Documents show NSA can crack most Web privacy encryption

Published: Sept. 6, 2013 at 3:00 AM

NEW YORK, Sept. 6 (UPI) --

NEW YORK, Sept. 6 (UPI) -- Web firm guarantees that criminals and Washington can't read encrypted emails, online banking and other data are not true, newly disclosed documents indicate.

Since 2000, the U.S. National Security Agency has secretly cracked and bypassed much of the digital scrambling hundreds of millions of people rely on to protect the privacy of sensitive data, including medical records, trade secrets, Web searches, Internet chats, and cell and land-line phone calls of Americans and others around the world, the top-secret documents revealed by former NSA contractor Edward Snowden show.

The agency, at a cost of more than $250 million in the current year's budget, employs custom-built, superfast computers to break codes with "brute force," uses covert measures to ensure NSA control over setting international encryption standards and, in the most closely guarded secret, collaborates with technology companies and Internet service providers in the process, said the documents published by The New York Times, the non-profit news organization ProPublica and a British newspaper, The Guardian.

In some cases, tech firms and ISPs said they were coerced into handing over their master encryption keys or building in hidden methods, known as "back doors," to bypass normal computer, cryptosystem and algorithm authentication systems, the Times and ProPublica said.

The documents do not identify which companies have been involved.

Similar activities have been going on with the NSA's British counterpart, the Government Communications Headquarters, or GCHQ, the documents state, indicating the British agency has been looking for ways into encrypted traffic of popular Internet companies Google Inc., Yahoo! Inc., Facebook Inc. and Microsoft Corp.'s Outlook.com, formerly known as Hotmail.

The NSA also hacks into target computers to grab messages before they're encrypted, said the news reports, based on more than 50,000 documents The Guardian shared with the Times and ProPublica.

Intelligence officials asked the news organizations not to publish their articles, saying publication might prompt foreign targets to switch to new encryption or communication forms that would be harder to collect or read.

The news outlets said in their reports they removed some facts but published the articles because they saw value in a public debate about government actions that weaken the most powerful tools for protecting the privacy of Web users in the United States and worldwide.

"For the past decade, NSA has led an aggressive, multi-pronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about NSA accomplishments by GCHQ.

"Vast amounts of encrypted Internet data, which have up till now been discarded, are now exploitable," the memo said.

Another memo said when GCHQ analysts, who often work alongside NSA officers, were shown a presentation about NSA progress, "Those not already briefed were gobsmacked!"

An intelligence budget document indicates the U.S. effort is still going strong.

"We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet

traffic," National Intelligence Director James Clapper wrote in his current-year budget request.

The NSA calls the secret decryption program by the code name Bullrun, taken from a major Civil War battle. Britain's counterpart program is code-named Edgehill, after the first major engagement of the English civil war, more than 200 years earlier.

NSA rules let the agency store any encrypted communication, domestic or foreign, for as long as the agency says it is trying to decrypt or analyze its technical features.

The NSA agency considers its deciphering of protected information one of its most closely guarded secrets, the documents provided by Snowden indicate.

The full extent of the decoding capabilities is known only to a select group of the most senior analysts from the NSA and its signals-intelligence counterparts in Britain, Canada, Australia and New Zealand, the Times and ProPublica said.

Those countries, whose intelligence operations are known as the Five Eyes, are part of a little-known alliance known as the United Kingdom-United States of America Agreement among the English-speaking countries.

Besides top analysts, a small cadre of trusted contractors was allowed to join Bullrun. Snowden does not appear to have been among them, the Times and ProPublica said, but he still managed to obtain dozens of classified documents referring to the program's capabilities, methods and sources.

Funding for Bullrun's Sigint Enabling Project is $254.9 million this year, dwarfing the $20 million budget of the NSA's previously leaked PRISM mass electronic surveillance data-mining program that gathered intelligence from various Internet companies.

Sigint stands for signals intelligence, the technical term for electronic eavesdropping.

Sigint "actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" to make them "exploitable," an intelligence budget document says.

Since 2011, the total spending on Sigint enabling has topped $800 million.