Cyber Espionage: Lessons to be learnt from Snowden Revelations

Article · August 2014

CITATIONS
0

1 author:

Muktesh Chander
Indian Institute of Technology Delhi
9 PUBLICATIONS **110** CITATIONS

SEE PROFILE

Cyber Espionage

Lessons To Be Learnt From Snowden Revelations

Cyber espionage is now targeting governments, corporates and individuals in an unprecedented manner. The perpetrator could be an individual cyber criminal, a group of hackers, non-state actors or states themselves. Cyber espionage is an attractive choice because of ease of operation, low cost, low risk, difficulty in attribution and high success rate.

Espionage has been an essential part of statecraft for ages. Chanakya, in his book *Arthashastra,* had laid great emphasis on spying on citizens, foreigners and enemies. During World War One and Two, espionage played an important role in deciding the outcome of the wars. The collection of intelligence related to defence, politics, economic matters, social and other important aspects of governance of a country by another has been an accepted fact. From traditional spying (human intelligence) to collection of intelligence from electronic signals (signal intelligence), the journey has been very interesting.

Today, out of the various other forms of intelligence collection methods such as human intelligence, imagery intelligence, open-source intelligence, telemetry intelligence, measurement and signature intelligence etc cyber intelligence has become very important in last few years because of the use of computers, networks, information and communication technology in every sphere of human activity globally. This is inevitable as cyberspace has emerged as fifth strategic domain after land, sea, air and space. With Internet packets flowing through radio waves, cables and other media, this is the golden age of spying.

Several intelligence agencies including National Security Agency of USA, Mossad of Israel, Government Communications Headquarter of UK, Government Communications Security Bureau of New Zealand, Australian Signals Directorate, Federal Security Service of Russian Federation, Communicating Security Establishment of Canada, have developed impressive cyber intelligence collection capabilities.

Industrial espionage has also been receiving attention these days due to theft of valuable intellectual properties and other vital information using cyber means. Several multinational companies have fallen prey to industrial espionage through exploitation of their computer systems. In November 2010, Xiang Dong Yu, a ten year veteran of the US automaker Ford Motor Company, admitted in Federal Court that he stole 4,000 secret design documents, worth more than US$ 50 million from company computers and shared them with a rival company. A major Manesar based multinational IT company has reportedly shifted its US$ 10 million R&D facility to Australia due to an incident of data theft in electronic form, which caused it an estimated loss of ₹ 7.54 billion.

Cyber espionage is now targeting governments, corporates and individuals in an unprecedented manner. The perpetrator could be an individual cyber criminal, a group of hackers, non-state actors or states themselves. Cyber espionage is an attractive choice because of ease of operation, low cost, low risk, difficulty in attribution and high success rate.

In June 2013, Edward Snowden disclosed thousands of classified documents revealing global surveillance programme by USA in association with some other countries collectively called "Five Eyes". For many cyber security researchers, Snowden revelations have not come as a surprise. Several cyber spying projects such as ECHELON, TOTAL INFORMATION AWARENESS Programme, MAGIC LANTERN, CARNIVORE, CYBER KNIGHT etc have been in news for a decade. It is the depth and spread of the surveillance programme, revealed by Snowden, which has surprised the world. Even before Snowden revelations, Julian Assange, the head of WikiLeaks had said "Facebook in particular is the most appalling spying machine that has ever been invented". Another startling aspect of the revelation is the willing or coercive cooperation offered by several Internet companies.

Snowden revelations offer us lessons which are of two types. The first obvious lesson is the threat to cyber assets of organisations from the insiders. Insider threat from disgruntled employees or ex-employees pose great risk to the organisation as they are conversant with the vulnerabilities and weaknesses of IT system of the organisation. Former employees, contractors, third party agents, partners and casual employees also pose similar threats.

Insiders can bypass physical and technical security measures designed to prevent unauthorised access. Insider threat mitigation involves monitoring employee activities, training, motivation, reward and punishment regime, deploying technical measures to guard against data pilferage, analysing access logs and other data and creating a culture of cyber security.

The other lesson, from the Snowden revelation, is the fact that cyber espionage is being employed by states in an unprecedented manner through which it is possible to spy on every single individual on this planet who is using Internet. "Tracking Ghost Net: Investigating a Cyber Espionage Network" report from Information Warfare Monitor documents a cyber espionage network in 103 countries whose victims included ministries, embassies, international organisations etc. Another report by the same agency titled "Shadows in the Cloud" reveals cyber espionage operation targeting computer networks in India and several other countries. Several social media networks were reportedly used for this purpose.

"Operation Aurora" attack on Google and other companies highlighted the danger from advanced persistent threats using zero-day-exploits. Although in cyber espionage, several methods are employed, use of "Spear phishing" attacks is very popular. In this kind of attack, the details about the target individual are obtained from social media, Internet and other means. A well crafted email, with a malicious attachment, is then sent to the target. The mail is either sent from a compromised account of a trusted entity or resembling it. The possibility of opening such mails, by unsuspecting and untrained person, is very high. On opening the attachment the target computer gets infected and attacker is able to take out all information from the target machine using command and control servers located anywhere in the world.

In 2012, "Flame", one of the most sophisticated malware of 50 MB size, targeting several countries in Middle East, for the purpose of cyber espionage, was discovered. In most of the cyber espionage cases, attribution is difficult due to the inherent nature of Internet, however, analysis of the malware pointed out involvement of certain states or state-sponsored-actors.

Cyber espionage by various entities is becoming a serious threat to the national security. We need to guard against this asymmetrical warfare by hardening our systems. The critical information infrastructures of the country need to be guarded ferociously through well defined policies and guidelines. In January 2014, National Critical Information Infrastructure Protection Centre of Government of India has been notified under Section 70-A of the Information Technology Act, 2000 along with its associated rules. These guidelines need to be implemented mandatorily in all critical and sensitive organisations. The corporate world also needs to adopt cyber security framework developed by Data Security Council of India or ISO 27000 series of information security standards as mandated under the Information Technology (Reasonable Security Practices and Procedure and Sensitive Personal Data and Information) Rules, 2011. Several concrete measures need to be taken to deal with the cyber espionage. Some of which could be:

- Sensitisation of the top management of the sensitive organisations and the government functionaries about the threat from cyber espionage.
- Identification and classification of vital information assets of organisations and country.
- Adopting a holistic information security management approach.
- Appointment of Chief Information Security Officer in every sensitive organisation / ministry.
- Providing adequate resources for information security function in proportion to the value and sensitivity of the information being protected.
- Use of indigenously developed operating systems, encryption algorithms and ICT products.
- Implementation of Guidelines for Protection of Critical Information Infrastructure of the country.
- 24x7 monitoring of Indian cyberspace for cyber attacks and taking necessary action towards prevention, prediction, early warning, detection, mitigation, response, deterrence and retaliation.

While we are planning to leverage ICT for the growth of the nation and marching towards smart cities, we must simultaneously take adequate cyber security measures so that this march is not halted or retarded due to cyber espionage. In cyber war and cyber terrorism, adversary is bound to use cyber espionage as a strategic tool and hence we need to be prepared to deal with this challenge. This can be achieved through active defence. The right of a sovereign state extends into cyberspace also and protecting Indian cyberspace is equivalent to protecting the sovereignty and integrity of India. The Treaty of Westphalia should not be presumed to be dead in cyberspace. DSA

MUKTESH CHANDER, IPS

The writer is Special Commissioner of Police heading Delhi Traffic Police. Prior to this he was Joint Commissioner of Police, Prime Minister's Security. He is former Centre Director of Centre for Cyber Deterrence and Information Assurance in NTRO, Govt of India. He has been DIG of Police, Goa, Additional Commissioner of Police Crime and Traffic, Delhi and Inspector General of Police, Daman and Diu. He graduated in Electronics and Telecommunication Engineering from Delhi University in first class with distinction. He also holds a law degree from Delhi University and Masters Degree in criminology. He has submitted his PhD thesis in Information Security Management to IIT Delhi. He has been awarded Police Medal for Meritorious Service and President's Police Medal for Distinguished Service.