Japan urges white-hat hackers to hack insecure IoT devices ahead of the 2020 Olympics

Today, in the logistics of major sporting events in general and Olympic in particular, network security is also an especially important factor.

Today, in the logistics of major sporting events in general and Olympic in particular, network security is also an especially important factor.For the first time in the history of the Olympics, there will be an enormous interest in digital safety, particularly at the 2020 Tokyo Olympics.The Japanese host is now calling on hackers to launch attacks to exploit vulnerabilities in all 'unsafe' IoT devices.The organizers would like to have a more objective view of how many utilities in this East Asian country can be hacked, thereby promptly making a remedy to prepare for the biggest sporting event on the way. Crystal will take place in Tokyo next year.

1. How can IoT help you enjoy 4.0-style meals?

Help from white hat hackers

At the beginning of last week, the Japanese parliament approved a law, allowing white-hat hackers, with cooperation from the government to attack unsafe IoT devices to grasp the information security situation. in this country.This is a move deemed necessary to ensure the success of the Tokyo 2022 Olympic Games.

The staff of the Japan National Institute of Information and Communication Technology (NICT) will conduct a large-scale survey, under the supervision of the Ministry of Home Affairs and Communications staff on security

issues. Security for devices in the Internet of Things network in this country.

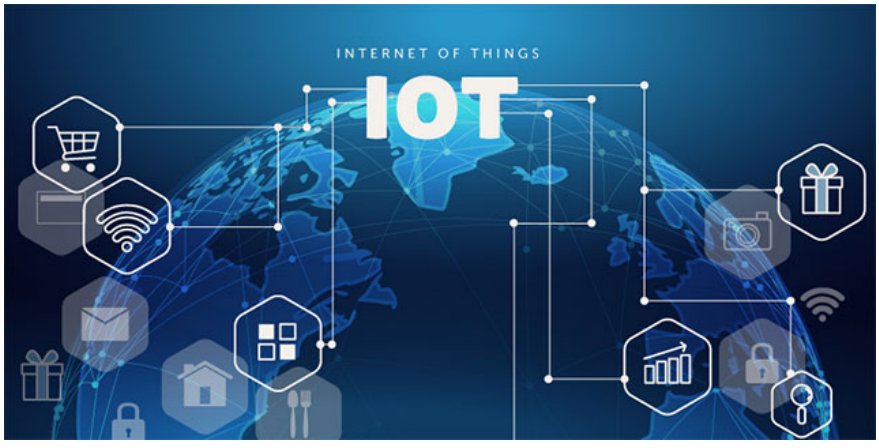
There will be very strict commitment rules enforced for privacy reasons, and NICT staff will only be allowed to use the authentication information and password dictionary to search and attack devices. hackable.

However, not everyone agrees with this host country's plan.Intelligence at Tenable, VP Gavin Millard, expressed doubts about the feasibility and effectiveness of the plan. According to Gavin Millard, the ability to find IoT devices has security problems. is not much:

'Rather than using hackers, perhaps NICT should inform users about IoT devices that are exposed to passwords or using too simple passwords.A quick Shodan search found only about 1000 devices currently connected in Japan using easy-to-guess passwords, so unless NICT experts use a scan tool like Nessus, otherwise This campaign will have a PR meaning, creating a reputation for the dedication of the Tokyo Olympic organizers rather than providing real security improvements. "

1. The most important programming languages ??in the Internet of Things era

The survey is expected to take place next month, with a list of more than 200 million IoT devices to be tested.Under the plan, NICT security experts will begin to check for networked routers and cameras.When identifying unsafe devices, they will provide details for ISPs and local authorities who have a duty to warn users about security risks from these devices.



As usual, IoT devices are at high risk of attack because many of them are equipped with unsafe default settings, and often do not receive updates and patches. Password required from the manufacturer.In addition, it is also because of these security holes that many IoT devices have been targeted by hackers, usurping the right to use and then being used as a 'material' to perform distributed attacks denying Service (DDoS).

However, one point that makes the Japanese Government's plan less effective is the scope of the implementation.The goal of the plan will be only vulnerable devices in Japan, while we all know that network security is an international process.Therefore, defending from one side is necessary but not enough to create absolute safety.

1. Kevin Mitnick shares tips and tricks that hackers often use

What do you think about the plan to identify vulnerable IoT devices before Japan's 2020 Tokyo Olympic Games?Leave comments in the comment section below!

See more:

1. US $ 1.7 billion of electronic money was beaten by hackers in 2018
2. Azorult Trojan steals user passwords while running in the background like Google Update
3. Android apps contain malicious code that uses motion sensors to avoid detection
4. The Internet is experiencing a huge problem with C / C ++, causing developers to "sweat"