

Cyberattack in 2008 prompted NEW Pentagon Cyberdefense Plan



Infected flash drive in laptop infiltrated Defense Department systems

Washington (CNN) -- An infected flash drive put in a U.S. military laptop in 2008 set off the most significant cyberattack ever against the military and brought a turning point in cyberdefense strategy, a top defense official wrote in an article published Wednesday.

Deputy Defense Secretary William J. Lynn III, in an article titled "Defending a New Domain" posted on Foreign Affairs magazine's web site, said the "previously classified incident was the most significant breach of U.S. military computers ever."

According to Lynn, the attack served as "an important wake-up call" that led to a new Pentagon counterattack strategy dubbed Operation Buckshot. "An enormous amount of foundational work remains, but the U.S. government has begun putting in place various initiatives to defend the United States in the digital age," Lynn's article said.

The attack started with the infected laptop at a U.S. base in the Middle East, according to Lynn.

"The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command," his article said. "That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control."

He continued: "It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."

Lynn's article provided no details on specific files lost or stolen in the attack, which he called one of countless attempts to intrude into U.S. military networks. Others also have succeeded, he said, with adversaries acquiring "thousands of files from U.S. networks and from the networks of U.S. allies and industry partners, including weapons blueprints, operational plans, and surveillance data."

In response, he wrote, the Pentagon has built layered defenses around military networks and launched the new U.S. Cyber Command to "integrate cyberdefense operations across the military." "The Pentagon is now working with the Department of Homeland Security to protect government networks and critical infrastructure and with the United States' closest allies to expand these defenses internationally," Lynn wrote.