SOPHOS

Project Warbike: Keeping It Legal

By **James Lyne**, Director of Technology Strategy

One of the big challenges we faced with this experiment was making sure that we stayed within the confines of the law while collecting useful data on Wi-Fi security. Of course, hackers and cybercriminals aren't going to stay within the law, and we recognize that the picture for Wi-Fi security could be even worse than what we found.

However, the results of our experiment do reveal a problem and help us raise security awareness with non-technical users.

Project Warbike: Keeping It Legal

Briefly in this document we outline the processes and practices we used to make sure that our experiment stayed within legal confines. If you have any concerns or questions please contact us at warbike@sophos.com.

1. We made no attempt to join or access any network.

2. We used the normal 802.11a/b/g/n wireless protocols as you would when walking down the street with a smartphone listing wireless networks you could connect to.

3. We did not use promiscuous mode, injection or other abnormal features used by penetration testers or hackers as they violate normal use of wireless and attempt to penetrate or hack systems.

4. We did not capture or store wireless data packets as has been the case in high profile and contentious cases related to wireless scanning over the past couple of years. Our configuration was set to not capture such information, only wireless network announcements.

5. We kept data on the wireless network names, locations and security levels long enough for us to do analysis, in accordance with regulations about holding data for an appropriate period of time for business use. We will not keep this data or release the names and locations of insecure networks.

6. We registered networks as open, WEP encrypted, WPA or WPA2, based on the broadcasts they normally make to networks in the area. We did not identify networks which were marked as hidden as part of this test. It is likely there are a large number of networks set to hide their SSID. But as discussed in our top tips for securing your wireless network, an attacker can easily discover them. We didn't do this in our test to stay within the law.

7. We didn't perform any active tests on wireless network security beyond capturing the type of protection. For example, a network may be using WPA2 AES, but the password may be "password." We didn't check credentials as we wouldn't have been able to secure permissions from the owners of the networks.

8. We used transmitters/receivers within the legal limit, not extreme high-power antennas, although these could have uncovered more networks and cybercriminals would not hold back from using them.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Article 08.12v1.dUK

SOPHOS