The NSA Breach of Telekom and Other German Firms

By Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer and Christian Grothoff

According to top-secret documents from the NSA and the British agency GCHQ, the intelligence agencies are seeking to map the entire Internet, including end-user devices. In pursuing that goal, they have broken into networks belonging to Deutsche Telekom.

When it comes to choosing code names for their secret operations, American and British agents demonstrate a flare for creativity. Sometimes they borrow from Mother Nature, with monikers such as "Evil Olive" and "Egoistic Giraffe." Other times, they would seem to take their guidance from Hollywood. A program called Treasure Map even has its own logo, a skull superimposed onto a compass, the eye holes glowing in demonic red, reminiscent of a movie poster for the popular "Pirates of the Caribbean" series, starring Johnny Depp.

Treasure Map is anything but harmless entertainment. Rather, it is the mandate for a massive raid on the digital world. It aims to map the Internet, and not just the large traffic channels, such as telecommunications cables. It also seeks to identify the devices across which our data flows, so-called routers.

Furthermore, every single end device that is connected to the Internet somewhere in the world -- every smartphone, tablet and computer -- is to be made visible. Such a map doesn't just reveal one treasure. There are millions of them.

The breathtaking mission is described in a Treasure Map presentation from the documents of the former intelligence service employee Edward Snowden which SPIEGEL has seen. It instructs analysts to "map the entire Internet -- Any device, anywhere, all the time."

Treasure Map allows for the creation of an "interactive map of the global Internet" in "near real-time," the document notes. Employees of the so-called "FiveEyes" intelligence agencies from Great Britain, Canada, Australia and New Zealand, which cooperate closely with the American agency NSA, can install and use the program on their own computers. One can imagine it as a kind of Google Earth for global data traffic, a bird's eye view of the planet's digital arteries.

Battlefield Map

In addition to monitoring one's own networks as well as those belonging to "adversaries," Treasure Map can also help with "Computer Attack/Exploit Planning." As such, the program offers a kind of battlefield map for cyber warfare.

The *New York Times* reported on the existence of Treasure Map last November. What it means for Germany can be seen in additional material in the Snowden archive that SPIEGEL has examined.

Treasure Map graphics don't just provide detailed views of German cable and satellite networks. Red markings also reveal to agents which carriers and internal company networks FiveEyes agencies claim to have already accessed. Of particular interest from the German perspective are two "Autonomous Systems" (AS) -- networks -- marked in red. They are labeled Deutsche Telekom AG and Netcologne, a Cologne-based provider.

The legend for the graphics in question explains the meaning behind the red markings: "Red Core Nodes: SIGINT Collection access points within AS." SIGINT refers to signals intelligence. In other words, networks marked with a red dot are under observation.

Regional provider Netcologne operates its own fiber-optic network and provides telephone and Internet services to over 400,000 customers. The formerly state-owned company Telekom, of which the German government still owns a 31.7 percent stake, is one of the dozen or so international telecommunications companies that operate global networks, so-called Tier 1 providers. In Germany alone, Telekom provides mobile phone services, Internet and land lines to 60 million customers.

According to the logic of the undated Treasure Map documents, that would mean that the NSA and its partner agencies are perhaps not only able to monitor the networks of these companies and the data that travels through them, but also the end devices of their customers. Where exactly the NSA gained access to the companies' networks is not made clear in the graphics. The red-marked AS of Deutsche Telekom by itself includes several thousand routers worldwide.

'Completely Unacceptable'

The German company is also active in the US and Great Britain. Furthermore, it is part of the TAT14 telecommunications cable

consortium; the cable runs via Great Britain to the east coast of the US. "The accessing of our network by foreign intelligence agencies," says a Telekom spokesperson, "would be completely unacceptable."

Because Netcologne is a regional provider, it would seem highly likely that the NSA or one of its Treasure Map partners accessed the network from within Germany. That would be a clear violation of German law and potentially another NSA-related case for German public prosecutors. Thus far, the only NSA-related casecurrently being investigated is the monitoring of Chancellor Angela Merkel's mobile phone.

Several weeks ago, SPIEGEL shared a GCHQ document with both companies in order to give them an opportunity to look into the alleged security breaches themselves. The security departments of both firms say they launched intensive investigations but failed to find suspicious mechanisms or data streams leaving the network.

Telekom and Netcologne are not the first German companies to have been successfully hacked by Anglo-American intelligence agencies, according to their own documents. In March, SPIEGEL reported on the large-scale attack by the British agency GCHQ on German satellite teleport operators Stellar, Cetel and IABG. Such providers offer satellite Internet connections to remote regions of the world. All three companies are marked red on the Treasuremap graphic, meaning that the NSA and its partner agencies have, according to their documents, internal "Collection Access Points."

SPIEGEL also contacted 11 non-German providers marked in the documents to request comment. Four answered, all saying they examined their systems and were unable to find any irregularities. "We would be extremely concerned if a foreign government were to seek unauthorized access to our global networks and infrastructure," said a spokesperson for the Australian telecommunications company Telstra.

'Key Staff'

Just how far GCHG and NSA go to improve their secret map of the Internet and its users can be seen in the example of Stellar.

The document describing the attack on the business, part of the so-called Mittelstand of small- to medium-sized companies that form the backbone of the German economy, originates from the Network Analysis Center of Britain's GCHQ, which is based in Bude along the Atlantic coast in Cornwall. The document lists "key staff" at the

company. The document states they should be identified and "tasked." "Tasking" somebody in signals intelligence jargon means that they are to be targeted for surveillance. In addition to CEO Christian Steffen, nine other employees are named in the document.

The attack on Stellar has notable similarities with the GCHQ surveillance operation targeting the half-state-owned Belgian provider Belgacom, which SPIEGEL reported on in the summer of 2013. There too, the GCHQ Network Analysis department penetrated deeply into the Belgacom network and that of its subsidiary BICS by way of hacked employee computers. They then prepared routers for cyber-attacks.

SPIEGEL reporters visited Stellar at its offices in Hürth, near Cologne, and presented passages of the documents in question to the CEO as well as three other employees cited by the British. A video of the visit can be seen here.

Among other things, Steffen and his colleagues were able to recognize in the GCHQ document a listing for their central server including the company's mail server, which the attackers appear to have hacked.

The document also includes details about the concrete findings of the spying efforts, including an internal table that shows which Stellar customers are being served by which specific satellite transponders. "Those are company secrets and sensitive information," said Stellar's visibly shocked IT chief, Ali Fares, who is himself cited as an employee to be "tasked."

'Fuck!'

Any remaining sanguinity is lost at the point the Stellar officials see the password for the central server of an important customer in the intelligence agency documents. The significance of the theft is immense, Fares says. The information, he continues, could allow the agencies to cut off Internet access to customers in, for example, Africa. It could also allow them to manipulate links and emails.

CEO Steffen commented on the document with a terse "Fuck!" He considers it to be final proof that his company's systems were illegally breached. "The hacked server stood behind our company's own firewall," he said. "The only way of accessing it is if you first successfully break into our network." The company in question is no longer a customer with Stellar.

When asked if there are any possible reasons that would prompt Britain, an EU partner country, to take such an aggressive approach to his company, Steffen just shrugged his shoulders, perplexed. "Our customer traffic doesn't run across conventional fiber optic lines," he said. "In the eyes of intelligence services, we are apparently seen as difficult to access." Still, he argues, "that doesn't give anyone the right to break in."

The founder and CEO of Stellar says he has no intention of letting this pass. "A cyber-attack of this nature is a clear criminal offense under German law," he said. "I want to know why we were a target and exactly how the attack against us was conducted -- if for no other reason than to be able to protect myself and my customers from this happening again." Six weeks ago, Steffen wrote a letter to the British government asking for an explanation, but he has not received an answer. Both GCHQ and NSA have likewise declined comment on the matter.

Meanwhile, Deutsche Telekom's security division has conducted a forensic review of important routers in Germany, but has yet to detect anything. Volker Tschersich, who heads the security division, says it's possible the red markings in Treasure Map can be explained as access to the Tat14 cable, in which Telekom occupies a frequency band in Britain and the US. At the end of last week, the company informed Germany's Federal Office for Information Security of SPIEGEL's findings.

The classified documents also indicate that other data from Germany contributes to keeping the global treasure map current. Of the 13 servers the NSA operates around the world in order to track current data flows on the open Internet, one is located somewhere in Germany.

Like the other servers, this one, which feeds data into the secret NSA network is "covered" in a data center.