Spain: mastermind of 'botnet' scam a mystery

DANIEL WOOLLS - Associated Press Writer - Associated Press

Spanish authorities who dismantled a network of up to 12.7 million virus-infected, data-stealing computers said Wednesday the mastermind of the scam remains a mystery, even though three alleged ringleaders have been arrested.

The "botnet" of infected computers included PCs inside more than half of the Fortune 1,000 companies and more than 40 major banks, police said. The tainted computers stole credit card numbers and online banking credentials.

Spanish investigators, working with private computer-security firms, arrested three young Spaniards last month as the alleged ringleaders of the so-called Mariposa botnet, which appeared in December 2008 and grew into one of the biggest weapons of cybercrime.

Spanish authorities are on the trail of a fourth suspect who might be Venezuelan, said Juan Salon of the Spanish Civil Guard's cybercrime unit.

But the people in custody did not design the malicious software behind the grid; rather they just bought it on the black market, Salon told a news conference called to detail the smashing of the network.

"We have not arrested the creator of the botnet. We have arrested the administrators of the botnet, the ones who spread it and were administering and controlling it," Salon said.

He declined to say how much money might have been plundered or name companies whose computers had been compromised.

Botnets are networks of infected PCs that have been hijacked from their owners, often without their knowledge, and put into the control of criminals. Linked together, the machines supply an enormous amount of computing power to spammers, identity thieves and Internet attackers.

There are an estimated 4,000 to 6,000 operating today and this one was the biggest one ever brought down, said Jose Antonio Berrocal, head of the Civil Guard's economic and technological crimes unit.

The Mariposa botnet spread to more than 190 countries, according to researchers. It also appears to be far more sophisticated than the botnet that was used to hack into Google Inc. and other companies in the attack that led Google to threaten to pull out of China.

AP correspondent Jordan Robertson contributed to this report from San Francisco, California.

Source URL (retrieved on *03/10/2014 - 12:34pm*):
http://www.ecnmag.com/news/2010/03/spain-mastermind-botnet-scam-mystery