

12 May 2008

By: Bogdan Botezatu, Hardware Editor

CISCO SYSTEMS



The fake hardware gear could allow unauthorized users access to critical information Cisco

## FBI's Own Offices "Infected" with Counterfeit Cisco Hardware

*The investigation unveiled 3500 fake network devices*

The United States government is reportedly using no less than 3500 fake Cisco-branded network devices, including routers, network switches and hubs. According to the investigation results, the fake devices are worth up to \$3.5 million. The FBI has been keeping an eye on the China imports of networking gear for some time now, as part of a large criminal probe, code-named Operation Cisco Raider. The counterfeit network gear is not only less stable and weaker as compared to Cisco's state-of-the-art corporate equipment, but it also poses a security risk for the government branches "infected" with fake gear. For instance, FBI believes that the [fake Cisco gear](#) could allow remote hackers to intercept ("sniff") network traffic to and from FBI's offices, as well as grant unauthorized persons access to secure government databases. According to FBI officials, the investigations took place at nine field offices operated by the agency itself and involved the execution of 39 search warrants. However, internal sources with FBI claimed that no security breaches have been discovered until now. The counterfeit networking gear includes Cisco Systems routers as well as switches, interface converters and wide area network (WAN) interface cards. FBI is not the only government agency affected by counterfeit gear. According to a report, fake Cisco gear also arrived at defense contractors and other private-sector buyers that refused to disclose the implications of using pirated hardware components. The FBI has started its investigation earlier this year and a leaked Power-Point presentation confirmed that the fake gear had already reached agency offices in Massachusetts, Ohio, Missouri, Minnesota, Oklahoma, Texas, Colorado and California. "This unclassified briefing was never intended for broad distribution or posting to the internet", said James Finch, assistant director of the FBI's Cyber Division. The agency claims that their investigation was completed and that they have seized all the forged equipment. However, there is no word on what happened to the perpetrators.