



CHESLEY BROWN  
INTERNATIONAL

# E-Briefs

A Biweekly Security Communiqué

Volume 7, Issue 9 April 28, 2009

## NEWS BRIEFS

### Computer Spies Breach Fighter-Jet Project

Several current and former government officials have revealed that cyber spies have repeatedly broken into the Pentagon's \$300 billion Joint Strike Fighter project, a plane that is being built by several of the nation's defense contractors. According to the officials, the cyber spies were able to take advantage of vulnerabilities in the networks of two or three of those contractors beginning in 2007 to compromise the system that is responsible for diagnosing the plane's maintenance problems during flight. The officials added that the breaches, which lasted at least into 2008, seemed to be an attempt to steal data about the design of the plane, its performance statistics, and its electronic systems. However, the breaches did not result in the compromise of the plane's most vital systems, such as flight controls and sensors, because those systems are physically isolated from the Internet. Nevertheless, some are concerned that the theft of the data could make it easier for whoever has the information to build planes that can defend against the craft. Investigators believe the attack originated from a Chinese IP address, though the attackers may have actually been located somewhere else since it is easy to mask identities online. Chinese officials have denied any involvement in the attack, and say that any allegations of cyber espionage are "intentionally fabricated to fan up China threat sensations."

### False Security: 'Scareware' Spreads

Computer experts report a surge in fraudulent antivirus programs. Incidents of scareware infections, as the rogue antivirus software is known, rose 48 percent in the second half of 2008, according to a new report by Microsoft Corp. The Anti-Phishing Working Group said the number of scareware programs rose three-fold from July to December 2008. Dave Marcus, director of security research and communications at McAfee Inc.'s McAfee Avert Labs, expects those figures to increase this year because they are so lucrative. Scareware infiltrates computers when a user visiting legitimate Web sites is redirected to unrelated sites that offer to sell antivirus software. The scam begins when a phony scan of the user's computer identifies a malware infection and the user is instructed to download antivirus software to correct the problem for a fee of about \$50. A user's Web browser and operating system are also subject to infection if they are not secure and up-to-date

### Classified Data on Marine One Leaked, Found on Iranian Computer

The Cranberry Township, Pa.-based peer-to-peer monitoring services provider Tiversa has discovered classified information about Marine One on a computer in Tehran. According to Tiversa Chief Operating Officer Chris Gormley, the information was stored in a publicly-available shared folder on a computer with an IP address belonging to an Iranian "information concentrator," which is someone who searches peer-to-peer networks for sensitive information. Tiversa said that the information--which includes data about the communications, navigation, and management electronics on Marine One--appears to have been leaked from a computer belonging to a Bethesda, Md.-based defense contractor sometime last summer. Although the leak took place nearly a year ago, the information is still available on peer-to-peer networks to anyone who knows how to look for it, Gormley said. He added that a recent search conducted by Tiversa also found that other documents with classified and sensitive military information had been leaked over peer-to-peer networks. Gormley refused to disclose what those other documents were.

## NEWS YOU CAN USE

### U.S. Weighs Changes in Strategy to Fight Pirates

U.S. military officials are considering a change in policy to encourage more commando raids as a way to reduce piracy off the coast of Somalia, in the Gulf of Aden. Rules of engagement usually prohibit dramatic hostage rescues, but some Pentagon officials say that a combination of special operations forces and conventional Navy assets could identify pirate gangs on land and then attack them in the water. The warships that have patrolled the Gulf since October are currently operating under United Nations resolution 1816, which authorizes "all necessary means" to detect piracy. Particular action is subject to interpretation by different nations, however, and sporadic, informal communications make it difficult for them to coordinate. While all nations generally believe it is appropriate to fire on pirate vessels to prevent them from hijacking merchant ships, most are unwilling to engage pirates once they have taken a ship. In the case of a hostage standoff, most U.S. military officials believe that navies could wear down pirates' wills, as ship hijackers are not driven by ideology and have limited resources. EU officials say that the United States would find few allies if it tried to coordinate commando operations for hijacked ships, as such action could result in "bloodbaths," according to one official. Analysts and shipping officials are concerned that loosening the rules of engagement when dealing with pirates would increase the risk of accidentally killing civilians and jeopardize the safety of crew members.

## ALERTS



CHESLEY BROWN  
INTERNATIONAL

### Security Condition SecCon 3



[Click Here for More Information](#)



If you have any feedback, or if you feel that you have received this in error, please e-mail [michaeltaylor@chesleybrown.com](mailto:michaeltaylor@chesleybrown.com) or call (770) 436-3097

Visit our website at <http://www.chesleybrown.com>