4 August 2010 Last updated at 13:46
&#65533;
Technology reporter, BBC News " border="0" title="bank scam" width="300" height="438" align="left" />
A network of thousands of compromised computers that is being used to harvest online banking details has been uncovered in the UK. The so-called botnet is made up of around 100,000 machines, according to researchers in Israel. Cyber criminals in Eastern Europe, who have control of the machines, are collecting personal data from the PCs.   This includes login details for online banks, credit and debit card numbers and other passwords. "The fraudsters are very familiar with UK banking systems," said Amit Klein, chief technology officer at Trusteer, the firm which uncovered the network. Mr Klein said that he had contacted the Metropolitan Police central e-crime unit to alert it to the scam, as well as affected banks. "We're aware of an allegation," said a spokesperson for the Metropolitan Police. "We are working with UK Payments and Trusteer and inquiries are under way." A spokesperson for UK Payments, which tackles financial fraud, said attacks like this had "become the norm". "100,000 computers being targeted by a trojan does not necessarily mean that 100,000 UK customers will have had their details successfully used by the fraudster. "In the highly unlikely event that any one of the 23 million UK customers who bank online is an innocent victim as a result of this attack they can expect to get their money back." Money grabber
&#65533;
The 100,000 Windows machines have been infected with a trojan known as Zeus, said Mr Klein. Trojans are a type of program or message that looks benign but conceals a malicious payload. There are currently hundreds of networks of computers infected with Zeus. However, Mr Klein said this one was unusual because it used a new variant of the malware and also predominantly targeted people in the UK. Researchers at Trusteer were able to identify the geographical location of victims, he said, after they gained access to the command and control centre of the network. "One of the nice features of that is that it provides you with stats regarding operating systems and the geographical information of the bots. "We actually used the fraudsters' own data to assess the botnet and determine that it actually targets the UK." The dashboard also allowed the firm to identify which banks had been targeted, but Mr Klein declined to name them. He said victims' computers had probably become infected by clicking on a link in a spam message or by visiting an infected website. "It was probably a UK-specific website or a message sent out on a UK-specific spam mailing list," he said. Once infected, the machines are effectively under the control of the cyber criminals. This allows them to monitor and collect all kinds of information, including bank details, he said. "This later allows the [criminals] to sign on to the account and wire money out," he said. It also allowed other more sophisticated crimes. "When you initiate a transaction, they may change the destination and the amount of money that you wire," he said. "Rather than sending &#65533;100 to your aunt, you may find that your account balance is sent to Ukraine." Mr Klein said that the scam was difficult to spot, but that people should be suspicious if there was any change in their bank's login procedures or they were prompted to resubmit password and other details
Spam machine
&#65533;
Mr Klein said it was likely that the criminals had targeted the UK because it had a developed banking

sector. "You've got half a dozen major banks and a dozen or so additional banks which cover the vast majority of financial transactions in the UK," he said. "If you can write malware to cover six to 12 banks in the UK, you're covering almost all the market." The Zeus Trojan is a common piece of malware that potentially infects millions of Windows machines globally. Networks of infected machines under the control of cyber gangs are known as botnets. These are commonly used to pump out spam. But Zeus specifically targets financial information. "Zeus is a major headache," said Mikko Hypponen of security firm F-secure. Botnets such as these are commonly hired out to criminals for their own use. There have been several arrests of people who have hired Zeus networks, including a couple in the UK in 2009. "These are always customers of Zeus gangs or individuals behind Zeus," said Mr Hypponen. "The main brains behind Zeus are not breaking the law. "Developing the trojan is not illegal, selling the trojan is not illegal, but using the trojan is."
Source: http://www.bbc.co.uk/news/technology-10865568