THE DESK
JOURNALISM AND SOCIAL MEDIA BY MATTHEW KEYS

American companies respond to new NSA hacking claims

By Matthew Keys on January 1, 2014 In The News

(Der Spiegel/Jacob Appelbaum)

Several American tech companies have responded to a report published in Germany's Der Spiegel magazine detailing how National Security Agency officials exploit vulnerabilities in their hardware and software.

The report, released in tandem with an address by security expert Jacob Appelbaum at Germany's 30C3 conference, was based on classified NSA documents that were among those presumably disclosed to journalists by former government contractor Edward Snowden.

Among the documents released over the weekend was a "catalog" of spy hardware and software developed by "ANT," a previously unknown unit at the NSA. The group is tasked with developing spy gadgets for use by agents at the NSA and elsewhere. The gadgets developed by ANT take advantage of previously-unknown vulnerabilities in computer hardware and software manufactured by at least nine American companies: Dell, Hewlett-Packard, Cisco, Juniper, Apple, Microsoft, Western Digital, Seagate/Maxtor and Oracle.

At the 30C3 Conference, Appelbaum questioned whether or not the American companies named in the documents were complicit in "leaving us vulnerable," but said it was ultimately important to name the companies because "some of them are victims.

"It's important to note that we don't yet understand which is which," Appelbaum said, "so it's important to name them so that they have to on record, and so that they can say where they are."

Apple calls NSA agents "malicious hackers"

On Tuesday, Apple released a statement denying it colluded with NSA agents on "any of our products, including iPhone." One document claimed NSA agents were able to commandeer many features found on Apple's iPhone, including pulling call logs, text messages, contact lists and other files from a user's phone.

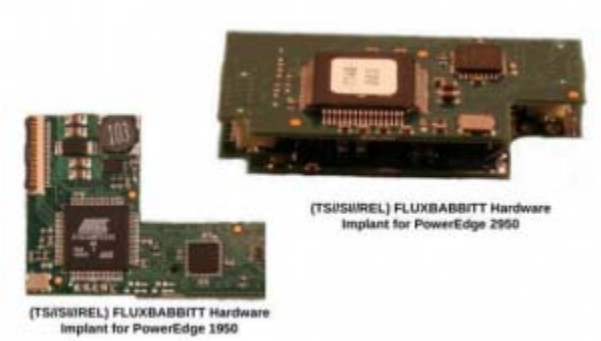
"Whenever we hear about attempts to undermine Apple's industry-leading security, we thoroughly investigate and take appropriate steps to protect our customers," Apple said in a statement. "We will continue to use our resources to stay ahead of malicious hackers and defend our customers from security attacks, regardless of who's behind them."

Cisco launches "investigation" into disclosed vulnerabilities

In a blog post published on Monday, Cisco's Chief Security Officer John Stewart said the company was looking into reports that its prized firewall software could be permanently breached through an exploit used by NSA agents. Initially, Cisco said it was "unaware of any new product vulnerabilities," but later said that it had "opened an investigation" after Der Spiegel published additional information on "techniques allegedly used by NSA TAO (agents) to infiltrate the technologies of numerous IT companies."

"We are deeply concerned with anything that may impact the integrity of our products or our customer's networks and continue to seek additional information," Stewart wrote.

Dell: We don't collude with any government



A gadget called "FLUXBABBLE" that the NSA purportedly uses to exploit certain Dell servers. (Der Spiegel/Jacob Appelbaum)

Dell echoed the same concern, rebuking any claims that it works with "any government — United States or otherwise — to compromise our products." Documents detailed how NSA agents were able to exploit hardware vulnerabilities on a number of Dell servers, including two servers — the Dell PowerEdge 1950 and Dell PowerEdge 2950 — that the company no longer sells.

"We take very seriously any issue that may impact the integrity of our products or customer security," Dell said in a statement to CRN Magazine (the same statement was emailed to *The Desk* on Thursday). "Should we become aware of a possible vulnerability in any of Dell's products we will communicate with our customers in a transparent manner as we have done in the past."

Hewlett-Packard doubts server was compromised

Documents show a similar exploit used against Dell servers was also used against a server manufactured by Hewlett-Packard, the HP ProLiant 380 G5. In a statement to *The Desk*, a company spokesperson said Hewlett-Packard was not aware of the claims made in the Der Spiegel report, but added it has "no reason to believe that the HP ProLiant G5 server mentioned was ever compromised as suggested in the article."

"HP's privacy and security policies are quite clear; we do not knowingly develop products to include security vulnerabilities," the spokesperson said. "We are also active in happy wheels testing and updating our products regularly to eliminate threats and make our products more secure. HP takes the privacy and security of our customer information with great seriousness. We will continue to put in place measures to keep our customers' information confidential and secure."

Western Digital denies knowledge of "implants"; Seagate deflects

One document describes how NSA agents can infect a hard drive with malicious firmware that would essentially allow agents to commandeer a computer for purposes of installing malware. Western Digital, Seagate and Maxtor were listed as brands of hard drives that could be exploited using the firmware.

In a statement emailed to *The Desk* late Wednesday, Western Digital spokesperson Steve Shattuck denied the company developed, or even had any knowledge of, such "implants" that could be used on its hard drives.

"Western Digital has no knowledge of, nor has it participated in, the development of technology by government entities that create 'implants' on Western Digital hard drives, as Der Spiegel described," Shattuck wrote.

On Friday, Seagate said it was aware of the report, but declined to comment citing lack of knowledge about the claims made in the Der Spiegel report. Seagate acquired Maxtor in 2006; the company no longer manufactures hard drives under the Maxtor brand.

Juniper "not aware" of "BIOS implants"; Oracle declines comment

One of the most-troubling revelations to come out of the Der Spiegel report dealt with firewall hardware manufactured by Cisco Systems, Juniper Networks and the Chinese company Huawei. The documents reveal that NSA agents designed malicious code that could attach itself to the a machine's "BIOS," usually the first piece of software that boots on a computer designed to "wake up" hardware and load an operating system.

As it is described, once the NSA software attaches itself to the BIOS of a machine, it grants NSA agents and presumably others a permanent "backdoor" into the hardware — that is, agents would have continuous access to a computer or a computer network. The NSA firmware was designed to be undetectable and "persistent" on a machine.

On Thursday, a Juniper spokesperson told *The Desk* it had no knowledge of any "BIOS implants" prior to the disclosure by Der Spiegel, and denied it "assisted any organization or individual in the creation of such implants."

"We take allegations of this nature very seriously and are working actively to address any possible exploit paths," Juniper spokesperson Corey Olfert said. "As a company that consistently operates with the highest of ethical standards, we are committed to maintaining the integrity and security of our products. We are also committed to the responsible disclosure of security vulnerabilities, and if necessary, will work closely with customers to implement any mitigation steps."

Similar firmware is used by NSA agents to infect the BIOS of a computer's motherboard running any number of operating systems, including Microsoft's Windows and Oracle's Solaris. In an email message sent to *The Desk* Thursday afternoon, Oracle spokeswoman Letty Ledbetter said the company had no comment on the report.

Microsoft: "Significant concerns" if "Government actions are true"

Various Microsoft products were named in several of the documents disclosed by Der Spiegel. Notably, NSA agents claimed they were able to take advantage of machines running versions of Microsoft's Windows operating system and, in some cases, intercept reports detailing bugs and other errors in Microsoft software that would normally be sent from a user's computer to the company.

Microsoft, which recently joined several other American tech companies in calling for surveillance reform, denied knowing about the exploits disclosed in the Der Spiegel report but said it "*would have significant concerns if the allegations about Government actions are true.*"

"*We are not familiar with ARKSTREAM," a Microsoft spokesperson said in an email message to The Desk* late Thursday evening. "Regardless…Microsoft does not provide any Government with direct or unfettered access to our customers' data."

When asked if Microsoft knowingly leaves security flaws in its products, the spokesperson replied: "No."

The Desk emailed all nine American companies named in the "ANT" catalog published by Der Spiegel and provided copies of the relative NSA document to each company; most emails were returned with a holiday "out of office" message.

The full collection of ANT documents released by Der Spiegel and Appelbaum on Monday can be found here.

http://thedesk.matthewkeys.net/2014/01/american-companies-respond-to-new-nsa-hacking-claims/