Hacker gang used tiny screen-grabbing 'bug' installed by bogus repairman in audacious cyber-heist plot to steal millions from Santander bank

An 'audacious' plot to siphon millions of pounds from a bank, using a device installed on one of its computers by a fake maintenance worker, has been smashed, police said today.

A gang targeted a Santander branch in Surrey Quays, London, and installed a gizmo on one of the computers that allowed the contents of the screen to be viewed remotely.

The hackers were hoping to use highly sensitive information displayed on the computer to access accounts and drain money from them, but the Hollywood-style cyber heist was foiled.

Hacking: The Met Police has said a device similar to this was used by criminals, which when plugged into a computer transmits screen contents to a remote PC

1 Bogus repairman fits device to computer
2 What worker sees on screen is recorded
3 Sensitive data is transmitted to the hackers' computer

THE HACKING GANG WHO NEARLY GOT AWAY WITH £229 MILLION

A similar cyber raid to the one at Santander was attempted in 2004 at the Japanese bank Sumitomo's London branch.

A security guard was involved in a plot by computer hackers to transfer a very large sum of money - around £229 million.

This plot was also foiled and conman 'Lord' Hugh Rodley, insider Kevin O'Donoghue and Soho sex shop owner David Nash were jailed in 2008 for the attempted high tech robbery.

Henchmen Jan Van Osselaer and Gilles Poelvoorde were also found guilty of conspiracy to steal.

Graham Cluley, now a freelance computer security analyst after 14 years as senior technology consultant for Sophos, said: 'The worry is these things are very difficult to detect, because anti-virus software is no use. You have to actually spot the device, and not many people bother looking behind the back of their computer.

'If they had got away with it the hackers could have moved a large sum of money into another account and spirited it somewhere else in the world before anyone had realised what had happened.

'There is nothing we, as customers, could do and we just have to have trust in the banks to stop this sort of thing happening.

'The days of the stocking over the head have long gone. There is less physical risk to holding up a bank now. Cybercrime can be carried out by robbers on the other side of the world.'

A spokesman for the bank said: 'The attempt to fit the device to the computer was undertaken by a bogus maintenance engineer pretending to be from a third party. It failed and no money was ever at risk.'

The device would be able to transmit information to someone in another part of the country, according to a Metropolitan Police spokesman.

He told MailOnline: 'The device is a little box that plugs into the back of the computer, in one of the ports where you might plug in a mouse or a keyboard. Once it's switched on it effectively transmits everything that is shown on that computer, who could be hundreds of miles away, potentially.

'It gives someone remote access and they can see everything that's going on.'

Eleven men were arrested after officers swooped on a suburban house in Hounslow, west London.
Another man was arrested later in central London over the plot that targeted the bank at Surrey Quays shopping centre in the south of the capital.

Property was also seized by police in at least six raids on other addresses in the London area.

A Scotland Yard spokesman said: 'Officers from the Metropolitan Police's Central e-Crime Unit (PCeU) have arrested 12 men in connection with an audacious attempt to take control of a bank's computer in order to steal from them.

'The offence involved deploying a KVM (keyboard video mouse) device, fitted to a computer within the bank branch, allowing the transmission of the complete desktop contents of the bank computer over the network. In effect, this allowed the suspects to take control of the bank computers remotely.

'Yesterday's time-critical, dynamic response was achieved by working in partnership with the banking sector, thwarting a very significant and audacious cyber-enabled offence, and avoiding multi-million-pound losses from Santander at Surrey Quays shopping centre.

'On Thursday, 12 September in Kingsley Avenue, Hounslow, officers arrested 11 men, aged between 23 and 50 years, in connection with an allegation of conspiracy to steal from Santander Bank.

'A further arrest of a 34-year-old man was made at Vauxhall Bridge Road in connection with the same offence.

© George Jaworskyj

Similarities: Last week a gang allegedly used a discreet gizmo plugged into a Santander computer to spy on its content

© Alamy

Police said those arrested had targeted a Surrey Quays branch of Santander

'Searches have been carried out at a number of addresses within Westminster, Hounslow, Hillingdon, Brent and Richmond, and also in Slough, where property has been seized.

'The arrests are the result of a long-term, intelligence-led, proactive operation by the PCeU.

'Those arrested are currently in custody at a London police station.'

Detective inspector Mark Raymond, of Scotland Yard's Police Central e-crime Unit, added: 'This was a sophisticated plot that could have led to the loss of a very large amount of money from the bank, and is the most significant case of this kind that we have come across. I would like to thank our partners from the industry who have provided valuable assistance throughout this investigation.

'The PCeU is committed to tackling cyber-crime and the damage it can cause to individuals, organisations and the wider economy.'

The Santander spokesman added: 'No member of Santander staff was involved in this attempted fraud. We are pleased that we have been able, through the robustness of our systems, to prevent the fraud and help the police gather the evidence they needed to make the arrests.'

Visit the ASP Website: http://www.advancedsecurityprotection.com/services/technical-surveillance-countermeasures-tscm-debugging