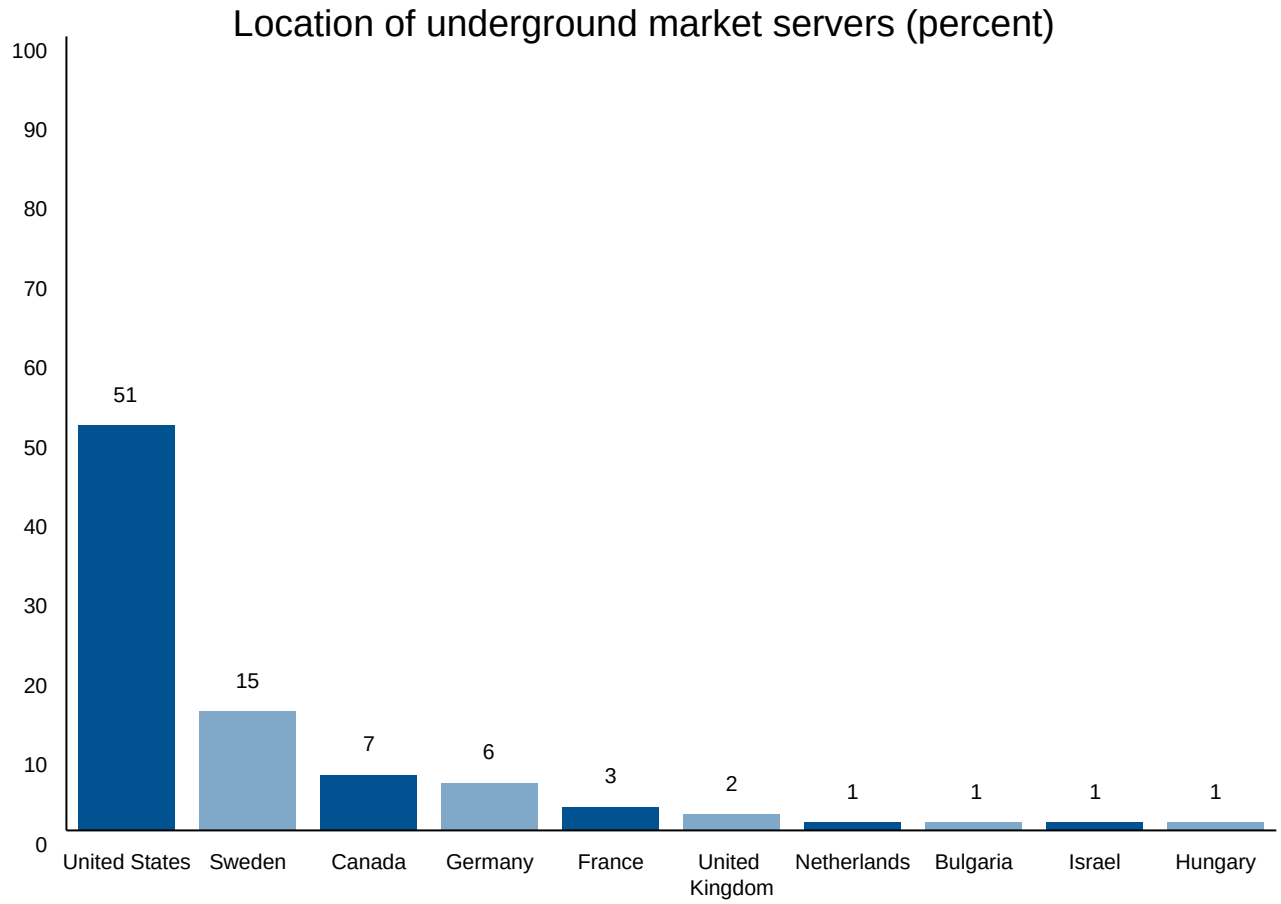
Crime Facts Info

Australian Government
Australian Institute of Criminology

No. 148 15 May 2007

Underground markets in stolen digital information

Malware (e.g. worms, viruses, backdoors and Trojans) facilitates high tech crime by providing criminals with the means of installing programs on computers that allow them to engage in criminal activities without the computer owners' consent or knowledge (for further information see Choo 2007). Financially motivated criminals and malware authors continue to develop malware to steal personal information, such as bank and online gaming account details. This stolen information can be used to facilitate other crimes such as identity theft and extortion. The availability of an underground market in which to sell stolen digital information provides criminals with more financial incentives to offend. The chart below shows the main locations of servers hosting such underground markets, with 58 percent located in north America and 39 percent in western Europe (Symantec 2007), as might be expected in countries with extensive computer infrastructure. Australia was not considered one of the top 10 countries with underground market servers.



Source: Adapted from Symantec 2007: Fig 2

References

Choo R 2007. Zombies and botnets. *Trends & issues in crime and criminal justice* no. 333. http://www.aic.gov.au/publications/tandi2/tandi333.html

Symantec 2007. *Symantec internet security threat report* vol. XI March. http://www.symantec.com/threatreport