

## Web hit by hi-tech crime wave

### **Hi-tech criminals are racking up more than 100 attacks a second on the world's computers, a survey suggests.**

While most of these attacks cause no trouble, the Symantec report suggests that one attack every 4.5 seconds does affect a PC.

The wave of attacks was driven by a steep rise in malicious software in circulation, said the annual report.

The number of malware (malicious software) samples that Symantec saw in 2009 was 71% higher than in 2008.

### **Crime family**

This meant, said Symantec, that 51% of all the viruses, trojans and other malicious programs it has ever seen were logged during 2009. In total, Symantec identified almost 2.9 million items of malicious code during that 12 month period.

The steep rise in malware was driven largely by the growing popularity of easy to use toolkits that novice cyber criminals are using to turn out their own malware, said Tony Osborne, a technology manager for the public sector at Symantec.

Some of the kits were available for free, said Mr Osborne but others cost a lot of money. One, called Zeus, was available for around \$700 (£458) and many had become so successful that their creators now offer telephone support for those who cannot get them to work.

#### **STAYING SAFE ONLINE**

- Use security software that can tackle viruses and spyware
- Use a firewall
- Apply operating system updates as soon as they become available
- Be suspicious of unsolicited e-mails bearing attachments
- Keep your browser up to date

During 2009, Symantec say more than 90,000 variants of the Zeus kit and it was responsible for the growth of one of the most prolific malware families during the year.

Zeus relies on spam to lure people to websites where victims will be tricked into installing malicious code or which sneaks on to a computer via a known vulnerability.

Often, said the report, this can help criminals set up botnets - networks of hijacked home PCs that can be used to send spam or plundered for lucrative personal data. In 2009, Symantec saw almost seven million distinct PCs that were members of botnets.

There was one very simple reason that novices bought and used the kits, said Mr Osborne.

"It's all about money," he said.

Established gangs were also showing no signs of holding back in their attempts to steal saleable information.

"Why would they?" he said. "It's easy money and it's very hard to catch people."

"It's become a day job for a lot of people," he said.

There was evidence, suggests the report, that professional cyber criminals were tuning their tactics to try and get better results. Many now scour social network pages for details about employees inside companies and craft their spam and other messages to capitalise on the details they can gather.

The continuing growth of hi-tech crime meant that many developing nations were starting to suffer significant numbers of attacks. Brazil and India were becoming hot spots of cyber crime, said Mr

Osborne.

This was because, he said, the infrastructure in those nations was rapidly improving as people move to broadband and use the web for more and more of their daily lives.

"Those are the places where education and understanding about security are taking a while to catch up," he said.

Story from BBC NEWS:

<http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/8630160.stm>

Published: 2010/04/20 04:12:56 GMT

© BBC MMX