

Authorities bust 3 in infection of 13M computers

JORDAN ROBERTSON - AP Technology Writer - Associated Press

Authorities have smashed one of the world's biggest networks of virus-infected computers, a data vacuum that stole credit cards and online banking credentials from as many as 12.7 million poisoned PCs.

The "botnet" of infected computers included PCs inside more than half of the Fortune 1,000 companies and more than 40 major banks, according to investigators.

Spanish investigators, working with private computer-security firms, have arrested the three alleged ringleaders of the so-called Mariposa botnet, which appeared in December 2008 and grew into one of the biggest weapons of cybercrime. More arrests are expected soon in other countries.

Spanish authorities have planned a news conference for Wednesday in Madrid.

The arrests are significant because the masterminds behind the biggest botnets aren't often taken down. And the story of investigators' hunt for them offers a rare glimpse at the tactics used to trace the origin of computer crimes.

Also, the suspects go against the stereotype of genius programmers often associated with cyber crime. The suspects weren't brilliant hackers but had underworld contacts who helped them build and operate the botnet, Cesar Lorenza, a captain with Spain's Guardia Civil, which is investigating the case, told The Associated Press.

Investigators were examining bank records and seized computers to determine how much money the criminals made.

"They're not like these people from the Russian mafia or Eastern European mafia who like to have sports cars and good watches and good suits — the most frightening thing is they are normal people who are earning a lot of money with cybercrime," Lorenza said.

The three suspects were described as Spanish citizens with no criminal records. They weren't named and their mug shots weren't released, which Lorenza said is standard in Spain to protect the privacy of defendants. They face up to six years in prison if convicted of hacking charges.

Authorities identified them by their Internet handles and their ages: "netkairo," 31; "jonyloleante," 30; and "ostiator," 25.

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

Authorities bust 3 in infection of 13M computers

Published on Electronic Component News (<http://www.ecnmag.com>)

together, the machines supply an enormous amount of computing power to spammers, identity thieves, and Internet attackers.

The Mariposa botnet, which has been dismantled, was easily one of the world's biggest. It 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.

The researchers that helped take down Mariposa first started looking at it in the spring of 2009.

Chris Davis, CEO of Ottawa-based Defence Intelligence, said he noticed the infections when they appeared on networks of some of his firm's clients, including pharmaceutical companies and banks.

It wasn't until several months later that he realized the infections were part of something much bigger.

After seeing that some of the servers used to control computers in the botnet were located in Spain, Davis and researchers from the Georgia Tech Information Security Center joined with software firm Panda Security, which is headquartered in Bilbao, Spain.

The investigators caught a few lucky breaks. For one, the suspects used Internet services that wound up cooperating with investigators. That isn't always the case.

Critically, one suspect also made direct connections from his own computer to try and reclaim control of his botnet after authorities took it down around Christmas. Investigators were able to identify him based on that traffic. They were able to back up their claims with records from domains he registered where he would eventually host malicious content.

It turned out that the botnet runners had infected computers by instant-messaging malicious links to contacts on infected computers. They also got viruses onto removable thumb drives and through peer-to-peer networks. The program used to create the botnet was known as Mariposa, from the Spanish word for "butterfly."

"I don't think there's anything about this guy that makes him smarter than any of the other botnet guys, but the (Mariposa) software, it's very professional, it's very effective," said Pedro Bustamante, senior research adviser with Panda Security. "It came alive and started spreading and it got bigger than him."

While arrests of people accused of running smaller botnets are fairly common, the biggest botnet leaders are rarely nabbed. That's partly because it's easy for criminals to hide their identities by disguising the source of their Internet traffic. Often, every computing resource they use is stolen.

For instance, there have been no busts yet in the spread of the Conficker worm,

Authorities bust 3 in infection of 13M computers

Published on Electronic Component News (<http://www.ecnmag.com>)

which infected 3 million to 12 million PCs running Microsoft Corp.'s Windows operating system and caused widespread fear that it could be used as a kind of Internet super weapon. The Conficker botnet is still active, but is closely watched by security researchers. The infected computers have so far been used to make money in ordinary ways, pumping out spam and spreading fake antivirus software.

Source URL (retrieved on 03/10/2014 - 12:15am):

http://www.ecnmag.com/news/2010/03/authorities-bust-3-infection-13m-computers?qt-recent_content=0