Cyber Threat Intelligence

Sri Vivek

February 12, 2016

The main reason for the talk is to awaken the cyber analysis in the user's. Cyber Threat intelligence helps the users/defenders to detect the effect in advance giving them a warning to be ready to fight or avoid it by giving counter-attack.

Some of the ways of detecting are:

1. Logs
2. Security Alerts
3. System Behavior

Companies do spend millions of dollars in security. This is all to secure the user's privacy in private and public matters. Everyday one can see number of minor attacks being happening in the society around us.
Still there are only 1% of threats being detected and surprisingly only 1% of those are being investigated. A group called FIN4 got arrested trying to attempt bypassing the credentials of companies involving in the cyber crime. They used Phishing attack on the companies displaying a message as follows your session expired, login again.

Growth of asymmetric threats is changing the world, i.e, the information security has become Human vs. Human problem. Hackers try to use different techniques of which some are like using a small device to breakdown the servers or to access them remotely and also like using a malware or malicious virus injected into someone's system sent through E-mail and exploiting the user's system completely accessing all the information.
If we apply the 80-20% rule to the information security, it implies that 20% of the attackers are creating 80% damage to the companies,of those 80% create known attacks that can be blocked and rest are partially identifiable but cannot be blocked. Higher the level of effort/investment , higher the percent of block against the threats. If the threat is in its initial stage it can be blocked by the SOC analyst, rather if it crosses the limit experts have to deal it.
The cyber analysis discipline has the following components:

1. Information security

2. Intelligence analysis

3. Forensic Science

These components have their importance in different fields.

Attackers do try to enter the DNS server where in they can find more classified data.

Cyber Analysis results: Cyber analysis paves path towards many aspects giving results that benefit the human-kind like Risk management, Threat discovery, decision making.
IBM has developed some strategies having the capability to detect various threats depending on either machine or human-enabled. Attackers generally exploit the software causing an unwanted behavior in the system.
There are some main points creating pain and are being focussed on to get the information about the attacker:
Threats hiding in the network.

1. origin of the threat.

2. Problems in making decisions to break the threat.

3. Too much data and resources used to attack.

There are some questions being raised from the users and they have been answered: 1. Is there evidence of undetected malware in N/W: search proxy in N/w, Discover the beaconing activity and Save parameters for alerting. 2. How can one know who would attack using threat intelligence: By shifting through the threat reporting, Always conducting the link analysis and Compared to the dark-web data.

Reflection: The guest speaker and the technology developer is very informative and have elaborately shared his ideas on how they are developing and trying to fight the attacks.I have learnt what are different ways/modes that can be used to attack a system or an organisation. And also there are many formats in which they are injected. For example, human understandable format, machine format. Although some of the important things that i have learnt from the talk are: Unknown IP address accessing the private network. actions to be taken if detected an attack.

I have heard that if one has the knowledge of the threats and attacks, they can easily overcome the attacks being happened to them or their organisation.