Researchers develope new method to defend against smart home cyberattacks

August 3 2020

Credit: CC0 Public Domain

Instead of relying on customers to protect their vulnerable smart home devices from being used in cyberattacks, Ben-Gurion University of the Negev (BGU) and National University of Singapore (NUS) researchers

have developed a new method that enables telecommunications and internet service providers to monitor these devices.

According to their new study published in *Computers & Security*, the ability to launch massive distributed denial-of-service (DDoS) attacks via a botnet of compromised devices is an exponentially growing risk in the Internet of Things (IoT). Such massive attacks, possibly emerging from IoT devices in home networks, impact the attack target, as well as the infrastructure of telecommunication service providers (telcos).

"Most home users don't have the awareness, knowledge, or means to prevent or handle ongoing attacks," says Yair Meidan, a Ph.D. candidate in the BGU Department of Software and Information Systems Engineering (SISE). "As a result, the burden falls on the telcos to handle. Our method addresses a challenging real-world problem that has already caused challenging attacks in Germany and Singapore, and poses a risk to telco infrastructure and their customers worldwide."

Each connected device has a unique IP address. However, home networks typically use gateway routers with NAT (network address translation) functionality, which replaces the local source IP address of each outbound data packet with the household router's public IP address. Consequently, detecting connected IoT devices from outside the home network is a challenging task.

The researchers developed a method to detect connected, vulnerable IoT models before they are compromised by monitoring the data traffic from each smart home device. This enables telcos to verify whether specific IoT models, known to be vulnerable to exploitation by malware for cyberattacks are connected to the home network. It helps telcos identify potential threats to their networks and take preventive actions quickly.

By using the proposed method, a telco can detect vulnerable IoT devices

connected behind a NAT, and use this information to take action. In the case of a potential DDoS attack, this method would enable the telco to take steps to spare the company and its customers harm in advance, such as offloading the large volume of traffic generated by an abundance of infected domestic IoT devices. In turn, this could prevent the combined traffic surge from hitting the telco's infrastructure, reduce the likelihood of service disruption, and ensure continued service availability.

"Unlike some past studies that evaluated their methods using partial, questionable, or completely unlabeled datasets, or just one type of device, our data is versatile and explicitly labeled with the device model," Meidan says. "We are sharing our experimental data with the scientific community as a novel benchmark to promote future reproducible research in this domain." This dataset can be found here: doi.org/10.5281/zenodo.3924770

This research is a first step toward dramatically mitigating the risk posed to telcos' infrastructure by domestic NAT IoT devices. In the future, the researchers seek to further validate the scalability of the method, using additional IoT devices that represent an even broader range of IoT models, types and manufacturers.

"Although our method is designed to detect vulnerable IoT devices before they are exploited, we plan to evaluate the resilience of our method to adversarial attacks in future research," Meidan says. "Similarly, a spoofing attack, in which an infected device performs many dummy requests to IP addresses and ports that are different from the default ones, could result in missed detection."

More information: Yair Meidan et al, A novel approach for detecting vulnerable IoT devices connected behind a home NAT, *Computers & Security* (2020). DOI: 10.1016/j.cose.2020.101968