The Australian Internet Security Initiative—Internet triage in action?

The ACMA-developed Australian Internet Security Initiative (AISI) provides information free of charge to internet service providers (ISPs) about 'bot' computers operating on their networks, that is, computers that have been infected by a virus or other form of malware. In 2009 the AISI reported more than 2.7 million instances of computer 'compromises' to Australian ISPs.

Under the AISI program, which was developed in-house by the ACMA, data is collected from various sources on computers exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to ISPs identifying IP addresses on their networks that have been reported in the previous 24-hour period. ISPs can then inform their customer that their computer appears to be compromised and provide advice on how they can fix it. The AISI has been in operation since 2005 and experience indicates that the vast majority of customers are unaware that their computers are infected by malware and are grateful for the assistance in making their computer secure.

Experience indicates that the vast majority of customers are unaware that their computers are infected by malware and are grateful for the assistance in making their computer secure.

The ACMA prioritises the data reported to ISPs in various forms. Daily reports are prioritised according to the severity of the compromise type, so that ISPs can deal with the most important compromises first. Fortnightly AISI reports—which were introduced in the second half of 2009—identify repeated sightings of particular IP addresses on ISPs' networks, indicating that the computer users associated with these IP addresses are likely to have been infected for some time and are in particular need of taking remedial action to disinfect their computer.

There are currently 75 Australian ISPs participating in the AISI, with the number of participants steadily increasing over time. It is estimated that participating ISPs cover more than 90 per cent of Australian residential internet users.

The consequences of having a compromised computer can be substantial, potentially involving harm to other internet users as well as to the individual with the compromise. Threats to the user of the infected computer include theft of financial and personally identifiable information which can lead to potential financial loss and reputational damage. External impacts can include being involved in spamming, distributed denial of service attacks on websites and the infection of other users' computers.

The ACMA considers it important that ISPs act swiftly on AISI reports. In particular, ISPs should focus on the highest priority reports so that the internet users concerned can clean up any infection they might have, change their passwords, or otherwise take the necessary mitigating actions to prevent further problems to themselves or other internet users.

Customers of ISPs often contact the ACMA to request more information about AISI reported incidents, particularly if the user is unable to find any sign of a security compromise on their computer. In the majority of these cases, the ACMA is able to identify and determine the capabilities of the malicious software involved and provide advice for its removal. Almost without exception, these users are unaware of the compromise at the time of the report.

Hidden costs—the business case

The ACMA's customer interactions with businesses identified through AISI reports illustrate the often hidden costs associated with computer compromises, as the eradication of malicious software is just a small part of the processes many organisations must undertake when they experience a security incident.

In a recent case, the systems administrator of an Australian pharmacy contacted the ACMA for further information on an AISI report sent by their ISP. Like many businesses and increasingly home users with multiple computers, the pharmacy's internet service is configured with a single public IP address shared by several computers. At the time of contacting the ACMA, the systems administrator had yet to determine which computer or computers was associated with the AISI report and required attention.

The pharmacy was particularly concerned because the infection could be on a computer used for storing customer records or for accessing systems related to the procurement of pharmaceutical goods. In either case, the breach would have to be reported to the relevant regulatory authorities, which would cost the pharmacy significantly more time and money than simply removing the malicious software. The ACMA was able to provide detailed information related to this particular malicious infection, which enabled the pharmacy to determine the appropriate course of action and allow the systems administrator to, in his words, 'sleep at night'.

Computer repair companies also often have 'post-disinfection' consideration concerns. Since these companies are in the business of dealing with malfunctioning computers, it is not surprising that many of those computers are infected. For many repair jobs, these computers are connected to the repair company's network to obtain drivers and patches from the internet. Unfortunately this has the effect of allowing infected machines onto the network, which may be able to communicate with 'clean' machines and the internet.

The ACMA receives a steady stream of contact from computer repair companies after their ISP tells them their IP address is compromised. Often these companies query how they can resolve the problem, and in such cases the ACMA has discussed strategies and network configuration alternatives to help them implement isolated 'insecure' networks, in which potentially infectious customer machines should be placed for diagnostics.

There are many other post-disinfection issues that require close consideration. For example, recovering from an infection by restoring from a backup will often leave the same vulnerability open for an attacker to strike again. Given that in many cases malware infections will collect passwords and keystrokes, it is prudent to change passwords after a compromise has been identified—from a known 'clean' computer, of course. Any privacy considerations associated with a compromise also need to be closely considered, such as that illustrated in the case of the pharmacy discussed above.

For more information on the AISI and for a list of member ISPs, visit the ACMA website at **www.acma.gov.au/aisi**.