質をより深く理解できるようになった今、脅威を打ち負かすための技術や手法が利用できるようになりました。多くの組織がセキュリティと状況認識を強化し、攻撃に直面した場合にも備えるようにすることを推奨します。」

Nozomi Networks の「OT/IoT セキュリティレポート」は、セキュリティの専門家に、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。

- 脅威の概要説明:
  - ランサムウェアの注目すべきアップデート
  - 2021 年後半におけるサプライチェーン攻撃
  - アクセスブローカー市場の状況
- ICS-CERT の脆弱性に関する最新統計 - 悪用傾向の深堀り
- 組織が新たな脅威の一歩先を行くための改善戦略

関連資料:

- OT/IoT セキュリティ レポート
- 最新レポート: 重要インフラへの攻撃動向と対策
- **ウェビナーにご登録ください:** 2021 年下半期 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
e-mail: nozomi@jspin.co.jp