Australians could be charged for WikiLeaks site attacks: expert

December 14 2010

Australians who took part in attacks that brought down the websites of firms refusing to transfer payments to WikiLeaks may find themselves in breach of the law, a University of Sydney cyber-security expert says.

Last week a Low Orbit Ion Cannon (LOIC) 'botnet' network brought down Visa, MasterCard and PayPal websites after overloading those sites with requests from individual computers. These requests, made in response to the companies' refusal to make payments to WikiLeaks, were generated after controllers of the LOIC botnet commanded thousands of members to bombard the sites.

Professor Michael Fry from the School of Information Technologies says LOIC members who responded to the call to bring down the sites were potentially in breach of computer crime laws.

"If readily identified, the owners of the machines participating in this LOIC botnet could see themselves charged with abuse of computer facilities," Professor Fry says.

Professor Fry says it is unusual to see so many people willingly partake in such cyber attacks, known as distributed denial-of-service (DDOS).

"Usually DDOS attacks occur after 'botmasters' illegally take over thousands of computers, turning them into 'zombies' that can be used for illegal activities including spam generation, identity theft and extortion through denial of service. More often than not, the primary users of

zombie machines are unaware their computer has been infected and used for illegal activity. By some estimates one in four home machines connected to the internet and one in eight corporate machines are zombies.

"What is fascinating and novel here is the latest attacks involved thousands of willing participants who knowingly allowed their machines to be infected in order to participate in politically motivated attacks. This suggests a huge level of emotive support for WikiLeaks and its activities, but also a level of naivety. It seems members of the group downloaded publicly available LOIC code, but took no steps to evade discovery and identification, unlike criminal botnets which use sophisticated evasion techniques. This makes members vulnerable to detection, potential prosecution and counter-cyberattack. Counter-attacks have indeed happened today, initiated by US political groups.

"Whether or not legal action is taken against offending participants is a thorny issue. This cyber war is gathering pace and prosecutions could generate another round of attacks. Either way we are seeing the beginning of a new era in political cyber-warfare with the widespread use of botnets."

Next year the University's School of Information Technologies and Centre for International Security Studies will jointly teach a postgraduate cyber-security course, developed in response to growing cyber-warfare.

Provided by University of Sydney