**National Forensic Sciences University**

**School of Cyber security and Digital Forensics**



**Subject: CTMSCS S2 P1 Network Security**

**(TA-II Assignment)**

**Submitted to: Mr. Nilesh Panchal**

**Submitted by: Disha Sharma (240103002014)**

**Submission Date: 16/04/2025**

**INDEX**

1. Summary and Background
2. Impact Assessment
3. PCAP Files Analysis
4. Conclusion
5. References

**SUMMARY AND BACKGROUND**

Numerous consumers in Ukraine were impacted by unplanned power disruptions that Ukrainian electricity companies encountered on December 23, 2015. Furthermore, spyware discovered in Ukrainian businesses across a range of vital infrastructure industries has also been reported. The BlackEnergy (BE) malware was found on the organizations' computer networks, according to public sources. However, it is crucial to remember that BE's involvement in this incident is yet uncertain until additional technical investigation.

To work together and learn more, an interagency team from the Department of Energy, Federal Bureau of Investigation, North American Electric Reliability Corporation, U.S. Computer Emergency Readiness Team (US-CERT), National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Cybersecurity and Communications Integration Center (NCCIC) traveled to Ukraine. The U.S. team and the Ukrainian government collaborated closely and transparently, exchanging intelligence to help stop future cyberattacks.

**IMPACT ASSESSMENT**

Researchers looking into the incident have determined that a power outage that occurred in December in a portion of Kiev, the capital of Ukraine, was a cyberattack.

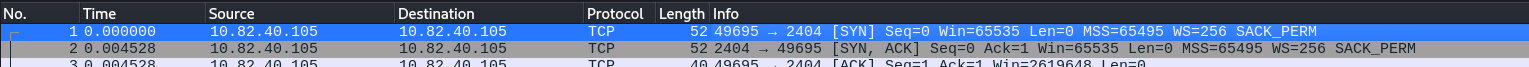
The blackout began just before midnight on December 17 and lasted for just over an hour.

Information Systems Security Partners (ISSP), a cyber-security firm, has connected the incident to a 2015 breach and blackout that impacted 225,000 people.

According to the national energy firm Ukrenergo at the time, the 2016 power outage had cost Kiev almost one-fifth of its nighttime power use.

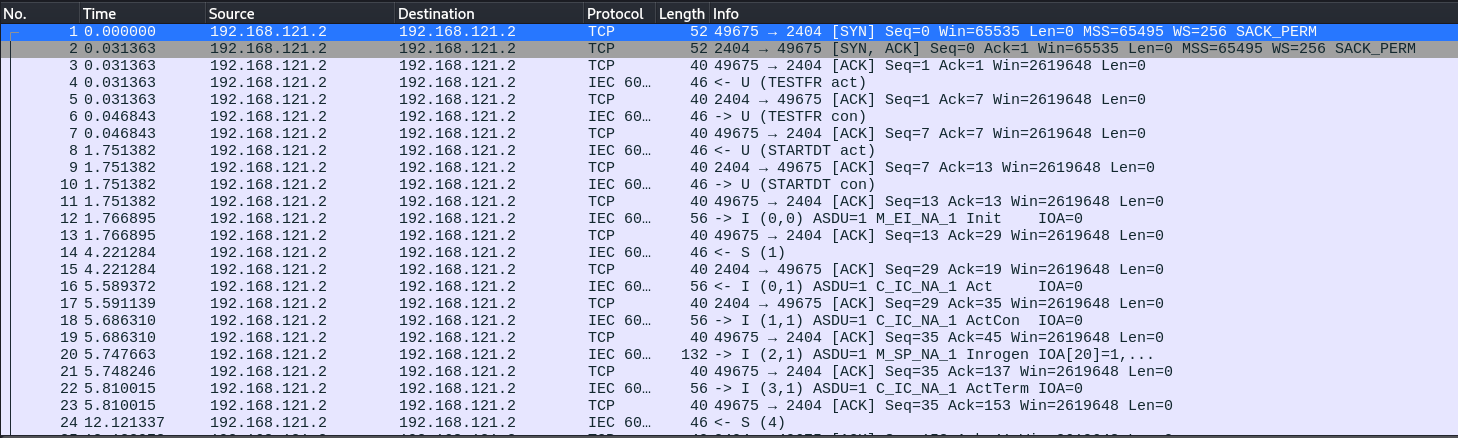
People in parts of the city and the surrounding area were left without energy until just after 1:00 a.m. due to the disruption of the Pivnichna substation outside the capital.

**PCAP FILE ANALYSIS**

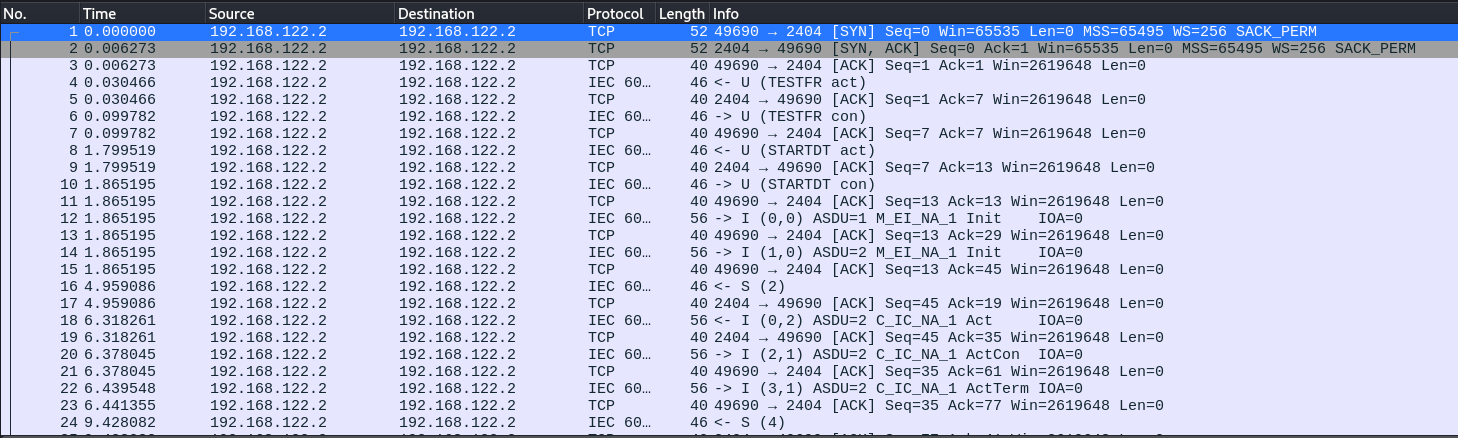


One of the PCAP files shows an attempt to connect to port 2404. Port 2404 (TCP) - IEC 60870-5 -104, used to send electric power telecontrol messages between two systems via directly connected data circuits. This can help us correlate the attempt to the Industroyer malware that affected the Ukraine power grid.

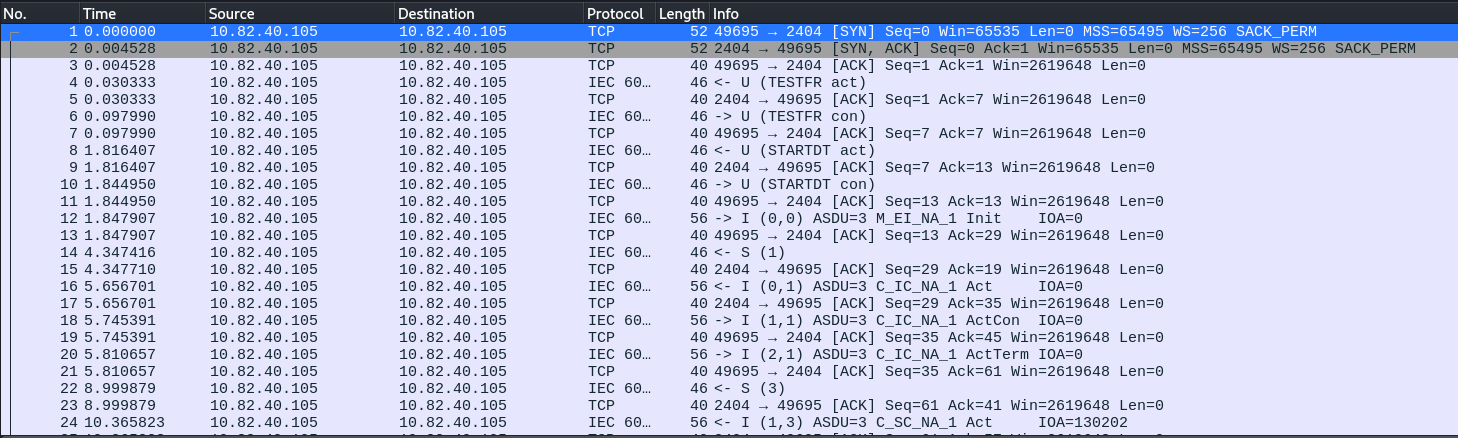
When the Industroyer2 virus was launched, it created three distinct threads, one for each IEC-104 server it needed to communicate with. If all three servers were accessible, the malware would speak to them simultaneously.



This thread communicates with the station at 192.168.121.2

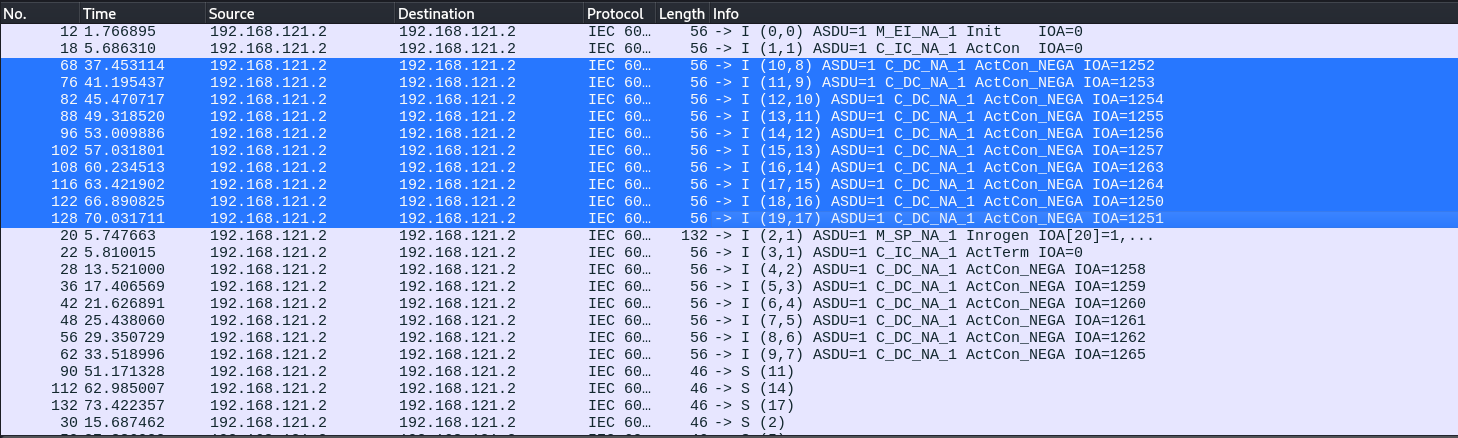


This thread communicates with the station at 192.168.122.2

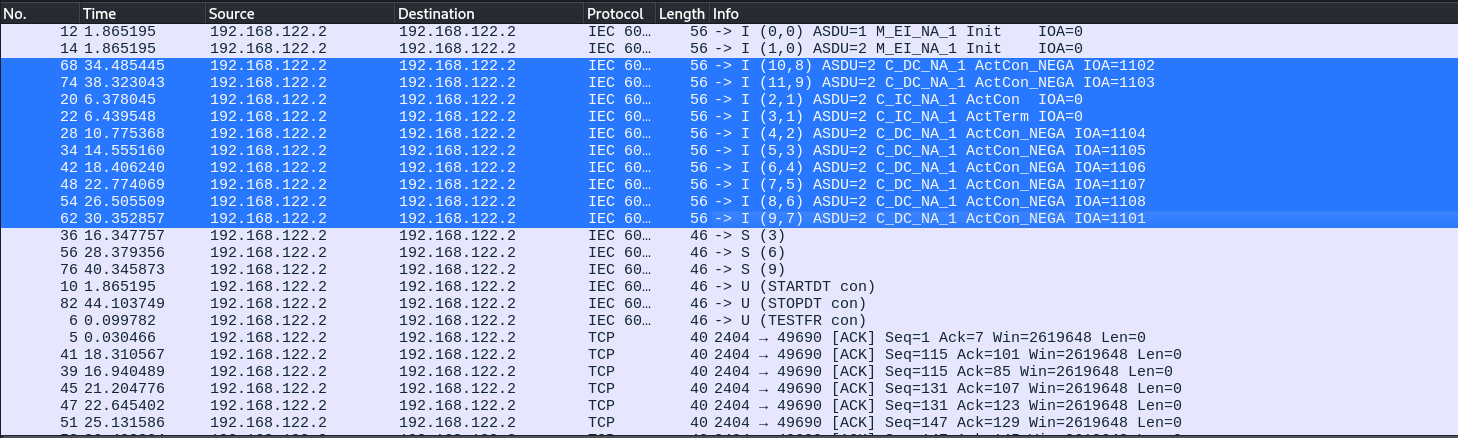


This station communicates with 10.82.40.105

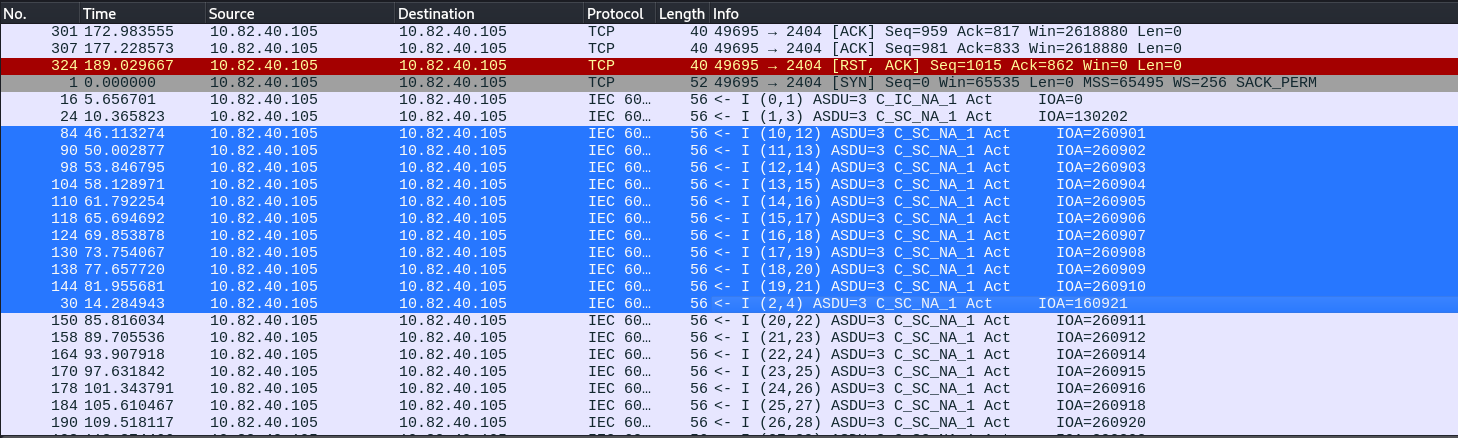
All outputs between 1250 and 1265 were toggled to OFF at Station Address 1 (often referred to as the "ASDU address" or "common address") by the thread that was connected to IP address 192.168.121.2. These outputs most likely regulate circuit breakers, which are used to cut off electricity to an electric utility substation, based on the command type that was utilized (ID 46 with short pulse length).



On 192.168.122.2 the malware targeted station address 2, where it toggled outputs between 1101 and 1108 to OFF.



The malware toggled a great deal of outputs on 10.82.40.105, which had station address 3. But in contrast to the other stations, many of these outputs were toggled to the “ON” state rather than “OFF”.



The malware's ability to toggle these particular outputs rather than merely turning them on or off at random suggests that the threat actors were technically knowledgeable about the substation or substations they were targeting. The attackers were also aware of each targeted output's IP addresses, station addresses, and IOAs. Additionally, they were aware of the appropriate ASDU Type ID for each output. Type ID 46, also called "double command" or C\_DC\_NA\_1, was used for IOAs 1101–1404, and Type ID 45, also called "single command" or C\_SC\_NA\_1, was used for IOAs 130202 and above.

**Critical Infrastructure Simulation in Cisco Packet Tracer**

**Network Topology**:

[Attacker PC (Python Script)]

[Cisco 4331 Router (NAT)]

* [Cisco Firepower 2110 (ACL: Permit TCP/2404)]
* [Control Center (SCADA Server)]

* {Substation 1 (RTU: 192.168.121.2)]
* [Substation 2 (RTU: 192.168.122.2)]

* {Substation 3 (RTU: 10.82.40.105)]

**REFERENCES**

* “Ukraine Power Cut ‘Was Cyber-Attack.’” *BBC News*, BBC, 11 Jan. 2017, www.bbc.com/news/technology-38573074.
* “Cyber-Attack against Ukrainian Critical Infrastructure: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. Accessed 16 Apr. 2025.
* “ENISA, European Union Agency for Cybersecurity.” *ENISA*, www.enisa.europa.eu/. Accessed 16 Apr. 2025.