Cyber Threat Intelligence

Nikhil Hiremath

February 11, 2016

Introduction

A brief note on **'Cyber Threat Intelligence'** by *Bob Stasio*, who gave a little sneak-peek into the practical threats that were faced by Government and non-government organization and also explained us how they were successful in tracking a few of them.

Is Security a need?

Why is security so important for anyone? The obvious and yet most reasonable answer is to protect information from being seen by unwanted people.

Several organization and governments are doing huge investments to reduce the security breaches. Like *Bob Stasio, a Sr. Product Manager* at **IBM**, said a rough figure here it is **$100 million** per year and still he mentions that at most **1%** of all the security breaches in a year were detected although there is huge money flowing into the security aspects.

Investors are smart, as any person wouldn't invest money in a product or service that yields protection on a scale of **1%** against all the threats. In fact the investment is done on research and analysis of the threats and building a stable building blocks to reduce the security breaches.
So 'Cyber analysis' or 'Cyber Threat Intelligence' includes major areas like,

- Information Security- This requires expertise at the level of Chief
- Information Security Office-**CISO**
- Intelligence Analysis- Procuring High security information from intelligence communities
- Forensic Analysis- Requires high expertise in Law enforcement and IR community

Practical Attacks

An example of a ***Spear Phishing*** attack that was advanced form of phishing attack, carried out by a group of **Ukarine** hackers called ***FIN4***, targeted the Wall Street listed companies during *December 2014*. They attacked a medical-pharma system in New Jersey by cross-scripting the Outlook web site and fetching the credentials of the employees. Hence they were able to track the movement of pharmaceutical drugs and used the data for illegal purposes.

This introduces us to the a term **'Asymmetric threat**, which exposes us to the fact that a little investment in **VB scripting** effort in ***FIN4*** caused the leakage of important information. Another attack was detected in **NSA**, after a huge tracking operation was raised when someone found out a leak of important information. Finally a small drive with a *malware* running on it was detected that caused a loss of crucial data by someone inside **NSA**. The device that was found connected to a classified network system was detected sending information to *Yahoo.com*.

BobStasio came up with another situation in a Financial Firm where his team tracked down an insider attack where crucial information for the firm may be customer and client information was pushed to the 'gmail' account. When a tracking system was set-up to track all the outflow of data greater than 5GB, then it came into light that around **50GB** of information was pushed and this was happening during the after office hours. So with this lead they had to set-up video surveillance on all the employees who came to office after working hours. And then they were able to find the people who took printout of information from their office systems and took that data with them. So in this case as response to such security breach, the managers were asked to track the employees in more efficient way and the hard copies of the data was recovered back from those employees.

Multidimensional Attacks and Analysis

This introduces us to some other facets of threat analytics that are *Link analysis*, *comparing Dark-Web data* and *improvements in threat reporting systems*. These levels of analysis are very important, because Bob came up with even dangerous attack with ***Stuxnet*** virus, that was a kind of master-work like labyrinthine; where the virus streamed the information from hundreds of targeted computer systems and though being dormant in all the other non-targeted systems.

This virus had been reportedly installed by some person using a memory sticks which indicates the physical involvement.

So we can understand that threat intelligence gets new dimensions with every new attack. **IBM** has developed tools that does,

- Context analytics
- process the data with Big Data analysis and
- finally visualize this data in the final report

Where it is important to have log management, video surveillance to track all the threats that have physical involvement.

So Bob suggests that every security product must cover **3 tiers** of satisfactory level,

- **Tier 1** - ***Hygiene***
- **Tier 2** - ***Specialization*** in Organized crime, semi-tailored fraud, crimeware tool, visibility and monitoring features
- **Tier 3** - ***Research***

There are other tools like **QRadar** that **IBM** has built, which provide threat protection by stopping conflictors at the firewall which reduces the threat by **80%**.

Conclusion

Although the percentage of threats detected and neutralized is far less, the research and implementation should be carried out to have stable building blocks of security.