More than 75K commercial computer systems hacked in large cyber attack

by Ellen Nakashima via Kismo - Washington Post *Thursday, Feb 18 2010, 5:29pm*
international / mass media / other press

> More than 75,000 computer systems at nearly 2,500 companies in the United States and around the world have been hacked in what appears to be one of the largest and most sophisticated attacks by cyber criminals discovered to date, according to a northern Virginia security firm.

The attack, which began in late 2008 and was discovered last month, targeted proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries in 196 countries, according to Herndon-based NetWitness.

News of the attack follows reports last month that the computer networks at Google and more than 30 other large financial, energy, defense, technology and media firms had been compromised. Google said the attack on its system originated in China.

This latest attack does not appear to be linked to the Google intrusion, said Amit Yoran, NetWitness's chief executive. But it is significant, he said, in its scale and in its apparent demonstration that the criminal groups' sophistication in cyberattacks is approaching that of nation states such as China and Russia.

The attack also highlights the inability of the private sector -- including industries that would be expected to employ the most sophisticated cyber defenses -- to protect itself.

"The traditional security approaches of intrusion-detection systems and anti-virus software are by definition inadequate for these types of sophisticated threats," Yoran said. "The things that we -- industry -- have been doing for the past 20 years are ineffective with attacks like this. That's the story."

The intrusion, first reported on the Wall Street Journal's Web site, was detected Jan. 26 by NetWitness engineer Alex Cox. He discovered the intrusion, dubbed the Kneber bot, being run by a ring based in Eastern Europe operating through at least 20 command and control servers worldwide.

The hackers lured unsuspecting employees at targeted firms to download infected software from sites controlled by the hackers, or baited them into opening e-mails containing the infected attachments, Yoran said. The malicious software, or "bots," enabled the attackers to commandeer users' computers, scrape them for log-in credentials and passwords -- including to online banking and social networking sites -- and then exploit that data to hack into the systems of other users, Yoran said. The number of penetrated systems grew exponentially, he said.

"Because they're using multiple bots and very sophisticated command and control methods, once they're in the system, even if you whack the command and control servers, it's difficult to rid them of the ability to control the users' computers," Yoran said.

The malware had the ability to target any information the attackers wanted, including file-sharing sites for sensitive corporate documents, according to NetWitness.

Login credentials have monetary value in the criminal underground, experts said. A damage assessment for the firms is underway, Yoran said. NetWitness has been working with firms to help them mitigate the damage.

Among the companies hit were Cardinal Health, located in Dublin, Ohio, and Merck, according to the Wall Street Journal. A spokesman for Cardinal said the firm removed the infected computers as soon as the breach was found.

Also affected were educational institutions, energy firms, financial companies and Internet service providers. Ten government agencies were penetrated, none in the national security area, NetWitness said.

The systems penetrated were mostly in the United States, Saudi Arabia, Egypt, Turkey and Mexico, the firm said.

Staff researcher Madonna Lebling contributed to this report.

http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html

---