BBC NEWS

Zombie plague sweeps the internet

The summer saw a surge in the number of hijacked home PCs or "zombies", say security experts.

The Shadowserver Foundation, which tracks zombie numbers worldwide, said it had seen at least a threefold increase in the last three months.

More than 450,000 computers are now part of zombie networks, or botnets, run by hi-tech criminals, it said.

The rise is believed to be linked to attacks that booby-trap websites to try to infect the machines of visitors.

Attack vector

Criminals are keen to recruit new machines to a botnet to create a resource that they can use or which can be hired out to other gangs.

Most spam or junk mail is routed through the hijacked machines forming a botnet. The collection of PCs are often used to launch attacks on other websites, as anonymous stores for stolen data and to help with phishing scams.

The vast majority of machines in these botnets will be PCs running a version of Microsoft Windows.

In June 2008 Shadowserver Foundation knew about more than 100,000 machines that were part of a botnet. By the end of August this figure had exceeded 450,000 machines.

The Shadowserver Foundation is a group of security professionals who volunteer their time to track and measure botnets to help law enforcement investigations.

The rise in numbers has been accompanied by a fall in the number of so-called command and control (C&C) servers tracked by the Shadowserver group suggesting that hi-tech criminals are concentrating their resources. As their name implies, the C&C servers co-ordinate the use of all the machines linked to them.

The jump in individual zombie numbers is linked to a series of wide-spread attacks that inject malicious code on to legitimate websites that tries to compromise any visiting machine.

In recent months many hi-tech criminals have turned to web attacks to recruit new victims rather than rely on sending viruses out via e-mail.

Typically, a machine is compromised via a vulnerability in one of the programs it runs. Inside this initial attack program will be code that directs it to contact a C&C server which then downloads software to put it completely under the control of a botmaster.

The machines in any individual botnet can be spread across many different nations.

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7596676.stm

Published: 2008/09/04 10:51:02 GMT