Snowden: Spy Agencies 'Screwed All of Us' in Hacking Crypto Keys

By Kim Zetter

February 24, 2015

NSA whistleblower Edward Snowden didn't mince words during a Reddit Ask Me Anything session on Monday when he said the NSA and the British spy agency GCHQ had "screwed all of us" when it hacked into the Dutch firm Gemalto to steal cryptographic keys used in billions of mobile SIM cards worldwide.

"When the NSA and GCHQ compromised the security of potentially billions of phones (3g/4g encryption relies on the shared secret resident on the sim)," Snowden wrote in the AMA, "they not only screwed the manufacturer, they screwed all of us, because the only way to address the security compromise is to recall and replace every SIM sold by Gemalto."

Gemalto is one of the leading makers of SIM cards used in billions of mobile phones around the world to secure the communications of telecom customers of AT&T, T-Mobile, Verizon, Sprint and more than 400 other wireless carriers in 85 countries. Stealing the crypto keys essentially allows the spy agencies to wiretap and decipher encrypted phone communications at will without the assistance of telecom carriers or the oversight of a court or government. The keys also allow the agencies to decrypt previously intercepted messages they hadn't been able to crack.

But in stealing the keys with the aim of targeting the communications of specific customers, the spy agencies undermine the security of billions of other customers.

"Our governments … should never be weighing the equities in an intelligence gathering operation such that a temporary benefit to surveillance regarding a few key targets is seen as more desirable than protecting the communications of a global system…" Snowden wrote.

As The Intercept reported last week, the spy agencies targeted employees of the Dutch firm, reading their siphoned emails and scouring their Facebook posts to obtain information that would help the agencies hack the employees. Once on employee systems, the spy agencies planted backdoors and other tools to give them a persistent foothold on the company's network. We

“believe we have their entire network,” the author of a PowerPoint slide, leaked by Snowden to journalist Glenn Greenwald, boasted about the hack.

Snowden commented on the story after being asked what he thought about recent revelations from Kaspersky Lab that it had uncovered a spy module, believed to belong to the NSA, designed for hacking the firmware of hard drives. Snowden said the firmware hacking was “significant” but even more significant was the theft of the crypto keys.

“[A]lthough firmware exploitation is nasty,” Snowden responded, “it’s at least theoretically reparable: tools could plausibly be created to detect the bad firmware hashes and re-flash good ones. This isn’t the same for SIMs, which are flashed at the factory and never touched again.”

Julian Sanchez of the Cato Institute shared Snowden’s sentiments about the crypto theft.

“We hear a great deal lately about the value of information sharing in cybersecurity,” he wrote in a blog post about the hack of Gemalto. “Well, here’s a case where NSA had information that the technology American citizens and companies rely on to protect their communications was not only vulnerable, but had in fact been compromised….[T]his is one more demonstration that proposals to require telecommunications providers and device manufacturers to build law enforcement backdoors in their products are a terrible, terrible idea. As security experts have rightly insisted all along, requiring companies to keep a repository of keys to unlock those backdoors makes the key repository itself a prime target for the most sophisticated attackers—like NSA and GCHQ.”