12. of June 2014

Introduction

Smartphones are subjected to silent attacks these days, you will never know that you are infected and no Anti-virus can detect these threats. This is in other words attacks that are stealthy and untraceable, and you have no means to protect yourself – until now.

These infections are done using SMS as a method of infecting the phone. Most of them are silent, and they infect the phone at the modem level where the operating system of the modem or SIM card is used to gain access to and install malicious software. These methods are used amongst others by the NSA, an attack method called Monkey Calendar.

However, the NSA is just a small part of this picture, and what we saw is that these infections are used from everything from draining your mobile account, to physically destroying your phone, to tapping into everything you have on your phone including voice and SMS, even encrypted voice can be monitored, to industrial espionage and targeted attacks on mobile banking solutions.

Rosberg System uncovered these serious infections on smartphones, and Dagbladet, who have won international press awards for their investigative journalism; published an article where we shared some of our knowledge on the subject.

Rosberg System have created the only scalable solution for preventing these attacks.

Here is a transcript of the Norwegian article:

For several years, someone could have utilized a number of "shortcuts" to gain unauthorized access to the content on your smartphone.

- Some of the methods are completely invisible to the user, who can neither see, hear or learn that you have an infection on your phone. This is not something people are aware of. It has never been communicated clearly in the regular news channels, says IT expert Odd Helge Rosberg to Dagbladet.

Get alerts

There are a number of other methods, which are duly mentioned earlier. These are often based on your own stupidity. For example if you connect to an unknown network or press "OK" on an installation from unknown sources. Then malicious software is installed.

But what if someone can enter into your phone and see everything, without your participation, and without you noticing anything? Such opportunities exist, and they are available for both criminal and intelligence agencies. The data conferences, hacker forums and among those with

special interests, these possibilities are known. Towards regular consumers, few warnings have been issued.

- It's probably someone who does not want the possibilities of these attacks to be too well known, says Rosberg.

Invisible command

The technological loopholes he refers to is the penetration that sends commands to the phone's modem.

- This happens at a level below the operating system, so you cannot see it with regular antivirus, said Rosberg.

He is referring to so-called "Service SMS messages" that never get beyond the modem, and therefore are never seen by the user or the operating system.

- We have attempted to check if penetration can be detected after it has been done. It does not seem to be possible, says Rosberg.

- We are aware of the opportunities Dagbladet describes here, and we have for some time been trying to warn about it. Unfortunately, mobile security has not received the attention it should have, says former director Tore Larsen Orderløkken at the Norwegian Centre for Information Security (NorSIS).

Works on the solution

The small company Rosberg System AS in Rogaland has quietly worked on solutions. Rosberg does not want to go into detail why, but Dagbladet knows that certain companies and services made contact to develop a means to protect exposed mobile phones.

- It requires a completely different solutions than what most telecom operators today uses, he says.

In connection with Snowden revelations a number of documents surfaced where it was described several techniques NSA used to take control of smart phones. These describe remote controllable microphone, tracking and recording of conversations.

It also seems to be possible to retrieve files, photos, messages, call data and other information. The documentation is from 2008 and shows how you have had links to Apple and Android, but also several other systems.

White and gray markets

Rosberg is concerned that the NSA should not dominate the debate about security, just because a lot of their old documentation is known.

- There is much that has been significantly improved since 2008, both by the NSA and others. There are many attacks that are not related to NSA and their technology. The solution is protection against all SMS-based attacks - both known and unknown - through filtering out everything that is not text messages the user sees, says Rosberg.

Dagbladet has even seen private companies that specialize in the sale of infiltration of mobiles. The services advertised against "government agencies".

- Where there is a legal market, there will always be a gray market, says Rosberg.

Tested Dagbladet

To demonstrate what is possible, Rosberg sends a system message to Dagbladet's phone. A few hours later we receive an email with a list of the operations we have performed on our smartphone during the same period. The experiment was performed on a smartphone Rosberg never held in their hands or otherwise have had access to manipulate.

- There is no advanced method we used in the test, it is only intended to show that it is possible. With more time and resources it is possible to build far more advanced methods, says Rosberg.

- Easy methods

Mobile Researcher Marius Kjeldahl the National Security Authority (NSM) believes smartphones are more secure than before.

- The operating system part of the smartphone has improved greatly. Previously, it was much easier to attack them. We have seen little vulnerability in mobile devices over the past two years, he says adding:

- However, although Snowden documents are relatively old, some of the methods described can still be utilized.

If anyone with resources has a desire to control smart phones, they have according to Kjeldahl other means of doing that than to "hack into it".

- U.S. companies like Google or Apple could theoretically be required by a secret court order to install anything on the phone that provides access. Another variant is the modification of the devices before they leave the store, said Kjeldahl.

According to Kjeldahl it has been reported that over 500,000 mobile devices have been modified so that they give full unauthorized access by remote control.

- If you want control, the method does not have to be very complicated, says Kjeldahl.