VULNERABILITY "IoT" SYSTEMS

Martyniuk I., stud., Stefan N.Z., scientific adviser
Odessa State Environmental University, Ukraine

Now more than ever, the issue of information security has been raised, and especially about the security of the devices that surround us. Almost every person at home has his or her Internet I (IT) environment (Internet of Things). And it consists of the usual devices, various kinds of smart electronics and household appliances, various sensors, video surveillance systems, and other digital devices connected to the "network".

As for conventional Internet networks and for Internet "things", protection is required, this area is still quite young and for this reason it still has quite a large number of vulnerabilities.

Having a poorly configured or vulnerable IOT device in the home network can have very sad consequences for its users.

One of the most common scenarios is the inclusion of the device in the botnet. This is perhaps the most innocuous option for its owner; other uses are more dangerous. Thus, devices from the home network can be used as an intermediate link (Proxy) to commit unlawful actions. In addition, an attacker who has access to an IoT device can spy on his users. And this is by no means the worst scenario (for users), an infected device can simply be broken.

The purpose of the scientific work is to describe and consider the main threats of the modern world for "smart" devices.

The following threats were considered in the work:

- malicious software that threatens IoT devices;
- problems with the "firmware" provided by device manufacturers;
- device settings by default from device manufacturers.

Now IoT devices are attacked about every 3-5 minutes, and it's all the merit of malicious software that spreads freely through the network due to unsecured vulnerabilities in the firmware provided by the manufacturers of devices.

During the research, the network was scanned and some samples of malicious software were discovered that provided unauthorized access to the

devices. And as malicious software that allows you to create on the basis of infected devices a "botnet" network.

Some of the malware samples found:

1) Botnet of the "Linux.BackDoor.Tsunami" family allows you to gain control overthe system and use it to conduct DDoS attacks or to install other malicious software on the captured system;

2) DDoS botnet "Linux.Mrblack" is designed to collect information about theattacked system and conduct DDoS attacks using TCP / IP and HTTP protocols;

3) "Linux.PNScan.1" its purpose is to hack systems and load backdoors into themaccording to the architecture of the device, it downloads the following malicious programs "Linux.BackDoor.Tsunami" - which is described above, "Tool.Linux.BrutePma" - malicious the program is designed to break into the administration panels of databases "PHPMyAdmin";

4) "Linux.PNScan.2" This version of Linux.PNScan scans the network in thesearch for servers with standard SSH server settings and after infecting them with one or more of many malicious programs, their purpose ranges from conducting DDoS attacks, sending out spam and hacking some CMS, which allows you to conduct attacks on users who visit infected sites;

5) Botnet "Mirai" - Botnet designed for DDoS attacks, became very famous for itsmassive attacks on various IoT devices and also the publication of its source code, which resulted in a very large number of its modifications;

6) "BrickerBot" - This is the simplest sample of malicious software that was found,and it has only one purpose to find and destroy vulnerable devices, to damage the firmware or device configurations to the point that it stops working.

Smart Device Firmware - At best, manufacturers are releasing software updates for their "smart" devices with a delay. At worst (the most frequent case) - the firmware is not updated at all, many devices do not even have the option of installing updates.

Another problem is the passwords set by the manufacturer. They can be the same not only for a single model, but, say, for the entire product line. At the same time, the situation is not so new that lists of login / password combinations can be easily found on the Internet, which is used by intruders. It makes it easier for them and the fact that a significant part of the smart devices "shine" outward through Telnet ports, SSH ports and web interfaces providing full access to them.

Also, not only manufacturers install the same passwords for their devices, but Internet providers also do this, and for quite good reasons, in order to simplify the settings of devices such as routers and switches, which in turn jeopardizes the entire subnet of providers and with them and users and their devices that are in them.

I would like to say a few words about simple safety recommendations that will help you protect your devices from infection:

1) If this is not required to use the device, do not access it from the externalnetwork;
2) Disconnect all network services that you do not need to use the device.
3) If the device has a standard or universal password that can not be changed, or apredefined account that can not be deactivated, disable the network services in which they are used, or close the network access to them from the outside.
4) Before using, change the default password by setting a new one, resistant todirect bust.
5) Regularly update the firmware of the device to the latest version (if you havesuch updates).

Compliance with these simple recommendations will help prevent most of the attacks of the now common malicious programs attacking the IoT system.

Conclusions. The increase in the number of malicious programs for Internet of Things and related incidents demonstrates how serious the security problem of smart devices is.

The problem is also the manufacturers who, with their good intentions, help users with their "smart" devices leave vulnerabilities in protecting these devices.

Now the development of appropriate documents and safety rules for manufacturers of IoT devices is already being actively developed. The ultimate goal of these documents is to make the information systems we rely on, more resilient to attacks, limit damage from attacks and make systems capable of recovery and more resilient.

References:

1. Бирюков А.А. - Информационная безопасность. Защита и нападение - 2017
2. Russell B., Duren D.V. - Practical Internet of Things Security – 2016 https://www.securitylab.ru/ http://www.tadviser.ru/
3. https://regmedia.co.uk/2017/08/17/nist-sec-drft5.pdf