the Availability Digest

www.availabilitydigest.com
@availabilitydig

How the Ukraine Power Grid Was Hacked

March 2016

As reported in the *Availability Digest's* January 2016 issue,[1] hackers disabled a major portion of Ukraine's power grid on the afternoon of December 23, 2015. Without power for six hours were 230,000 customers. Though operators were able to restore power by traveling to the substations and manually closing circuit breakers that had been opened by the attack, operators still are unable to control the circuit breakers remotely from their control centers.

After a great deal of forensic analysis, details now are forthcoming about how this attack was carried out.

The Preparation for the Attack

Based on evidence discovered after the attack, preparation by the hackers had been in progress for at least six months. Ukraine has 24 regions with a different power distribution company serving each region. During mid-2015, a phishing campaign delivered emails to workers at three of the companies. To each email was attached a Word document that contained a malicious macro. A popup asked the recipient to enable macros for the document. If done, the macro opened a backdoor that allowed the malware package BlackEnergy to infect the machine.

BlackEnergy has been found in control systems the world over. Though it is capable of doing damage to the computers it infects, it is used primarily for data gathering. Over the next several months, the attackers used BlackEnergy to map the network topology of the infected power distribution companies and to steal the credentials of the network operators. Observing the actions of the operators, the hackers also learned how to switch off the circuit breakers.

The Execution of the Attack

The attackers launched their assault in three steps:

- Step 1 – The UPSs (uninterruptible power supplies) at the control centers was reconfigured so that the attackers could control them. When the UPSs were turned off, this put the operators in the dark.

- Step 2 – The hackers wrote malicious firmware to replace the legitimate firmware in the Ethernet controllers that control the substations. This firmware would prevent the operators from sending commands to the substation circuit breakers to reset them.

- Step 3 – The attack began.

[1] Can Hackers Take Down Our Power Grid?, *Availability Digest*; January 2016. http://www.availabilitydigest.com/public_articles/1101/power_grid_hacks.pdf

On the fateful afternoon of December 13th, the attack began. The hackers disabled the UPS systems, plunging the control centers into the dark. They entered the SCADA (supervisory control and data acquisition) networks using the workers' stolen credentials (two-factor authentication was not being used, which would have prevented the attackers from gaining access to the SCADA systems). They also launched a Telephone Denial of Service (TDoS) attack against the customer call centers to prevent customers from calling in and reporting outages. A TDoS attack involves flooding a call center with thousands of bogus telephone calls.

In addition, the hackers overwrote the firmware in the Ethernet controllers with their own malicious firmware. This prevented commands from being sent from the control centers to the substations.

The progress of the attack was described by one worker. He noticed that the cursor on his computer suddenly started moving across the screen of its own accord. He watched as it navigated towards buttons controlling the circuit breakers at one of the substations. The cursor clicked on a control button to open a circuit breaker and then clicked the confirmation box. The circuit breaker was opened.

The operator tried to seize control of the cursor, but it was unresponsive to his commands. The computer then logged him off. He couldn't log back on. It was discovered later that the attackers had changed his password.

Circuit breaker after circuit breaker was opened by the remote-controlled cursor. The substation was quickly taken offline. This process continued at the three control centers under attack, taking thirty substations offline and killing power for hundreds of thousands of Ukrainians.

The operators tried desperately to close the circuit breakers and to restore power but to no avail. No control executed at the control center could be sent to the substations in the field because of the malicious firmware injected into the Ethernet controllers. Personnel ultimately had to be sent into the field to close the circuit breakers manually. It took six hours to restore power.

The Aftermath of the Attack

Months after the attack, the hacked power-grid control centers still are not fully operational. The infected control systems have to be replaced with systems with the proper firmware. Until that is completed, the circuit breakers still must be manually controlled at the substations.

The attackers also deleted the logs and other forensic data that would allow investigators to determine how the attack occurred. It therefore has been difficult to determine exactly what happened and how the power grid was taken down.

Who Was Responsible for the Attack?

The culprit was never identified. Russia was suspected but has denied any involvement. Russia had just annexed the Ukrainian territory of Crimea, and Ukrainian saboteurs had cut the power cables supplying power from the Ukraine to Crimea, plunging parts of Crimea into darkness for two weeks.[2] The attack against Ukraine could have been a Russian retaliation for the Crimea attack, but that does not explain the fact that planning for the assault had begun six months prior.

What has been determined is that the hackers made phone calls from Russia and that they used a Russian-based Internet service provider as part of the attack. U.S. researchers surmised that the attack was likely the work of Sandworm, a Russian-backed hacking group.

[2] Crimea Loses Power for Two Weeks, *Availability Digest*; December 2015.
http://www.availabilitydigest.com/public_articles/1012/crimea.pdf

Summary

This is the first known instance of malware being used to generate a power outage. It certainly sends a warning to countries around the world, including the U.S., as to the dangers of hacking attacks.

Experts say that the control systems in Ukraine were surprisingly more secure than some in the U.S., since they were well-segmented from the control-center business networks with robust firewalls. But in the end, they weren't secure enough. Workers logging into the SCADA network that controlled the grid weren't required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to the systems that controlled the circuit breakers.

Such an attack could come from another nation, though this seems unlikely since the attacking nation would be subject to a retaliatory attack (though the identity of the attacker easily is hidden by attacking through a circuitous route).

However, there is no such reluctance imposed on terrorist groups that are unaffiliated with a nation-state. It is imperative that the industrial control systems and the SCADA systems that control the power grids of the world be highly secure and that provisions are in place to rapidly restore power in the event that a hacking attack is successful.

Acknowledgements

Material for this article was taken from the following sources:

Crimea Loses Power for Two Weeks, *Availability Digest*; December 2015.
Can Hackers Take Down Our Power Grid?, *Availability Digest*; January 2016.
Malware wasn't the sole cause of Ukraine power station outage, *Computerworld*; January 10, 2016.
Power Grid Cyber Attack Was Months in the Making, Ukrainian Energy Minister Says, *Motherboard*; February 13, 2016.
Ukraine power outage was a cyberattack – U.S. doesn't finger Russia (officially), *Computerworld*; March 1, 2016.
Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, *Wired*; March 3, 2016.
Ukraine Cyber Attack Analysis, *Radiflow*.