

Broad New Hacking Attack Detected

Global Offensive Snagged Corporate, Personal Data at nearly 2,500 Companies; Operation Is Still Running

By SIOBHAN GORMAN

Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft, according to a computer-security company that discovered the breach.

The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property.

The hacking operation, the latest of several major hacks that have raised alarms for companies and government officials, is still running and it isn't clear to what extent it has been contained, NetWitness said. Also unclear is the full amount of data stolen and how it was used. Two companies that were infiltrated, pharmaceutical giant [Merck & Co.](#) and [Cardinal Health Inc.](#), said they had isolated and contained the problem.

Starting in late 2008, hackers operating a command center in Germany got into corporate networks by enticing employees to click on contaminated Web sites, email attachments or ads purporting to clean up viruses, NetWitness found.

In more than 100 cases, the hackers gained access to corporate servers that store large quantities of business data, such as company files, databases and email.

They also broke into computers at 10 U.S. government agencies. In one case, they obtained the user name and password of a soldier's military email account, NetWitness found. A Pentagon spokesman said the military didn't comment on specific threats or intrusions.

At one company, the hackers gained access to a corporate server used for processing online credit-card payments. At others, stolen passwords provided access to computers used to store and swap proprietary corporate documents, presentations, contracts and even upcoming versions of software products, NetWitness said.

Data stolen from another U.S. company pointed to an employee's apparent involvement in criminal activities; authorities have been called in to investigate, NetWitness said. Criminal groups have used such information to extort sensitive information from employees in the past.

The spyware used in this attack allows hackers to control computers remotely, said Amit Yoran, chief executive of NetWitness. NetWitness engineer Alex Cox said he uncovered the scheme Jan. 26 while installing technology for a large corporation to hunt for cyberattacks.

That discovery points to the growing number of attacks in recent years that have drafted computers into cyber armies

known as botnets—intrusions not blocked by standard antivirus software. Researchers estimate millions of computers are conscripted into these armies.

"It highlights the weaknesses in cyber security right now," said Adam Meyers, a senior engineer at government contractor SRA International Inc. who reviewed the NetWitness data. "If you're a Fortune 500 company or a government agency or a home DSL user, you could be successfully victimized."

Disclosure of the attack comes on the heels of [Google Inc.](#)'s allegation that it and more than 20 other companies were breached by Chinese hackers. This operation appears to be more far-reaching, infiltrating some 75,000 computers and touching 196 countries. The highest concentrations of infected computers are in Egypt, Mexico, Saudi Arabia, Turkey and the U.S.

NetWitness, based in Herndon, Va., said it was sharing information with the companies infected. Mr. Yoran declined to name them. The company provides computer security for U.S. government agencies and companies. Mr. Yoran is a former Air Force officer who also served as cyber security chief at the Department of Homeland Security.

Besides Merck and Cardinal Health, people familiar with the attack named several other companies infiltrated, including Paramount Pictures and software company [Juniper Networks Inc.](#)

Merck said in a statement that one computer had been infected. It said it had isolated the attack and that "no sensitive information was compromised."

Cardinal said it removed the infected computer from its network. Paramount declined to comment. Juniper's security chief, Barry Greene, wouldn't speak about any specific incidents but said the company worked aggressively to counter infections.

NetWitness, which does extensive work for the U.S. government and private-sector clients, said it was sharing its information with the Federal Bureau of Investigation. The FBI said it received numerous allegations about potential compromises of network systems and responded promptly, in coordination with law-enforcement partners.

The computers were infected with spyware called ZeuS, which is available free on the Internet in its basic form. It works with the Firefox browser, according to computer-security firm SecureWorks. This version included a \$2,000 feature that works with Firefox, according to SecureWorks.

Evidence suggests an Eastern European criminal group is behind the operation, likely using some computers in China because it's easier to operate there without being caught, said NetWitness's Mr. Yoran.

There are some electronic fingerprints suggesting the same group was behind a recent effort to dupe government officials and others into downloading spyware via emails purporting to be from the National Security Agency and the U.S. military, NetWitness's Mr. Yoran said.

That attack was described in a Feb. 5 report from the Department of Homeland Security, which said it was issuing an alert to the government and other organizations to "prevent further compromises."

A DHS official said that ZeuS was among the top five reported tools for malware infections.

Write to Siobhan Gorman at siobhan.gorman@wsj.com