A Summary Report on Cyber Threat Intelligence

Siva Chintapalli

February 11, 2016

Cyber Threat Intelligence

In CTI (Cyber Threat Intelligence) session first introduction about Bob Stasio work experience and his accomplishments. Bob is currently employee at IBM i2 safer planet as a senior production manager for cyber analysis. He also worked for government as Cyber Commander at NSAs Cyber Center, U.S Armys Signals Intelligence Corps, the FAA and NASA. Bob started explaining about Cyber Threat Intelligence and why is it necessary. According to Bob everyday some where there is a Cyber Attack occurs identifying these attacks are very difficult. As we compare with Cyber Crimes investigated so far is 1percent. Bob explained about type of attacks how they can be? For some type of attacks physical we need to insert some type of devices to get in to network for some are fishing attacks. An example given by Bob was A couple of months ago a former trader in Wall Street tried to steal the credential and pass them to hackers in Ukraine. Another example is how a person walked in to bank as IT technician and installed device in bank and robbed 1.3 billion. These type of attacks are hard to identify. There is an 80-20 rule which can be minimize the attacks. If u have good fire wall we can prevent 80percent of attacks only 20percent of attacks are critical when these type of events occur how to respond to them is critical for these event we need extra measures. There is another type of attack which happen in Sony. In these attack first they intrude in to network and stay in network and start exploits bit by bit and gain access to the network completely in 6 months and steal the 30GB information. What is Cyber Threat Intelligence?

The basic idea behind the cyber threat intelligence is taking a security measure on timely manner, when we recognize the indication of attack.

There are three components which are mainly need to focus when we start Cyber Threat Analysis.

1. Information Security

2. Intelligence Analysis
3. Forensic Science

There are four main point why we are no able to identify attacks

1. There are so many hidden threats.
2. Where should we look while analyzing the issues
3. There is a lack of actionable intelligence.
4. There is too much data and too may resources.

Before he conclude about the session he explained about an EIA tool that is developed in IBM for Cyber Analysis. There are three aspects that EIA tool covers, search program logs periodically and discovering the Beaconing Activities that occurs in network and save some parameters for alerting if any suspicious activity occurs. He concludes with cyber security isnt easy for anyone, over the time and analysis only we can prevent them. He ended the session with interactive Questions.

Bob Stasio is inspired us with his speech and he has projected the problem what real world is facing with beautiful examples. From his experience he gave few examples what might happen and what analyst might have been done to minimize the effect. These examples has gave me the clear understanding on attacks and how we are facing with security. What we need to do to prevent them happening by learning the incidents that are happened. What I realized from this session is attack on security is not a onetime activity, its a continuous event which occurs over the long time. Because of this we need to monitor the events and analyses those activities and think intelligently and take the appropriate measure to prevent them. I am looking forward to know more about the EIA tool.

https://github.com/SivaChintapalli1/SecurityAlgorithm.git