BBC NEWS

FBI tries to fight zombie hordes

The FBI is contacting more than one million PC owners who have had their computers hijacked by cyber criminals.

The initiative is part of an ongoing project to thwart the use of hijacked home computers, or zombies, as launch platforms for hi-tech crimes.

The FBI has found networks of zombie computers being used to spread spam, steal IDs and attack websites.

The agency said the zombies or bots were "a growing threat to national security".

Signs of trouble

The FBI has been trying to tackle networks of zombies for some time as part of an initiative it has dubbed Operation Bot Roast.

This operation recently passed a significant milestone as it racked up more than one million individually identifiable computers known to be part of one bot net or another.

The law enforcement organisation said that part of the operation involved notifying people who owned PCs it knew were part of zombie or bot networks. In this way it said it expected to find more evidence of how they are being used by criminals.

"The majority of victims are not even aware that their computer has been compromised or their personal information exploited," said James Finch, assistant director of the FBI's Cyber Division.

Many people fall victim by opening an attachment on an e-mail message containing a virus or by visiting a booby-trapped webpage.

Many hi-tech criminals are now trying to subvert innocent webpages to act as proxies for their malicious programs.

Once hijacked, PCs can be used to send out spam, spread spyware or as repositories for illegal content such as pirated movies or pornography.

Those in charge of botnets, called botherders, can have tens of thousands of machines under their control.

Operation Bot Roast has resulted in the arrest of three people known to have used bot nets for criminal ends.

One of those arrested, Robert Alan Soloway, could face 65 years in jail if found guilty of all the crimes with which he has been charged.

In a statement about Operation Bot Roast the FBI urged PC users to practice good computer security which includes using regularly updated anti-virus software and installing a firewall.

For those without basic protections anti-virus companies such as F Secure, Trend Micro, Kaspersky Labs and many others offer online scanning services that can help spot infections.

The organisation said it was difficult for people to know if their machine was part of a botnet.

However it said telltale signs could be if the machine ran slowly, had an e-mail outbox full of mail a user did not send or they get e-mail saying they are sending spam.

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6752853.stm

Published: 2007/06/14 13:18:58 GMT