

Tackling cybercrime

Tackling animal rights extremism by disruption of Internet activities and funding streams is an important part of the government's strategy. But it is not always easy, as this article demonstrates.

In addition, the scientific community should embrace and adapt to current technology and remain vigilant to ensure our systems are protected against the danger posed by cybercrime.

Animal rights extremists are becoming increasingly adept at using technology to further their goals and reach a wider audience. You only need to look at the popularity of some of the social networking websites to see how easy it is for activists to push their propaganda to a staggeringly large audience.

For example, take a look at the MySpace phenomenon. As a social networking website, its aim is to allow individuals and groups of people to rapidly share their thoughts, messages, photos and videos with anybody who cares to look. Its popularity with teenagers and younger adults provides a fresh and keen audience for the activists; a quick check of the MySpace profiles for SHAC, WAR and NARN reveals nearly 20,000 people who have added these groups to their own MySpace profiles. Of course, each of the groups' profiles contain links to the other groups, creating a ring of activist profiles that can be navigated at a click of the mouse.

In this respect, the research community is in the position of playing catch-up to the AR groups' massive online presence. If there are any pro-research MySpace profiles on the Internet, they are well hidden.

With this ever-increasing uptake of technology as a means of furthering their cause, it will come as no surprise that some animal rights extremists are turning their skills into weapons of protest. The recent prosecution and conviction of four defendants in the Newchurch case highlighted the role that computers and technology played in the campaign. The police seized over 20 computers during the investigation and worked hard to pull information from them; the use of encryption makes this forensic work very difficult and activists are increasingly adept at using this technology to thwart investigations. On one laptop, investigators discovered personal

details of the Halls, family members, friends and employees plus details of birth, marriage and death certificates.

Working with the FBI, Microsoft and the American Embassy in London, detectives were able to secure evidence from a defendant's Hotmail email account. This was made possible using the US Patriot Act which is intended to help investigators track terrorist activity in the USA. Such cooperation with a UK police force is rare, but it does highlight the seriousness with which animal rights extremism is handled by international law enforcement agencies.

Whilst cases such as this involve the use of computers to facilitate the crime, the use of the computer is itself not actually a crime. Activists are well aware of this and know how far they can go before running foul of the law. When it comes to committing cybercrime, extremists are rather tight-lipped – in contrast with their other activities which so well publicised. Whether we consider hacking into computer systems, denial of service (DoS) or website defacement, it is difficult to find reliable evidence to provide accurate figures for the level of online cybercrime activity by animal rights extremists.

We know of only a handful of cases where high-profile companies have had their websites defaced and replaced with pictures of mutilated animals and long diatribes against the use of animals in research. Defacing webpages, however, can be seen as a bad idea for animal rights extremists. It leaves evidence, publicises the fact that the group or individual is involved in illegal activity and increases the chances of being prosecuted. The most common type of online crime committed by activists is likely to be designed to obtain sensitive or commercial information pertaining to the target companies, their staff, suppliers and contractors (see also the article on information security, right).

During the course of our 2006 network security work, we have tested privileged access to our clients' networks and have never been detected until we deliver our report to the client. If we reverse this scenario and consider activists and their hacking endeavours, it becomes clear that we will never be able to accurately determine the extent of hacking crimes and further, many companies will never know if they are secure or if they have already been hacked into. The reluctance of companies to alert the authorities to hacking-related incidents further emboldens hackers, as they know they face little chance of prosecution.

DoS attacks have so far been of little consequence to companies and individuals in the research industry. Technically difficult to undertake with any success, hackers must be highly skilled to maintain a denial of service attack, often relying on vast armies of hacked computers (known as 'zombies') to flood the target system with so much information that it stops responding. More common are floods of malicious emails which are a nuisance, but rarely constitute a danger to the integrity or availability of computer systems. This is a legal grey area at present with no known convictions under the Computer Misuse Act 1990.

It is incumbent upon us all to become at least as savvy as the activists with regard to using new media and technology. There exists great potential for harm to the research industry if we do not embrace and adapt the technology that is being so successfully used by animal rights activists. Further research is required in order to determine the extent of the use of hacking as an extremist tactic, but until this is undertaken we must remain vigilant to ensure our systems are suitably protected against the very real danger posed by cybercrime.