GhostNet cyber-spying network uncovered

A Chinese spying network, dubbed *GhostNet* by the Toronto researchers who uncovered it, has been found to have taken over more than 1,000 computers in 103 countries, up to 30% in "high-value sites" including foreign ministries, embassies, international organizations and news media

ANATOMY OF A HACK

Location: http://www.website.com

"Social engineering" attack: User downloads *gh0st RAT* software either via web link to infected site or as email attachment

Trojan: Hacker gains access to internal files

Webcam, microphone: Hacker able to operate attached audio and video devices to monitor surroundings

Hacker can send and receive files

COMMAND AND CONTROL
GhostNet servers

Sweden ❶

Southern California **1**

1,295 computers infected

❷ South Korea

❶ *Control servers enable hackers to control network via simple website*

0 *Command/ control servers also host **malware** – bad software – downloaded by unsuspecting web users*

Beijing: Denies any involvement in cyber-crime. No conclusive evidence of state involvement

❸

CHINA

❹ ——— Jiangsu

Sichuan ———— **2**

Guangdong

Hong Kong

Taiwan

❺

3

❻

Hainan Island Location of *Lingshui Signals Intelligence* facility

4

CHINESE HACKS
2008: White House computer system
2007: Pentagon network
2003: *Titan Rain* attacks on U.S. Department of Defence