The wireless hacker project

Do wireless hackers really exist? What tools do they use? When do they strike?

These questions have preyed on the minds of IT directors and system administrators over the last year, yet nobody seems to have a satisfactory answer. Many pundits and new media gurus deny the existence of wireless hackers whilst others claim they are endemic.

Many statistical studies have been published that show how insecure wireless technology is or the number of accessible networks in an area. However, these types of assessment do not contribute to the understanding of risks associated with wireless technology.

KPMG's Wireless hacker project is a scientific assessment designed to assist in understanding the true risk of wireless hackers by identifying the types of attacks that are being waged on wireless networks and whether these attacks are as prevalent as some are claiming.

What we wanted to know

Is the image of the free-surfer a myth?

Would people that can afford laptop computers and expensive wireless equipment brave the cold and rain for free Internet access.

Do drive-by hackers exist?

We wanted to know if the drive- by-hacker existed or if good-intentioned war-drivers were being maligned for the convenience of security vendors.

What is the drive-by hackers toolkit?

If drive-by-hackers do exist, we wanted to establish if they used conventional attacks or did they have a special armoury of 802.11 attacks.

What is it?

HONEYPOT - A weird name for a security device, but the derivation is clear. How do you catch nuisance wasps or bees? - well you use an old jam-jar or honeypot, with a bit of jam at the bottom. Hence the name.

In security, a HONEYPOT is a device thats "sole purpose is to be hacked". It is not used to trap anyone or prevent them going about their business, lawful or otherwise but to study their behaviour.

How we did it

We used a custom built wireless honeypot of our own design based on a bespoke Linux installation. These devices appear to be a legitimate corporate wireless network but actually record and analyse activity of any user who tries to access them

Of course, all access to this network was "unauthorised" because the honeypot is a dummy network with no legitimate users to complicate analysis. We classified the types of users we identified into three broad categories:

- War-driver - someone who probes the network but makes no attempt to access any resources.
- "Free surfer" - someone who connects to the network and attempts to surf the Internet.
- Wireless-hacker - someone who connects to the network and attempts to access or disrupt systems.

We deployed the honeypot in three separate locations around central London for a period of a week, including the weekend, to learn the truth behind what hackers are really doing.

Did you know

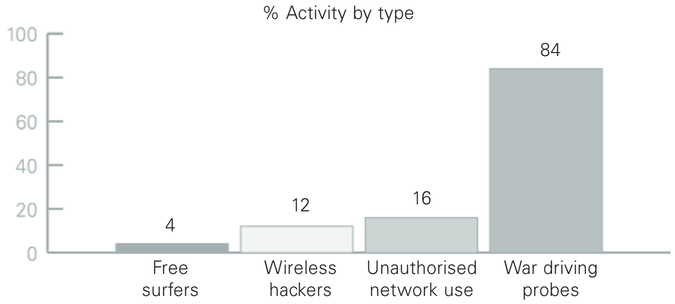
. . . that if your IT department has deployed a wireless LAN the chances are that:

- All data travelling across your wireless network is readily accessible by a journalist, competitor or wireless hacker.
- The wireless network will probably be accessed by four or five unauthorised users a day but because of restrictions in most common technologies these will not be detected.

These activities might be an attempt to gain free Internet access , or more accurately, to gain free access to the Internet link that your company is paying for. Although not malevolent in itself, this access can result in a breach of law, industry guidelines or regulatory requirements. However, it is more likely that the access is made by a hacker who will attempt entry into your systems.

The results

The results were staggering



A total of 51 different wireless cards were detected issuing probes designed to detect the presence of our network.

Some 84% of these took no further action, simply identifying the existence of our network and then quietly (and harmlessly) moving on.

This behaviour typifies the war-driver. However, 16% of these probe attempts resulted in eventual network access.

About hackers

The major surprise is that most (75%) of the confirmed accesses to the network (12% of the total) undertook activity that would be described by any reputable classification system as hostile.

The technical reader will recognise the disruptive nature of activities recorded including the use of snmp and known IIS vulnerabilities (specifically the Translate f and the .idq vulnerabilities).

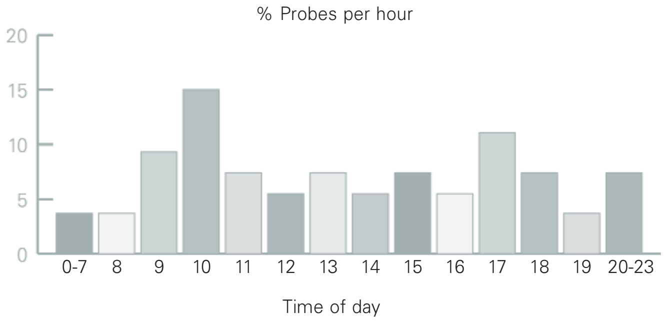
Anyone will appreciate that trying to logon as “administrator” when you are not one is an unfriendly act. These findings certainly dispel the popular notion that there are no malevolent forces within the “wireless community”.

If the end-game of individuals is free Internet surfing, we can assume that they are willing to take it from those that might not be willing to give it!

Whatever the reason for such activity, the following conclusions can be drawn:

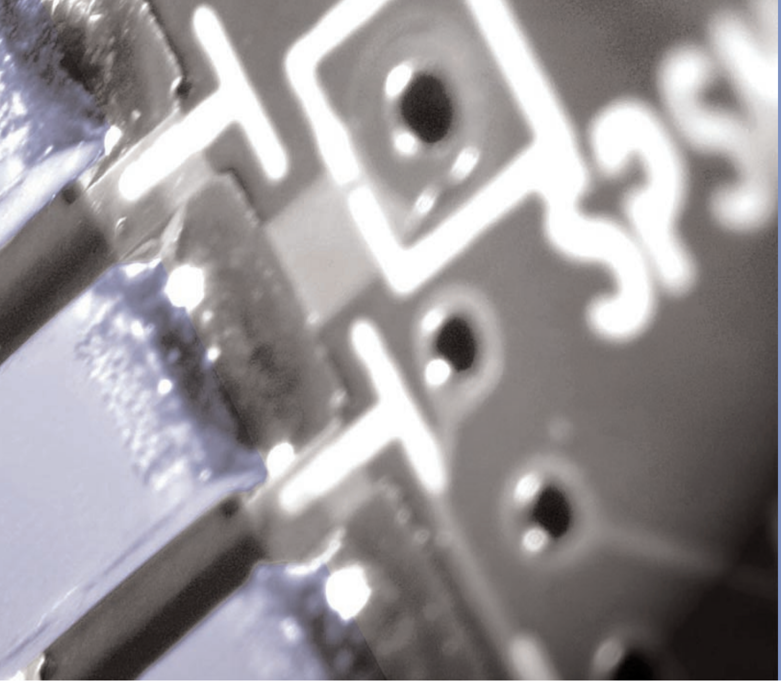
- The activity recorded could definitely adversely effect a typical business
- The majority of hackers had a less than basic knowledge of computers and network routing. This was evident from the types of activity recorded in the system logs.
- Detection of such attacks would be much harder on a typical corporate LAN with typical 802.11 equipment. This type of environment has legitimate users and generally insufficient monitoring techniques.

And about war-drivers

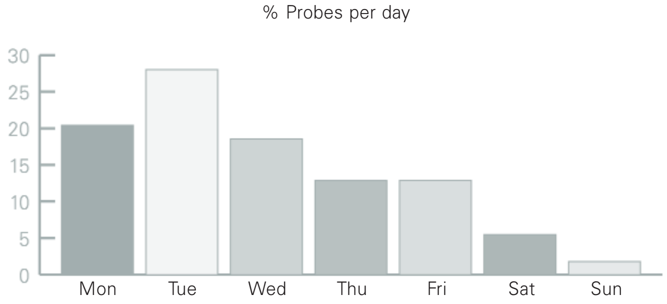


Certainly the evidence points to the fact that this is a growing hobby in its own right. The vast majority seem to use tools that reduce the noise they produce on any wireless commercial network they might discover - making it fairly innocuous. This is known as passive scanning.

Most of our war-drivers also seem to do their driving between 9-10.30am.



Or in the evening 5-7 pm. Does this mean they do it to and from work? This would certainly seem likely as there is virtually no activity during the weekends.

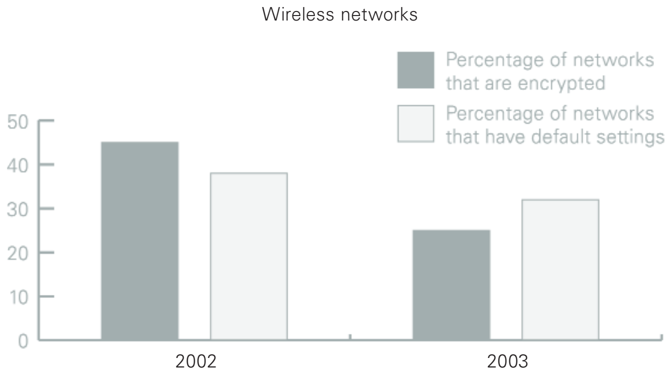


And these individuals are certainly not without a keen sense of humour. Inspecting the raw packets produced, when viewed in hexa-decimal will reveal comical network names, addresses and nicknames. Examples we have seen include:

- 0xEA7DEADBEEF - (EAT DEAD BEEF)
- KAHZ1E - (KAHZIE)
- ET AIRPORT

War driving London - what would hackers see

To augment the study, we undertook a basic “war-driving” exercise to establish the number of potential victim wireless networks in the locale of our honeypot. Conducting such an exercise is straight forward - you drive (hence the term war-drive) round the vicinity recording networks accessed with simple to use software like Netstumbler, Kismet or WIDZ.



In the survey area, we discovered 331 network cards. Of these, 208 represented Access Points which are potential entry points for hackers onto the corporate network. This figure is nearly double the number detected in 2002.

Less than half (45.19%) of these access points had encryption configured. This means that the majority of all network traffic could be intercepted by anyone with a PC, although this is a small improvement on the 2002 figure of 37%. During the assessment, there was no use of MAC-address protection identified.

A worryingly high percentage (26.44%) of networks were using manufacturers default settings.

A total of 36 identified the name of the organisation and two were obviously banks. This makes target selection easy for the hacker. We are still not sure what the network named “gorgeous” represented.

Glossary

Access point

- special devices which join a wired network to a wireless network and are potential entry points for hackers onto the corporate network.

Passive scanning

- method of detecting nearby networks with specialised software that produces zero noise on the victim network by only listening for wireless traffic.

Active scanning

- method of detecting nearby networks with specialised software that asks for victim networks to respond. 802.11 - the current standard for wireless LAN technology. This is commonly called WiFi or wLAN.

802.11/ IEEE 802.11

- the IEEE’s proposed standard for wireless LANs which is being used extensively.

MAC-address protection

- a way of adding allowing access to a network based on the ID of the network card being used.

If you have any further questions please contact
Mark Osborne, Director of Security Engineering:

e: mark.osborne@kpmg.co.uk
t: +44 (0) 20 7311 5468

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

The wireless hacker project March 2003

Designed and produced by UK Creative Services London Information Graphics

No: 204494