CONFIDENTIAL

CSIS INTELLIGENCE BRIEF

IB 2002-3/09 2002.08.29

[redacted]

ALBERTA INTERNATIONAL "WAR-DRIVING" DAY: WIRELESS COMPUTER NETWORK INSECURITY

SUMMARY

Many entities within the retail, health care, financial services, education and public sectors in Canada have adopted the use of wireless computer networks because of their ease of installation, low cost and of the mobility they offer. (U)

Hackers can break into wireless computer networks in homes, businesses and government offices using a laptop or portable PC, an antenna, a wireless access card and wireless-sensing software. The action of using these tools in a vehicle to locate and exploit such networks is called "war-driving." (U)

A number of cities in BC, Alberta, Saskatchewan, Ontario and Nova Scotia have been the focus of war-driving activity and the results were presented on Internet Web sites. The first International War-Driving Day is slated to occur worldwide on 31 August 2002.

Stephane Currier

Glen Brassard
2003-02-24
2:30 pm

HANDLING INSTRUCTIONS

GENERAL

Unless otherwise indicated, CSIS agrees that this report may be distributed THROUGH AUTHORIZED INTELLIGENCE CHANNELS to government personnel possessing the APPROPRIATE SECURITY CLEARANCE and having a CLEARED TO KNOW the information contained herein.

SECURITY INSTRUCTIONS

Classified material must be handled, stored and communicated in accordance with Government Security Policy requirements.

USE OF SINGLE SOURCE INTELLIGENCE REPORTS AND BRIEFS: Unless otherwise indicated, single source intelligence reports may be used in compiling intelligence summaries or reviews provided:

(a) the material incorporated in paraphrased and preferably disguised with collateral information and attributed, i.e. "According to a CSIS report...";

(b) the summaries or reviews receive at least the same security classification and are subject to the same handling and security instructions as the original single source reports.

LIAISON REPORTS: This indicates that the report has been obtained from a foreign intelligence or security service through established liaison channels. No independent description of the source, estimate of source reliability, or evaluation of the validity of the information is normally available beyond that provided by the originating service. Unless otherwise indicated, the gist of such reports may be incorporated into intelligence summaries or reviews, but verbatim quotations are NOT permissible and the paraphrased text must not reveal, even by implication, which liaison service provided the intelligence. Liaison reports are made available to CSIS on the understanding that they are not passed on to nationals of any third country. Canadian officials may not, therefore, divulge the contents of Liaison reports to any but other Canadian officials as set out in the Handling Instructions above.

EXTRACTING AND COPYING: Where it has been agreed that a department may extract or copy single source material for retention on file, such files must be accorded the same handling restrictions and security classification as the original single source reports from which they are drawn, and should be attributed to CSIS.

PHOTOGRAPHS, PLANS & SKETCHES: Photographs, plans and sketches attached to single source reports may not be copied or otherwise reproduced without the consent of CSIS.

SOURCE DESCRIPTIONS: Source descriptions are drafted in such a way as to assist clients to appreciate and utilize the information in single source reports. Clients will, of course, recognize the need to protect the identity of sources.

Any queries with respect to the material or these instructions should be addressed to CSIS.

Introduction

1. Many entities within the retail, health care, financial services, education and the public sector have adopted the use of wireless computer networks because of their ease of installation, low cost and of the mobility they offer. A number of these networks are not configured in a secure manner, and many hackers know how to exploit this vulnerability. As a result, wireless hackers (sometimes called "wireless") can break into these computer networks in homes, businesses and government offices using a laptop or portable PC, an antenna, a wireless access card and wireless-sensing software. The action of using these tools to locate and exploit such networks is called "war-driving"[1] or "war-walking", depending on the form of transportation used. Hackers worldwide, including some in Canada, will be participating in the First International War-Driving Day, scheduled for 31 August 2002. (U)

The First Alberta International War-Driving Day

2. A number of computer enthusiasts and media-related Internet Web sites provide the results of war-driving scans that have occurred in the US, the UK, Europe, Australia, and within Canada in BC, Ontario, Nova Scotia, Saskatchewan and Alberta.

3. A computer enthusiast from Edmonton issued a press release on 21 August 2002, stating that he was arranging a war-driving exercise in Red Deer, Alberta, on 31 August 2002 as a component of the internationally scheduled event. He stated that wireless networks in Calgary, Edmonton and other communities in Alberta had been mapped, and that he was undertaking a significant scan of Red Deer. (U)

4. Wireless technology makes it easier for system intruders to search for data and invade the privacy of network users, since computer networks have no physical barriers.

[1] The term "war-driving" is derived from the term "war-dialling," which is the process of using a computer, modem, telephone and a computer program to identify phone numbers that can successfully make a connection with a computer modem. The program automatically dials a defined range of phone numbers and logs and enters in a database those numbers that successfully connect to the modem. Some programs can also identify the particular operating system running in the computer and may also conduct automated penetration testing. In such cases, the computer program runs through a predetermined list of common user names and passwords in an attempt to gain access to the system. As a result, the terms "war-driving" and "war-walking" describe the mobile process of scanning for wireless computer networks using laptops or portable PCs, and wireless access cards and antennas. (U)

Vulnerabilities of Wireless Computer Networks

5. Given the right tools, it is easy to detect the existence of a wireless network and determine if the network is open, closed or protected. While most wireless networks and LANs can encrypt network traffic using the security protocol Wired Equivalent Privacy (WEP), a capability of the wireless network software, many administrators do not enable this capability.

There are numerous reports in the media of hackers breaking into wireless LANs with off-the-shelf software tools such as AirSnort or WEPcrack. Any wireless computer network that provides a potential route to valuable resources requires more security than that offered by WEP. (C)

9. Wireless computer network vulnerabilities can be reduced