Fighting the Conficker worm

The Conficker worm gained publicity earlier this year when it was set to update itself on 1 April 2009, making one of the largest botnets in the world potentially even more powerful. The ACMA has been collaborating internationally to enhance its Australian Internet Security Initiative (AISI) data towards combating Conficker infections in this country.

Richard Perlotto presents on current malware trends to industry representatives over lunch.

Conficker is a powerful computer virus that attacks Microsoft Windows operating systems by spreading through low-security networks, computers without current anti-virus software, and external devices such as USB sticks. While the individual malware installation techniques it employs are not new to industry experts, its combination of such advanced techniques renders it difficult to eradicate. The authors of the Conficker worm track security efforts and release new versions of the infection to overcome anti-malware defences. There are currently five known variants of the Conficker worm.

Computers infected with the Conficker worm connect to websites in order to receive instructions from the command centre. These instructions could potentially direct the compromised computers to perform harmful activities such as sending spam, stealing passwords and personal information, and launching powerful distributed denial of service attacks on websites. While previously Conficker used up to 250 domain names per day to send botnet instructions, from 1 April 2009 it activated a special algorithm to randomly generate 50,000 internet domains per day. The vast number of the sites makes it difficult for researchers to target and block access to them.

In response to the Conficker threat, Microsoft established the Conficker Working Group, a body of technology industry experts who are collaborating to implement a united, global approach to combating the worm.

The ACMA's e-Security team have been working with members of the Conficker Working Group to fight infections in Australia by capturing data on the worm and reporting it to Australian internet service providers (ISPs) through the AISI.

The AISI operates by collecting data on computers on Australian networks infected with malware and providing this data to ISPs in daily reports. ISPs can then use the reports to notify their customers of infections and help fix problems. Currently 64 ISPs use AISI data to identify compromised computers on their networks. Over 90 per cent of Australian home internet users are estimated to be covered by the AISI.

The collaboration between the ACMA and members of the Conficker Working Group has resulted in a significant increase in the quantity of data the ACMA provides to AISI participants on Conficker infections—and a significant role for the ACMA in helping combat Conficker infections in Australia.

The ACMA has a longstanding relationship with a founding member of the Conficker Working Group, the Shadowserver Foundation in the US. The Shadowserver Foundation is a watchdog organisation whose mission is to improve the security of the internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware. It comprises a group of security professionals who gather, track, and report on malware, botnet activity, and electronic fraud.

Richard Perlotto from Shadowserver visited the ACMA's Melbourne office recently during a tour of Australia and New Zealand, where he is conducting workshops on Shadowserver's activities. Mr Perlotto met with the ACMA's e-Security team to learn more about the operation of the AISI, including how data is processed, reported and managed.

Mr Perlotto also presented at an industry event hosted by the ACMA on malware and e-security trends, which was attended by e-security representatives from the banking industry, Australian Federal Police, the Australian High Tech Crime Centre, the Attorney-General's Department and local ISPs participating in the AISI.

The information session was an opportunity for e-security representatives to meet with counterparts from other industries and organisations to discuss current internet security and malware trends. The ACMA's e-security activities often involve liaison with state and federal police agencies, the banking industry and ISPs regarding malicious botnet and related cybercrime activity detected though the AISI.

Mr Perlotto's coverage of the Conficker worm in his presentation, including his insight into the extent of the worldwide threat, generated much interest from participants. Given the success of the information session, the ACMA hopes to hold similar industry events in the future.

More information on the AISI is available on the ACMA website **www.acma.gov.au** (go to For the public: Consumer & community advice: Spam & e-Security > Protecting yourself online > Australian Internet Security Initiative).

More information on the Conficker Working Group can be found at **www.confickerworkinggroup.org**.

More information on The Shadowserver Foundation can be found at **www.shadowserver.org**.