Baking and boiling botnets could drive energy market swings and damage

August 5 2020, by John Toon

A study presented at Black Hat USA 2020 suggests that botnets made up of high-wattage devices such as ovens and air conditioners could be used to manipulate electric energy markets. Credit: John Toon, Georgia Tech

Evil armies of internet-connected EV chargers, ovens, hot-water heaters, air-conditioners, and other high-wattage appliances could be hijacked to

slightly manipulate energy demand, potentially driving price swings and creating financial damage to deregulated energy markets, warns a new report scheduled to be presented Aug. 5 at the Black Hat U.S. 2020 conference.

By turning the compromised equipment on or off to artificially increase or decrease power demand, botnets made up of these energy-consuming devices might help an unscrupulous energy supplier or retailer (electric utility) alter prices to create a business advantage, or give a nation-state a way to remotely harm the economy of another country by causing financial damage to its electricity market. If done within the bounds of normal power demand variation, such an attack would be difficult to detect, the researchers said.

"If an attacker can slightly affect electricity market prices in their favor, it would be like knowing today what's going to happen in tomorrow's stock market," said Tohid Shekari, a graduate research assistant in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. "If the manipulation stays within a certain range, it would be stealthy and difficult to differentiate from a typical load forecasting error."

Believed to be the first proposed energy market manipulation cyberattack, the operation would depend on botnets composed of thousands of appliances that could be controlled centrally by attackers who had taken over their Internet of Things (IoT) controllers. Malicious actors have already demonstrated IoT botnet attacks such as Mirai, which used a network of compromised internet-connected cameras and routers to launch attacks on key internet infrastructure.

The attack, dubbed "IoT Skimmer," would be made possible by the deregulation of energy markets, which has created a system to efficiently supply electrical power. To meet the demand for electrical energy, utility

companies must predict future demand and purchase power from the day-ahead wholesale energy market at competitive prices. If the predictions turn out to be wrong, the utilities may have to pay more or less for the energy they need to meet the demands of their customers by participating in the real-time market, which has more volatile prices in general. Creating erroneous demand data to manipulate forecasts could be profitable to the suppliers selling energy to meet the unexpected demand, or the retailers or utilities buying cheaper energy from the real-time market.

The researchers weren't able to determine whether such an attack might have already taken place because IoT devices—beyond being insecure—also lack the kind of monitoring that would be necessary to detect such hijacking. But they used real data sets from two of the largest U.S. energy markets—New York and California—to evaluate the feasibility of their proposed attack.

"We did a lot of simulation and mathematical analysis to show that this kind of transfer could occur," said Raheem Beyah, the Motorola Foundation Professor in the School of Electrical and Computer Engineering who is also Georgia Tech's vice president for Interdisciplinary Research and co-founder of the company Fortiphyd Logic. "We also did a feasibility analysis of the supporting areas to show that this would be possible from various perspectives."

The researchers assume that such botnets already exist, and that attackers could simply rent their use on the dark web. More than 20 million smart thermostats already exist in the North American market, and they are connected to at least one high-wattage device—a heating and air-conditioning system that could be controlled by attackers on an intermittent basis.

"If you consider all of the smart thermostats and internet-connected

electric ovens, water heaters, and electric vehicle chargers that are already in use, there are plenty of devices to be compromised," Shekari said. "Homeowners would likely never notice if the EV charger turns on when electricity demand is highest, or if the air conditioning cools a little more than they expected when they are not home."

To counter the potential attack, researchers suggest both detection and prevention steps. Through integrated monitoring of the normal power use of high-wattage IoT-connected devices, unexpected peaks or valleys in power consumption triggered by an attacker could be detected. And access to data on expected energy demand—which is now made available publicly—could be restricted to those who actually need it.

The primary factor that makes this attack possible is the detailed online data sharing of electricity market information, which is usually updated every five minutes.

"This energy demand information is really a data privacy issue, and we need to think long and hard about the balance between transparency and security," Beyah said. "There's always a tension there, but limiting the amount of detail could make it more difficult for attackers who want to hide their manipulations to know what the normal variations are."

The potential attack highlights the need for considering cybersecurity threats in technology areas where they had perhaps never been possible before.

"This is an interesting intersection between the IoT security world and energy markets," said Beyah. "Right now, it seems that there is a large gap between the two worlds. Our point is that there are implications for combining IoT technology and high-wattage devices that can compromise markets in ways we would never have thought of before."

The presentation, "IoT Skimmer: Energy Market Manipulation Through High-Wattage IoT Botnets," will be presented on Wednesday, Aug. 5, at 2:30 p.m. as part of the Black Hat U.S. 2020 conference.

Provided by Georgia Institute of Technology