http://www.msnbc.com/news/824622.asp?cp1=1
Hackers target wireless networks
Worldwide 'war drive' set for Saturday
By William M. Bulkeley

Oct. 23 - Technology sophisticates who specialize in exposing corporate-security lapses will orchestrate a world-wide "war drive" to strut their stuff Saturday.

IN 25 LOCALES in seven countries from Alberta, Canada, to New Zealand, they plan office-building drive-bys armed with laptops, radio scanners and antennas, aiming to intercept signals from the ever-spreading wireless networks used to connect corporate computers with each other and the Internet.

For many of the hacker types who will participate, war driving is a benign electronic scavenger hunt meant to alert companies and others to unprotected wireless access points that can leave owners vulnerable to spying or sabotage.

MARKETING OPPORTUNITY

But to computer-security experts, "war-driving" has turned into a marketing opportunity. Past war drives embarrassed a number of companies, and in preparation for the big event this weekend, some of these experts have been pitching their services.

This week, for example, International Business Machines Corp. has been urging sales representatives to warn corporate clients of the need to secure their wireless networks. The merchandising tie-in: Your network can be safeguarded by an IBM security service that goes for $15,000 to $30,000.

In London, risk experts at the British affiliate of accountants KPMG LLP have developed a fake wireless network called a "honeypot" that was announced at a security conference in Paris last week. It's a countermeasure designed to attract and record unauthorized wireless-access efforts-in effect, alerting network owners that they are being homed in on by war drivers or other unauthorized people. The firm hopes that the honeypot will enable it to sell more of the security services it offers through its consulting arm. Among the services: a team of "tame hackers" who attempt, under contract with the owners, to break into financial-service-company networks to expose risks.

Another company tuned into war driving is Guardent Inc., a Waltham, Mass., computer-security firm that offers monthly assessments of its customers' networks to spot rogue access points. "We make sure people are aware" of the war drive because it shows the need for vulnerability analysis, says Jonas Hellgren, director of product management at Guardent. But he adds that focusing only on the event isn't as valuable as a continuing sales effort.

War driving bedevils security types partly because it is so cheap and easy to do. Drivers amble around with a directional antenna sometimes fashioned from a coffee or potato-chip can. Their software of choice, called NetStumbler, comes free on the Web and detects the low-level radio waves coming out of wireless-network access points.

War drivers say their goal is to publicize the need for network owners to change their passwords. But people with knowledge of the location of an unprotected wireless network can also use it for free Web surfing, or to send out e-mail messages or junk mail known as spam without disclosing their identities. With more sophisticated hacking, people could use the wireless gateway as an entry point to corporate networks, security experts say.

In a related activity, called "war-chalking," participants make chalk marks on sidewalks or building fronts to signal the availability of access points. One widely used symbol for an open access point looks like this:)(. Knowing such locations permits people with laptops to avoid paying for Internet access.

In its letter to customers, IBM notes that "war driving participants generally map unsecured access points as a hobby." But it warns "since your company has a great deal invested in intellectual capital, reputation, and stakeholder trust, it makes sense to take appropriate steps to avoid unnecessary exposure."

'MORE PARANOID'

War driving was christened two years ago by Peter Shipley, a Berkeley, Calif., data-security consultant, who named it with a nod to the "war-dialing" exploits of hackers who use phone lines in their efforts to penetrate corporate computer networks. Mr. Shipley, who isn't involved in the current war drives, says that in urban areas there are now so many wireless access points that mapping them is almost irrelevant. Still, he says, war driving has been making companies "more paranoid, which is what they should be."

War drivers generally need to be within 1,500 feet or less of an access point to detect it. NetStumbler is designed to pick up wireless access points in which the owner has failed to change the default Service Set Identifier that broadcasts its location for others on the network to find. According to various Web sites, popular home wireless networks made by Linksys Inc. use the default "linksys." For Cisco Systems Inc.'s more expensive corporate networks, the default password is "tsunami." Cisco declined to comment but said that extensive security capabilities are built into its wireless equipment.

John Girard, a security consultant with Gartner Group, Stamford, Conn., says war driving "is easy to do because people don't turn on security. They leave themselves exposed." But he says vendors are partly to blame. "The documentation people get is generally poor, and they're not motivated to figure it out."

According to the Web site worldwidewardrive.org, organizers with screen names such as Roamer, Big Ezy and Tapper are helping coordinate Saturday's drive. They either declined to comment or didn't return e-mails for this story.

This will be the second such organized effort, following one in August. War-drive Web sites feature maps showing unsecured access points, denoted by green circles along highways in such technology centers as Boston; the Silicon Valley and Orange County in California; and Barcelona, Spain. According to a table of statistics, nearly 30% of the access points found were using the default passwords.