Industry:
Energy and Utilities

Use cases
- Expand visibility
- Improve detection coverage & accuracy
- Accelerate incident response

corelight

Case study

National CERT disrupts coordinated zero-day attack on European critical infrastructure

A SILENT, COORDINATED ATTACK ON THE ENERGY GRID

In May 2023, a European nation's critical energy infrastructure faced its most extensive cyberattack to date. Over a few days, a sophisticated threat actor launched a coordinated, multi-wave campaign that compromised 22 different energy companies. The attackers demonstrated deep preparation, knowing exactly which companies to target without error.

The attack began by exploiting a critical zero-day vulnerability (CVE-2023-28771) in widely deployed firewalls protecting industrial control systems (ICS) and operational technology (OT) across the decentralized energy sector. The first wave was a model of stealth; attackers compromised 11 companies by sending a single, specially crafted data packet to gain control of their firewalls. By targeting firewalls, ICS, and OT (devices without typical endpoint defenses), attackers can create highly sophisticated attacks that evade traditional defenses.

Just as the sector's cybersecurity center and its members worked to contain the first wave, a second evasive attack began—this time using additional zero-day vulnerabilities (later identified as CVE-2023-33009 and CVE-2023-33010). This wave also showed connections to infrastructure previously used by the Sandworm APT group, raising the stakes significantly. The attackers' ability to bypass traditional defenses and operate with such precision created a systemic risk capable of disrupting the nation's power and heat supply.

FINDING THE "ONE PING ONLY" WITH HIGH-FIDELITY NETWORK EVIDENCE

Defense efforts hinged on a cross-sector sensor network powered by Corelight, which provided deep visibility into network traffic across hundreds of member companies. This centralized monitoring was the key to seeing the bigger picture. While an individual company might miss a single anomalous packet, the broader view revealed a coordinated pattern.

When the first wave hit, Corelight's detailed logs enabled analysts to quickly identify the 16 targeted companies and confirm the 11 successful compromises. Corelight's value became even more apparent during the second wave, particularly with the potential involvement of an advanced persistent threat.

The breakthrough came when analysts detected traffic to an IP address previously attributed to Sandworm. The communication consisted of a single TCP packet of just 1,340 bytes, with no response—a maneuver designed to evade detection. Without high-fidelity evidence from Corelight, this nearly invisible signal would have been lost in a sea of data. This discovery enabled the national team to confirm a serious intrusion, alert authorities, and guide members to take immediate action, such as going into "island mode" to sever internet connections and protect OT environments.

CRITICAL INFRASTRUCTURE SECURED, LESSONS LEARNED

Thanks to rapid detection and response enabled by Corelight, the attack was neutralized before the actors could pivot from compromised firewalls into critical OT networks.

There was no operational impact on the nation's electricity or heat supply.

Key outcomes:

- **Attack disruption:** A sophisticated, multi-wave attack across 22 organizations was stopped before adversaries could gain control of critical infrastructure.
- **Systemic risk averted:** Cross-sector visibility exposed a systemic threat invisible to individual companies.
- **Rapid, coordinated response:** High-fidelity network evidence supported swift collaboration with suppliers and authorities, including guiding some organizations into "island mode" for days to ensure complete eradication.

This incident validated a collaborative, visibility-first defense model. It proved that even the most advanced and stealthy attacks can be defeated with the right network evidence and a coordinated response.

WHY CORELIGHT?

In a scenario where attackers exploit zero-day attacks use evasive techniques designed to "fly under the radar," traditional security tools are insufficient. Corelight provides the decisive layer of high-fidelity network evidence necessary to see what other tools miss. Protocol-rich logs transform billions of packets into structured, queryable data, making it possible for a small team to find a single malicious packet that unraveled the entire campaign.

corelight

To learn more about zero-day attacks, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497