Hackers thinking small
Andy Sullivan in Washington
JUNE 21, 2005

A RECENT computer security breach that left 40 million credit cards vulnerable to fraud shows how online criminals are scoring big by thinking small, experts say.

Cybercriminals are increasingly crafting more focused attacks with a potential for profit as they target one or two companies at a time, rather than blasting out internet virus attacks across the globe, according to security experts.

The payoffs can be enormous. MasterCard International said on Friday that an outsider gained access to as many as 40 million credit and debit cards from CardSystems Solutions, a payment processor. A MasterCard spokeswoman said on Monday that the attacker had placed a malicious computer script on CardSystems computers.

In Israel, police are investigating a massive case of industrial espionage that used a "Trojan horse" computer program to copy confidential information from some of the country's top businesses.

Security vendors say such attacks are increasingly common.

"We have seen several examples of targeted, manually crafted Trojans that people write and implement for a very small number of companies," said Aladdin Security Vice President Shimon Gruper.

MessageLabs chief technical officer Mark Sunner said that since January the company has seen a 150 per cent increase in attacks that only target one or two companies.

Experts said there are a number of reasons behind the shift. Playful hackers looking for kicks could write viruses that plagued companies and computers around the world but brought them no financial return. They have been elbowed aside by organised criminals, often based in Eastern Europe, who are motivated by profit and willing to launch a sustained, sophisticated assault.

Targeted attacks have another key advantage: they are usually small enough to stay off the radar of internet security firms that are looking for broader attacks. That gives the high-tech criminals the time to research a company thoroughly before trying to penetrate it.

"You know there's specific technology, a piece of intellectual property, how much money is in their accounts," said RSA Security chief executive Art Coviello. "That's the advantage - you have a little bit more knowledge."

Attackers can then send individual, personalised emails to the target company's employees, or pose as an IT administrator who needs to install a software update. Once in, they can use simple spyware programs to pick up passwords, account numbers and other valuable information.

"When you see a focused attack like this, this is kind of your worst-case scenario. These are people who are going to actually do something with those credit cards once they get them," said Mike Gibbons, a Unisys vice president and former FBI cybercrime chief.

Email viruses have lost their teeth now that more people are using antivirus software properly, said Alfred Huger, senior director of engineering at the antivirus provider Symantec.

While old viruses continue to circulate, "they're background noise", he said.

At the same time, Microsoft has patched the most gaping holes in its Windows operating system and companies have learned to install those patches quickly, said John Pescatore, a vice resident at the consulting firm Gartner.

Identity thieves who used to go through rubbish bins to find credit-card receipts have learned that it's more worthwhile to extract such information from companies that collect it.

"Two years ago I would say one of the things you should do is shred your trash. Now that is completely obsolete advice," said Bruce Schneier, chief technical officer for Counterpane Internet Security.

"This report appears on australianIT.com.au."