Summary of Cyber Threat Intelligence

Nandanam Vikas

02/11/2016

The seminar was regarding the cyber attacks/threats. The talk has covered few interesting aspects of the security and also described how important it is to get protected from cyber threats. Few examples were given on cyber attacks like FIN4 which came under phishing attack. The other was the attack on bank where the network was disturbed by installing new devices on banks networks and huge amount of money was stolen. The other interesting point was the 80-20 principle which stated that 20% of hackers perform 80% attacks and others 80% are just the threats.
To get secured from cyber threats, there are three important components
i)**Information Security**: Here all the information regarding the threats are collected.
ii) **Intelligence Analysis**: The collected information is analyzed and finds for anomalies.
iii) **Forensic Science**: If any anomalies are found, here it is used to find out the individual or group which are attacking and deals with legal procedures.

The fact about cyber threats is that only 1% of attacks were detected. By the above fact it can be sensed that it is very difficult to prevent cyber attacks because of asymmetric nature of the attacks. All the attacks mentioned above can be prevented by using a better firewall but even having a good firewall also may lead to attacks. The Sony attack is good example where having a good firewall protection also lead to cyber attack. But by taking few measures the attack can also be prevented, even in Sony attack before the main attack occurred they have found 25 small attacks but it was not concentrated at root level which later was a huge threat to the company.
There few difficulties for cyber threats to detected like

1. Hidden threats

2. ISIS threats (Where should analysis look for)

3. Political threats (lack of actionable intelligence) and

4. Finally too much data, too many services.

Reflection:
The seminar has given the knowledge on cyber attacks and its ways of attacking. The talk has shown where the present cyber security stands. The most interesting point is that having invested huge amount of money in cyber security only 1% of threats are detected. It can be considered that having a better security is not enough but taking preventive measures the threats can be detected at root level and can prevented from further big attacks. The way of implementation of cyber security should be changed in order to detect more threats. It can be observed that threats/attacks can be occurred at any time, so to provide better security preventive measure have to be taken by keeping continuous observation i.e if system detects any passive attacks/threats there should be an immediate action taken and mitigate the threat at root level so that it doesnt become a huge threat in future.

This is my github repository link: https : //github.com/Nandanam/Cyber − Threat − Intelligence.git