PHYS.ORG

Lockheed attack highlights rise in cyber espionage

May 30 2011, By CHIP CUTTER and LOLITA C. BALDOR , Associated Press

In this April 9, 2009 file photo, a sign outside the Lockheed Martin plant in Marietta, Ga. is shown. Lockheed Martin on Saturday, May 28, 2011 admitted it was the recent target of a "significant and tenacious" cyber attack, although the defense contractor and the Department of Homeland Security insist the hack was thwarted before any critical data was stolen. (AP Photo/John Amis, File)

This cyber attack didn't go after people playing war games on their PlayStations. It targeted a company that helps the U.S. military do the real thing.

Lockheed Martin says it was the recent target of a "significant and tenacious" hack, although the defense contractor and the Department of Homeland Security insist the attack was thwarted before any critical data was stolen. The effort highlighted the fact that some hackers, including many working for foreign governments, set their sights on information that has the potential to be far more devastating than accessing credit cards.

Information security experts say a rash of cyber attacks this year - including a massive security breach at Sony Corp. last month that affected millions of PlayStation users - has emboldened hackers and made them more willing to pursue sensitive information.

"2011 has really lit up the boards in terms of data breaches," said Josh Shaul, chief technology officer at Application Security, a New York-based company that is one of the largest database security software makers. "The list of targets just grows and grows."

Lockheed Martin Corp. said in a statement Saturday that it detected the May 21 attack "almost immediately" and took countermeasures.

"Our systems remain secure; no customer, program or employee personal data has been compromised," the Bethesda, Md.-based company said. Neither Lockheed Martin nor federal agencies would reveal specifics of the attack, or its origins. Company spokeswoman Jennifer Whitlow declined to comment further on the case Sunday.

This isn't the first time Lockheed Martin has been targeted. Nearly four years ago, officials revealed that hackers had breached Lockheed's Joint Strike Fighter program. Officials said no classified information about the military program was compromised, but heightened protections were added.

Analysts said the latest attack would likely spur rival defense contractors like Northrop Grumman Corp., Raytheon Co., General Dynamics Corp. and Boeing Co. to take additional steps to safeguard their systems.

"I guarantee you every major defense contractor is on double alert this weekend, watching what's going on and making sure they're not the next to fall victim," Shaul said.

Boeing declined to comment on the company's network security measures. Northrop Grumman spokesman Randy Belote said in an e-mailed statement that "we do not comment on whether or not Northrop Grumman is or has been a target for cyber intrusions," adding that the company "continuously monitors and proactively strengthens the security of our networks."

Over the past several years, the U.S. government has become more aggressive in its efforts to tackle cybercrime, developing strategies to beef up government computer systems, expand cooperation with other countries and improve coordination with the private sector. President Barack Obama declared cybersecurity a top priority shortly after taking office in 2009, setting off several government-wide reviews to develop strategies to better secure government, business and public online activity.

The Pentagon last May set up a new Cyber Command, based alongside the National Security Agency at Fort Meade, Md., in recognition of the expanding threat against the Defense Department and the need to better coordinate the nation's offensive and defensive cyber operations. The Department of Homeland Security is also slowly employing an automated system - known as Einstein 2 and Einstein 3 - to protect government agencies' computer systems.

Still, the attacks have continued. William J. Lynn III, the deputy defense secretary, said in January that more than 100 foreign intelligence agencies have tried to breach U.S. defense computer networks, largely to steal military plans and weapons systems designs.

China is often pointed to as a source of cyber attacks because a large amount of malware, or malicious software, originates from there. The government denies it is involved but experts say the high skill level of some attacks suggests the Chinese military, a leader in cyberwarfare research, or other agencies might be stealing technology and trade secrets to help state companies.

Meanwhile, attacks against corporations have been growing this year. In March, RSA, the security division of data storage company EMC, acknowledged that its computer network was hacked. The implications are serious because RSA's technology underpins the security of some of the world's most closely guarded data. RSA makes small security devices that supply constantly changing numbers that are used as secondary passwords for accessing corporate networks and email.

Last month, more than 100 million online accounts were affected by the hacking of Sony's PlayStation Network gaming service and other online services.

Companies have gotten better at detecting attacks through so-called "intrusion software" that uncovers odd behavior on networks, said Alfred Huger, vice president of development at security firm Sourcefire. As recently as five years ago, Huger said, it was difficult for companies to even determine if they were being hacked.

Even with enhanced technology to fight cyber espionage, experts say it will continue and evolve.

Rich Mogull, analyst and CEO of Phoenix-based security research firm Securosis, noted that governments and defense agencies have been spying on each other throughout history. Computers have just made it easier to do so electronically.

"This is just what countries do," he said. "It's the unfortunate reality of how the world works."

Citation: Lockheed attack highlights rise in cyber espionage (2011, May 30) retrieved 19 April 2024 from https://phys.org/news/2011-05-lockheed-highlights-cyber-espionage.html