

Spain smashes global 'zombie' computer network: police

March 3 2010



A 'skull-and-crossbones' symbol is placed above a computer keyboard. Spanish police have revealed they have collaborated with the FBI to smash the world's biggest network of virus-infected computers, which hijacked over 13 million PCs. Three people were arrested in the .

Spanish police said on Wednesday they had arrested three men suspected of building the world's biggest network of virus-infected computers which hijacked more than 13 million PCs.

The network infected computers from homes, universities, companies and government agencies in almost every country in the world with a virus that stole credit card data, online banking passwords and other

information.

"This is the biggest network of zombie computers ever discovered," the head of a Spanish police unit specialised in tech crimes, Jose Antonio Berrocal, told a news conference in Madrid.

Zombie computers can be remote-controlled by outsiders.

The network was so big that it could have been used to stage a "major cyber terrorism attack," police said in a statement.

The authorities believe the suspected ringleader of the operation and his two alleged partners earned a living by renting out the infected computer network to third parties who used them for criminal purposes.

The authorities provided no estimate for how much money could have been stolen from owners of infected computers but security experts said removing the virus from the affected PCs could cost tens of millions of dollars.

"We were lucky that this network was in the hands of someone who was not conscious of the (full) extent of its potential for crime," lead investigator Juan Salom said.

All three suspects are Spanish nationals. They are between the ages of 25 and 31.

While the authorities have dismantled major zombie computer networks in the past, arrests of the masterminds of such networks are rare.

The authorities found personal data from more than 800,000 computer users on the PC belonging to the suspected ringleader of the operation which was taken from his home in Spain's northern Basque region.

Police described the 31-year-old as a "petty criminal" who lived "modestly" from his hacking activities.

His two alleged partners, aged 30 and 25, are from Murcia in southeastern Spain and Galicia in the northwest.

The Mariposa network they created, named after the Spanish word for butterfly, was first detected in May 2009 by Canadian information security firm Defence Intelligence which alerted the FBI. It was shut down in December 2009.

It affected more than half of the Fortune 1,000 largest US companies and more than 40 major banks, according to investigators.

"It would be easier for me to provide a list of the Fortune 1000 companies that weren't compromised, rather than the long list of those who were," Defence Intelligence chief executive Christopher Davis said in a statement.

Shortly before the network was shut down, Defence Intelligence suffered a cyber attack which knocked down one of its Internet Service Providers in what Spanish police believe was retaliation carried out by the creators of the Mariposa network.

(c) 2010 AFP

Citation: Spain smashes global 'zombie' computer network: police (2010, March 3) retrieved 23 April 2024 from <https://phys.org/news/2010-03-spain-global-zombie-network-police.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.