Dmitriy Lohunov
E.A. Masalskaya, research supervisor
V.V. Gubkina, language adviser
National Mining University, Dnipro, Ukraine

Vulnerabilities that Allow to Make Botnets from IoT Devices

Nowadays people want each of their devices to be smart and connected to the network. This idea is called Internet of Things (IoT). The list of modern devices that support IoT includes smartphones, watches, appliances, cameras, cars and much more. It allows user to control its house just with one smartphone.

But there is no perfect system, and comfort for users usually means lots of security problems. Lots of IoT devices developers think that creating a good security system for the bulb or kettle is just a waste of money. But IoT devices are simple computers that can be hacked in the same way as regular PCs. Only one unprotected device in a big network of smart appliances usually leads to the whole system being hacked.

As result, we have giant botnets created with millions of IoT devices all over the world that can realize huge DDoS attacks. For example, at the end of 2016, a huge DdoS attack, the power of which amounted to 620 Gbps, was conducted and led to the lack of access to many services. One of the sources of this attack was a famous botnet Mirai.

There are some security problems of IoT gadgets:

Exploit the vulnerability of numerous devices

Most IoT systems are constantly being investigated by hackers for possible connection. In some cases, remote access attempts are made up to 800 times per hour.

Statistically, average IoT device get around 400 access attempts, 66% of them are successful. After connecting unprotected gadget to the network, it can be hacked in 6 minutes.

Interception of cell network signal

Lots of IoT devices, for example cars, are using cell network instead of Wi-Fi. That easily allows hackers to exploit vulnerabilities in cars' security systems and to get access to remote control of its functional. These cars have open IP addresses, no firewalls and they are not isolated from each other.

Reverse engineering

Many different developers of IoT devices store secret keys and passwords, which are used to confirm the "legality" of access, in their own firmware. This allows a hacker to create fake firmware and upload it to victim devices.

So, as you can see, the biggest problem of IoT devices is in their developers. While they do not understand, that security of every gadget is important, botnets like Mirai will continue their DDoS attacks.