



AusCERT

Australia's National Computer Emergency Response Team

MEDIA RELEASE

8 November 2005

[MR05-01]

AUSCERT WELCOMES NEW INITIATIVE TO CLEAN UP COMPROMISED AUSTRALIAN COMPUTERS.

The launch of the Australian Internet Security Initiative (ISI) by the Australian Communications and Media Authority (ACMA) was welcomed by Australia's national computer emergency response team, AusCERT.

AusCERT general manager, Graham Ingram said that the trial ISI program launched yesterday (November 7) by Federal Communications Minister Senator Helen Coonan would help close down "compromised" or "zombie" computers in Australia.

"It is an excellent example of where government can make a difference on a wide scale to improve Internet security and we are very happy to support it," Mr Ingram said

"If we can reduce the number of zombies in Australia we will reduce the level of online malicious activity both in Australia and abroad".

"The ISI will help us do our job better. A key part of our role as the national CERT is to help stop active computer attacks on the Internet. Often this involves locating the attacking computer and asking the responsible ISP to disconnect it from their network" said Mr Ingram.

"The initiative will be even more effective if we can get other countries to implement similar approaches," said Mr Ingram. "Our CERT counterparts overseas are watching the trial with interest".

Under the trial program, ACMA will provide selected ISPs with a list of the infected internet addresses on their networks. Each ISP will then contact customers with infected computers to advise them on what they may need to do to fix the problem.

In some cases, if after being advised of the problem the owner either cannot or will not fix the problem and their computer remains a threat to other Internet users, the ISP may take steps under its Acceptable Use Policy to disconnect the computer until the problem is resolved.

Mr Ingram said compromised computers typically come to our attention because they are being used for other criminal purposes, without the owner being aware.

“The owner of compromised zombie computers may also find themselves paying for bandwidth they did not intend to use, being defrauded, or potentially being held liable for criminal activities launched from their computer,” he said.

Mr Ingram said the best way for a consumer or small business to prevent their computer being infected or compromised in the first place is to follow the recommended minimum guidelines outlined by AusCERT in its paper “Protecting Your Computer form Malicious Code” available from <http://www.auscert.org.au/3352>.

This includes using an up-to-date operating system, using anti-virus software, a personal firewall, anti-spyware and anti-spam software.

Media contact: Graham Ingram, General Manager on (07) 3365 4417.

References: “Protecting Your Computer form Malicious Code” available from <http://www.auscert.org.au/3352>