TLP:CLEAR Distribution is not limited.

NRECA Threat Analysis Center

April 2025

Full report is available to NRECA Threat Analysis Center (TAC) Participants.
Contact: TAC@nreca.coop

Report Summary: 2024 Threat Intelligence Year-In-Review – Impacts to Cooperative Electric Utilities

The NRECA Research[1] (NRECA) Threat Analysis Center (TAC) and Electricity Information Sharing and Analysis Center (E-ISAC), with contributions from Meridian Cooperative, National Information Solutions Cooperative (NISC), and Federated Insurance, have published a joint report to provide an overview of the major threat activities throughout 2024. Of the cybersecurity activities witnessed in 2024, two primary themes emerge which impact the cooperative electric utility community:

1. Nation-state actors are increasingly using sophisticated, difficult-to-detect methods to penetrate critical infrastructure networks with strategic disruption and espionage goals, and
2. Ransomware-as-a-Service tools have reduced the cost of running ransomware attacks and facilitated "double extortion" techniques, i.e. encrypt and exfiltrate, to force payments for both decryption and to avoid data exposure.

Generally, many cooperative utilities may have had a lower cybersecurity risk profile than other electric utilities due to their size. However, this may change due to heightened threat actor and opportunistic ransomware attacks. Consequently, each utility is strongly encouraged to assess their risk profile and consider the appropriate mitigations to reflect this new landscape.

The report authors have identified the use of phishing-resistant multi-factor authentication (MFA) across both the information technology (IT) and operational technology (OT) networks as one of the most valuable risk mitigation strategies that a utility can implement, if they have not done so already. This report highlights other high-impact mitigation techniques in associated threat sections. Review of the cybersecurity incidents experienced throughout the cooperative utility community in 2024 by the report authors indicate that these highlighted mitigations may have prevented many of the successful attacks and reduced the frequency and severity of "near-miss" events.

Beyond these mitigations, conducting a self-assessment is a valuable method to identify gaps and prioritize cybersecurity investments for risk reduction. The NRECA Co-op Cyber Goals program provides foundational steps for cooperative electric utilities to advance their cybersecurity maturity, but more detailed industry assessments can provide a granular understanding of current cybersecurity posture. For further reading, reference the Goal 2 (Self-Assessment) resources provided with the NRECA Co-op Cyber Goals program and the NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan.

In the Physical Security domain, 2024 threat levels remained elevated throughout the year with more than 4,500 physical security incidents shared with the E-ISAC. Of that number, less than 3 percent of incidents, largely arising from vandalism, theft, ballistic damage, and tampering of equipment, resulted in some level of operational impact to the electric grid. Additionally, drones remain a security concern and an emerging risk to critical infrastructure, specifically within the electricity industry.

Cooperative utilities are encouraged to join both the TAC and the E-ISAC to receive and share threat intelligence to counter cybersecurity and physical threats that impact us all. Contact: TAC@nreca.coop

[1] NRECA Research is a wholly controlled subsidiary of NRECA. It is a 501(c)(3) charitable organization.

NRECA America's Electric Cooperatives

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER