Cyber Threat Intelligence

Himaja Kethiri

Thursday,February 12,2016

The guest lecture was by IBM guy Bob Stasio.It was very interesting and he discussed about cyber threat attacks.The lecture was begin by showing FIN4 attack by which the attackers hacked the pharmaceutical companies credentials with the help of phishing attack.The hackers attacked the IT employees bank information and they hacked their mails. With the help of mail they tried to know the It company future plans in which they were working.Then they robbed this companys millions of dolloars from the bank with the help of remote access device which costs 30dollors.Eventhough the companys system is using firewalls ,intruders will make use of asymmetric attacks to hack the information.

Next the actual percentage of attacks defended on the original system was shown in the form of graphical representation which was only 1%.But the effort to defend the attacks was high.There are some type of attacks which can be found in some period of time.Tactical attacks can be found in 1-5 days of time.The operational time between 5-60 days.After this he gave some examples of attacks and how to mitigate them in the field of medicine and security.These attacks can be prevented by using Hygiene and some research.

Bob focused on a important attack which was Sony attack for better understanding of how an attack can impact hugely and how can we take safety measures to mitigate those type of attacks.In this Sony attack a huge number of intruder were entered into their system They almost deleted 30GB of data without insiders involvement.Before that there were many number of attacks done on the same system.But they didnt concentreded much on these attacks.These attacks were occurred when the intruders were trying to hack the system credentials.If they have tried to concentrate on these attacks then it may not possible for them to loss this much amount of data.They thought these small attacks will not effect the system which lead to this situation.He explained the present scenario of the security system which is not effective.But, we can achieve best cyber security by the following measures like Information Security,Intelligence analysis and Forensic analysis which are proposed be IBM to prevent threat attacks in to the network.Information security provides confidentiality and reliability to the network so that no body can hack the network.In intelligence analysis we are going to collect the data and store the data.In forensic analysis based on investigation the attacks can be prevented. The cyber security intelligence mainly focuses on the 4 poins.First, the threats are unknowingly hiding in the network.Second,how to search for the attack.Third,how should we focus on intelligence.Lastly,how to deal which huge data.

1 Lessons learned:

The cyber analysis revealed that there is 80% of data is hacked by only 20% of hackers.Which says the hackers are becoming more intelligent.So,we have to take some safety measures like we should keep on upgrading our system.This will not stop the attacks.But, it will some how prevent the system to be hacked.

Git Hub: `https://github.com/himajakethiri/cyberthreat.git`