BBC NEWS

The fight against net crime

By Marc Cieslak
Reporter, BBC Click

The recent high profile investigation into a UK-based internet paedophile ring has served to highlight the dark side of the web.

Images of child abuse are shared across closed chatrooms and underground peer-to-peer file-sharing networks. The sites hosting the content are generally set up to last for a few days at a time, often jumping servers, making them difficult for the authorities to track.

A number of agencies have been formed across the world to prevent and deter online child abuse. These agencies use broad skill-sets including law enforcement, forensic computing specialists, covert internet investigators and, in some cases, help from the public.

Visiting any website leaves tell-tale signs: an individual computer's temporary internet folder, server logs and a record of that machine's individual IP address.

All of these things can build up a picture of that machine's web activity.

Users may feel the web offers a degree of anonymity but with the right tools and know-how, tracking where and what a computer has been doing is entirely possible.

Law enforcement

A list of websites which are known to contain images of child sexual abuse are banned from major search engines and some ISPs.

This list is maintained by the Internet Watch Foundation. It fields reports from members of the public who have come across material on the web they think might be illegal. In the last year it received 32,000 reports.

"The IWF has a team of trained analysts, they process every report that we receive," said the IWF's Sarah Robertson. "They develop intelligence from those reports and, once that assessment's made, the content is then traced to find which server it's hosted on around the world.

"If it is indeed illegal content we will pass all of the intelligence about those reports onto the Child Exploitation Online Protection centre.

"Because so little of this content is hosted in the UK that's then for them to pass out to the relevant law enforcement agencies in the host country. That goes out via Interpol."

The Child Exploitation Online Protection Centre (CEOP), is a law enforcement body created by the UK government to protect children from exploitation and abuse. It has a particular focus on the internet.

In June 2007, Operation Chandler saw CEOP infiltrate a paedophile peer-to-peer network.

"Our strategy was to identify the co-ordinator of that peer-to-peer network," explained Jim Warnock, head of operations at CEOP.

"We gathered evidence against him by applying some covert internet investigators within that group; once it was successfully infiltrated we prosecuted that person."

After the arrest of the site's administrator, officers working from CEOP's covert investigation suite assumed his online identity, spending 10 days posing as him to gather further evidence against other users.

The man running the site, Timothy Cox, was handed an indeterminate sentence, which means he could serve life in prison. Police forces across the world are following up intelligence gathered in the operation.

Forensic evidence

Gathering intelligence and performing arrests requires law enforcement experience, but gathering further evidence from computers, hard drives and other electronic devices requires specialist computer forensic skills.

When forensic teams arrive at a physical crime scene their goal is to not disturb the scene and record the evidence as faithfully as possible. The same is true when it comes to computer forensics.

"Whatever action we take shouldn't change or in any way alter what we're looking at," said IT forensics expert Robert Brown.

"Typically we will use a piece of hardware for taking a copy of the hard drive, which prevents us from making any changes to the disc itself or the data it contains. In effect we take a cloned copy of all of the data.

"That's not just the data that you the user can see or can work with, but information that you may not even know exists, information that's created as a result of your actions or activities, information that's created simply by the working of the computer.

"So if you're accessing the internet there's a trail of evidence that extends beyond your computer to other computers on the internet, as well as the servers that you might be accessing, the systems that you go through, perhaps the computer that you connect to.

Computers provide excellent evidence for net detectives; they leave digital fingerprints everywhere they go. No matter how cautious or careful, nobody is really invisible on the web.

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/programmes/click_online/6897121.stm

Published: 2007/07/13 13:31:24 GMT