Cybersecurity in TIC-Scientist Network Infrastructures by Honeypots: Catching Cyber Threat Passively

Juan Luis Martin Acal, Pedro A. Castillo Valdivieso, Gustavo Romero López, and Juan Julián Merelo Guervós

Springer-Verlag, Computer Science Editorial III, Postfach 10 52 80,
69042 Heidelberg, Germany
jlmacal@correo.ugr.es
{pcv, gustavo}@ugr.es
jjmerelo@gmail.com
http://www.springer.de/comp/lncs/index.html

Abstract. It should be a balance between security concerns and the right to privacy in the use of IT infrastructures. Scientist networks have a high risk of attack as a source of valuable information and resources because they were designed with an open and decentralized philosophy, in favour of the transmission of knowledge when security wasn't a critical section[1]. Private and scientific information have a enormous value for an attacker but the end user is worried about his privacy too. For this reason passive detection methods in cybersecurity like honeypots are the cornerstone in its defence plan. We expose the practical case of the University of Granada in the application of honeypots for the detection and study of intrusions which avoid intrusive techniques like the direct analysis of the traffic through networking devices. Also we expose the difficulties founded in the information's analysis gathered. Finally we propose the application of machine learning to overcome them in future works.

1 Introduction

From the earliest days, networks have been experiencing an increasing number of attacks. Nowadays, the number of attacks increases continuously[2][3]. Scientist networks are a special and interesting case, in one hand there is a strong demand of security in the network and the services which are listening. On the other hand, the end users demand privacy in his network traffic. In this scene the honeypots have an important role in the detection and protection against cyber attacks.

1.1 Cyber-Space and Cyber-Threats

The cyberspace is a virtual space that wraps all types of digital communication infrastructures and the entities that use them. The hostile actions from these entities against the security and safety of the information and others entities are ciberthreats. Internet is the most popular inhabitant of this space and for years we have seen how the number and complexity of attacks against information and resources has increased. This increase is motivated by for economic, politic or military interests or by the same entities interested in exercise a bigger control over communication freedom in the cyberspace[3][4].

1.2 Scientist Networks

In contrast to the corporate networks which usually have grown from the inside to outside and which have most hosts behind the demilitarized zone (DMZ), the scientist networks were born with a open philosofy without focusing on security but on technical requirements due to the limited number of public IPs, were expanding private services to the intranet.[1]

The information related to research, patents, computer and human resources is a juicy target for hostile agents. Also, the big size of the DMZ makes it prone to a massive attack and increases the possibility of finding a security breach or hidden advance vectors of attack.

1.3 Privacy and Passive Sensors

A honeypot is a trap that exposes itself, while is scanned, probed or compromised by a hostile entity, the trap collect information about the malicious activity. We differentiate between hierarchy and interaction in our taxonomy. The hierarchy is the complexity goes from a simple service like SSH, through a network, to a cloud. The interaction is the degree of fidelity in the response of the trap and goes from low to high.

TABLE HERE.

There isn't a ideal configuration of features because is the nature of the threats and the infrastructure which we want to protect, the key for a correct selection of them. In a software development environment, high interactions is used for test a new product with *fuzzers* or another type of pentesting[1] tool in order to discover potential vulnerabilities. On the other hand, low interaction honeypots are used like intrusion detection systems, warning about activity of scans or jumping attempts from compromised internal hosts. Both share a common point: they are not intrusive with the network traffic.

2 Deployment of a Security System Based in Honeypots

The architecture of the system is divided in two fronts: detection and management of the ciberthreats. The detection front usually are based on honeypots, one the most valuable tools at hand for this purpose.

2.1 Sensors and Collector

Sensors were deployed in different production subnets and each content honeypot software. Specifically Dionaea[5] and Kippo[6] which are low and medium interaction honeypot respectively. Each sensor has local data bases for save the information attacks efficiently in space while is waiting for its saved in the collector in order to keep the information by duplicate and not to increase the network traffic in case of massive scans or attacks. Obviously, in the time space between information dumps each sensor sends by telegram incidents defined by the security operator like critical.

The collector is a corporate database that feeds the incidents management system and is the core of all information analysis.

[1] Penetration Testing.

2.2 Attacks Profiles

We distinguish three attributes for each cyberthreat's profile:

- Vector, which will be single or multiple according to the number of simultaneous vulnerabildiades that the cyberthreat explodes.
- Persistence, if the cyberthreat is continuous in time and establishes monitoring and control mechanisms with hostile agent.
- Advanced, if the cyberthreat used mechanisms in order to hide its activity in the system.

One of the greatest dangers for IT infrastructure of governments, public administrations and companies are advance persistence threats. Usually APT are related with ciberspying and elite groups of cibercrime and they are attacks directed against specific infrastructure. For this reason it is a priority to detect and study them.

For three years each sensor collected information of more of half million of connections. The information's analysis shows the next points:

- External attacks are more frequent than internal attacks.
- In one hand the most frequent type of external attacks was weak credentials disclosure. On the other hand the most frequent type of internal attacks was malware propagation.
- Countries outside OTAN are the most active in the process of scanning and searching for vulnerabilities but curiously most of the intrusions come from OTAN member or member candidate countries. It is important to note that this data is dependent on the geolocation of where they are taken.

DATOS DEL ZETSU

Malware propagations usually owns to advance and persistence threats, also have a simple vector of attack. Malware scans infected through the ms08_67 for immediately attempt to connect with a command ad control server (C&C). The exploitation of SSH or MySQL weak credentials is the first step to gains control o access to data in a server but a few connections show a clever behavior of advanced or persistent threat.

MAS DATOS DEL ZETSU

AQUI ESTADISTICAS POR PUERTOS EJEMPLO MULTIVECTOR CAPTURADO EJEMPLO PERSISTENCIA

3 Weaknesses and Strengths of Honeypots

TODO MOLA SALVO CUANDO TIENES QUE PONERTE A INVESTIGAR APT

4 Honeypots, Elements in Hybrid Machine Learning S.I.E.M

VECTORES HONYPOT VS CONJUTOS DE DATOS DEL LEARNING MACHINE GROUP FALTA CHICA, CAPA DE RED, TCPDUMP O IDS PILLANDO DATA

5 Conclusions and Future Works

HAY QUE METER MACHINE LEARNING Y MINERIA DE DATOS DE LA BUENA A ESTOS DISPOSITIVOS.

References

1. Subdirección General de Organización y Automación, Secretaía General Técnica, Ministerio de Educación y Ciencia: Proyecto IRIS. November 1985. URL:https://www.rediris.es/rediris/historia/programa-iris.pdf
2. ESSET Latino América: Tendencias 2015: El mundo corporativo en la mira. January 2015. URL: http://http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_2015_eset_mundo_corporativo.pdf Note: Chapter 2, page 6
3. CNI-Centro Critográfico Nacional: Informe de Amenazas CCN-CERT IA-03/14: Ciberamenazas 2013 y Tendencias 2014. October 2014. URL:https://www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_IA-03-14-Ciberamenazas_2013_Tendencias_2014-publico.pdf Note: Prologue, page 7,8
4. CNI-Centro Critográfico Nacional: CCN-CERT IA-09/15 Ciberamenazas_2014 Tendencias_2015 - Resumen Ejecutivo April 2015. URL:https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf
5. Mark Schloesser: URL: http://dionaea.carnivore.it/
6. desaster: https://github.com/desaster