Cyber Threat Intelligence

Bhargav Uppalapati

02/11/2015

One of the main challenges facing security developers, analysts and organizations is, implementing security protocols and services cost effectively and efficiently on the existing infrastructure. Major Cyber security threats are generally targeted towards huge government or private establishments. Cyber threat analysis helps secure data. The analysis helps understand different threats involved to sensitive data and also helps catch the responsible for an attack. Before understanding cyber threat analysis, it is good to understand what a threat and what a cyber analysis is.

Threat: anything that prompts intrusion, interfering or destruction of any profitable service in an organization. The threat can be of "human" or "nonhuman" root, threat investigation must examine every component that might lead to a security risk. Cyber analysis is learning data vulnerabilities hidden in the system or threats hidden in the network. With respect to cyber security, this kind of threat-oriented approach helps prevent attacks from happening and also retaliation in case of an attack. Also, the intended outcome of threat analysis is increasing security efficiently and effectively without losing data integrity or data confidentiality.

Post attack security analyst needs to figure out:
point of origin of the attack.
Hidden threats in the system and threats hidden in the network.
overcome lack of actionable intelligence.
Too much data from multiple sources to go through.

Cyber analysis or the cyber threat analysis combines three disciplines:
Information security- safeguarding information/data from unauthorized access within or outside the network.
Intelligence analysis- mainly a military practice, is a way of reducing ambiguity of a situation or a scenario by taking known information and using it to reduce the ambiguity.
Forensic science- is a science applied to solve criminal cases, where the science is applied to collect and analyze evidence.

In a real time scenario a security analyst can model and create an overview of a threat by:
1. Identifying how many valuable assets the system can protect.
2. Understanding the application and creating a security profile for that particular application. This can be done by decomposing the application and understanding the underlying network infrastructure. The ultimate goal is to find the vulnerabilities.
3. With the help of diagrams and tables an architectural overview of the application can be obtained.
4. By getting into the shoes of the attacker, developer needs scrutinize the work. Which helps in better identifying the vulnerabilities.
5. Logging and documenting each and every identified threat.
6. Prioritizing the threats, so that an action plan can be formulated. This helps in risk analysis and approximating mitigation costs.

Reflection:
Being a level 1 certified ethical hacker, the aspects of hacking, system/data security always geeks and intrigues me. Attending the talk Cyber Threat Intelligence by Bob Stasio, IBM. I can confidently say that it is like adding another feather in my cap. The talk was very educational and served as an opportunity for every student to learn what is really happening in the real world scenario.

The talk involved Bob discussing the following aspects:
How the asymmetric threats are becoming a real problem, where hackers posing as IT technicians stole more than 2.1 million dollars by connecting remote controlled devices connected to the banks servers.
It is alarming that less than 1% of the cyber-attacks are reported to the UK police. The low percentages of threats stopped are due to less effort or investment put in.
Comparing medical analogies to security. For ailments like slight physical injury or rashes, wearing protective gear and maintaining hygiene could help. For bigger problems like wounds, critical care and medical routine should be followed to recover. Life threatening problems like cancer research and lifetime medication is needed. The same analogy can be applied to security where small threats can be avoided by changing passwords frequently, for persistent threats like national threats mitigation strategy is cyber analysis.
Machine enabled, human enabled strategic threat analysis is imperative.
Anomaly research which reveals threats and attacks that went unnoticed.
Product description of IBM i2 cyber analysis and forensics tool.

This is my GitHub repository: `https://github.com/bhargavram1993/Latex-Projects.git`