NSA uses supercomputers to crack Web encryption, files show

Michael Winter, USA TODAY *10:44 p.m. EDT September 5, 2013*

Snowden documents reveal spy agency campaign to compromise online privacy for national security.

(Photo: Patrick Semansky, AP)

U.S. and British intelligence agencies have cracked the encryption designed to provide online privacy and security, documents leaked by former intelligence analyst Edward Snowden show.

In a clandestine, decade-long effort to defeat digital scrambling, the National Security Agency, along with its British counterpart, the Government Communications Headquarters (GCHQ), have used supercomputers to crack encryption codes through "brute force" and have inserted secret "back doors" into software with the help of technology companies, *The Guardian (http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security),The New York Times (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0)* and ProPublica (http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption) reported Thursday.

The NSA has also maintained control over international encryption standards.

As the *Times* points out, encryption "guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world."

The American Civil Liberties Union, which has filed a federal suit challenging the government's collection of telephone communications data, called the NSA's efforts to defeat encryption "recklessly shortsighted" and said they make the Internet less secure for all.

In a statement, the ACLU said the actions will "further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies."

"The encryption technologies that the NSA has exploited to enable its secret dragnet surveillance are the same technologies that protect our most sensitive information, including medical records, financial transactions and commercial secrets," said Christopher Soghoian, principal technologist of the ACLU's Speech, Privacy and Technology Project. "Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the Internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance."

The spy agencies have focused on compromising encryption found in Secure Sockets Layer (SSL), virtual private networks (VPNs) and 4G smartphones and tablets. The NSA spent $255 million this year on the decryption program — code named Bullrun (http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide) — which aims to "covertly influence" software designs and "insert vulnerabilities into commercial encryption systems" that would be known only to the agency.

The documents leaked by Snowden, who has been granted temporary asylum in Russia, do not name specific companies or encryption technologies, and refer to customers and users as "adversaries."

The NSA calls its decryption efforts the "price of admission for the U.S. to maintain unrestricted access to and use of cyberspace."

A 2010 memo describing an NSA briefing to British agents about the secret hacking said, "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies. Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."

The GCHQ is working to penetrate encrypted traffic on what it called the "big four" service providers — Google, Yahoo, Facebook and Microsoft's Hotmail.

One document shows that by 2012, the British agency had developed "new access opportunities" into Google's systems.

Most major tech companies did not immediately respond. In the past, they have said they cooperate with government agencies only as prescribed by law.

Google said in a statement: "We do not provide any government, including the U.S. government, with access to our systems. As for recent reports that the U.S. government has found ways to circumvent our security systems, we have no evidence of any such thing ever occurring. We provide user data to governments only in accordance with the law."

A spokesman for Microsoft, Dominic Carr, said Thursday night that "the company has significant concerns about the allegations of government activity reported today.'' He cited a previous Microsoft statement denying it provides "any government with the ability to break the encryption.''

The NSA says code-breaking is fundamental to its mission of protecting national security by deciphering communications from terrorists, spies or other U.S. adversaries.

During the 1990s, the agency fought unsuccessfully to have a secret government portal included in all encryption protocols.

Experts and critics say that while "back doors" may help intelligence gathering, they weaken the Web's overall security and trust, and could be used against Americans.

"The risk is that when you build a back door into systems, you're not the only one to exploit it," Matthew Green, a cryptography researcher at Johns Hopkins University, told the *Times*. "Those back doors could work against U.S. communications, too."

Bruce Schneier, a security technologist, examined the documents before they were published and authored an analysis for the *Guardian.* He told USA TODAY that they are the biggest revelations yet from the documents leaked by Snowden and said they show NSA has "subverted" much of the Internet and tech companies that form its backbone.

"They fundamentally undermine the social contract of the Internet — which is that you get what you think you get and it works,'' Schneier said. "An agency has subverted vast swaths of this to turn the Internet into a surveillance engine. Now the Internet doesn't do what people thought it did.''

"They've done it through secret agreements with companies, so essentially all the companies you deal with on the Internet have been lying to you. They have basically sucked the trust out of the Internet — the NSA and these companies. It's a public-private partnership to turn the internet into a surveillance engine.''

The Center for Democracy and Technology, a non-profit group that advocates for a free Internet, called the NSA efforts "a fundamental attack on the way the Internet works.''

"In an era which businesses as well as the average consumer trust secure networks and technologies for sensitive transactions and private communications online, it's incredibly destructive for the NSA to add flaws to such critical infrastructure," said Joseph Lorenzo Hall, CDT Senior Staff Technologist.

"The NSA seems to be operating on the fantastically naïve assumption that any vulnerabilities it builds into core Internet technologies can only be exploited by itself and its global partners. The NSA simply should not be building vulnerabilities into the fundamental tools that we all rely upon to protect our private information," Hall added.

The *Times* and ProPublica said intelligence officials asked them not to publish the article, arguing that the revelations "might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read."

After removing "some specific facts," they chose to publish "because of the value of a public debate about government actions that weaken the most powerful tools for protecting the privacy of Americans and others."

ProPublica published a separate article explaining its decision to publish:

> The story, we believe, is an important one. It shows that the expectations of millions of Internet users regarding the privacy of their electronic communications are mistaken. These expectations guide the practices of private individuals and businesses, most of them innocent of any wrongdoing. The potential for abuse of such extraordinary capabilities for surveillance, including for political purposes, is considerable. The government insists it has put in place checks and balances to limit misuses of this technology. But the question of whether they are effective is far from resolved and is an issue that can only be debated by the people and their elected representatives if the basic facts are revealed.

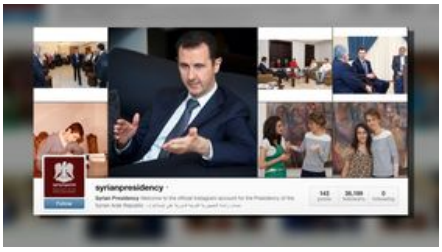
The non-profit news organization noted that "American history is replete with examples of the dangers of unchecked power operating in secret," specifically the President Nixon, who "tried to subvert law enforcement, intelligence and other agencies for political purposes, and was more than willing to violate laws in the process."

"Such a person could come to power again. We need a system that can withstand such challenges power the government possesses. Today's story is a step in that direction," ProPublica wrote.

Contributing: Alistair Barr in San Francisco; William M. Welch in Los Angeles

SHARE CONNECT (https://twitter.com/intent/tweet?url=http://www.usatoday.com/story/news/nation/ :56 ET 77272

USA NOW



See the Assads on Instagram | USA NOW video (/media/cinematic/video/27706 47/usa-the-assads-on-instagram-usa-now-video/)

Sep 05, 2013

UP NEXT

E-cigarette use doubles among U.S. teens

(/story/news/nation/2013/09/05/e-cigarette-use