Hacked Air Conditioners And IoT Could Shut Down Power Grid

Technocrats who are building out the Internet of Things are unable to secure their creations against hackers. If air conditioner motors in a single large city were all started at the same time, it would break the power grid for a multi-state area. TN Editor

When the cybersecurity industry warns about the nightmare of hackers causing blackouts, the scenario they describe typically entails an elite team of hackers breaking into the inner sanctum of a power utility to start flipping switches. But one group of researchers has imagined how an entire power grid could be taken down by hacking a less centralized and protected class of targets: home air conditioners and water heaters. Lots of them.

At the Usenix Security conference this week, a group of Princeton

University security researchers will present a study that considers a little-examined question in power grid cybersecurity: What if hackers attacked not the supply side of the power grid, but the demand side? In a series of simulations, the researchers imagined what might happen if hackers controlled a botnet composed of thousands of silently hacked consumer internet of things devices, particularly power-hungry ones like air conditioners, water heaters, and space heaters. Then they ran a series of software simulations to see how many of those devices an attacker would need to simultaneously hijack to disrupt the stability of the power grid.

Their answers point to a disturbing, if not quite yet practical scenario: In a power network large enough to serve an area of 38 million people—a population roughly equal to Canada or California—the researchers estimate that just a one percent bump in demand might be enough to take down the majority of the grid. That demand increase could be created by a botnet as small as a few tens of thousands of hacked electric water heaters or a couple hundred thousand air conditioners.

“Power grids are stable as long as supply is equal to demand,” says Saleh Soltan, a researcher in Princeton’s Department of Electrical Engineering, who led the study. “If you have a very large botnet of IoT devices, you can really manipulate the demand, changing it abruptly, any time you want.”

The result of that botnet-induced imbalance, Soltan says, could be cascading blackouts. When demand in one part of the grid rapidly increases, it can overload the current on certain power lines, damaging them or more likely triggering devices called protective relays, which turn off the power when they sense dangerous conditions. Switching off those lines puts more load on the remaining ones, potentially leading to a chain reaction.

“Fewer lines need to carry the same flows and they get overloaded, so then the next one will be disconnected and the next one,” says Soltan. “In the worst case, most or all of them are disconnected, and you have a blackout in most of your grid.”

Power utility engineers, of course, expertly forecast fluctuations in electric demand on a daily basis. They plan for everything from heat waves that predictably cause spikes in air conditioner usage to the moment at the end of British soap opera episodes when hundreds of thousands of viewers all switch on their tea kettles. But the Princeton researchers' study suggests that hackers could make those demand spikes not only unpredictable, but maliciously timed.

The researchers don't actually point to any vulnerabilities in specific household devices, or suggest how exactly they might be hacked. Instead, they start from the premise that a large number of those devices could somehow be compromised and silently controlled by a hacker. That's arguably a realistic assumption, given the myriad vulnerabilities other security researchers and hackers have found in the internet of things. One talk at the Kaspersky Analyst Summit in 2016 described security flaws in air conditioners that could be used to pull off the sort of grid disturbance that the Princeton researchers describe. And real-world malicious hackers have compromised everything from refrigerators to fish tanks.

Given that assumption, the researchers ran simulations in power grid software MATPOWER and Power World to determine what sort of botnet would could disrupt what size grid. They ran most of their simulations on models of the Polish power grid from 2004 and 2008, a rare country-sized electrical system whose architecture is described in publicly available records. They found they could cause a cascading blackout of 86 percent of the power lines in the 2008 Poland grid model with just a one percent increase in demand. That would require the equivalent of 210,000 hacked air conditioners, or 42,000 electric water heaters.

The notion of an internet of things botnet large enough to pull off one of those attacks isn't entirely farfetched. The Princeton researchers point to the Mirai botnet of 600,000 hacked IoT devices, including security cameras and home routers. That zombie horde hit DNS provider Dyn with an unprecedented denial of service attack in late 2016, taking down a broad collection of websites.

Building a botnet of the same size out of more power-hungry IoT devices

is probably impossible today, says Ben Miller, a former cybersecurity engineer at electric utility Constellation Energy and now the director of the threat operations center at industrial security firm Dragos. There simply aren't enough high-power smart devices in homes, he says, especially since the entire botnet would have to be within the geographic area of the target electrical grid, not distributed across the world like the Mirai botnet.

Read full story here…