Clinton subject to hack attempts from China, Korea, Germany

By KEN DILANIAN, JACK GILLUM and STEPHEN BRAUN

Oct. 7, 2015 10:44 PM EDT

WASHINGTON (AP) — Hillary Rodham Clinton's private email server, which stored some 55,000 pages of emails from her time as secretary of state, was the subject of attempted cyberattacks originating in China, South Korea and Germany after she left office in early 2013, according to a congressional document obtained by The Associated Press.

While the attempts were apparently blocked by a "threat monitoring" product that Clinton's employees connected to her network in October 2013, there was a period of more than three months from June to October 2013 when that protection had not been installed, according to a letter from Sen. Ron Johnson, R-Wis., chairman of the Homeland Security and Government Affairs Committee. That means her server was possibly vulnerable to cyberattacks during that time.

Johnson's letter to Victor Nappe, CEO of SECNAP, the company that provided the threat monitoring product, seeks a host of documents relating to the company's work on Clinton's server and the nature of the cyber intrusions detected. Johnson's committee is investigating Clinton's email arrangement.

Clinton has not said what, if any, firewall or threat protection was used on her email server before June 2013, including the time she was secretary of state from 2009 to 2013 and the server was kept in her home in the New York City suburbs.

A February 2014 email from SECNAP reported that malicious software based in China "was found running an attack against" Clinton's server. In total, Senate investigators have found records describing three such attempts linked to China, one based in Germany and one originating in South Korea. The attacks occurred in 2013 and 2014. The letter describes four

attacks, but investigators have since found records about a fifth, officials who were not authorized to discuss the matter publicly said.

It was not immediately clear whether the attempted intrusions into Clinton's server were serious espionage threats or the sort of nuisance attacks that hit computer servers the world over. But the new revelations underscore the extent to which any private email server is a target, raising further questions about Clinton's decision to undertake sensitive government business over private email stored on a homemade system.

Any hackers who got access to her server in 2013 or 2014 could have stolen a trove of sensitive email traffic involving the foreign relations of the United States. Thousands of Clinton emails made public under the Freedom of Information Act have been heavily redacted for national security and other reasons.

Clinton "essentially circumvented millions of dollars' worth of cybersecurity investment that the federal government puts within the State Department," said Justin Harvey, chief security officer of Fidelis Cybersecurity.

"She wouldn't have had the infrastructure to detect or respond to cyber attacks from a nation-state," he said. "Those attacks are incredibly sophisticated, and very hard to detect and contain. And if you have a private server, it's very likely that you would be compromised."

A spokesman for the Clinton campaign did not answer detailed questions from The Associated Press about the cyber intrusions. Instead, spokesman Brian Fallon attacked Johnson by linking him to the House Benghazi committee inquiry, which the campaign dismissed in a recent media ad as politically motivated.

"Ron Johnson is ripping a page from the House Benghazi Committee's playbook and mounting his own, taxpayer-funded sham of an investigation with the sole purpose of attacking Hillary Clinton politically," campaign spokesman Fallon said by email. "The Justice Department is already conducting a review concerning the security of her server equipment, and Ron Johnson has no business interfering with it for his own partisan ends."

The FBI is investigating whether national security was compromised by Clinton's email arrangement.

In June 2013, after Clinton had left office, the server was moved from her Chappaqua, New York, home to a data center in northern New Jersey, where it was maintained by a Denver technology company, Platte River Networks, records show.

In June 2013, Johnson's letter says, Platte River hired SECNAP Network Security Corp. to use a product called CloudJacket SMB, which is designed to block network access by "even the most determined hackers," according to company literature. But the product was not up and running until October, according to Johnson's letter, raising questions about how vulnerable Clinton's server was during the interim.

SECNAP is not a well-known computer security provider. The company's website and promotional literature describe CloudJacket as a monitoring system designed to counter unauthorized intrusions and monitor threats around the clock. Corporate documents show SECNAP has been in existence since at least 2002, selling computer spam filter and firewall products.

A SECNAP representative declined to comment, citing company policy.

The AP reported last month that Russia-linked hackers sent Clinton emails in 2011 — when she was still secretary of state — loaded with malware that could have exposed her computer if she opened the attachments. It is not known if she did.

The attacks Johnson mentions in his letter are different, according to government officials familiar with them. They were probing Clinton's server directly, not through email.

http://bigstory.ap.org/article/5ad0f6bb57eb487f84e98fe9a74a08b1/clinton-subject-hack-attempts-china-korea-germany