Cyber Threat Intelligence - Summary

Sandeep Reddy Salla

February 12, 2016

It is also known as **Threat Intelligence**. The main aim of threat intelligence is to help organizations understand risks of external threats like advanced persistent threats, exploits, etc. It needs in-depth information to help organization protect from different types of attacks. Growth of asymmetric threats: It has become a problem among humans for providing information security. Attackers can login to any system and can hack data which can be useful in many ways. Hackers can log into any bank terminal and can transfer the money to different accounts. One percent of threats are stopped till date. Intelligence Time Horizon: There are different types of attacks; some of them are tactical attack, operational attack and strategic attack. As per the intelligence time horizon, tactical attack takes place in 1-5 days, operational attack can takes place in 5-60 days where as the strategic attack can take place in 61+ days.

Threat Examples and Mitigation Strategy:
Tier one- Hygiene: Threat Example: Hackers use widely used tools and the mitigation technique is to change passwords frequently, uninstall or remove the services that are unused.
Tier Two Specialization: Threat Example: Hackers use crime ware tools and the mitigation technique is monitoring, alerting, real-time security analytics.
Tier Three- Research: Threat Example: Hackers use high resources and advanced persistent threats and the mitigation technique is to analyse threat intelligence trend analysis and tracking them.

Cyber Analysis Discipline: It consists of 3 subcomponents. They are Information Security, Intelligence Analysis and Forensics Science. Confidentiality, malware, network defence threats comes under Information technology where as in Intelligence Analysis the Intel cycle collects the information which is processed and analysed and in Forensic Science consists of investigative process, evidence discovery and handling. Results of Cyber Analysis are threat discovery, enterprise awareness, risk management, enabling the decisions, etc.
Cyber Analysts has an in-depth understanding of the threats that can target any organization. Strategic Intelligence for Machine enabled Real-time processing and security operations come under security intelligence platform. In Real-time processing, anomalies have been detected, correlates real-time data, etc where

as in security operations it manages the workflow, graphing, reporting of the events and activities.

Strategic Intelligence for Human Enabled: Multi-Dimensional Analysis and Human-Led Intelligence Discovery come under Cyber Analysis Platform. In Multi-Dimensional Analysis all source intelligence can be analysed, discovery of anomalies and visibility of ecosystem. Decision making products for leaders, analysis of physical data, linked data can be visualized; all these come under Human-Led Intelligence Discovery.

Lessons Learned:
Bob Stasio explained about 80-20 rules, which means 80 percent of the work done by intelligent people can be done by only 20 percent of the hackers. It clearly states that, hackers are more advanced. Each and every individual has to be more careful in securing the data. They may steal our personal information like contacts, photos, and may valuable information like credit card details, bank account details if we store at any place. One of the example, while browsing the internet we get so many alert messages, which is asking for you to enter your username and password for login. They will create similar structure which is same as that of any official website. If an attacker hacks into any bank, companies, it will be huge loss in terms of information, money, etc.

Resource:
`http://www.slideshare.net/IBMSmarterovernment/ib-mi2-cyber-awakening-rsv1-52141947`

GitHubRepository:
`https://github.com/ssreddy2020/CyberThreatIntelligence`