Cyber Threat Analysis

Dixita Sharegar

Thursday, February 11, 2016

Cyber Threat Analysis as defined by Bob Stasio is the art of analyzing sparse multi-dimensional data sets by a group of people to identify the attack. It also includes identifying patterns and anomalies to get a holistic view.

The session started with examples of attacks like FIN4 where they used spear phishing attacks on pharmaceutical companies and the company suffered a loss of $ 100 million. The second example was one where the hacker used a KVM device to hack a bank of $ 2.1 million. He deployed the device on one of the bank servers and the money was transferred in 128 transactions. As we can see the hacker invested only $ 30 in the device and the bank must have invested a lot of money in its security system, there is an asymmetric relationship in the attack i.e. the amount of money invested by the hacker is very low and the amount of money invested by the companies for security is very high.

According to the 80:20 rule 80 % of the attacks or damage is caused by 20 % of the hackers. So to protect against the attacks we should implement a security framework and also perform cyber analysis. A security system is analogous to a medical system, so we have specializations or tiers in the system. Level 1 threats could be an individual hacker trying to get information from a user, which can be mitigated by changing passwords or removing unused services etc. Level 2 threats could include well planned and organized crimes and malware. This can be mitigated by monitoring the system regularly and using real time security analysis. Level 3 threats are the most dangerous threats (national level) that need cyber analysis and threat intelligence analysis.

Cyber analysis is made up of 3 main components information security, forensics science and intelligence analysis. Multiple datasets and information from various sources needs to be analyzed to understand a threat that is targeting an organization. Data from security alerts, system scans, user access logs, badge logs etc. need to be analyzed within an organization, whereas outside data from social media, government alerts, hacker forums etc. also need to be analyzed.

The four main problems in cyber security today are:

- Hidden threats in hidden network: how to find the data that indicates the threat.

- Where should analysts look: there is no defined place to look for data.
- Lack of actionable intelligence: What actions should be taken when you discover a threat and what the risks are?
- Too much data, too many sources: It is difficult to get a holistic view of the threat with too much information.

The tipping, queueing and anomaly research example specifies an event threshold maintained i.e. when number of threats occurred exceed the threshold limit an alert is generated. According to the example, minor attacks like phishing attempts, sending malicious emails were not paid attention too as they were below the threshold. All these minor attacks together caused one major attack in the later stage.

The IBM i2 Enterprise Insight Analysis is a cost effective tool that uncovers hidden patterns by analyzing massive amount of data. It helps in threat analysis by discovering beaconing activity, searching proxy logs etc.

What I learned

It is very important to analyze the data from various sources and try to get a complete picture. An example mentioned in the talk was that of an employee stealing sensitive information. First a list of employees who work late hours and take a huge amount of printouts was found. Then camera recordings were checked, social media accounts were monitored to find negative comments about the organization and at the end appropriate measures were taken so that the sensitive information is not leaked to the competitors.

Cyber threat analysis is huge in nature and it needs a lot of skilled resources and time. It includes

- Data collection from multiple sources
- Extracting information from that data
- Storing it in a safe place
- Analyzing the data to get a whole view
- Visualizing it to understand better.