TIME
NATION

Thursday, Aug. 25, 2005

Inside the Chinese Hack Attack

How a ring of hackers, codenamed Titan Rain by investigators, probed U.S. government computers

By NATHAN THORNBURGH

Hackers breaking into official U.S. networks are not just using Chinese systems as a launch pad, but are based in China, sources tell TIME. Their story: Sometime on November 1st, 2004, hackers sat down at computers in southern China and set off once again on their daily hunt for U.S. secrets. Since 2003 the group had been conducting wide-ranging assaults on U.S. government targets to steal sensitive information, part of a massive cyberespionage ring that U.S. investigators have codenamed Titan Rain. On this particular night, the hackers' quarry was military data, and they were armed with a new weapon to reach out across cyberspace and get it.

This was a scanner program that "primed the pump," according to a former government network analyst who has helped track Titan Rain, by searching vast military networks for single computers with vulnerabilities that the attackers could exploit later. As with many of their tools, this was a simple program, but one that had been cleverly modified to fit their needs, and then used with ruthless efficiency against a vast array of U.S. networks. After performing the scans, the source says, it's a virtual certainty that the attackers returned within a day or two and, as they had on dozens of military networks, broke into the computers to steal away as much data as possible without being detected.

They hit hundreds of computers that night and morning alone, and a brief list of scanned systems gives an indication of the breadth of the attacks. At 10:23 p.m. pacific standard time (PST), they found vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona. At 1:19 am PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia. At 3:25 am, they hit the Naval Ocean Systems Center, a defense department installation in San Diego, California. At 4:46 am PST, they struck the United States Army Space and Strategic Defense installation in Huntsville, Alabama. As with prior attacks, the targeted networks were unclassified systems; the military's classified networks are not connected directly to the Internet. But even unclassified systems store sensitive information and provide logistics support throughout the armed forces. Government analysts say the attacks are ongoing, and increasing in frequency. But whether the Titan Rain hackers are gathering industrial information or simply testing their ability to infiltrate a rival nation's military systems, the U.S. government is taking the threat very seriously.

In next week's magazine, available at Time.com on Sunday and on the newsstands Monday, TIME presents the Titan Rain investigation in depth — what they stole, how they stole it, and what the United States is doing to stop them.