Critical Broadcast Program

TLP:GREEN All-Points Bulletin 22-05
December 5, 2022

CBP APB 22-05 – Recent Physical Security Attack Against the Grid

Summary

In 2022, especially since August, the E-ISAC has observed an increase in serious physical security incidents on the grid involving vandalism, tampering, arson and ballistic damage. These incidents have been classified as attacks based on their level of severity including the targeting of electrical substations, and to a lesser extent, transmission lines throughout North America, particularly in the Pacific Northwest and Southeast sections of the United States.

At this time, the E-ISAC is not aware of any additional specific threats to the grid. However, it assesses with **medium confidence** that such attacks are likely to continue. The E-ISAC closely tracks a variety of threats to the grid through close coordination with industry members, law enforcement, and intelligence partners at the Federal Bureau of Investigation (FBI), National Counter Terrorism Center, the Department of Homeland Security Office of Intelligence and Analysis, and the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response. Through these partnerships, the E-ISAC has shared a multitude of government bulletins, open-source reporting, and analytical products with industry raising awareness on emerging threats to electrical infrastructure, including threats from domestic violent extremists.

Analysis

The December 3 ballistic attacks in North Carolina occurred on two substations, a 115 kV and a 230 kV. The attacks targeted the substations' transformer radiators as well as their circuit breakers. This resulted in the substations being removed from service, forcing five additional undamaged 115 kV substations to be powered down and causing outages for approximately 42,000 customers (see post here).

Prior to this event, the E-ISAC shared information regarding a series of attacks at six different substations in Oregon and Washington State, four of which involved damage to control houses (see December 1 post here). The additional two incidents involved ballistic attacks on an 115kv transformer and two reactors through the use of small caliber firearms. Five of the six incidents resulted in power disruptions. The suspects(s) in these incidents remain at-large.

The E-ISAC has observed a variety of tactics from these events, firearm use being the most common. Although the tactics have varied between incidents, the events have shown general consistency. Some observations:

- Ammunition and caliber casings recovered include: .380, 9mm, and .223
- Shots were taken from both inside and outside the perimeter of the substations

TLP:GREEN

Other tactics include manual manipulation of controls; damage caused by hammers and blunt instruments; and arson, including metal cables thrown at bus work.

Analyst Comment

Given the number of attacks, geographic distribution, and nature of incidents, the E-ISAC assesses with **medium confidence** that these events are a mix of individual criminal activity, lone-wolf attempts, and small-cell actions intended to disrupt the grid. While the motivations and inspiration of the attacker(s) are currently unknown, the E-ISAC assesses with **low confidence** that the attacks are motivated by a mix of ideologies and extremist content. There have been several publications this year of extremist manuals and documents encouraging attacks on critical infrastructure, and there is a constant drumbeat in the online sphere encouraging vandalism and sabotage. Previous E-ISAC posts on specific incidents and extremist content are provided for reference below.

Members are encouraged to be aware of this trend involving serious attacks and to continue to remain vigilant and work with your local law enforcement partners to understand any local threats. Be on the lookout for pre-event surveillance reconnaissance activity. If you experience damage to equipment or assets, carefully assess whether the incident was intended to cause an outage or sabotage key assets and share that information and assessment with law enforcement partners and the E-ISAC. In addition, if you experience a serious incident at a site, be alert for potential follow-on attempts at the same site or other sites in the local area within the following days or weeks.

A summary of clustered and repeated attacks this year is attached to this post, including a list of protective measures during periods of high alert.

Recommended Protective Measures

The E-ISAC encourages members to maintain a heightened awareness of suspicious activity in and around their facilities and assets. Additionally, due to the number of serious incidents taking place right now combined with the heightened threat environment, we encourage members to review any suspicious or criminal activity at your sites and consider the possibility that these events could potentially have been acts of sabotage. We also strongly suggest you share any information with your FBI field office or Joint Terrorism Task Force to ensure they have visibility on such incidents and to provide support and assistance as needed. Members are also encouraged to coordinate with local law enforcement to determine if any extremists, anarchists, activist groups, or affiliated organizations have discussed the targeting of critical infrastructure in their operating areas, including heightened attention to insider threats.

These measures address actions during periods of elevated risks:

- Consider implementing 24/7 assessment of closed-circuit television and intrusion detection systems at all critical facilities and projects.
- Increase frequency of random checks of vehicles, vehicle contents, persons, and personally carried items entering or accessing project assets.

TLP:GREEN

- Implement access control measures to identify and process all personnel, visitors, vehicles, vendors, and contractors (i.e., photo IDs, uniforms, marked vehicles, visitor passes, contractor IDs displayed by all personnel while in critical buildings or areas).
- Limit access to critical facilities or features to authorized persons through measures such as unique or restricted keying systems, remote "smart locks," or access card systems.
- Deploy security forces to regularly inspect facility perimeters, buildings, parking lots, locker rooms, equipment, trash containers, HVAC systems, and sensitive or critical areas for signs of security issues.
- Advise all personnel at each facility to report the presence of unknown suspicious persons, vehicles, mail, and other suspicious activities.
- Maintain awareness of the potential psychological stressors the current environment could have on utility employees. Review (or consider developing) employee wellness programs, insider threat mitigations, and policies and processes to ensure employees have access to and are aware of the resources available to address such concerns.
- Increase monitoring, surveillance, and inspection of sensitive and critical areas, people, vehicles, materials, and equipment. Reassign staff to assist with surveillance, monitoring, and inspection duties.
- Request increased patrol checks of your critical sites from local law enforcement.
- Maintain unity of message with corporate communicators and local authorities to counter the spread of misinformation—consider coordinating with your trade association or the Electricity Subsector Coordinating Council.
- Consider hosting a Vulnerability of Integrated Security Analysis Workshop to effectively assess your site's physical protection system. Contact physicalsecurity@eisac.com to request a no-charge workshop.

For additional suggested protective measures, see Suggested Protective Measures for Alert Periods and VBIED Protective Measures, along with Transmission Line Corridor: Physical Security Considerations.

Potential indicators of threat activity which could also be the result of a threat actor probing a utility's physical protection system:

- Recent threats received via phone, email, or in-person
- Recent acts of vandalism to site or equipment, including objects thrown onto site to potentially trigger alarm or security systems
- Recent acts of intrusion, cut fences, broken locks

For questions, comments, or to share information, email operations@eisac.com, call 202-790- 6000, or post appropriate information on the E-ISAC Portal.

The E-ISAC will continue to monitor for related activity if observed in the electricity sector or closely related sectors, and will provide relevant updates to further the information described in the Microsoft report as it becomes available. If you have any questions or comments, please contact operations@eisac.com or dial

TLP:GREEN

Watch Operations at **202-790-6000**. Members and partners are also encouraged to share information through these channels and posting vetted information on the E-ISAC Portal where appropriate.

References

Additional information regarding extremists groups and attributable incidents is available on the E-ISAC Portal:

Recent Incident References

- TLP:AMBER – 000015522
- TLP:GREEN – E-ISAC Physical Security Incident Cluster of Incidents at Substations in Pacific Northwest
- TLP:GREEN – E-ISAC Physical Security Bulletin: FBI LIR Report – RMVE Threat to Electrical Infrastructure
- TLP:GREEN – Neo-Nazi and Eco-fascist Telegram Channels Promote BES Sabotage
- TLP:GREEN – Security Operations Online Threat Analysis Report
- TLP:GREEN – Eco-fascist Terrorgram Channel Promotes Burning Down Power Stations
- TLP:AMBER – 000015026

Historical References for Targeting the Grid and/or Accelerationist Groups

- TLP:WHITE – White Supremacy Terror Plot Targeting Power Grid
- TLP:GREEN – Group with Ties to Racially Motivated Violent Extremists Charged with the Targeting of Energy Facilities
- TLP:GREEN – Situational-Awareness Only Additional Images Promoting the Targeting of Electricity Assets Circulated on Encrypted Apps
- TLP:GREEN – Neo-Nazi forum circulates post appearing to target electrical infrastructure

For more information or assistance, please contact E-ISAC Operations (via email) or at **202-790-6000**.