



THURSDAY, AUGUST 4, 2011

Exploits by hackers get more sophisticated

Persistent crooks have gained access to at least 72 companies

By Byron Acohido
USA TODAY

LAS VEGAS — Fresh evidence that the Internet has become saturated with hacking groups relentlessly striving to crack into company networks grabbed attention as the Black Hat cybersecurity conference got underway here Wednesday.

Anti-virus giant McAfee revealed how a single hacking group, dubbed Shady Rat, has infiltrated at least 72 companies and governments over the past five years, including some 49 victim organizations in the U.S.

And Dell SecureWorks senior researcher Joe Stewart presented results of his analysis of nearly 1,000 corrupted servers. Stewart isolated 18 servers actively being used to relay information to and from infiltrated PCs inside company networks to command servers in two regions of China.

Security analysts and researchers at the conference say that's the tip of the iceberg. Nation-state spies and cybergangs "are trying to get at sensitive intellectual property and government information every hour and every minute of the day," says Andy Grolnick, chief executive of tech systems-monitoring company LogRhythm.

The majority of hacks fail, but "sophistication is increasing, and some are getting through," says Grolnick. "There's value in the data they're trying to get at."

McAfee has been aware of Shady Rat's activities since 2009. Then, last March, Dmitri Alperovitch, McAfee's vice president of threat research, located a server storing a list of successfully infiltrated organizations.

Some 49 of the 72 hacked companies were in the United States, four in Canada and the rest sprinkled through Europe and Asia.

The hackers most likely targeted a specific employee to receive an e-mail carrying an infected Web link or attachment, then tricked the employee into activating the infected link or file, McAfee says.

McAfee declined to name any of the 72 organizations that were infiltrated. The shortest time the hackers remained inside a company's network was less than a month; the longest, 28 months.

Stewart's research zoomed in on two hacking groups going after intellectual property.

"The final destination for all the activity we're seeing is a couple of hubs in China," says Stewart. "It tells us that somebody has invested specific resources to control this operation."