Hackers Posing A Threat To Industry

A*nonymous* is a loosely associated hacktivist group. Hacktivism being the use of computers and computer networks as a means of protest to promote political ends. *Anonymous* originated in 2003 on the imageboard 4chan, representing the concept of many online and offline community users simultaneously existing as an anarchic, digitised global brain. It is also generally considered to be a blanket term for members of certain internet subcultures, a way to refer to the actions of people in an environment where their actual identities are not known. It strongly opposes internet censorship and surveillance, and has hacked various government websites. It has also targeted major security corporations. In public, its members are distinguished at various protests by wearing Guy Fawkes masks.

In July this year, *Anonymous* supported a protest against the tar sands oil industry, which ended in protesters dancing on the meeting table of the Governor of Montana.

Anonymous networked like ants in the internet to get word out about this civil disobedience, and about the issue at hand. Anonymous spent weeks researching the corporations involved, uncovering mountains of email addresses and contact info of employees who Anonymous considers to "work to destroy our planet for profit."

The group was in protest of the Keystone XL pipeline and made a week-long information campaign against the project and spread word of Washington D.C. protests where over 850 people were arrested at the White House for peaceful sit-ins.

Anonymous said, "our journey has manifested into a full-on conquest to expose the corruption in the companies who plan to mine this oil and build the Keystone XL pipeline from Canada to the Gulf of Mexico."

Anonymous proceeded to release hundreds of corporate emails that were obtained from servers of oil industry websites. The mailservers of Transcanada were shut down for two days.

At the time, Wikileaks, a group that Anonymous supports, published a series of cables and according to Anonymous: "directly prove that Statoil corporation, a major player in the tar sands industry, has fired workers in Venezuela for their political leanings, in collusion with state-owned petroleum company PDVSA."

The Embassy Caracas Venezuela cable reference number 08CARACAS264 stated, "Norway's StatoilHydro received a far more lucrative compensation package for its lost equity in the former Sincor strategic association than reported in the press."

Another quotes Canadian Environmental Minister Prentice as saying he is deeply concerned with the effect of the tar sands on the image of Canada," claimed Anonymous.

Group Anonymous is not the only hackers out there posing a threat to the Industry. On the 14 October the United States admitted they believe a series of cyber attacks on domestic banks and some foreign oil company's carried out over the last year are the handy work of a group of hackers linked to the Iranian government.

Leon Panetta, Defence Secretary said the cyber-threat from Iran has grown, and declared that the Pentagon is prepared to take action if America is threatened by a computer-based assault. The hackers are apparently part of a group of less than 100 computer security specialists from Iranian universities and network security firms, according to *theHackernews.com.*

American officials have said they are able to discover the source of the recent cyber-attacks. The Iranian official said Tehran has already offered help to boost the companies cyber-security, as Iran has itself recently been the victim of cyber-attacks on its offshore oil platforms.

The cyber-attacks hit the Saudi Arabian state oil company Aramco and Qatari natural gas producer RasGas using a virus, known as Shamoon, which can spread through networked computers and ultimately wipes out files by overwriting them. Iran blames Israel and the United States for the attacks.

In Australia there has been numerous cases of Group Anonymous cyber attacks on the Australian Government. With no reports thus far on any attacks on Australian based oil and gas companies. This is not to say it would or could not happen in the future.

The Australian Federal Police gave *PESA News Resources* some organisational-specific preventative hacking tips to readers including;

- Educating staff on maintaining the confidentiality of systems and information so as not to leave them open to corporate espionage.
- Implementing policies which do not permit employees to access social media sites at work, as these sites can allow malware to access company systems.
- Maintaining firewalls and other protective measures across the workplace network.
- Information Communication Technology (ICT) organisations spend a lot of time, money and effort on identifying potential vulnerabilities in their products and providing 'patches' to the public to overcome this.
- However, it is still up to the individual user or company to ensure that they make the most of all the protection options available to them. ■

Members of the group Anonymous wearing Guy Fawkes masks in Los Angeles, 2008.