SPIEGEL ONLINE
09/09/2013 12:25 PM

iSpy

How the NSA Accesses Smartphone Data

By Marcel Rosenbach, Laura Poitras and Holger Stark

The US intelligence agency NSA has been taking advantage of the smartphone boom. It has developed the ability to hack into iPhones, android devices and even the BlackBerry, previously believed to be particularly secure.

Michael Hayden has an interesting story to tell about the iPhone. He and his wife were in an Apple store in Virginia, Hayden, the former head of the United States National Security Agency (NSA), said at a conference in Washington recently. A salesman approached and raved about the iPhone, saying that there were already "400,000 apps" for the device. Hayden, amused, turned to his wife and quietly asked: "This kid doesn't know who I am, does he? Four-hundred-thousand apps means 400,000 possibilities for attacks."

Hayden was apparently exaggerating only slightly. According to internal NSA documents from the Edward Snowden archive that SPIEGEL has been granted access to, the US intelligence service doesn't just bug embassies and access data from undersea cables to gain information. The NSA is also extremely interested in that new form of communication which has experienced such breathtaking success in recent years: smartphones.

In Germany, more than 50 percent of all mobile phone users now possess a smartphone; in the UK, the share is two-thirds. About 130 million people in the US have such a device. The mini-computers have become personal communication centers, digital assistants and life coaches, and they often know more about their users than most users suspect.

For an agency like the NSA, the data storage units are a goldmine, combining in a single device almost all the information that would interest an intelligence agency: social contacts, details about the user's behavior and location, interests (through search terms, for example), photos and sometimes credit card numbers and passwords.

New Channels

Smartphones, in short, are a wonderful technical innovation, but also a terrific opportunity to spy on people, opening doors that even such a powerful organization as the NSA couldn't look behind until now.

From the standpoint of the computer experts at NSA headquarters in Fort Meade, Maryland, the colossal success of smartphones posed an enormous challenge at first. They opened so many new channels, that it seemed as if the NSA agents wouldn't be able to see the forest for the trees.

According to an internal NSA report from 2010 titled, "Exploring Current Trends, Targets and Techniques," the spread of smartphones was happening "extremely rapidly" -- developments that "certainly complicate traditional target analysis."

The NSA tackled the issue at the same speed with which the devices changed user behavior. According to the documents, it set up task forces for the leading smartphone manufacturers and operating systems. Specialized teams began intensively studying Apple's iPhone and its iOS operating system, as well as Google's Android mobile operating system. Another team worked on ways to attack BlackBerry, which had been seen as an impregnable fortress until then.

The material contains no indications of large-scale spying on smartphone users, and yet the documents leave no doubt that if the intelligence service defines a smartphone as a target, it will find a way to gain access to its information.

Still, it is awkward enough that the NSA is targeting devices made by US companies such as Apple and Google. The BlackBerry case is no less sensitive, since the company is based in Canada, one of the partner countries in the NSA's "Five Eyes" alliance. The members of this select group have agreed not to engage in

any spying activities against one another.

Exploiting 'Nomophobia'

In this case, at any rate, the no-spy policy doesn't seem to apply. In the documents relating to smartphones that SPIEGEL was able to view, there are no indications that the companies cooperated with the NSA voluntarily.

When contacted, BlackBerry officials said that it is not the company's job to comment on alleged surveillance by governments. "Our public statements and principles have long underscored that there is no 'back door' pipeline to our platform," the company said in a statement. Google issued a statement claiming: "We have no knowledge of working groups like these and do not provide any government with access to our systems." The NSA did not respond to questions from SPIEGEL by the time the magazine went to print.

In exploiting the smartphone, the intelligence agency takes advantage of the carefree approach many users take to the device. According to one NSA presentation, smartphone users demonstrate "nomophobia," or "no mobile phobia." The only thing many users worry about is losing reception. A detailed NSA presentation titled, "Does your target have a smartphone?" shows how extensive the surveillance methods against users of Apple's popular iPhone already are.

In three consecutive transparencies, the authors of the presentation draw a comparison with "1984," George Orwell's classic novel about a surveillance state, revealing the agency's current view of smartphones and their users. "Who knew in 1984 that this would be Big Brother …" the authors ask, in reference to a photo of Apple co-founder Steve Jobs. And commenting on photos of enthusiastic Apple customers and iPhone users, the NSA writes: "… and the zombies would be paying customers?"

In fact, given the targets it defines, the NSA can select a broad spectrum of user data from Apple's most lucrative product, at least if one is to believe the agency's account.

The results the intelligence agency documents on the basis of several examples are impressive. They include an image of the son of a former defense secretary with his arm around a young woman, a photo he took with his iPhone. A series of images depicts young men and women in crisis zones, including an armed man in the mountains of Afghanistan, an Afghan with friends and a suspect in Thailand.

No Access Necessary

All the images were apparently taken with smartphones. A photo taken in January 2012 is especially risqué: It shows a former senior government official of a foreign country who, according to the NSA, is relaxing on his couch in front of a TV set and taking pictures of himself -- with his iPhone. To protect the person's privacy, SPIEGEL has chosen not to reveal his name or any other details.

The access to such material varies, but much of it passes through an NSA department responsible for customized surveillance operations against high-interest targets. One of the US agents' tools is the use of backup files established by smartphones. According to one NSA document, these files contain the kind of information that is of particular interest to analysts, such as lists of contacts, call logs and drafts of text messages. To sort out such data, the analysts don't even require access to the iPhone itself, the document indicates. The department merely needs to infiltrate the target's computer, with which the smartphone is synchronized, in advance. Under the heading "iPhone capability," the NSA specialists list the kinds of data they can analyze in these cases. The document notes that there are small NSA programs, known as "scripts," that can perform surveillance on 38 different features of the iPhone 3 and 4 operating systems. They include the mapping feature, voicemail and photos, as well as the Google Earth, Facebook and Yahoo Messenger applications.

The NSA analysts are especially enthusiastic about the geolocation data stored in smartphones and many of their apps, data that enables them to determine a user's whereabouts at a given time.

According to one presentation, it was even possible to track a person's whereabouts over extended periods of time, until Apple eliminated this "error" with version 4.3.3 of its mobile operating system and restricted the memory to seven days.

Still, the "location services" used by many iPhone apps, ranging from the camera to maps to Facebook, are useful to the NSA. In the US intelligence documents, the analysts note that the "convenience" for users ensures that most readily consent when applications ask them whether they can use their current location.

Cracking the Blackberry

The NSA and its partner agency, Britain's GCHQ, focused with similar intensity on another electronic toy: the BlackBerry.

This is particularly interesting given that the Canadian company's product is marketed to a specific target group: companies that buy the devices for their employees. In fact, the device, with its small keypad, is seen as more of a manager's tool than something suspected terrorists would use to discuss potential attacks.

The NSA also shares this assessment, noting that Nokia devices were long favored in extremist forums, with Apple following in third place and BlackBerry ranking a distant ninth.

According to several documents, the NSA spent years trying to crack BlackBerry communications, which enjoy a high degree of protection, and maintains a special "BlackBerry Working Group" specifically for this purpose. But the industry's rapid development cycles keep the specialists assigned to the group on their toes, as a GCHQ document marked "UK Secret" indicates.

According to the document, problems with the processing of BlackBerry data were suddenly encountered in May and June 2009, problems the agents attributed to a data compression method newly introduced by the manufacturer.

In July and August, the GCHQ team assigned to the case discovered that BlackBerry had previously acquired a smaller company. At the same time, the intelligence agency had begun studying the new BlackBerry code. In March 2010, the problem was finally solved, according to the internal account. "Champagne!" the analysts remarked, patting themselves on the back.

Security Concerns

The internal documents indicate that this was not the only success against Blackberry, a company that markets its devices as being surveillance-proof -- and one that has recently lost substantial market share due to strategic mistakes, as the NSA also notes with interest. According to one of the internal documents, in a section marked "Trends," the share of US government employees who used BlackBerry devices fell from 77 to less than 50 percent between August 2009 and May 2012.

The NSA concludes that ordinary consumer devices are increasingly replacing the only certified government smartphone, leading the analysts to voice their concerns about security. They apparently assume that they are the only agents worldwide capable of secretly tapping into BlackBerrys.

As far back as 2009, the NSA specialists noted that they could "see and read" text messages sent from BlackBerrys, and could also "collect and process BIS mails." BIS stands for BlackBerry Internet Service, which operates outside corporate networks, and which, in contrast to the data passing through internal BlackBerry services (BES), only compresses but does not encrypt data.

But even this highest level of security would seem not to be immune to NSA access, at least according to a presentation titled, "Your target is using a BlackBerry? Now what?" The presentation notes that the acquisition of encrypted BES communications requires a "sustained" operation by the NSA's Tailored Access Operation department in order to "fully prosecute your target." An email from a Mexican government agency, which appears in the presentation under the title "BES collection," reveals that this is applied successfully in practice.

Relying on BlackBerry

In June 2012, the documents show that the NSA was able to expand its arsenal against BlackBerry. Now they were also listing voice telephony among their "current capabilities," namely the two conventional mobile wireless standards in Europe and the United States, "GSM" and "CDMA."

But the internal group of experts, who had come together for a "BlackBerry round table" discussion, was still not satisfied. According to the documents, the question of which "additional enrichments would you like to see" with regards to BlackBerry was also discussed.

Even if everything in the materials viewed by SPIEGEL suggests the targeted use of these NSA surveillance options, the companies involved are not likely to be impressed.

BlackBerry is faltering and is currently open to takeover bids. Security remains one of its top selling points

with its most recent models, such as the Q10. If it now becomes apparent that the NSA is capable of spying on both Apple and BlackBerry devices in a targeted manner, it could have far-reaching consequences.

Those consequences extend to the German government. Not long ago, the government in Berlin awarded a major contract for secure mobile communications within federal agencies. The winner was BlackBerry.

Translated from the German by Christopher Sultan

URL:

http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

Related SPIEGEL ONLINE links:

NSA Affair Germans Conduct Helicopter Flyover of US Consulate (09/09/2013)
http://www.spiegel.de/international/germany/0,1518,921257,00.html
Photo Gallery Spying on Smartphones
http://www.spiegel.de/fotostrecke/fotostrecke-101201.html
Uncomfortable Monument Art Fills Former Spy Station in Berlin (09/06/2013)
http://www.spiegel.de/international/germany/0,1518,920875,00.html
'Success Story' NSA Targeted French Foreign Ministry (09/01/2013)
http://www.spiegel.de/international/world/0,1518,919693,00.html
Snowden Document NSA Spied On Al Jazeera Communications (08/31/2013)
http://www.spiegel.de/international/world/0,1518,919681,00.html
German Interior Minister 'US Takes Privacy Concerns Seriously' (08/28/2013)
http://www.spiegel.de/international/germany/0,1518,918770,00.html
Codename 'Apalachee' How America Spies on Europe and the UN (08/26/2013)
http://www.spiegel.de/international/world/0,1518,918625,00.html
Boom Triggered By NSA German Email Services Report Surge in Demand (08/26/2013)
http://www.spiegel.de/international/germany/0,1518,918651,00.html
Miranda Detention 'Blatant Attack on Press Freedom' (08/26/2013)
http://www.spiegel.de/international/world/0,1518,918592,00.html
Black Helicopters Britain's Blind Faith in Intelligence Agencies (08/21/2013)
http://www.spiegel.de/international/world/0,1518,917689,00.html
Cover Story How the NSA Targets Germany and Europe (07/01/2013)
http://www.spiegel.de/international/world/0,1518,908609,00.html