NSA Uses Private Companies For Spying, Whether Willing Or Unwilling

By Kelli Sladick

NSA insiders in major corporations in the US and abroad are aiding the agency in intercepting communications by degrading encryption and accessing parts of the supply chain.

Peter Maass and Laura Poitras reveal in the newest Intercept article, two NSA Programs, Sentry Eagle and TAREX, designed to subvert encryption.

Sentry Eagle

This program originating in 2004 is composed of six sub-programs designed to exploit computer networks and spying, computer network defense, cooperation with other intelligence agencies, break encryption systems, attacking computer networks, and collaborating with private companies. Private companies knowning and unknowningly are employing agents.
"The briefing document states that among Sentry Eagle's most closely guarded components are ?facts related to NSA personnel (under cover), operational meetings, specific operations, specific technology, specific locations and covert communications related to SIGINT enabling with specific commercial entities (A/B/C)...?(A/B/C)? is used in the briefing document to refer to American companies, though on one occasion it refers to both American and foreign companies. Foreign companies are referred to with the placeholder ?(M/N/O).??
Historically, many cryptologists from the military and other intel agencies move to the telecommunications industry after federal employment.
"There is a long history of overt NSA involvement with American companies, especially telecommunications and technology firms. Such firms often have employees with security clearances who openly communicate with intelligence agencies as part of their duties, so that the government receives information from the companies that it is legally entitled to receive, and so that the companies can be alerted to classified cyber threats. Often, such employees have previously worked at the NSA, FBI, or the military."
However, some companies do not want to aid in the surveillance of their customers. NSA deployed agents infiltrated the private industries who didn't want to forward customer communications, trade secrets, and encryption keys.
"But the briefing document suggests another category of employees?ones who are secretly working for the NSA without anyone else being aware. This kind of double game, in which the NSA works with and against its corporate partners, already characterizes some

of the agency's work, in which information or concessions that it desires are surreptitiously acquired if corporations will not voluntarily comply. The reference to ?under cover? agents jumped out at two security experts who reviewed the NSA documents for The Intercept."
Previously, it has been leaked that devices created by the NSA have been incorporated in foreign companies products to steel personal communications. TAREX
The briefing sheet's description of Sentry Owl indicates the NSA has previously unknown relationships with foreign companies. According to the document, the agency ?works with specific foreign partners (X/Y/Z) and foreign commercial industry entities? to make devices and products ?exploitable for SIGINT??a reference to signals intelligence, which is the heart of the NSA's effort to collect digital communications, such as emails, texts, photos, chats, and phone records. This language clarifies a vague reference to foreign companies that appears in the secret 2013 budget for the intelligence community, key parts of which were published last year from the Snowden archive.
TAREX

TAREX stands for Targeted Exploitation and falls under Sentry Eagle's sub program called Sentry Ospry that utilizes Human Intelligence (HUMINT) to infiltrate the supply chain side of the house.
"According to another NSA document, off-net operations are ?covert or clandestine field activities,? while supply-chain operations are ?interdiction activities that focus on modifying equipment in a target's supply chain.?

The NSA's involvement in supply-chain interdiction was previously revealed in No Place to Hide, written by Intercept co-founder Glenn Greenwald. The book included a photograph of intercepted packages being opened by NSA agents, and an accompanying NSA document explained the packages were ?redirected to a secret location? where the agents implanted surveillance beacons that secretly communicated with NSA computers. The document did not say how the packages were intercepted and did not suggest, as the new documents do, that interception and implants might be done by clandestine agents in the field."
Last year, corporation vehemently opposed the 4th Amendment Protection Act in several states. These programs may reveal the reason why. The efforts to subvert encryption, aid in surveillance, and to us devices as Trojan Horses to send personal communications must be ubiquitous if they fear state repercussions.

Corporations should embrace the 4th Amendment Protection Act rather than challenge it. Distrust among customers has huge financial consequences to corporations. Without the 4th Amendment Protection Act the NSA has corporate cooperation whether the corporation likes it or not.

Corporations will generally follow the lead of their customers, but when they operate in a vacuum, they pretty much do as they please. . Consumer pushback serves as a very effective tool in modifying corporate behavior. The CHOICE Act provides a powerful way to incentivize companies to stop working with the NSA and other agencies violating your privacy.

This piece of legislation forces companies to choose: do business with the NSA and support its rights violating operation, or refuse to provide such support and do business with the state.

Article Originally Appeared On OffNow.org

For more information on the CHOICE Act, click HERE.