Longitude149

Title: Mission Impossible at the Sumitomo Bank
Published: 13 Apr 2005
Author(s): Peter Warren, Michael Streeter
Original Source: theregister.com[1]

Mission Impossible at the Sumitomo Bank

Key loggers, blank tapes and a cold trail

The investigation into the attempt to steal an estimated £220m from the Sumitomo Mitsui Bank in the City of London is focusing on a hi-tech plot using members of the cleaning staff and bugging devices.

In an Mission Impossible-style scam, it was claimed last night, some cleaning staff placed hardware bugs onto the keyboard sockets at the back of the bank's computers where they could not be seen and then reattached the keyboards.

When the plot was uncovered investigators working for the bank found some of the devices still attached to the back of the computers.

The gang are understood to have also got around the bank's 24 hour video surveillance of its offices as tapes that would have shown the cleaners at work have now been found to be blank.

According to sources, police in Israel are now interviewing a former member of the cleaning staff.

Attempts to trace the gang as it tried to move the cash are believed to have failed after the exact instructions on what accounts it should be transferred into vanished although elements of the gang are thought to have been under surveillance.

"You could say that the trail has gone cold in cyberspace," said a computer security expert, adding: "The problem with this is that the skill sets of the attackers are very high."

A spokeswoman for the National High Tech Crime Unit (NHTCU) in London said: "No money has been lost."

The ongoing investigation into the attack at the Japanese bank is now focussing on the use of sophisticated hardware devices that may have been inserted into a USB keyboard port on some of the bank's computers.

The leads include a walkman battery-sized device known as a hardware 'keylogger', which can be bought from spy shops for around £20, and can be connected to the keyboard.

[1] https://www.theregister.com/2005/04/13/sumitomu_bank/

They cannot be seen unless someone physically examines the back of the machine. The devices can then download passwords and other data that is used to gain access to the computer system.

Due to the panic caused by the discovery of the keyloggers many banks are now super-gluing keyboards and other devices into their computers.

Sumitomo is rumoured to have also banned the use of wireless keyboards in its offices.

"This type of scam has been going on for a while. This is an old, old issue and people have been talking about it being a weakness for at least two years now," said a source.

Security expert Paul Docherty of Portcullis Security uttered a stark warning to other companies in the City: "It is known that people have been using devices like these. Because you can buy them from shops it is highly likely that they have been used in other scenarios."

An Israeli man has been charged with attempting to move £20m through his bank account but according to members of the computer security industry he is thought to be a junior member of the plot.

British businesses have been facing a growing wave of hi-tech so-called cyber crime in recent years, both from insiders and from organised criminal gangs who are finding such crimes lucrative and relatively low-risk.

The use of hardware and software to capture key-strokes is the latest addition in a growing list of technological weapons being deployed by high tech crime gangs.

Gangs also routinely take over the computer systems of home users - especially those on high-speed connections - with computer viruses. These strip the PCs of their passwords and the machine are then used to launch co-ordinated attacks at business computers to bring down company websites.

The criminals then demand protection money. The home user may have no idea their machine has been turned into a so-called "zombie computer".

According to figures released by the National High Tech Crime Unit at the E-Crime Congress computer viruses now cost UK industry £747m, online financial fraud £690m and computer-related extortion a staggering £558m.

A spokesman for the bank today refused to comment on the ongoing investigation.

Further details from Future Intelligence here.

###