ADN.com

adn.com Anchorage Daily News

Snowden used low-cost tool to best NSA

By DAVID E. SANGER and ERIC SCHMITT

The New York TimesFebruary 8, 2014

WASHINGTON -- Intelligence officials investigating how Edward J. Snowden gained access to a huge trove of the country's most highly classified documents say they have determined that he used inexpensive and widely available software to "scrape" the National Security Agency's networks, and he kept at it even after he was briefly challenged by agency officials.

Using "Web crawler" software designed to search, index and back up a website, Snowden "scraped data out of our systems" while he went about his day job, according to a senior intelligence official.

"We do not believe this was an individual sitting at a machine and downloading this much material in sequence," the official said. The process, he added, was "quite automated."

The NSA's mission includes protecting the nation's most sensitive military and intelligence computer systems from cyberattacks, especially the sophisticated attacks that emanate from Russia and China. Snowden's "insider attack," by contrast, was hardly sophisticated and should have been easily detected, investigators found.

Moreover, Snowden succeeded nearly three years after the WikiLeaks disclosures, in which military and State Department files, of far less sensitivity, were taken using similar techniques.

A Web crawler, also called a spider, automatically moves from website to website, following links embedded in each document and can be programmed to copy everything in its path.

From his first days working as a contractor inside the NSA's underground Hawaii facility for Dell, a computer maker, and then at a different Hawaiian location for Booz Allen Hamilton, a technology consulting firm that sells and operates computer security services used by the government, Snowden learned something critical about the NSA's culture: While the organization built enormously high electronic barriers to keep out foreign invaders, it had rudimentary protections against insiders.

"Once you are inside the assumption is that you are supposed to be there, like in most organizations," said Richard Bejtlich, the chief security strategist for FireEye, a Silicon Valley computer security firm, and a senior fellow at the Brookings Institution. "But that doesn't explain why they weren't more vigilant about excessive activity in the system."

Officials said the Web crawler functioned like Googlebot, a widely used Web crawler that Google developed to find and index new pages on the web. What officials cannot explain is why the presence of such software in a highly classified system was not an obvious tip-off to unauthorized activity.