Advanced Persistence Threat and Cyber warfare

Pratik Hinge[1], Rajeshwari Gundla[2], Siddharth Nanda[3]
[1]*U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India*
[2]*Senior Faculty-IT, iNurture, Bangalore, India*
[3]*Faculty-IT, iNurture, Bangalore, India*

Abstract- There are various kinds of intrusion which may harm the organization and which can also damage the big projects, but today we will learn about the Advanced Persistence Threat (APT) and cyber warfare. Advanced persistence threat is crafty attack where the group or organization try to access the computer network and try to get illegal access without getting noticed. This kind of attack is long lasting and difficult to figure out.
Cyber warfare has no such definition which is widely adopted but in simple words it can be defined as one country trying to destroy or steal the information of other countries through cyber-attacks ,cyber-attacks are also done by the people who are unauthorized or who performs them for their personal issues such as terrorists organization, politicians, hackers etc.

I. INTRODUCTION

Advanced persistence attack (APT) is an encroachment attack which mainly targets the government sites, military sites, once the attacker gets the appropriate information and once performed with right procedure the organizations can be scanned and could be attacked in many several ways such as sql injection ,backdoor etc.
In past there were many different methods of war, but later the tactics were changed and cyber-attack became the easier and convenient attack, it was a great threat to military. Such kind of attack can be created anywhere in a small amount of time by a small group and can be implemented on others without warning on any part of the earth and can close down any target in a given time. Various countries have started taking preventions including North Korea, Israel and Russia. To prevent such cyber-attacks every country should look forward on their cyber warfare doctrine, which can give them the pre-information about when intrusions will occur.

a. APT Phases

It is a type of attack which requires many parameters to sneak in huge amount of network to maintain the long period access. To describe the various phases which are common in APT are as a kill chain and attack life cycle. Kill chain consists of interference or multiple interference, in APT the main campaign consists of multiple kill chains. Kill chain dwells interference this interference and these signals can be identify signals or signal attempt of the same movement. The main work is to find the problem or even avert signal before the attack so it can be cured.In the initial period of information gathering it is not necessary for the attacker to directly interact with the target. It is burdensome to find the culprit or how the attacker performed the reconnaissance. As further the analysts can only focus on the advice gathered and will add them into the investigation report.

b. Doctrine

Doctrine, in simple form can be explained as the body which has set the rules\principles of the governing fundamentals. It is mostly adopted by the military to look for the other countries that they do not plan anything against our individual country. For governing a war of cyberspace the CWD presents set of law and principles. It is based on the data gathered of making tactical decisions within a territory. To form cyber warfare doctrine, there must be powerful doctrines body as they are governing people's life, so they should be inspected. The cyber warfare doctrine body must have the knowledge of how to interact with others, perusing prosperity and how to protect the given information or how to secure it. Further we will be looking forward for three doctrines (1) Political doctrine (2) legal doctrine (3) Military doctrine.

c. Political doctrine

In the western part of the earth, it is basically believed that the people should have common understanding which will help them to interact with each other. Political doctrine enunciate with such principles this helps to increase social and political structures of the nations and helps them to get established. The perfect example for the political doctrine is the constitution, constitution sets the law for the country and once the law is breached then there is suitable punishment for it, this brings the system in the country and helps the country to the advanced development. The constitution embedded with the political constitution brings enthusiasm in the people about the new orders and the new way of governance.
In this paper it is explained, the values of the governing and how the nation is brought to the shape. The constitution of any country brings defines the country's past and also plans for the future. The constitutional example is USA, they adopted their constitution in the year 1787 at the critical movement. There were many fights against Britain and Spain and they were in the need of the government.

d. Apt analysis

To understand the techniques, strategies used in APT campaigns it is very much important to perform analysis. To improve the counterattacks it is important to update the security system which can be done by knowing appropriate information about APT.
Chen et al an organization have used to recycle the details and also searched for the APT attack models for the comparison of this campaigns. The result which was later declared was not having enough information and also the comparison is relatively philosophical. As there are no proper results or low no. of attacks it is difficult to understand what are the common types of attacks used.

Vilvis et al, also have executed their task on the four well known campaigns and also had lot of media attentions. These are compared on the basis of capabilities of the used malware even though they do not have details of the APT campaigns.

Therefore, It is more difficult to find the countermeasures of different characteristics for the APT attacks.

Fig.1:

In the image (1.1) it shows how different types of attacks happen takes place in the different parts of the world at the same time. As shown above the number of attacks performed at one time are much difficult to handle and to find solution on this is much tougher task. The red marked are the zones where the attacks are mostly done. Many of them tried to counterattack but the it was unable to gather the appropriate information about the APT attack which was not able to develop suitable countermeasures.

Table of comparison

APT	Cyber warfare
A person or the group tries to get an unauthorized access to your system without getting noticed.	There is no specific definition for cyber warfare but it is defined as one country tries to attack other country through cyber attacks
It may have either political motive or business motive	There is no specific political or business motive the only aim is to gather the information about the rival nation

Apt basically refers to group or the government, with having the capability of both intent and target.	Cyber warfare have introduced doctrine in which they have made it to persist the attacks.
The main function of this attack is to add a malicious code and do the specific task without getting unnoticed.	There are three types of doctrine which are political doctrine, legal doctrine and Military doctrine
Knowing about the attackers artifacts, such as file names it will be easy for the professionals to gather all affected systems.	All the attacks are covered by the three types of doctrine.

Scope of APTS more widespread

It has been found that there are 200 different families of malwares which are used to gather information or used to keep an eye on the system without getting noticed. Now days it is much difficult to identify the attacks as there are millions of types of malware variations. It is a stealthy attack. With the help control and command techniques associated with the APT can be identified by sophisticated method.

II. CONCLUSION

As we found many relatively research paper but muscularity of the campaigns contained spear fishing, used standard lateral movement for the use of command and control. Dump credentials is the another type of activity which can be performed to support the lateral movement. These helps the attacker to between various traffics and make it difficult and allow them to pass through the security.

Whether such a confrontation is provoked by third-party cyber criminals or statesponsored forces, a country would do well to be prepared. Many other defense forces are also developing or mobilizing themselves for cyber conflicts on a national and international level

III. REFERENCES

[1]. Haq, T., Zhai, J. and Pidathala, V.K., FireEye Inc, 2017. Advanced persistent threat (APT) detection center. U.S. Patent 9,628,507.

[2]. Ussath, M., Jaeger, D., Cheng, F. and Meinel, C., 2016, March. Advanced persistent threats: Behind the scenes. In 2016 Annual Conference on Information Science and Systems (CISS) (pp. 181-186). IEEE.

[3]. Jajodia, S., Shakarian, P., Subrahmanian, V.S., Swarup, V. and Wang, C. eds., 2015. *Cyber warfare: building the scientific foundation* (Vol. 56). Springer.

[4]. https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20134120/kaspersky-the-net-traveler-part1-final.pdf accessed on 11th April 2019