Summary & Reflection on "Cyber Threat Intelligence by Bob Stasio"

Saranya Radhakrishnan

02/11/2015

Summary

Bob Stasio, Senior Product Manager for Cyber Analysis at IBM i2 Safer Planet, shared his knowledge and experience in the field of Cyber Threat and Analysis on 10^{th} February , 2016.

Being part of many global financial firms like Bloomberg, he gave the example of FIN4, a group responsible for getting insider information for stock trading. This group fetched email login credentials of some individuals who were known to have confidential information. Using the information from these individuals they traded on the financial markets to make approximately $100 million.

The speaker also spoke of the most recent $35 million attack on Sony. According to the speaker, the attackers were present in the Sony's network for a number of months in order to successfully break it. The attackers made multiple attempts to break the system. Each failed attempt taught the attackers where they were going wrong. So, they made appropriate changes for their next attempt and eventually breaking the system.

Speaking on Cyber Attacks, he mentions that 80% of the attacks can be successfully blocked by taking small precautions, but it is the remaining 20% are the most difficult one's to block. The four points to consider for Cyber Security are as follows :

1. Finding the Hidden Threats in a Network
2. Finding the anomalies in the network.
3. Analyzing the anomalies and their relations with each other.
4. Understanding the implication of each anomaly and mitigating the attack.

So,In order to provide Cyber Security, Cyber Analysis is of utmost importance. Cyber Analysis can be broken down into 3 parts as mentioned below.

1. **Information Security** : which deals with ensuring safety of data using various methods. Protecting the data from malware to ensure confidentiality.
2. **Forensic Science** : which deals with gathering and processing appropriate information to form evidence.
3. **Intelligence Analysis** : which deals with processing the gathered information in order to take appropriate decisions. It deals with collecting, processing, analyzing and distributing of appropriate data.

The speaker concluded by saying that one can never master all the three sub divisions of Cyber Analysis but we can always start with one of them. Being from a non military background, mastering Intelligence Analysis can be a difficult task but Information Security and Forensic Science are available for civilians.

Reflection

Bob Stasio was an inspirational speaker. His experience with financial giants like Bloomberg, NASA and military can be seen from the examples he mentioned during the session. His knowledge of the Cyber Threat and analysis system is awe-inspiring.

Being a person who is interested in the financial sector, his example of FIN4 attack struck the chord with me. The real-time examples were the highlight of the session. It helped us understand the steps undertaken to uncover Cyber Threats, Analyze them and eventually process them for legal actions.

After attending the session, I realized that Cyber Attack is a not a spontaneous activity. It is a continuous effort on the part of the attackers. In order to protect the system from attack, it is important that we monitor the activities and analyze them on regular basis. We should take precautions and improve the security based on the observations.

In the future sessions, I look forward to a more technical insight into the product i2 or any other tool available for Cyber Threat Analysis.

References

1. Bob Stasio

Link to the repository: GitHub Repository