Written by **Thomas R. Eddlem** on January 2, 2014

Apple Strikes Back at NSA's "Malicious Hackers"

Apple Inc. executives have labeled leadership of the U.S. government's National Security Agency "malicious hackers" and have vowed to fight against reported NSA software hacks of all of Apple's iPhones. NSA documents published by the German magazine *Der Spiegel* boast that its program DROPOUTJEEP "includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc."

In other words, if the NSA wants to pull any information from someone's iPhone, or wants to listen to what's being said (even if there's no active call), there's nothing a user can do about it. Moreover, the NSA can track Americans' movements through the phones' GPS systems. DROPOUTJEEP is a software program produced by the NSA's ANT program.

The *Der Spiegel* revelations come just months after various news agencies revealed that the NSA had employed its espionage techniques against innocent Americans. An NSA auditor found that the NSA violated privacy law thousands of times in 2012, and the NSA admitted that its staff had used its technology to spy on wives and girlfriends — so-called LOVEINT — in defiance of both statutory law and the Constitution's Fourth Amendment (which requires a warrant, probable cause, and specificity for searches to be "reasonable" and constitutional).

"Apple has never worked with the NSA to create a backdoor in any of our products, including iPhone. Additionally, we have been unaware of this alleged NSA program targeting our products," Apple said in a statement released December 31. "Whenever we hear about attempts to undermine Apple's industry-leading security, we thoroughly investigate and take appropriate steps to protect our customers. 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."

Apple is not alone among major computer companies who have allegedly become victims to NSA hacks of the products they sell to their customers. *Der Spiegel* revealed a full spectrum of NSA hacks of consumer and commercial electronics:

> JETPLOW hacks Cisco firewalls
>
> IRONCHEF hacks Hewlett Packard servers
>
> SOMBERKNAVE and GINSU target Windows computers
>
> IRATEMONK hacks "Western Digital, Seagate, Maxtor and Samsung hard drives."

Cisco has also expressed concern over alleged attacks on its servers and routers. "We are deeply concerned with anything that may impact the integrity of our products or our customers' networks and continue to seek additional information," Cisco's Senior Vice President John Stewart said in a blog on the company's website December 29, the day the *Der Spiegel* report was published. Stewart is the

company's chief security officer in charge of Threat Response, Intelligence and Development. "At this time, we do not know of any new product vulnerabilities, and will continue to pursue all avenues to determine if we need to address any new issues. If we learn of a security weakness in any of our products, we will immediately address it."

Stewart claimed that the JETPLOW and any other alleged hacks of Cisco products were not made with the knowledge or consent of the company. "As we have stated prior, and communicated to *Der Spiegel*, we do not work with any government to weaken our products for exploitation, nor to implement any so-called security 'back doors' in our products."

Likewise, Microsoft has protested claims that the NSA has used "error" messages as a means of importing an NSA hack of various Microsoft operating systems. "Microsoft does not provide any government with direct or unfettered access to our customer's data," a company representative told CBS News in a December 29 e-mail. "We would have significant concerns if the allegations about government actions are true."

It remains to be seen if these corporate protests will result in better corporate security, and in more pressure on Congress by corporate lobbyists to rein in the NSA's unconstitutional snooping, or if they are just reactive statements released for public relations purposes.

Photo of sign displaying Apple logo outside company's headquarters in Cupertino, Calif.: AP Images