**MALWARE ANALYSIS FORENSIC TRAIGE IN SOC**

With the evolution in the society and our increasing dependence on Information systems, the crimes related to these systems are also growing fast. This change in the trend is responsible for gaping the bridge between actors and the victims. They basically target the vulnerability of the system that as a matter of fact is and come always be found. The next reason that acts a motivating factors for the increasing number of attacks is the no physical trace left on the crime scene, leading to a hard time while looking out for the perpetrator.

The most common method of collecting the information related to malware and cyber threat is by reverse engineering the sample malware and this becomes the next most crucial factor while investigating a scene that involves a new malware for infecting the machine. There are many methods currently used ,such as setting up of honeypots and crawling forums etc. The next basic issue revolving around the analyzation of the files is their size.

Malware hunting is one of the most important aspect that is to be looked upon while evaluation and analyzation of the impact of disaster, mainly focusing on the sample or exhibit that had the malicious nature.

Incident response

Taken often after the attack has had occurred. The most significant tasks is to stop any further damage to be caused due to the malware. The analysis here aims out at monitoring the attack vector and the way in which it affects the system. During incident response the invrestigator searches for any suspicious activity, involving the source of malware, and also the fact of the “ suspected file” actually being a malware. Detection of malware and it’s related information can serve as a basis for future intrusion system analysis , thus preventing any future damage from the malware.

Setting up honeypots

The next most used technique is to lure the threat actor by keeping yourself as a bait using a honeypot. The basic procedure that it follows is to monitor the system used for enaction and further can enhance the files that were either used in commition or were left behind.

The thing to be kept in mind is the designing of the bait as per the attacker you want to attract. Mostly a honeypot is a pile of vulnerabilities , enabling easy access to the actor. Though even the technique can be implemented but it is seen in many of the cases that APTs become well aware about the honeypot detection .

VirusTotal

Virus total basically, allows free uploading and scanning of the files that are to be checked for the presence or absence of the malware offering 50+solutions for the same. The process begins by running the environment by anti-virus solution activation. The search is run , returning the system either to be malware free or malware positive; being closely monitored. The efficiency is maximized when used for when referred to as a specific sample.

YARA

YARA enables detailed searching and analyzation using files as reference based on the conditions given by the user. The condition in this case, are often referred to as rules. This could be explained as:

Rule classname : class

{

Meta:

Description : “This is a class”

Thread\_level = 9000

Strings:

$a = “ This is “

$b = {DE AD BE EF}

Condition :

$ a and b

}

The rules are used to find out if similar file was uploaded; which is that a positive match is found or not. The file can be downloaded from here for further malware hunting.

YaraRETuses a oneliner mode, enabling a faster scanning over the disk. YaraRET basically searches for magic numbers that would detect file structure, as per the sample reference. The shell mode provides file selection option based on Yara and IoC detection.

File feed

Includes the continuity amongst each sample being uploaded on service with the result report, which is sent to the user directly. The plus point here being the largest available pool for reference sample.