IT WORLD
AN OPEN EXCHANGE

Print Close Window

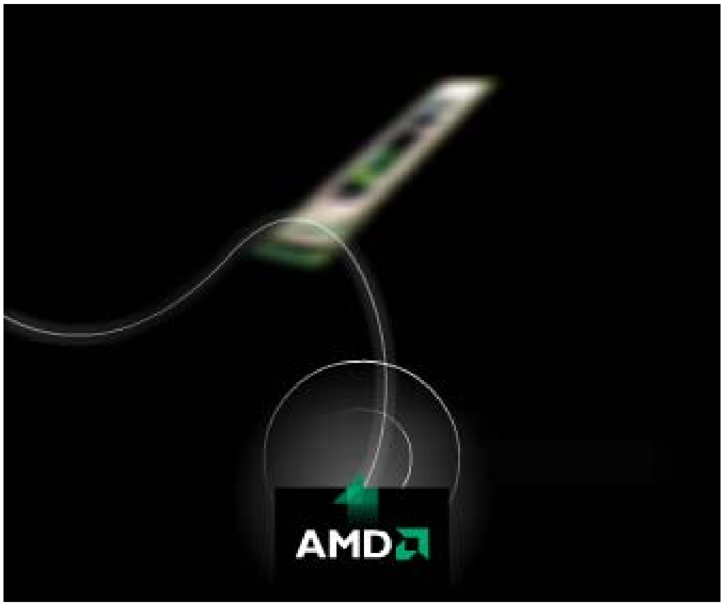
From: www.itworld.com

Researcher finds evidence of massive site compromise

by Gregg Keizer

October 3, 2008 —Several criminal gangs have acquired administrative log-in credentials for more than 200,000 Web sites -- including the one used by the U.S. Postal Service -- and have used the compromised domains to attack unsuspecting users' PCs with a notorious hacker exploit kit, a researcher said today.

More than a month ago Ian Amit, director of security research at Aladdin Knowledge Systems Inc., found and infiltrated a server belonging to a long-time customer of Neosploit, a hacker toolkit used by cybercriminals to launch exploits against browsers and popular Web software such as Apple Inc.'s QuickTime or Adobe Systems Inc.'s Adobe Reader.



On that server, Amit uncovered logs showing that two or three hacker gangs had contributed to a massive pool of Web site usernames and passwords. "We have counted more than 208,000 unique site credentials on the server," said Amit, "and over 80,000 had been modified with malicious content."

The site credentials were not the end, but only the means. The 80,000 modified sites were used as attack launch pads: Each served up exploit code provided by the Neosploit kit to any visitor running a Windows system that had not been fully patched.

By examining the server logs, Amit was able to identify the sites whose log-ins had been compromised. He is now working with law enforcement agencies in both the U.S. and overseas, as well as with organizations like US-CERT , to tell site operators they need to change their administrative passwords, purge the malicious code and secure their sites.
The only compromised site he would name was the U.S. Postal Service's at www.usps.gov . That site, and others, have been cleaned of the code that calls Neosploit down on unsuspecting visitors. Also on the list were sites for governments and Fortune 500 companies, universities, and other businesses, including several unnamed weapons manufacturers. More than half the affected sites belong to European companies and organizations.

Other evidence that Amit gathered ranged from the way the criminals processed the site log-ins to the number of IP addresses authorized to access the credentials.

"The server-based application that validated the credentials and then modified the sites was completely automated," said Amit. "Access to that application was restricted to about six or seven IP addresses, [so] it's clear that that access was intended only for the use of the criminals using the server." Based on the number of IP addresses and their distribution, he estimated that two or three separate groups were involved.

More than half of the site credentials -- approximately 107,000 -- had been validated by the cybercrooks' custom application as providing administrative access to the sites.

The groups apparently pooled resources, with site log-in information contributed by multiple users. Amit was not, however, able to determine how the criminals came to the site credentials in the first place. It's possible, he said, that the log-ins were purchased from others, or harvested by a botnet dedicated to the job.

But even with such clues, Amit isn't confident that authorities might be able to identify the hackers: "As much as I'd like to optimistic, I'm not fooling myself. They're using a software-as-a-service model, and it will be hard to track down all of them." However, he acknowledged that authorities had "a few solid leads" on who's responsible for the server, which may lead to the hackers. The server, for instance, was relocated since last week from Argentina, and is now being hosted in the U.S.

"We've exposed the back-end infrastructure of the organization," Amit said. "We've been chasing bugs for a couple of decades now and we need a different approach. That's what we have here. Now we know more about their M.O. and their business model.

"I hope that this will help both law enforcement and security researchers stay ahead of the game," he said.

Computerworld