HACKER SMACKDOWN

Who are the toughest hackers on the Net? **Gary Marshall** fires up his firewall, protects his ports and sorts the L33T from the lamerz

HACKING IS FUN. You spend your days breaking into mainframe computers, stealing people's bank details and occasionally triggering World War III when you fall asleep on the keyboard. Either that or you sneak into people's home PCs, zap their bank accounts and mess with their heads.

At least, that's what some sections of the media would have you believe. In reality, hackers are the good guys of the Internet – without them, we wouldn't have the software and technologies we take for granted today. The bad guys are the crackers and script kiddies: the former are people who use hacking techniques to break things or cause trouble, and the latter use off-the-shelf 'toolz' to deface Web sites and annoy people they've fallen out with.

That doesn't mean that hackers aren't mischievous types, though. As you'll see, hacking crews are responsible for all kinds of exploits. But who are the most influential hacking advocates? Was the US/China cyberwar the actions of a real hacking crew, or just script kiddies with too much time on their hands? And what on earth is a 'Deth Vegetable'? Find out in the first ever **.net** hacker smackdown.

Cult of the Dead Cow

www.cultdeadcow.com

Cult of the Dead What?

Cult of the Dead Cow, the World's most famous hacking collective and home to Tequila Willy, the Deth Vegetable and Sir Dystic.

Deth Vegetable? You can't be serious?

We are, and so is cDc – well, occasionally. When its members aren't winding up as many people as they can or training its secretive Ninja army, cDc is famous for its Back Orifice.

That doesn't sound very hygienic.

Not if you become one of its victims, no. Back Orifice is a remote administration tool for Windows – in other words, a Trojan horse. Once installed on your PC, it enables a remote user to control your computer without your knowledge.

It's an evil hacker tool, then?

Not really. cDc could have made it much more powerful and scary if it'd wanted to. As cDc member Nightstalker explained on Slashdot (**www.slashdot.org**): "[Back Orifice] was released to show up the miserable security of Windows, in the hope that MS would do something other than issue press releases and that users would be made aware of the pitiful security on their machines, particularly when connected to the Internet."

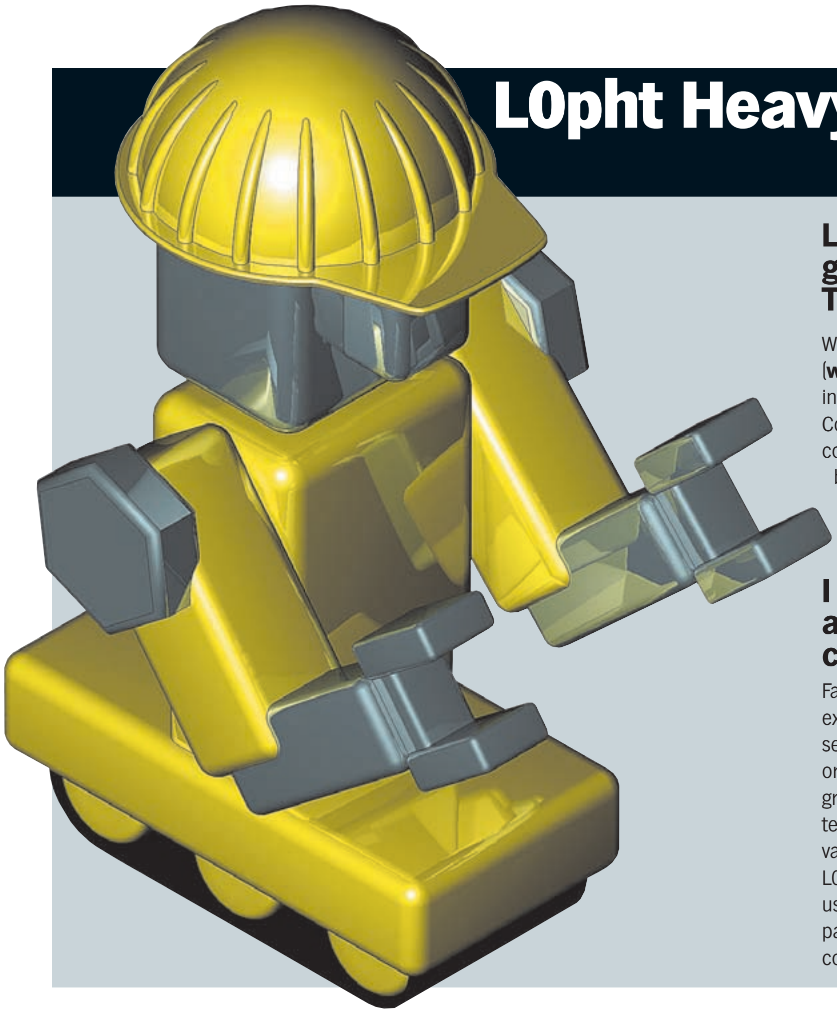
So it's all about embarrassing Microsoft?

That, talking about Jennifer Lopez, wearing appalling trousers and changing the world. cDc Foreign Minister Oxblood Ruffin, is at the forefront of 'hacktivism', and the Hacktivismo Declaration (**www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html**) describes how hackers can be a powerful force for human rights. cDc is putting its money where its mouth is with Peekabooty – an application designed to evade Internet censorship.

Peekabooty? Wasn't that due out ages ago?

It was, yes. Privacy activist Greg Walton explains the delay: "It's gone back to the drawing board. Why? Because if people could lose their lives because of it, it's got to work. It's not a word processor."

HACKER POINTS 10/10



L0pht Heavy Industries

www.lopht.com

L0pht? Hasn't that group sold out to The Man?

Well, it is now part of @Stake (**www.atstake.com**), a security firm that includes former employees of Digital and Compaq. But L0pht offered security consulting long before the big money beckoned – and it was always more interested in fixing security problems than exploiting them.

I thought they were a bunch of no-good crackers?

Far from it. As cDc's Oxblood Ruffin explains: "Most work revolved around security issues, whether in programs or across networks. And over time the group began to assemble an arsenal of technology upon which it would test its various inventions and exploits. The L0pht would then publish its findings, usually as L0pht Advisories [formal white papers]; detailing the minutiae of poor code formations that screamed for correction. It has held software and hardware vendors' feet to the fire and forced them to clean up their act and release better products. L0pht members have also spoken widely and well to issues concerning Internet security. Space Rogue, another L0pht member, launched the Hacker News Network, one of the few places on the Web that covers hacker issues with any credibility."

So they're good guys?

Definitely. L0pht repeatedly made monkeys out of Microsoft with its L0phtcrack utility and the L0pht/cDc collaboration Back Orifice 2000, it scared the US Government by explaining how easy it was to take down the Internet, and it was invited to join Bill Clinton's Internet security advisory panel. More importantly, the group has inspired a legion of hackers. As Ruffin notes: "There wasn't a kid in the world interested in hacking who did not at one time – usually many times – visit the L0pht Web site to feast on a world of learning that changed their lives forever."

HACKER POINTS 9/10

The Sub7 Crew

sub7crew.org

Sub7? Isn't that a dangerous Trojan program?

It is indeed. If your PC gets infected with Sub7, a hacker can delete files, access your passwords or just mess with your head.

Presumably it's got legitimate uses as well?

Sub7 creator Mobman reckons so. In an interview on Lockdown (**bots.lockdowncorp.com/mobman.html**), he explains that, "It didn't start out as malware [malicious software], and I don't keep working on it because it's intended for malicious use. Most of the people don't see, or don't want to see many of the positive uses. I've talked to admins who use it remotely to have complete control of other PCs, to parents who use it to watch their kids, Internet clubs, and so on."

So it's not evil, then?

That depends on who's using it. The documentation for Sub7 suggests using the program's Webcam features as follows: "Do you want to see what your victim [is] doing? Do you think he's hacking into your PC? Do you want to take some screen shots to prove that you got in his PC? Is your victim a very hot chick? Do you want to watch a strip show? Use this NOW."

So it is evil, then?

Certainly the Sub7 crew have a sick sense of humour. Crew member HeLLfiReZ managed to con an IRC user into an online wedding, before dropping the bombshell that the blushing bride had, er, some extra equipment. If you're not easily offended, you can read transcripts here: **sub7crew.org/wedding/wedding.shtml**.

So the Sub7 crew really are evil, then?

Only if you've married one of them on IRC.

HACKER POINTS 7/10

2600

www.2600.com

2600? Isn't there some sort of cornflake connection?

Sort of. *2600* magazine is the hacker's bible and a focal point for hardcore tech types; it takes its name from a frequency. Long before the Internet was even in short pants, John Draper, better known as Captain Crunch, discovered that the toy whistle given away in Captain Crunch breakfast cereal boxes generated a tone of 2600Hz. By blowing the whistle down the phone, you could get free calls to anywhere in the world. This form of hacking, known as phreaking, was the ancestor of today's PC hacks.

So 2600 is obsolete, now then?

Not at all. Although it originated in the phreaking scene, *2600* magazine has embraced every aspect of the hacking community. These days, it's essential reading for anybody interested in any kind of hacking – and it's essential reading for anybody interested in suing hackers.

Suing?

2600's visibility makes it an easy target for hungry lawyers, and the magazine's stance on hacking DVD copy protection and music file protection means the magazine regularly faces legal challenges. The controversy over the DeCSS code – which enables Linux developers to create DVD software for the platform – has dragged on for two years now. Entertainment industry lawyers allege that, by linking to the DeCSS code, 2600 (and a huge number of other Web sites) is guilty of contributory copyright infringement. If the magazine loses, the implications for free speech on the Internet are horrific. The signs aren't good: as we went to press, the US courts rejected 2600's appeal in the DeCSS case.

HACKER POINTS 8/10

Damage, Inc.

surf.to/damage_inc

Damage, Inc.? Isn't that a Metallica song?

It is – and it's not a very good one. However, the Damage, Inc. we're interested in isn't connected with heavy metal: it's a collective of Canadian hackers and phone phreaks.

Canadian hackers? What do they hack – moose?

Slagging off hackers probably isn't the most sensible thing to do, you know.

So what's so special about this lot?

As founder Blackened explains on the site: "Since 1993, we've been fighting against corruption, greed, Big Brother, censorship, ignorance, conformity and mainstream 'society'".

How do they do that?

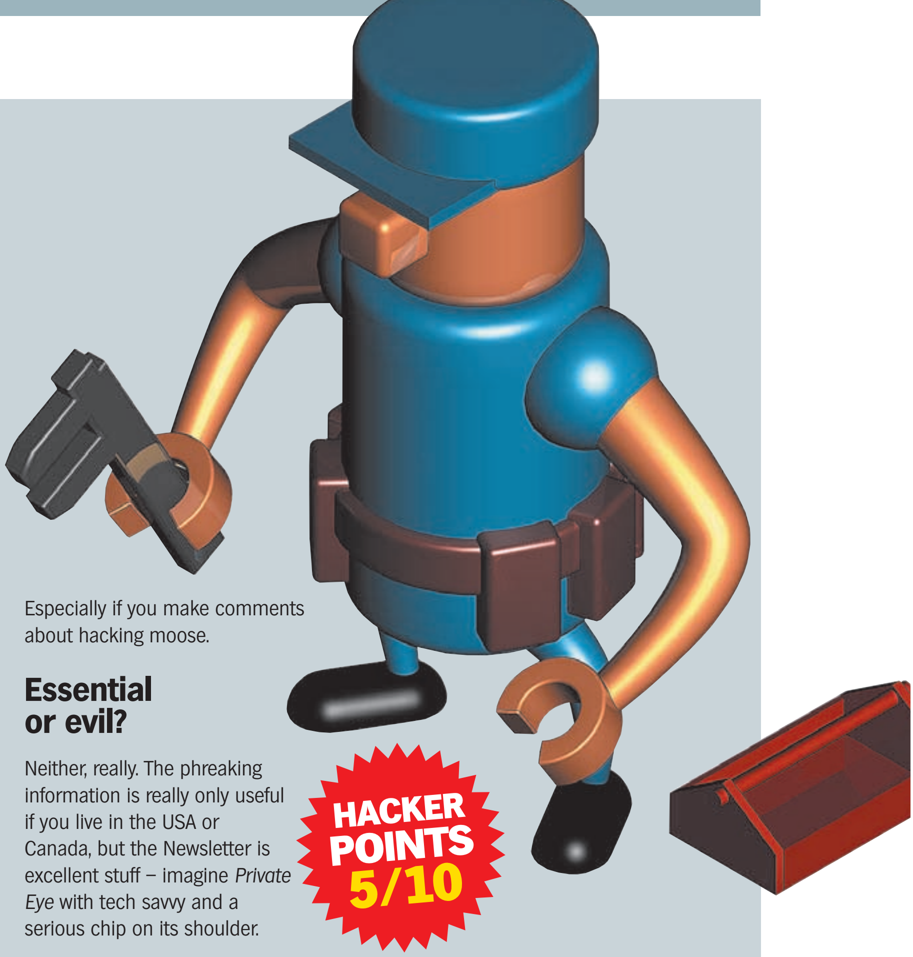
Damage, Inc. isn't just a group of hacking experts – although finding 'secret' phone numbers is one of the group's key skills and it has become a major thorn in the side of US telephone firms. The group also publishes an online newsletter that appears every few months. While it's first and foremost about the hacking and phreaking scene, the Damage, Inc. newsletter also covers issues of censorship, globalisation and Internet freedom. Although inevitably the newsletter sticks close to its Canadian roots, much of the content is relevant to hackers and Net users around the world.

So it just mouths off about the evils of the world?

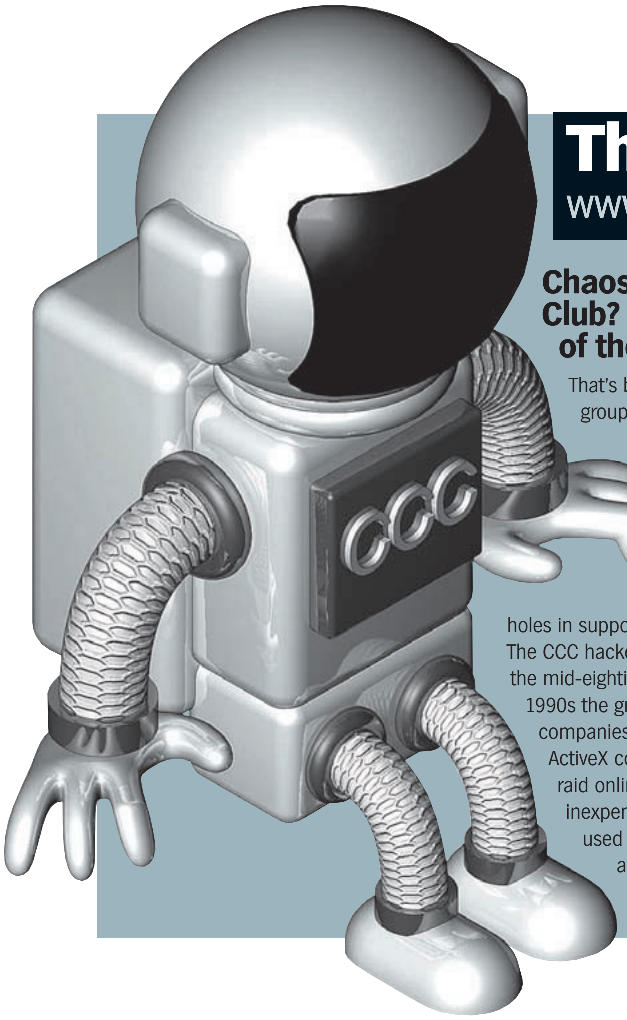
No, the group write programs and collate information, too. The Damage, Inc. Web site is packed with useful information for phone phreaks, and there's also a collection of nifty utilities that can nuke your entire hard disk in a few seconds. Especially if you make comments about hacking moose.

Essential or evil?

Neither, really. The phreaking information is really only useful if you live in the USA or Canada, but the Newsletter is excellent stuff – imagine *Private Eye* with tech savvy and a serious chip on its shoulder.



HACKER POINTS 5/10



The Chaos Computer Club

www.ccc.de

Chaos Computer Club? Never heard of them.

That's because the US hacking groups tend to get all the publicity. The CCC was founded in Germany in the early eighties, and gained a well-deserved reputation for spotting security holes in supposedly invincible systems. The CCC hacked into NASA's systems in the mid-eighties, and throughout the 1990s the group embarrassed big companies by demonstrating how ActiveX controls could be used to raid online banking systems, how inexpensive equipment could be used to fool cash machines and – brilliantly – taking around £50,000 from the German Post Office (they returned the money immediately).

Let me guess, another bunch of ethical hackers?

Exactly. The CCC played a key role in making the German Government aware of Internet issues, and campaigns against all kinds of bad laws. As the CCC explains: "The Chaos Computer Club is a galactic community of human beings, including all ages, genders, races and social positions. We demand unlimited freedom and flow of information without censorship."

So they do more than hacking?

Much more. Founder member and Chairman, Wau Holland, predicted the Internet explosion and campaigned to ensure that everyone – not just Governments and big businesses – would benefit from the Internet revolution. As a result, the CCC did everything from hacking big businesses to distributing wiring diagrams and kits to help people build modems.

Mr Holland sounds like a top bloke.

He was. Sadly, Holland died of a stroke in July 2001. However, the organisation he founded is still going strong: the CCC is currently campaigning on behalf of Russian hacker Dmitry Sklyarov and against the US Digital Millennium Copyright Act.

HACKER POINTS 8/10

SAY WHAT?

A bluffer's guide to hacker jargon

Hacker
A computer expert who takes systems apart – usually without the owner's permission – to find out what makes them tick and what could be changed and improved.

Cracker
A person who uses their hacking skills to cause damage, pirate software or commit other crimes.

Script Kiddie
A wannabe hacker who uses off-the-shelf tools (written by real hackers) instead of developing their own. Script kiddies' antics are usually malicious.

L33T H4X0R
Script kiddie-speak for 'elite hacker'.

Lamer
Derogatory term for a clueless or wannabe hacker.

Phreak, Phreaker
A person who hacks phone systems, often to obtain free calls.

HDC

www.hackers.com

Who is HDC?

HDC – short for Hackers Dot Com – is one of the world's best known ethical hacking groups. The group evolved from the bulletin board scene in the nineties, and as its site explains, "From the beginning, Hackers.Com represented the ethical side of the underground, the side that penetrated systems not to destroy, but to create knowledge in the minds of everyone who viewed its contents."

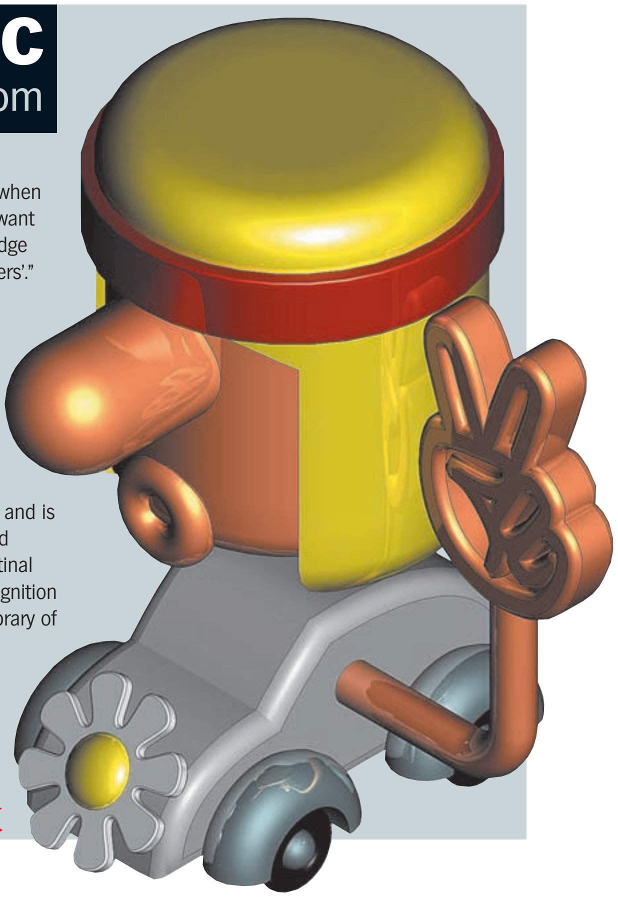
So they're not fans of script kiddies, then?

HDC explains: "We refuse to promote and distribute information on destructive and ignorant things, like carding, viruses, software pirating and email bombing. Hackers have undeservedly held a tarnished name for too long, and we plan to build that name back up. Instead of thinking 'criminal' or 'vandal' when hearing the word hacker, we want the public to think of 'knowledge seekers' and 'curious wanderers'."

Oh God, they're hippies.

That's unfair. HDC is interested in old-school hacking. At the time of writing, HDC was working on software for phone phreaking and is developing ways to get around biometric security such as retinal scanners and fingerprint recognition systems. They've also got a library of files covering everything from cryptography to denial of service (DOS) tools.

HACKER POINTS 8/10



HFX International

www.hfactorx.org

HFX International? Sounds a bit corporate.

HFX, or the hacker group previously known as Hack Factor X, is one slick operation. The group even has a mission statement that concludes: "Our projects and development teams are constantly thinking of new and better innovative ideas to make computers and other related technology a little better for everyone. We hope our endeavours will pave the way for global advancements and a brighter tomorrow."

Will they teach me to be a L33T H4X0R?

No. But if you're interested in hacking, the HFX site is a huge library of detailed tech information, tools and how-to guides.

What makes HFX special?

It's one of the most respected 'white hat' organisations – hackers who believe in understanding systems, not breaking them or defacing sites. It tries to battle the negative portrayal of hacking in the media, and it encourages wannabe hackers to think about ethics. To that end, HFX runs a hacking convention (HFXCon) and publishes an ezine that discusses every aspect of the hacking scene.

So they're not going to hack my PC?

No – true hackers aren't interested in that sort of thing. But if you think your security systems are the bee's knees, don't be too surprised if someone finds vulnerabilities you'd never have thought of – and emails you with details.

HACKER POINTS 7/10

Attrition

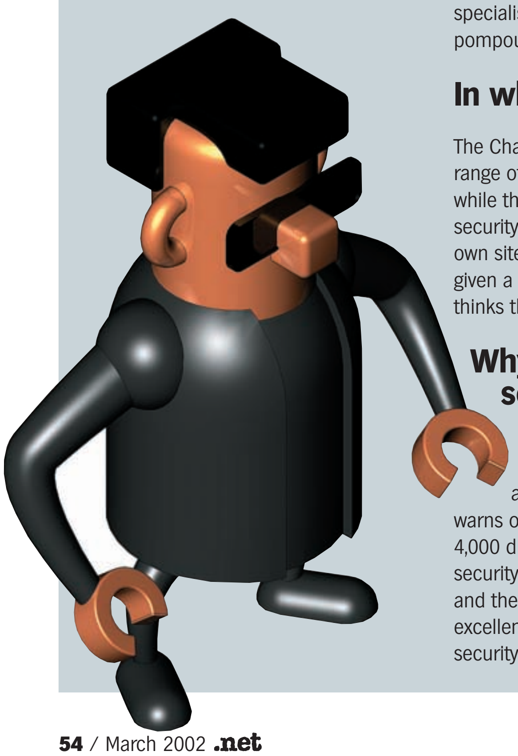
www.attrition.org

Hasn't the Attrition site shut down?

Apparently not, although it's been difficult to access recently. The site has been the victim of Denial of Service attacks and a few defacements, too.

Oh, the irony.

Well, Attrition has a lot of enemies. In the last few years, it has been accused of promoting cyber-crime, it's been investigated by the FBI, and it's been repeatedly threatened with legal action. Then there are the accusations that the site's an FBI front designed to ensnare hackers, while others have suggested Attrition is a front for a hacker group such as Girlies for Hacking.



Never a dull moment?

Exactly. It's hardly surprising that Attrition makes so many enemies, though: it's a very influential site that specialises in giving wedgies to the pompous, the fake and the plain mental.

In what way?

The Charlatans section exposes a wide range of fakes and snake oil sellers, while the Irony section points out the security flaws in Internet security firms' own sites and systems. Journalists are given a particularly hard time if Attrition thinks they've been scaremongering.

Why doesn't it do something constructive?

It does. Attrition's security advisory section warns of almost 4,000 different security problems, and the site is an excellent source of security news.

HACKER POINTS 8/10

PoizonB0x

Defacements mirrored at www.alldas.de

I've heard of this PoizonB0X. Isn't he a cyberterrorist?

Not really. What he – or she – does is deface Web sites. According to the defacement mirror at **www.alldas.de**, PoizonB0x is responsible for 921 defacements since March. That's almost one-third of all site defacements.

That's a lot of broken sites. So what's PoizonB0x's problem?

Nobody knows. It's unclear whether PoizonB0x is an individual or a group of individuals, but he or she (or they) has certainly been busy. In addition to defacing sites and starting a cyberwar with Chinese crackers, PoizonB0x is believed to be responsible for a massive Denial of Service attack on an American ISP.

Anything else?

Oh, yes. When New Zealand security firm Co-Logic set up a honey trap to lure and track hackers, PoizonB0x bypassed the trap and hacked into Co-Logic's main systems. Co-Logic was a bit embarrassed by that.

Hacker, cracker or script kiddie?

PoizonB0x certainly isn't a true hacker: all the attacks are malicious and bear the hallmarks of a script kiddie. The site defacements were carried out using a software program that exploits an old security hole in Web servers; similarly, the alleged Denial of Service attacks on the ISP are the sort of thing you'd expect from a script kiddie using off-the-shelf tools. The Co-Logic exploit could be the work of an inspired cracker; however, it's equally possible that PoizonB0x was once again using others' tools to break into the system. File under script kiddie, albeit a particularly prolific one.

HACKER POINTS 1/10