Confirmation of a Coordinated Attack on the Ukrainian Power Grid

ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

SANS ICS

Michael Assante
January 6, 2016

After analyzing the information that has been made available by affected power companies, researchers, and the media it is clear that cyber attacks were directly responsible for power outages in Ukraine. The SANS ICS team has been coordinating ongoing discussions and providing analysis across multiple international community members and companies. We assess with high confidence based on company statements, media reports, and first-hand analysis that the incident was due to a coordinated intentional attack.

The attackers demonstrated planning, coordination, and the ability to use malware and possible direct remote access to blind system dispatchers, cause undesirable state changes to the distribution electricity infrastructure, and attempt to delay the restoration by wiping SCADA servers after they caused the outage. This attack consisted of at least three components: the malware, a denial of service to the phone systems, and the missing piece of evidence of the final cause of the impact. Current evidence and analysis indicates that the missing component was direct interaction from the adversary and not the work of malware. Or in other words, the attack was enabled via malware but consisted of at least three distinct efforts.

The Multiple Elements

The cyber attack was comprised of multiple elements which included denial of view to system dispatchers and attempts to deny customer calls that would have reported the power out. We assess with high confidence that there were coordinated attacks against multiple regional distribution power companies. Some of these companies have been reported by media to include specifically named utilities such as Prykarpattyaoblenergo and Kyivoblenergo. The exact timeline for which utilities were affected and their ordering is still unclear and is currently being analyzed. What we do know is that Kyivoblenergo provided public updates to customers, shown below, indicating there was an unauthorized intrusion (from 15:30 - 16:30L) that disconnected 7 substations (110 kV) and 23 (35 kV) substations leading to an outage for 80,000 customers.

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

The key significance here is that 80,000 customers comprise a significant portion of their residential load. Power was restored to all customers by (18:56L). They also reported technical failures with their call line interfering with receiving customer's calls as shown below.

12/24/2015

Dear customers!

23 December 2015 there was a technical failure in the infrastructure, making it difficult to dial call center PJSC "Kyivoblenergo."

We apologize for any inconvenience.

Quick action by utility staff to switch to "manual mode" and restore the system was impressive. Statements from utility staff to local media indicated the distribution system was being run without the benefit of their SCADA as it was still infected. Field staff at the impacted power companies manned required substations, transferring from "automatic to manual mode", and manually re-closed breakers to energize the system. Restoration varied but all services were restored in 3-6 hours. It is important to note that there are risks operating your system without the benefit of an automated dispatch control center and utilities that are more reliant on automation may not be able to restore large portions of their system this way. In many ways, the Ukrainian operators should be commended for their diligence and restoration efforts.

Cyber Attack Milestones as Reported To Date:

From what has been reported, here is the information to date that we are confident took place. The exact timing of the events is still being pieced together.

- The adversary initiated an intrusion into production SCADA systems
- Infected workstations and servers
- Acted to "blind" the dispatchers
- Acted to damage the SCADA system hosts (servers and workstations)
    - Action would have delayed restoration and introduce risk, especially if the SCADA system was essential to coordinate actions
    - Action can also make forensics more difficult
- Flooded the call centers to deny customers calling to report power out

Probable Cyber Attack Milestones as Reported to Date:

In analyzing the evidence and reports there are still missing pieces to the attack. Understanding the initial foothold of the adversary, the eventual impact, and the types of systems in place can help to make assessments on what the adversary likely had to have done but the items stated below are currently probable and not known. We are working to verify and uncover more information.

- The adversaries infected workstations and moved through the environment
- Acted to open breakers and cause the outage (assessed through technical analysis of the Ukrainian SCADA system in comparison to the impact)
- Initiated a possible DDoS on the company websites

Malware Enabled but Not Likely Malware Caused

It is interesting and important to understand the role of the malware sample SANS ICS previously reported that came from one of the infected networks. There have been two prominent theories in the community and speculation to the media that either the 'KillDisk' component was just inside the network and unrelated to the power outage (a reliability issue where malware just happened to be there) or that the 'KillDisk' component was directly responsible for the outage. It is our assessment that neither of these are correct. Malware likely enabled the attack, there was an intentional attack, but the 'KillDisk' component itself did not cause the outage.

It is also important to note that many of the samples being analyzed in the community to date as reported by others are not guaranteed to have been involved in this incident. The malware campaign reported, tied to BlackEnergy and the Sandworm team by others, has solid links to this incident but it cannot be assumed that files such as the excel spreadsheet and other malware samples recovered from other portions of that campaign were at all involved in this incident. It is possible but far too early in the technical analysis to state that. The type of analysis being done by the security researchers and companies assessing this is valuable

analysis and they should be commended. At the worst it will provide lessons learned and training opportunities for the community. But analysts should be careful not to overstate current analysis of malware samples due to their link to the larger campaign as being specific to this incident. Simply put, there is still evidence that has yet to be uncovered that may refute the minutia of the specific components of the malware portion of the attack.

More importantly, the link of the KillDisk wiper to the actual cause of the outage is not likely. This is stated because power systems and SCADA schemes simply do not work in that manner. In other words, the incident observed with consideration to timing, sites, and impact does not at all align with the narrative of the 'KillDisk' component itself causing the impact. I have observed the loss of many SCADA systems for periods of time that resulted in no outage or impact to the power system. Running a power system without the benefit of your SCADA system at the distribution-level adds risk, but without something to change the 'state' (for example to force a circuit to de-energize) then the system will continue to serve power. We assess currently that the malware allowed the attackers to gain a foothold at the targeted utilities, open up command and control, and facilitate the planning of an attack by providing access to the network and necessary information. The malware also appears to have been used to wipe files in an attempt to deny the use of the SCADA system for the purposes of restoration to amplify the effects of the attack and possibly to delay restoration.

Final Thoughts

We are very interested in helping power utilities learn as much as they can from this real world incident. We would also note the competent action by Ukrainian utility personnel in responding to the attack and restoring their power system. As a community the power industry is dedicated to keeping the lights on. What is now true is that a coordinated cyber attack consisting of multiple elements is one of the expected hazards they may face. We need to learn and prepare ourselves to detect, respond, and restore from such events in the future. The SANS ICS team will be continuing our analysis and presenting findings and updates to the community in multiple formats. On Jan 20th we will host a webcast focusing on understanding the industrial control systems and SCADA networks of the Ukrainian power grid to identify what was even possible in terms of attack scenarios. Following that, we will release more information at the SANS ICS Summit with a full breakdown of what we know and its value to the community. Finally, we will be releasing a comprehensive whitepaper on the incident in our Defense Use Case (DUC) series in our ICS Digital Library. The DUC will highlight both the cyber and physical components to this incident and the lessons learned for the community.

We sincerely thank all the effort going on in the community by numerous passionate researchers and companies across both the information technology and the ICS community. It takes all of us working together to understand and respond to these types of incidents.

To view all our upcoming courses and events, click here.

Free Stuff Reminder

- Download the "What Will Your Attack Look Like" poster here
- Get the latest ICS resources here
- Join the conversation in the ICS Community Forum where ICS professionals share lessons learned, ask questions and connect with others passionate about securing our critical infrastructure.