Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world

May 18 2024

Credit: Pixabay/CC0 Public Domain

On a cold winter night in 2016, Ukrainians experienced the first-ever known blackout caused by malicious code (malware) designed to

autonomously attack the power grid. One-fifth of Kyiv's citizens were plunged into darkness as attackers used malware to target the capital city's power grid. Six years later, in the early months of the ongoing Russia-Ukraine war, a second attack attempted to combine kinetic and cyber attacks to take down Ukraine's power grid.

Malware attacks against physical infrastructure have long been a looming threat in the realm of cybersecurity, but these two in Ukraine were the first attacks of their kind, and have received little attention from the academic community. Carried out by a Russian intelligence agency against Ukraine, they warn of the evolution of cyber attacks to the built world, and highlight the need to better understand and defend against this type of malware.

A new paper presents the first study into how Industroyer One and Two, as these malware attacks are called, operated and interacted with the physical power system equipment. The paper is set to be presented on May 20 at the IEEE Symposium on Security and Privacy (the Institute of Electrical and Electronics Engineers flagship conference on cybersecurity) and was lead by a team of UC Santa Cruz students including Luis Salazar, Sebastian Castro, Juan Lozano and Keerthi Koneru, and advised by Associate Professor of Computer Science and Engineering Alvaro Cardenas.

"I want to emphasize how vulnerable our systems are—I don't know why this hasn't been more impactful in terms of security awareness, and also policy and planning," Cardenas said. "When you see a nation state designing malware to take down the power grid of another country, that seems to be a big deal. Our critical infrastructures are vulnerable to these kinds of attacks, so we need to be better prepared to defend."

Understanding Industroyer One and Two

The malware used in the 2016 attack has been named Industoyer One, and the similar but distinct malware used in 2022 was dubbed Industroyer Two. The Five Eyes, an intelligence alliance including Australia, Canada, New Zealand, the United Kingdom, and the United States, have attributed both of these attacks to the GRU, which is Russia's military intelligence agency.

The first attack can be seen as example of intimidation and a flex of power without warfare, Cardenas said, while the second is a look into warfare in the modern world

"It's an example of modern war in that it combines physical and cyber attacks," Cardenas said. "It's not an isolated event, these events in the cyber world and physical world are reinforcing each other to create the most damage they can. After our paper was accepted, we received notice of yet another attack that targeted Ukraine's power grid simultaneously with a cyber attack and a kinetic attack."

The malware attacks are not only the first and only examples of cyber attacks against a power grid, but are part of only a small number of known malware attacks against physical infrastructure in general.

The first example of a malware attack against physical infrastructure was the Stuxnet attack discovered in 2010 and deployed some years earlier with the intention to destroy the centrifuges of a uranium enrichment plant in Iran. Before that, malware attacks had only targeted classical computing systems like IT and financial systems.

The Industroyer attacks caused hours-long local blackouts. These types of attacks require operators to fix the problem locally and reconnect back to the main systems, and are far less catastrophic than a system collapse, in which an error cascades through the "bulk" system and could bring down an entire country's power grid.

"These attacks were able to create local blackouts, but so far, there hasn't been a system-wide collapse. An attack that can collapse the grid will be far more dangerous as the whole country would be without power for several days," Cardenas said.

Creating a sandbox for study

The UCSC researchers are not the only to study the two attacks, but Cardenas' team found that the industry white papers did not provide satisfying answers about how the details of the malware operated and interacted with the equipment controlling the infrastructure. Their report is the first to detail exactly how the malware interacted with the physical world.

Cardenas was able to obtain copies of the malware, which enabled the researchers to build a sandbox—a software environment that fooled the malware into thinking it was within the industry-specific environment of the Ukrainian power grid so the researchers could understand exactly how it interacted with the system. They emulated a power grid operator's control room with remote connections to substations, as well as a substation network with local connections to electrical equipment. Their sandbox is openly available for other researchers to use.

Using the sandbox, the researchers found similarities between the attacks, but observed a clear evolution in the malware.

Both of the Industroyer attacks were completely automated, meaning once they were deployed there was no human involvement, and breached areas of the power grid which were designed to be disconnected from the internet to provide them higher security. Both attacks compromised a Windows computer in a substation or control room to manipulate the status of circuit breakers in the grid.

Industroyer One acted like a swiss army knife in that it could attack both older systems operating with serial lines as well as modern systems operating with modern communication systems. It was developed without a specific target and could attack directly from within a grid substation or from the control center hundreds of miles away. It expected configuration files from the system itself to guide its attack. However, these characteristics did not mean it was without flaws.

"It had this flexibility of attacking from everywhere, but we also found that it had a lot of bugs," Cardenas said. "There were several implementation bugs that didn't follow the protocol. Maybe it was [meant to be] very targeted, but we tested with several different types of equipment and it worked with some and not with others because of the bugs."

Industroyer Two, on the other hand, was very specific, with its targets baked into the malware itself, eliminating the need to read configuration files. The researchers could see that it was targeting three IP addresses which coordinated with specific devices, presumably to control circuit breakers in specific substations. The bugs that were present in Industroyer One were eliminated.

"Maybe it was because over time they had time to polish the malware to get rid of the bugs, but they also knew better what they were after," Cardenas said.

In observing how the Industoyer attacks targeted varied numbers of circuit breakers, the researchers found that different types of disconnection attacks can have different results in the power grid. They found that counterintuitively, shutting off all circuit breakers at once doesn't cause these big problems, as disconnecting load and generation at the same time balances out the system. More strategic attacks might aim to create imbalances, which can cause larger problems for the bulk

system.

Planning future defense

Overall, this evolution observed in the Industroyer attacks shows that malware attacks are becoming stealthier. While both attacks targeted computers housed within control centers, researchers believe that future attackers could try to control "intelligent electronic devices" (IEDs) embedded within the systems themselves. While there is no malware targeting these for now, they might make attractive targets in the future as hackers could send them malicious commands while having them report back to the human operators that everything is working properly.

While the Industroyer attacks happened geographically far from the United States, the distance does not ensure safety.

"The attacks could happen here, or pretty much anywhere in the world," Cardenas said. "Systems are now all controlled by computers and have pretty much the same technology."

With this in mind, the researchers are working to configure their sandbox into what is called a "honeypot," a type of decoy software that pretends to be a working system in the operational network of a utility. System operators know not to use this decoy, so if activity is seen in the honeypot they will know it comes from an outside attacker, alerting them to the attack.

The researchers are designing their honeypot to be generic enough to work in various control systems, such as oil refineries or water treatment systems, in addition to functioning in power grids.

They also plan to facilitate the incorporation of AI assistants into operating networks, which would help decode and respond to attacks in

real time when they occur.

Collaborators on this project included Cardenas' Ph.D. students Luis Salazar, Sebastian Castro, Juan Lozano, and Keerthi Koneru, as well as Emmanuele Zambon at the Eindhoven University of Technology, Bing Huang and Ross Baldick at the University of Texas at Austin, Marina Krotofil at Information Systems Security Partners, and Alonso Rojas at the Axon Group.

More information: A Tale of Two Industroyers: It was the Season of Darkness, 2024 IEEE Symposium on Security and Privacy (SP), DOI: 10.1109/SP54263.2024.00162 , www.computer.org/csdl/proceedi … 3000a162/1Ub24B7070k

Provided by University of California - Santa Cruz