Hackers used e-mail access to gov't computers

Worker opened rigged message in late May letting hackers in

http://www.msnbc.msn.com/id/18186800/

WASHINGTON - A break-in targeting State Department computers worldwide last summer occurred after a department employee in Asia opened a mysterious e-mail that quietly allowed hackers inside the U.S. government's network.

In the first public account revealing details about the intrusion and the government's hurried behind-the-scenes response, a senior State Department official described an elaborate ploy by sophisticated international hackers. They used a secret break-in technique that exploited a design flaw in Microsoft software.

Consumers using the same software remained vulnerable until months afterward.

Donald R. Reid, the senior security coordinator for the Bureau of Diplomatic Security, also confirmed that a limited amount of U.S. government data was stolen by the hackers until tripwires severed all the State Department's Internet connections throughout eastern Asia. The shut-off left U.S. government offices without Internet access in the tense weeks preceding missile tests by North Korea.

Reid was scheduled to testify Thursday at a cybersecurity hearing for a House Homeland Security subcommittee. He was expected to tell lawmakers an employee in the State Department's Bureau of East Asian and Pacific Affairs — which coordinates diplomacy in countries including China, the Koreas and Japan — opened a rigged e-mail message in late May giving hackers access to the government's network.

The chairman of the Homeland Security Committee, Rep. Bennie Thompson, D-Miss., said hackers are no longer considered harmless, bored teenagers. "These are experienced, sophisticated people who are trying to exploit our vulnerabilities and gain access to our information," Thompson said.

Reid was not expected to disclose the identities or nationalities of the hackers believed to be responsible for the break-ins or to disclose whether U.S. authorities believe a foreign government was responsible. The department struggled with the break-ins between May and early July.

The panel's chairman, Rep. James R. Langevin, D-R.I., called cybersecurity an often-overlooked line of defense. "Since much of our critical infrastructure is dependent on computers and networks and is interconnected and interdependent, a cyberattack could disrupt major services and cripple economic activity," Langevin said.

The mysterious State Department e-mail appeared to be legitimate and included a Microsoft Word document with material from a congressional speech related to Asian diplomacy, Reid said. By opening the document, the employee activated hidden software commands establishing what Reid described as backdoor communications with the hackers.

The technique exploited a previously unknown design flaw in Microsoft's Office software, Reid said. State Department officials worked with the Homeland Security Department and even the FBI to urge Microsoft to develop quickly a protective software patch, but the company did not offer the patch until Aug. 8 — roughly eight weeks after the break-in.

Microsoft said it works as quickly as possible to provide customers with security updates.

(MSNBC.com is a Microsoft-NBC Universal joint venture.)

"If we release a security update that is not adequately tested, we could potentially put customers at risk, especially as the release of an update can lead to reverse-engineering the fix and lead to broader attacks," said Microsoft's senior security strategist, Phil Reitinger. "Updates must be able to be deployed by customers with confidence."

At the time, Microsoft described the software flaw as "a newly discovered, privately reported vulnerability" but did not suggest any connection to the U.S. government break-in. It urged consumers to apply the update immediately. It also recommended that consumers not open or save Microsoft Office files they receive from sources they don't trust or files they receive unexpectedly from trusted sources.

The State Department detected its first break-in immediately, Reid said, and worked to block suspected communications with the hackers. But during its investigation, it discovered new break-ins at its Washington headquarters and other offices in eastern Asia, Reid said.