INFOSEC

General security

Japan's IoT scanning project looks for vulnerable IoT devices

October 15, 2020 by **Rodika Tollefson**

Share:

The growing world of IoT — and security concerns

The Internet of Things (IoT) is still a baby compared to other computing technologies, but the market has already exploded and continues to expand at a healthy pace. Telecommunications giant Ericsson estimates the number of IoT connections to grow from 10.8 billion in 2019 to 24.9 billion in 2025, or a 15 percent compound annual growth rate (CAGR).

Estimates from the International Data Corporation (IDC) are even more robust. IDC forecasts that by 2025, the number of connected IoT devices will grow to 41.6 billion — together generating 79.4 zettabytes of data. That's enough data to stream close to 26.5 trillion hours of Netflix in high definition.

Related Articles

General security December 16, 2020
Information Security (IS) Auditor Salary and Job Prospects

General security December 16, 2020
Average CCSP Salary

General security December 16, 2020
Average Web Application Penetration Testing Salary

General security December 16, 2020
Average Chief Technology Officer Salary

General security December 16, 2020
Average SSCP Salary in 2018

Related Bootcamps

Computer Forensics

Ethical Hacking

The mind-boggling growth of the world of IoT comes with a hefty challenge. Securing connected devices has been a problem all along, as IoT devices are notoriously vulnerable to attacks. The old but still good story about hackers breaching a casino network through a connected fish tank may be the best illustration of the IoT risks.

Connected toasters and light bulbs may not be the first things to come to mind in matters of national security concerns, but Japan thought otherwise. As the country prepared for the 2020 Summer Olympics (since postponed until 2021), the Japanese government forged ahead with a project to scan its citizenry's IoT devices for weaknesses.

The thinking behind Japan's IoT scanning initiative

Information and Communication Technology, or NICT (Japan's sole national research and development agency), to access IoT devices for five years. The government approved a plan in January 2019 to carry out the survey shortly after. The reported goal was to evaluate the country's vulnerability to cyberattacks.

NICT obtained the cooperation of telecommunication providers for the project, called NOTICE (National Operation Toward IoT Clean Environment).

The plan was this, according to NICT news reports:

- Widely publicize NOTICE with posters and signage in public transportation areas and home appliance stores
- Scan some 200 million devices for those with weak credentials (using credential stuffing with about a hundred different passwords), as well as those infected with malware
- Notify owners of vulnerable devices through their ISPs

NICT planned to use easy-to-guess and default passwords (such as "password" and "123456") for the login attempts and said no personal information would be collected. Individual users weren't notified in advance about their specific devices being scanned. "The survey will not intrude into the device or acquire information other than that required for the survey," the agency said in a press release.

Mirai: The poster child for weak IoT security

NICT noted in its press release that cyberattacks targeting IoT devices have been growing in the last few years.

"IoT devices have characteristics that are easily targeted by cyberattacks, such as limited functions, difficulty in maintenance and a long lifecycle," the agency stated. "In other countries, in fact, serious damage has been reported, including internet outage caused by a large-scale cyberattack (DDoS attacks) that co-opted IoT devices."

One such large-scale cyberattack was the 2016 targeted DDoS (distributed denial-of-service) attack on DNS provider Dyn that caused major disruption to internet access for millions of users in the United States. The attack was carried out through the Mirai botnet, leveraging unsecure consumer IoT devices like DVRs and webcams.

The botnet continuously scanned the internet for devices with default or hard-coded passwords, using a table of about 60 different passwords. Compromised devices were then infected with the Mirai malware. Since the devices could continue to function normally, their owners would have no clues that something may be amiss. Some estimates put the number of IoT devices involved in the Dyn attack in the millions and the attack strength at 1.2 Tbps.

example, was built by an undergrad college student who wanted to use it for Minecraft scams and the source code was published on a hacker forum. That means anyone else could adapt the techniques for other malware attacks.

DDoS attacks are just one security concern. IoT devices can also expose the sensitive data that they collect and can have their functionality disrupted or sabotaged (some connected pacemakers, for example, have been found vulnerable to hacking). And as the infamous casino hack demonstrated, connected devices can also be used to access a corporate network. In other words, Japan had plenty to worry about ahead of the Summer Olympics to warrant the NOTICE project.

So what did the IoT scans in Japan discover?

In June 2020, NICT published the project's results to date. Media reports said that about 50 ISPs have participated in NOTICE, with around 110 million IP addresses surveyed. So far, the scans found 100,000 devices that had ports open to the internet and could accept login credentials. Of those, 2,259 used weak passwords.

Additionally, the project found an average of 162 devices a day that were infected with malware such as the Mirai variant. The agency also noted there was a significant spike in infected devices around February and March of this year, closer to 500 a day — indicating that the Mirai botnet may have been reactivated. (Coincidentally or not, these spikes occurred just as the COVID-19 pandemic brought an onslaught of phishing and malware campaigns, overall heightening cybersecurity concerns as people started working from home en masse.)

Should other countries take notice of NOTICE?

While some security experts believe Japan's NOTICE could be a model for other countries, these types of initiatives aren't likely to put any type of dent in IoT security concerns. NOTICE goes as far as notifying the consumers who have weak devices — but then what? Many people don't know how to change default passwords and won't go to the trouble of learning how to. And default passwords are only a small part of IoT device security.

Raising consumer awareness is a good thing, but improving IoT security would take a much bigger effort. It needs to happen at industry level — and potentially with some regulations thrown in. But Japan got something right, nonetheless. If insecure IoT devices can bring the internet to its knees (and do so much more), it's not a stretch for other countries to look at smart toasters or webcams as a matter of national security.

Sources