Connected home entertainment devices pose a security threat

David Jacoby, security analyst at Kaspersky Lab, conducted a research experiment in his living room to find out how safe his home is in terms of cyber security. He inspected home entertainment devices such as network-attached storages (NAS), smart TVs, router, Blu-ray player, etc. to find out if they are vulnerable to cyber-attacks.

Image: securelist.com

The Kaspersky Lab expert examined two NAS models from different vendors, one smart TV, a satellite receiver, and a connected printer. As a result of his research, Jacoby managed to find 14 vulnerabilities in the network attached storages, one vulnerability in the smart TV and several potentially hidden remote control functions in the router.

In line with its responsible disclosure policy, Kaspersky Lab does not disclose the names of the vendors whose products were subject to research until a security patch closing the vulnerabilities is released. All vendors were informed about the existence of the vulnerabilities. Kaspersky Lab specialists work closely with vendors to eliminate any vulnerabilities they discover.

"Individuals and also companies need to understand the security risks around connected devices. We also need to keep in mind that our information is not secure just because we have a strong password, and that there are a lot of things that we cannot control. It took me less than 20 minutes to find and verify extremely serious vulnerabilities in a device that looks like a safe one and even alludes to security in its own name. How would similar research end if it was conducted on a much wider scale than just my living room? This is just one of many questions that need to be addressed by device vendors, the security community and users of such devices collaboratively in the near future. The other important question is the lifecycle of devices. As I've learned from conversations with vendors, some of them will not develop a security fix for a vulnerable device when its lifecycle is over. Usually, the lifecycle lasts for one or two years, while the real life of devices - NAS' for instance - is much longer," said Jacoby.

Remote code execution and weak passwords

The most severe vulnerabilities were found in the network-attached storages. Several of them would allow an attacker to execute system commands remotely with the highest administrative privileges. The tested devices also had weak default passwords, lots of configuration files had the wrong permissions and they also contained passwords in plain text. In particular, the default administrator password for one of the devices contained just one digit. Another device even shared the entire configuration file with encrypted passwords to everyone on the network.

Using a separate vulnerability the researcher was able to upload a file in an area of the storage memory inaccessible for an ordinary user. Should this file be a malicious one, the compromised device would become a source of infection for other devices connecting to this NAS - a home PC, for instance - and even serve as a DDoS bot in a botnet. Moreover, since the vulnerability allowed the file to be uploaded in a special part of the device's file system, the only way to delete it was by using the same vulnerability. Obviously, this is not a trivial task even for a technical specialist, let alone the average owner of home entertainment equipment.

Man-in-the-Middle via smart TV

While investigating the security level of his own smart TV, the Kaspersky researcher discovered that no encryption is used in communication between the TV and the TV vendor's servers. That potentially opens the way for Man-in-the-Middle attacks that could result in the user transferring money to fraudsters while trying to buy content via the TV.

As a proof of concept, the researcher was able to replace an icon of the smart TV graphic interface with a picture. Normally the widgets and thumbnails are downloaded from the TV vendor's servers and due to the lack of encrypted connection the information could be modified by a third party. The researcher also discovered that the smart TV is able to execute Java code that, in combination with the ability to intercept the exchange of traffic between the TV and internet, could result in exploit-driven malicious attacks.

Hidden spying functions of a router

The DSL router used to provide wireless internet access for all other home devices contained several dangerous features hidden from its owner. According to the researcher, some of these hidden functions could potentially provide the ISP (Internet Service Provider) remote access to any device in a private network.

What's more important is that, according to the results of the research, sections of the router web interface called "Web Cameras", "Telephony Expert Configure", "Access Control", "WAN-Sensing" and "Update" are "invisible" and not adjustable for the owner of the device. They could only be accessed via exploitation of a rather generic vulnerability making it possible to travel between sections of the interface (that are basically web pages, each with own alphanumeric address) by brute forcing the numbers at the end of the address.

Originally these functions were implemented for the convenience of the owner of the device: the remote access function makes it fast and easy for the ISP to solve possible technical problems on the device, but the convenience could turn into a risk if the controls fell into the wrong hands.

How to stay safe

Make the hacker's life harder: all your devices should be updated with all the latest security and firmware updates. This will minimise the risk of exploiting known vulnerabilities.

Make sure that the default user name and password is changed - this is the first thing an attacker will try when attempting to compromise your device.

Most of the home routers and switches have the option of setting up your own network for each device, and also restrict access to the device - with the help of several different DMZs (a separate network segment for systems with a greater risk of compromise)/VLANs (a mechanism for achieving logical separation between different logical networks on the same physical network). For example, if you have a TV, you might want to restrict access to that TV and only allow it to access a

particular resource within your network. There isn't much reason for your printer to be connected to your TV.

See the full text of the research study Internet of Things: How I Hacked My Home

For more, visit: https://www.bizcommunity.com