NSA developing real time map of all Internet-connected devices

Thomas Gaist
16 September 2014

The US National Security Agency (NSA) penetrated the systems of leading German technology and communications companies as part of a global operation seeking to track all of the planet's data flows and Internet-capable electronic devices, according to NSA documents leaked by Edward Snowden and published jointly in *Der Spiegel* and the *Intercept*.

The leaked NSA slides reveal that the agency infiltrated data-capturing software into the systems of major German firms including Deutsche Telekom, Netcologne, Stellar, Cetel and IABG as part of a program codenamed Treasure Map. The slides display the targeted German firms as nodes in a worldwide network, with nodes highlighted red to indicate the maintenance of NSA "Collection Access Points" on their servers.

Treasure Map is an astonishingly expansive electronic surveillance and data mapping operation conceived by the NSA and the British GCHQ as "a near real-time, interactive map of the global internet," according to the documents. The information has been made accessible to the "five eyes" alliance that also includes Canada, Australia and New Zealand.

Der Spiegel writes that its aim is to map "every single end device that is connected to the Internet somewhere in the world—every smartphone, tablet and computer…"

Treasure Map "ingests approximately 16-18 million trace routes per day" according to NSA documents. By endlessly analyzing the connections between Internet-linked data sources, the agency is seeking to "map the entire Internet" and locate "Any device, anywhere, all the time" through continuous updating of a comprehensive global Internet map, the slides state.

The program, described by the *Intercept* as a "Google Earth for global internet traffic, a bird's eye view of the planet's digital arteries," processes "30+ gigabytes of additional data added and replaced per day" and has "new capabilities delivered every 90 days," according to the leaked documents.

The information gives the NSA, the GCHQ and its allies broader powers to monitor individuals within their countries as well as those targeted for attack. The article in *Der Spiegel* noted, "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 leaked slides further show that the NSA is developing a number of auxiliary programs to supplement and exploit Treasure Map data for operational purposes, including:

· Toygrippe, which maintains a "repository of VPN [virtual private network] endpoints";

· Vitalair2, which automatically scans IP addresses to search for vulnerabilities that can be exploited by the NSA's in-house hacker unit, known as Targeted Access Operations (TAO);

· IPGeoTrap, which supplies the exact latitude and longitude of targeted IP addresses.

In support of Treasure Map, the NSA maintains at least 13 covert data-gathering operations embedded inside "unwitting data centers" in Malaysia, Singapore, Taiwan, China, Indonesia, Thailand, India, Poland, Russia, Germany, Ukraine, Latvia, Denmark, South Africa, Argentina and Brazil, the leaked slides show.

The NSA rightly views the German tech firms as useful access points for snooping on international data flows. Deutsche Telekom and Netcologne operate global fiber optic networks that are integral components of globalized communications infrastructure, including the TAT14 trans-Atlantic fiber optic cables responsible

for handling much of the Internet traffic passing between the US and Europe.

Telekom, which was formerly owned outright by the German government and retains close ties to the state, serves at least 60 million customers in Germany alone. Based on its penetration of the German telecommunications firm Stellar, the NSA could “shut down the Internet in entire African countries,” according to an employee at the company who saw the documents.

In order to get access to the information from Stellar, the CEO said that the spy agencies would have to have broken into their network by overcoming the company’s firewall. “A cyber-attack of this nature is a clear criminal offense under German law,” he said.

These are only the latest revelations of spying by US and British imperialism against German companies in particular. Surveillance operations by Britain’s GCHQ intelligence agency targeting Stellar, Cetel, IABG and other companies were previously exposed by Snowden leaks published in March 2014. Internal documents from GCHQ’s Network Analysis Center showed that UK intelligence agents were engaged in “tasking” of “key staff,” that is, in continuous data gathering and analysis targeting “central employees” at these companies.

Snowden leaks published last October showed that the NSA had been spying on the telephone of German Chancellor Angela Merkel since 2002, and that the NSA was collecting some 500 million communications every month from German sources.