How 30 Lines of Code Blew Up a 27-Ton Generator

wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator

Andy Greenberg October 23, 2020

Earlier this week, the US Department of Justice unsealed an indictment against a group of hackers known as Sandworm. The document charged six hackers working for Russia's GRU military intelligence agency with computer crimes related to half a decade of cyberattacks across the globe, from sabotaging the 2018 Winter Olympics in Korea to unleashing the most destructive malware in history in Ukraine. Among those acts of cyberwar was an unprecedented attack on Ukraine's power grid in 2016, one that appeared designed to not merely cause a blackout, but to inflict physical damage on electric equipment. And when one cybersecurity researcher named Mike Assante dug into the details of that attack, he recognized a grid-hacking idea invented not by Russian hackers, but by the United State government, and tested a decade earlier.

The following excerpt from the book SANDWORM: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, published in paperback this week, tells the story of that early, seminal grid-hacking experiment. The demonstration was led by Assante, the late, legendary industrial control systems security pioneer. It would come to be known as

the Aurora Generator Test. Today, it still serves as a powerful warning of the potential physical-world effects of cyberattacks—and an eery premonition of Sandworm's attacks to come.

On a piercingly cold and windy morning in March 2007, Mike Assante arrived at an Idaho National Laboratory facility 32 miles west of Idaho Falls, a building in the middle of a vast, high desert landscape covered with snow and sagebrush. He walked into an auditorium inside the visitors' center, where a small crowd was gathering. The group included officials from the Department of Homeland Security, the Department of Energy, and the North American Electric Reliability Corporation (NERC), executives from a handful of electric utilities across the country, and other researchers and engineers who, like Assante, were tasked by the national lab to spend their days imagining catastrophic threats to American critical infrastructure.

At the front of the room was an array of video monitors and data feeds, set up to face the room's stadium seating, like mission control at a rocket launch. The screens showed live footage from several angles of a massive diesel generator. The machine was the size of a school bus, a mint green, gargantuan mass of steel weighing 27 tons, about as much as an M3 Bradley tank. It sat a mile away from its audience in an electrical substation, producing enough electricity to power a hospital or a navy ship and emitting a steady roar. Waves of heat coming off its surface rippled the horizon in the video feed's image.

Assante and his fellow INL researchers had bought the generator for $300,000 from an oil field in Alaska. They'd shipped it thousands of miles to the Idaho test site, an 890-square-mile piece of land where the national lab maintained a sizable power grid for testing purposes, complete with 61 miles of transmission lines and seven electrical substations.

Now, if Assante had done his job properly, they were going to destroy it. And the assembled researchers planned to kill that very expensive and resilient piece of machinery not with any physical tool or weapon but with about 140 kilobytes of data, a file smaller than the average cat GIF shared today on Twitter.

Three years earlier, Assante had been the chief security officer at American Electric Power, a utility with millions of customers in 11 states from Texas to Kentucky. A former navy officer turned cybersecurity engineer, Assante had long been keenly aware of the potential for hackers to attack the power grid. But he was dismayed to see that most of his peers in the electric utility industry had a relatively simplistic view of that still-theoretical and distant threat. If hackers did somehow get deep enough into a utility's network to start opening circuit breakers, the industry's common wisdom at the time was that staff could simply kick the intruders out of the network and flip the power back on. "We could manage it like a storm," Assante remembers his colleagues saying. "The way it was imagined, it would be like an outage and we'd recover from the outage, and that was the limit of thinking around the risk model."

But Assante, who had a rare level of crossover expertise between the architecture of power grids and computer security, was nagged by a more devious thought. What if attackers didn't merely hijack the control systems of grid operators to flip switches and cause short-term blackouts, but instead reprogrammed the automated elements of the grid, components that made their own decisions about grid operations without checking with any human?

An electrical substation at Idaho National Labs' sprawling, 890-square-mile test site.

Courtesy of Idaho National Laboratory

In particular, Assante had been thinking about a piece of equipment called a protective relay. Protective relays are designed to function as a safety mechanism to guard against dangerous physical conditions in electric systems. If lines overheat or a generator goes out of sync, it's those protective relays that detect the anomaly and open a circuit breaker, disconnecting the trouble spot, saving precious hardware, even preventing fires. A protective relay functions as a kind of lifeguard for the grid.

But what if that protective relay could be paralyzed—or worse, corrupted so that it became the vehicle for an attacker's payload?

That disturbing question was one Assante had carried over to Idaho National Laboratory from his time at the electric utility. Now, in the visitor center of the lab's test range, he and his fellow engineers were about to put his most malicious idea into practice. The secret experiment was given a code name that would come to be synonymous with the potential for digital attacks to inflict physical consequences: Aurora.

The test director read out the time: 11:33 am. He checked with a safety engineer that the area around the lab's diesel generator was clear of bystanders. Then he sent a go-ahead to one of the cybersecurity researchers at the national lab's office in Idaho Falls to begin the attack. Like any real digital sabotage, this one would be performed from miles away, over the internet. The test's simulated hacker responded by pushing roughly 30 lines of code from his machine to the protective relay connected to the bus-sized diesel generator.

The inside of that generator, until that exact moment of its sabotage, had been performing a kind of invisible, perfectly harmonized dance with the electric grid to which it was connected. Diesel fuel in its chambers was aerosolized and detonated with inhuman timing to move pistons that rotated a steel rod inside the generator's engine—the full assembly was known as the "prime mover"—roughly 600 times a minute. That rotation was carried through a rubber grommet, designed to reduce any vibration, and then into the electricity-generating components: a rod with arms wrapped in copper wiring, housed between two massive magnets so that each rotation induced electrical current in the wires. Spin that mass of wound copper fast enough and it produced 60 hertz of alternating current, feeding its power into the vastly larger grid to which it was connected.

A protective relay attached to that generator was designed to prevent it from connecting to the rest of the power system without first syncing to that exact rhythm: 60 hertz. But Assante's hacker in Idaho Falls had just reprogrammed that safeguard device, flipping its logic on its head.

At 11:33 am and 23 seconds, the protective relay observed that the generator was perfectly synced. But then its corrupted brain did the opposite of what it was meant to do: It opened a circuit breaker to disconnect the machine.

When the generator was detached from the larger circuit of Idaho National Laboratory's electrical grid and relieved of the burden of sharing its energy with that vast system, it instantly began to accelerate, spinning faster, like a pack of horses that had been let loose from its carriage. As soon as the protective relay observed that the generator's rotation had sped up to be fully out of sync with the rest of the grid, its maliciously flipped logic immediately reconnected it to the grid's machinery.

The moment the diesel generator was again linked to the larger system, it was hit with the wrenching force of every other rotating generator on the grid. All of that equipment pulled the relatively small mass of the diesel generator's own spinning components back to its original, slower speed to match its neighbors' frequencies.

On the visitor center's screens, the assembled audience watched the giant machine shake with sudden, terrible violence, emitting a sound like a deep crack of a whip. The entire process from the moment the malicious code had been triggered to that first shudder had spanned only a fraction of a second.

Black chunks began to fly out of an access panel on the generator, which the researchers had left open to watch its internals. Inside, the black rubber grommet that linked the two halves of the generator's shaft was tearing itself apart.

A few seconds later, the machine shook again as the protective relay code repeated its sabotage cycle, disconnecting the machine and reconnecting it out of sync. This time a cloud of gray smoke began to spill out of the generator, perhaps the result of the rubber debris burning inside it.

Assante, despite the months of effort and millions of dollars in federal funds he'd spent developing the attack they were witnessing, somehow felt a kind of sympathy for the machine as it was being torn apart from within. "You find yourself rooting for it, like the little engine that could," Assante remembered. "I was thinking, 'You can make it!'"

The machine did not make it. After a third hit, it released a larger cloud of gray smoke. "That prime mover is toast," an engineer standing next to Assante said. After a fourth blow, a plume of black smoke rose from the machine 30 feet into the air in a final death rattle.

The test director ended the experiment and disconnected the ruined generator from the grid one final time, leaving it deathly still. In the forensic analysis that followed, the lab's researchers would find that the engine shaft had collided with the engine's internal wall, leaving deep gouges in both and filling the inside of the machine with metal shavings. On the other side of the generator, its wiring and insulation had melted and burned. The machine was totaled.

In the wake of the demonstration, a silence fell over the visitor center. "It was a sober moment," Assante remembers. The engineers had just proven without a doubt that hackers who attacked an electric utility could go beyond a temporary disruption of the victim's operations: They could damage its most critical equipment beyond repair. "It was so vivid. You could imagine it happening to a machine in an actual plant, and it would be terrible," Assante says. "The implication was that with just a few lines of code, you can create conditions that were physically going to be very damaging to the machines we rely on."

But Assante also remembers feeling something weightier in the moments after the Aurora experiment. It was a sense that, like Robert Oppenheimer watching the first atomic bomb test at another US national lab six decades earlier, he was witnessing the birth of something historic and immensely powerful.

"I had a very real pit in my stomach," Assante says. "It was like a glimpse of the future."

Greenberg reading a passage from this chapter for Literary Hub.
