Report: NSA Intercepts Computer Deliveries

Raphael Satter, Associated Press

LONDON (AP) — A German magazine lifted the lid on the operations of the National Security Agency's hacking unit on December 29, 2013, reporting that American spies intercept computer deliveries, exploit hardware vulnerabilities, and even hijack Microsoft's internal reporting system to spy on their targets.

Der Spiegel's revelations relate to a division of the NSA known as Tailored Access Operations, or TAO, which is painted as an elite team of hackers specializing in stealing data from the toughest of targets.

Citing internal NSA documents, the magazine said that TAO's mission was "Getting the ungettable," and quoted an unnamed intelligence official as saying that TAO had gathered "some of the most significant intelligence our country has ever seen."

Der Spiegel said TAO had a catalog of high-tech gadgets for particularly hard-to-crack cases, including computer monitor cables specially modified to record what is being typed across the screen, USB sticks secretly fitted with radio transmitters to broadcast stolen data over the airwaves, and fake base stations intended to intercept mobile phone signals on the go.

The NSA doesn't just rely on James Bond-style spy gear, the magazine said. Some of the attacks described by Der Spiegel exploit weaknesses in the architecture of the Internet to deliver malicious software to specific computers. Others take advantage of weaknesses in hardware or software distributed by some of the world's leading information technology companies, including Cisco Systems and China's Huawei Technologies, the magazine reported.

Der Spiegel cited a 2008 mail order catalog-style list of vulnerabilities that NSA

spies could exploit from companies such as Irvine, California-based Western Digital Corp. or Round Rock, Texas-based Dell. The magazine suggested the agency was "compromising the technology and products of American companies."

Old-fashioned methods get a mention too. *Der Spiegel* said that if the NSA tracked a target ordering a new computer or other electronic accessories, TAO could tap its allies in the FBI and the CIA, intercept the hardware in transit, and take it to a secret workshop where it could be discretely fitted with espionage software before being sent on its way.

Intercepting computer equipment in such a way is among the NSA's "most productive operations," and has helped harvest intelligence from around the world, one document cited by Der Spiegel stated.

One of the most striking reported revelations concerned the NSA's alleged ability to spy on Microsoft's crash reports, familiar to many users of the Windows operating system as the dialogue box which pops up when a game freezes or a Word document dies. The reporting system is intended to help Microsoft engineers improve their products and fix bugs, but Der Spiegel said the NSA was also sifting through the reports to help spies break into machines running Windows. One NSA document cited by the magazine appeared to poke fun at Microsoft's expense, replacing the software giant's standard error report message with the words: "This information may be intercepted by a foreign sigint (signals intelligence) system to gather detailed information and better exploit your machine."

Microsoft said that information sent by customers about technical issues in such a manner is limited.

"Microsoft does not provide any government with direct or unfettered access to our customer's data," a company representative said in an email Sunday. "We would have significant concerns if the allegations about government actions are true."

Microsoft is one of several U.S. firms that have demanded more transparency from the NSA — and worked to bolster their security — in the wake of the revelations of former intelligence worker Edward Snowden, whose disclosures have ignited an international debate over privacy and surveillance.

Der Spiegel did not explicitly say where its cache NSA documents had come from, although the magazine has previously published a series of stories based on documents leaked by Snowden, and one of Snowden's key contacts — American documentary filmmaker Laura Poitras — was listed among the article's six authors.

No one was immediately available at *Der Spiegel* to clarify whether Snowden was the source for the latest story.

Another company mentioned by *Der Spiegel*, though not directly linked with any NSA activity, was Juniper Networks, a computer network equipment maker in Sunnyvale, CA.

"Juniper Networks recently became aware of, and is currently investigating, alleged security compromises of technology products made by a number of companies, including Juniper," the company said in an email. "We take allegations of this nature very seriously and are working actively to address any possible exploit paths."

If necessary, Juniper said, it would, "work closely with customers to ensure they take any mitigation steps."

Geir Moulson contributed to this report from Berlin. Ryan Nakashima contributed from Los Angeles.