## Featured news

- A new, streamlined version of Cryptowall is doing rounds
- Crypto e-mail provider ProtonMail pays ransom to stop DDoS attack, attack continues
- Cheap OmniRAT malware used to spy on Android, Windows, Linux, Mac devices
- Surviving in the IoT world: Risks of smart home devices
- Most employees are not malicious, but their carelessness can be just as damaging
- It's official! People want a more trustworthy Internet
- IT priorities are changing: Cloud-first strategy to rise
- Trojanized versions of 20,000 popular apps found secretly rooting Android devices
- Sale of legitimate code-signing certs booms on darknet markets
- Crypto-ransomware encrypts files "offline"
- Four ways organizations can prevent PII from becoming black market public record
- 90% of directors believe regulators should hold firms liable for hacks
- Firefox 42 features privacy and security improvements
- Researchers map out hard-to-kill, multi-layered spam botnet
- vBulletin, Foxit forums hacked, attacker exploited an 0-day?
- 11 0-days uncovered in Samsung Galaxy S6 Edge
- Open source tool checks for vulnerabilities on Android devices
- Researchers identify potential security hole in genomic data-sharing network



# Surviving in the IoT world: Risks of smart home devices

Posted on 06 November 2015.

Investigating some of the latest Internet-of-Things (IoT) products, Kaspersky Lab researchers have discovered serious threats to the connected home. These include a coffeemaker that exposes the homeowner's Wi-Fi password, a baby video monitor that can be controlled by a malicious third-party, and a smartphone-controlled home security system that can be fooled by a magnet.

In 2014, Kaspersky Lab security expert David Jacoby decided to investigate how susceptible the devices he owned were to a cyber attack. He discovered that almost all of them were vulnerable. This year, a team of antimalware experts repeated the experiment with one difference: while David's research was concentrated mostly on network-attached servers, routers and Smart TVs, this latest research was focused on various connected devices available on the smart home market. The investigation discovered that almost all of the devices contained vulnerabilities.

The baby-monitor camera used in the experiment could allow a potential attacker, whilst using the same network as the camera owner, to connect to the camera, watch the video from it and launch audio on the camera itself. Other cameras from the same vendor allowed for the ability to collect owner passwords and the experiment showed it was also possible for someone on the same network to retrieve the root password from the camera and maliciously modify the camera's firmware.

When researching the app-controlled coffeemakers, it was discovered that it's not even necessary for an attacker to be on the same network as the victim. The coffeemaker examined during the experiment was sending enough unencrypted information for an attacker to discover the password for the coffeemaker owner's entire Wi-Fi network.

On the other hand, researchers found that the smartphone-controlled home security system's software had just minor issues and was secure enough to resist a cyberattack. Instead, the vulnerability was found in one of the sensors used by the system.

The contact sensor used, which is designed to set off the alarm when a door or a window is opened, works by detecting a magnetic field emitted by a magnet mounted on the door or window. During the experiment, experts were able to use a simple magnet to replace the magnetic field of the magnet on the window, allowing them to open and close a window without setting off the alarm. This vulnerability is also impossible to fix with a software update; the issue is in the design of the home security system itself. Furthermore, the magnetic field sensor-based devices are a common type of sensors, used by multiple home security systems on the market.

"Our experiment, reassuringly, has shown that vendors are considering cyber-security as they develop their IoT devices. Nevertheless, any connected, app-controlled device is almost certain to have at least one security issue. Criminals might exploit several of these issues at once, which is why it is so important for vendors to fix all issues - even those that are not critical. These vulnerabilities should be fixed before the product even hits the market, as it can be much harder to fix a problem when a device has already been sold to thousands of homeowners," - said Victor Alyushin, Security Researcher at Kaspersky Lab.

In order to help consumers stay protected from the risks of vulnerable smart home IoT devices, Kaspersky Lab experts advise the following:

**1. Before buying any IoT device, search the Internet for news of any vulnerabilities within that device**
Researchers are constantly finding security issues in IoT products: from baby monitors to app controlled rifles. It is very possible that the device you are going to purchase has already been examined by security researchers and you can find out whether the issues found in the device have been patched.

**2. Avoid the temptation of purchasing new products recently**

## Spotlight

1 2 3 4 5

### Trojanized versions of 20,000 popular apps found secretly rooting Android devices

Researchers have discovered 20,000 apps that secretly root users' phone and install themselves as system applications, which makes them nearly possible to remove.



## Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address Subscribe



## Daily digest

Receive a daily digest of the latest security news.

Email @ Address Subscribe

**released on the market**
Along with the standard bugs you get in new products, recently-launched devices might contain security issues that haven't yet been discovered by security researchers. It is better to buy products that have already experienced several software updates.

**3. When choosing what part of your life you're going to make a little bit smarter, consider the security risks.**
If you set up a home security system, consider a professional alarm system that can be setup in such a way that any potential vulnerabilities would not affect its operation. Or if you need to purchase a baby monitor, it may be wise to choose the simplest RF-model on the market, one that is only capable of transmitting an audio signal, without Internet connectivity.

hardware | Internet of Things | tips



DON'T MISS
Fri, Nov 6th

A new, streamlined version of Cryptowall is doing rounds

Surviving in the IoT world: Risks of smart home devices

Firefox 42 is out, with many privacy and security improvements

Crypto-ransomware encrypts files "offline"

Researchers map out hard-to-kill, multi-layered spam botnet

Back to TOP