



ISSUE # 2 JULY 2009

CORPSEC TSCM NEWSLETTER

IN THIS ISSUE

- ↳ IPHONE VULNERABLE TO HACKERS
- ↳ WHO'S BUGGING THE BRITAINS GOT TALENT JUDGES?
- ↳ BUGGING CLAIMS BY MANCHESTER UNITED
- ↳ CORPORATE ESPIONAGE – NOT IF, BUT WHEN.

IPHONE VULNERABLE TO HACKERS

Flaw could allow hackers to remotely execute code.

Security experts are warning of a serious vulnerability in the iPhone that could allow hackers to remotely execute code on the device.

"The vulnerability seems to allow unsigned code to run, which circumvents a core part of iPhone's security model. The iPhone is usually only able to run signed code, i.e. apps that have been approved by Apple. No user interaction is required, which is unlike current mobile malware.

Security researcher Charlie Miller is reported as saying, "The vulnerability could enable hackers to remotely turn on the GPS function to monitor the handset's location, or turn the microphone on to listen in on conversations."

I request
a Cone
of
Silence!



WHO'S BUGGING THE BRITAINS GOT TALENT JUDGES?

Police were called to the audition venue for Britain's Got Talent today after a bugging device was discovered under the judges' table.

The surveillance equipment had been left overnight in the judges' room, where Simon Cowell, Amanda Holden and Piers Morgan embarked on a second day of filming.

Suspicious were aroused when the device caused interference with the sound and film equipment for the recording of the audition process of the hit Saturday night ITV1 show.

A bugging device was found under the Britain's got talent judges' table

When the equipment was found police were called to the venue, the Palace Theatre in Manchester, where fire-eaters, acrobats, dancers and singers are hoping to get the chance to make their name on the show.

There was a 20-minute delay in filming this morning as police investigated.

Cowell said afterwards: "This shows the extent to which people will go to to get inside knowledge on what is going on."

TV bosses believe there is a possibility that a freelance journalist could have planted the device to find out what was being said in the judges' room.

BUGGING CLAIMS BY MANCHESTER UNITED

Manchester United have launched an investigation into claims that their dressing room was bugged during the Premiership victory over Chelsea.

Audio tapes apparently recorded at Old Trafford were obtained by The Sun, which handed them to the club.

A club statement said: "We have launched our own investigation and if necessary will involve the police."

The tapes apparently contain recordings of pre-match and half-time team talks, plus celebrations after the 1-0 win.

Manager Sir Alex Ferguson had been under pressure before the game after United's 4-1 Premiership defeat to Middlesbrough and a 1-0 reverse to Lille in the Champions League.

On the tapes, Ferguson can reportedly be heard giving an inspirational team talk to his players before the game, and then issuing tactical advice at half-time when his side led 1-0.

In the wake of the victory, which ended Chelsea's 40-game unbeaten run, United's players are recorded congratulating each other.

CORPORATE ESPIONAGE – NOT IF, BUT WHEN.

Corporate espionage is defined as the theft of commercially valuable information. This may be the secret formulation of a new product, but equally it could be the names and salaries of senior executives or simply the date of your next marketing initiative.

This type of corporate crime costs the world's 1,000 largest companies in excess of \$45bn (£22.4bn) every year, according to research from consulting firm PricewaterhouseCoopers.

Some of the world's largest corporations have been targeted: for example, in 2000, Microsoft fell victim to what the company called "a deplorable act of industrial espionage" when hackers broke into the company's system and accessed Windows and Office source code. Hackers had access to the source code for up to three months.


Corporate espionage has increased rapidly in the past decade, as more information is put onto corporate networks — and potentially within the reach of hackers, Dirro explains. Certainly, PricewaterhouseCoopers reported that corporate espionage losses doubled between 1990 and 2000.

Knowing whether you're at risk of corporate espionage isn't easy, admits Paul King, a senior security advisor with Cisco UK. In fact, you could be a victim of corporate espionage and never even realise it, King says. "At Cisco, we don't ask ourselves why we might be at risk of this stuff, we ask why not?" he says. The company's security experts constantly scan the internet for reports of attacks on other organisations, and assess their own risk to similar attacks.

It's difficult to know exactly how common corporate espionage is because most victims never report the attack to the police, fearful of the consequences of going public, says King. And if a hacker is sufficiently skilled, many companies won't even realise they've been attacked. "I think the best we can do is monitor our systems carefully and if we hear of an attack on another organisation, ensure that it couldn't affect us," he says.

This is an information Newsletter and your feedback on any future contents would be greatly appreciated in order to keep it news worthy.

Corpsec Pty Limited is available to answer any questions or enquiries you might have on the subject of Technical Surveillance Counter Measures (TSCM)



Looking after your future
Listening to your needs

Nick Graves
Phone: +61 2 9267 0661
Email: ngraves@corpsec.biz

If you do not wish to receive any further Newsletters please contact Nick Graves by email.