# New cyberattacks against urban water services possible, warn researchers

August 9 2018

Ben-Gurion University of the Negev (BGU) cyber security researchers warn of a potential distributed attack against urban water services that uses a botnet of smart irrigation systems that water simultaneously. A botnet is a large network of computers or devices controlled by a command and control server without the owner's knowledge.

Ben Nassi, a researcher at Cyber@BGU, will be presenting "Attacking Smart Irrigation Systems" in Las Vegas at the prestigious Def Con 26 Conference in the IoT Village on August 11.

The researchers analyzed and found vulnerabilities in a number of commercial smart irrigation systems, which enable attackers to remotely turn watering systems on and off at will. The researchers tested three of the most widely sold smart irrigation systems: GreenIQ, BlueSpray, and RainMachine smart irrigation systems.

"By simultaneously applying a distributed attack that exploits such vulnerabilities, a botnet of 1,355 smart irrigation systems can empty an urban water tower in an hour and a botnet of 23,866 smart irrigation systems can empty ?ood water reservoir overnight," Nassi says. "We have notified the companies to alert them of the security gaps so they can upgrade their smart system's irrigation system's firmware."

Water production and delivery systems are part of a nation's critical infrastructure and generally are secured to prevent attackers from infecting their systems. "However, municipalities and local government entities have adopted new green technology using IoT smart irrigation systems to replace traditional sprinkler systems, and they don't have the same critical infrastructure security standards."

In the study, the researchers present a new attack against urban water services that doesn't require infecting its physical cyber systems. Instead, the attack can be applied using a botnet of smart irrigation regulation systems at urban water services that are much easier to attack.

The researchers demonstrated how a bot running on a compromised device can (1) detect a smart irrigation system connected to its LAN in less than 15 minutes, and (2) turn on watering via each smart irrigation system using a set of session hijacking and replay attacks.

"Although the current generation of IoT devices is being used to regulate water and electricity obtained from critical infrastructures, such as the smart-grid and urban water services, they contain serious security vulnerabilities and will soon become primary targets for attackers," says Nassi, who is also Ph.D. student of Prof. Yuval Elovici's in BGU's Department of Software and Information Systems Engineering and a researcher at the BGU Cyber Security Research Center. Elovici is the Center's director as well as the director of Telekom Innovation Labs at BGU.

The research team also included Ph.D. student Yair Meidan supervised by Dr. Asaf Shabtai, as well as two interns, Moshe Sror and Ido Lavi.

Previous research focused on a new method to detect illicit drone video-filming.

Provided by American Associates, Ben-Gurion University of the Negev

Citation: New cyberattacks against urban water services possible, warn researchers (2018, August 9) retrieved 9 April 2024 from https://phys.org/news/2018-08-cyberattacks-urban.html