VISIÓN ELECTRÓNICA

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

A Case-Study Vision

THE ADVANCED PERSISTENT THREATS (APT) AND ITS METHOD OF DELINQUENCY

LA AMENAZA PERSISTENTE AVANZADA (APA) Y SU MÉTODO DE DELINCUENCIA

Kristel Solange Novoa Roldán [1] Johan Vargas Verdugo [2] Edwing Oswaldo Berdugo Romero [3]

Abstract: The APT (advanced persistent threats) has objective to obtain key information, allowing the attacker to use this information to manipulate or control an organization's informatics equipment for their own benefit. For these reasons it is important to know the functions and operating procedures of an APT. To diagnose and analyze it's early detection and understand how it functions. This article describes how to know the operation and scope of these threats using tests from a server by taking a laboratory machine and identifying the threats according to the level of persistence. This helps to determine the internal controls of the organization, allowing the development of contingency plans in advance.

Key Words: Threats, Anomaly, Organization, Persistent, Safety, Vulnerability.

---

[1] BSc. In Electronic Control and instrumentation, Universidad Distrital Francisco José de Caldas, Colombia; Specialist in Industrial Informatics. Current position: Professor Universidad Distrital Francisco José de Caldas; Research Group in Autonomous Robotic - ROMA-. E-mail: ksnovoar@udistrital.edu.co
2 BSc. In Electronic Technology, Universidad Distrital Francisco José de Caldas, Colombia. Current position: ATH analist. E-mail: jmvargasv @correo.udistrital.edu.co
3 BSc. In Industrial Engineering, Universidad Antonio Nariño, Colombia; Specialist in Edumatic, Universidad Autónoma de Colombia, Colombia. Current position: Professor Universidad Militar Nueva Granada, Colombia. E-mail: eoberdugor@umng.edu.co.

Resumen: La denominada Amenaza Persistente Avanzada (APA) tiene como objetivo obtener información clave, de manera que el atacante pueda usar esta información para manipular o controlar el equipo informático de una organización para su propio beneficio. Por estas razones es importante conocer las funciones y procedimientos operativos de una APA, diagnosticar y analizar su detección temprana y entender cómo funciona. El presente artículo, describe la forma de conocer el funcionamiento y el alcance de estas amenazas usando pruebas desde un servidor tomando una máquina de laboratorio e identificando las amenazas de acuerdo con el nivel de persistencia. Esto ayudará a determinar controles internos de la organización, permitiendo desarrollar planes de contingencia de anticipación.

Palabras clave: Amenazas, Anomalía, Organización, Persistente, Seguridad, Vulnerabilidad,

1 Introduction

The APT (advanced persistent threat) is form of a cyberattack that does not only affect governments, but prays on financial systems of big corporations. Nowadays, this is a major concern and a real threat for small an upcoming companies. Their main objective is to steal information, due to its main function there are many vector of attack (Malware, vulnerabilities, Spyware, corrupt E-mails) these methods offer a great opportunity to infiltrate and steal information avoiding detection from the corporations interior safety controls.

A few years ago, there have been reported attacks by the term APT (by the acronym of Advanced Persistent Threats), and each time a report is published with this terminology, means that there is no talk of common malicious code in which it is sought to achieve massive infection, But seeks specific objectives.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

Beyond the increase in reports of targeted attacks and APTs, It had an impact in 2015 on certain attacks that generated controversy based on leaked information, cases like Hacking Team and Ashley Madison.

It is very difficult to know when or how a company will become the target of a group of cybercriminals, and it is this point in which it must be taken into account, to be prepared and protect themselves from any attack, whether targeted or not [1] .

Phishing, skimming and malware are the main methods to steal financial information. The financial sector is attractive for cybercriminals because they can obtain higher values for their criminal activities. The chain information for crimes begins with the theft of information (authentication data, personal and confidential information), through mechanisms such as phishing, hacking or malware. After that, anyone can buy the information, which means a payment to the hacker, when this information can be used to perform more sophisticated attacks, such as fraudulent movement accounts, industrial espionage or threats advanced persistent (APT) [2].

In a large number of cases, these attacks were carried out by too well known techniques such as social engineering, USB infected and malicious emails. We must not fall into the false sense that this only happens in Windows environments because it doesn’t. Any platform is capable of being attacked by APT, as already appreciating other large software vendors [3].

The most famous APT attacks have been cases of Stuxnet, a virus designed for the destruction of Iran's uranium centrifuges, as well as attacks on RSA that were made to steal your design SecurID security token. Later there was an attack on Lockheed Martin, US arms

manufacturer, where the information extracted from RSA was used to achieve bypass security systems and become, in a clear example of APT [4].

Organizations that begin to address the information security significantly reach a point in their maturity when they have a lot of machine data. The challenge that many CISOs face is how to leverage that data quickly and dynamically correlate events across the enterprise to locate advanced persistent threats (APT). The incident hacking of Sony Pictures Entertainment last November highlighted the importance of security monitoring and rapid response to incidents to curb damage before a disaster occurs [5]. The article is organized as follows: in Section 2 defines APT; In section 3 the APT phases are indicated; In 4, the need to study APT is shown; In section 5, tests of APT are indicated; in section 6 the APT detections are indicated; And finally the conclusions

2. What are APT?

Advance Persistent Threats are programs designed to evade the established systems of control in the target. Its objectives range from espionage, identity theft, damage of reputation. This is a clear threat because there is an attacker with an illicit intention that is well established. They are persistent and take long lapses of time, these APT can be maintained operational for over years, and many times they can be stealthy and avoid detection without causing any damage of the victims web, waiting to obtain specific data, and stealing key information. These advanced attacks are perpetrated by people with extensive knowledge in programing and security information. This allows them to see vulnerabilities and employ them in attacks from 0-day, this way acquiring access to the organization’s web and its administrative privileges to later infiltrate in various equipments to locate mainframe and attack it simultaneously avoiding detection [6].

Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

A Case-Study Vision

3 Stages of APT

These attacks take form in a set of campaign stages, such attacks can develop in this way [7]:

A. Strategic recollection of all valuable information: this preliminary stage consist of collecting all information on the company that is available for public in the web such as (infrastructure, licitations, e-mails, names of users, personal information, social media, etc.) all information on the company's employees, their families and their providers.

B. Initial intrusion in the web: this phase utilizes different tactics to effectively infiltrate employees and their purveyors by fraudulent emails through this installing the APT in their servers. i.e. sending personalized messages through social media or contacting through know associates (Spear-Phishing), DND Spoofing through Man in the Middle, Using more manual methods like (USB, CDs, DVD's etc) infecting a single exploit that allowing to take advantage of a single vulnerability from 0-day.

C. Ensure ongoing communication: This phase is about establishing complete blackout and stealth through a backdoor, the ATP can be actualized through addition of modules and exploits from 0-day in-between the existing communication of servers in its current state of command and control of these attacks are also replicated to obtain control of different equipment, this guarantees their exchange of information.

D. Search of sensible information: during this phase advanced Malware starts its exploration through the web, searching sensitive information. This Malware utilizes different techniques to obtain administrative privileges in the organization's equipments, ranging from access to

amped units, detail information in the web. This allows the acquisition of important files in the organization and stay in them.

E. Data Extraction: Once the information on the main objective is obtained by the attackers and proceed to send this information in code through existing protocols permitted within the organization like HTTP or FTP and many alike. Like many external servers controlled by the attackers. These packages are sent in times of high data traffic or in periods of the organization's server system actualization to avoid detection. Figure 1.

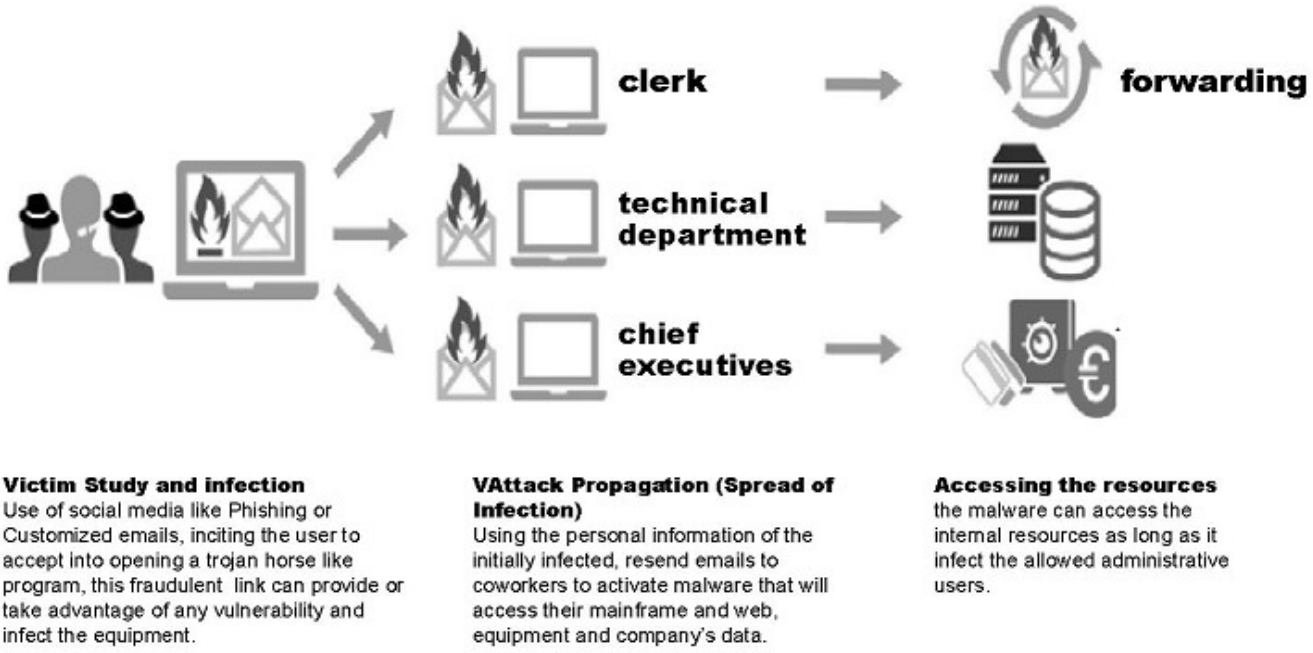

Figure 1 Attack Process APT National Institute of Communication Technologies 2013. Source: own.

4. Awareness about studio APT

A study was conducted to raise awareness about APT, Security professionals in some large and medium companies, where the results of the survey showed that many appreciations taken into the security environment questions were asked. Do you think the APT is similar or different from conventional threats? 65% consider them to be different and 35% believe that they are similar (figure 2) which lets us know that in most companies are aware of the kind of

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

threat which an APT and the risk is that it is not like any conventional threat. To counter conventional threats controls are implemented as antivirus, antimalware, navigation filters, IPS, Firewall, among others, which stop the threat, but APT exploit 0-day threats so they are not detectable by its kind traditional controls to counter threats.

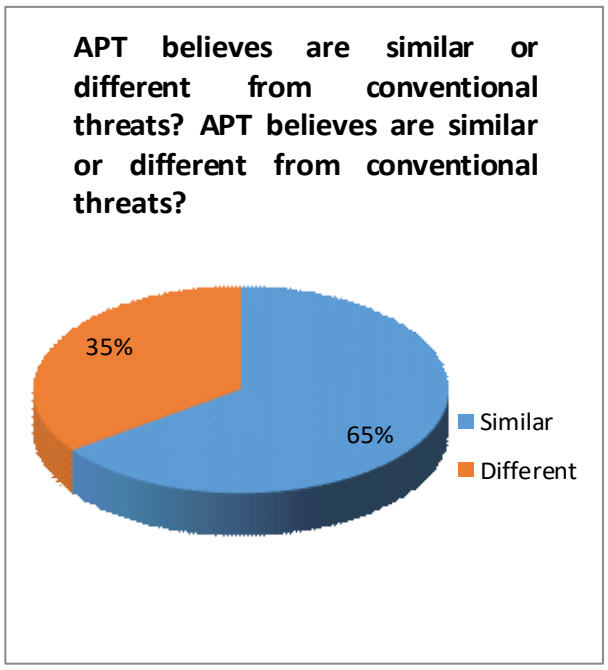

Figure 2. Awareness Survey Advanced Persistent Threats. Source: own.

Another question was asked. Does your company has increased training for employees about the APT? 87% reported that training has not increased for greater awareness of the risk of APT (figure 3). It is very important that organizations consider that currently there are risks of falling victim to an attack by APT, to implement mechanisms that allow for detection of the same, additionally have response plans APT attack in the organization, reducing potential impacts that may arise in the organization.

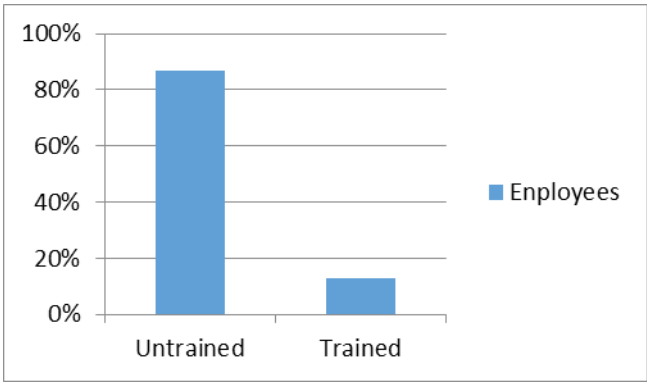

Figure 3. Awareness Survey Advanced Persistent Threats. Source: own

5. Proofs performed

To know the operation and scope of these threats a server was used in order to perform the tests, It was taken as a laboratory machine operation and to identify himself as to avoid being attacked by these threats.

The first proof performed (figure 4) basically it involves making APT sending an e-mail to our test machine, which then will be installed automatically when you open a malicious email that was sent. Then traffic capture is performed to check whether data is being sent from the machine to another server, that is to say if you are making information theft machine. After attempting to capture checks in IPS to see if some attack signatures are detected and if you can block them , finally you try to perform a lock to hold the attack that occurs and prevent theft of information.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

A Case-Study Vision

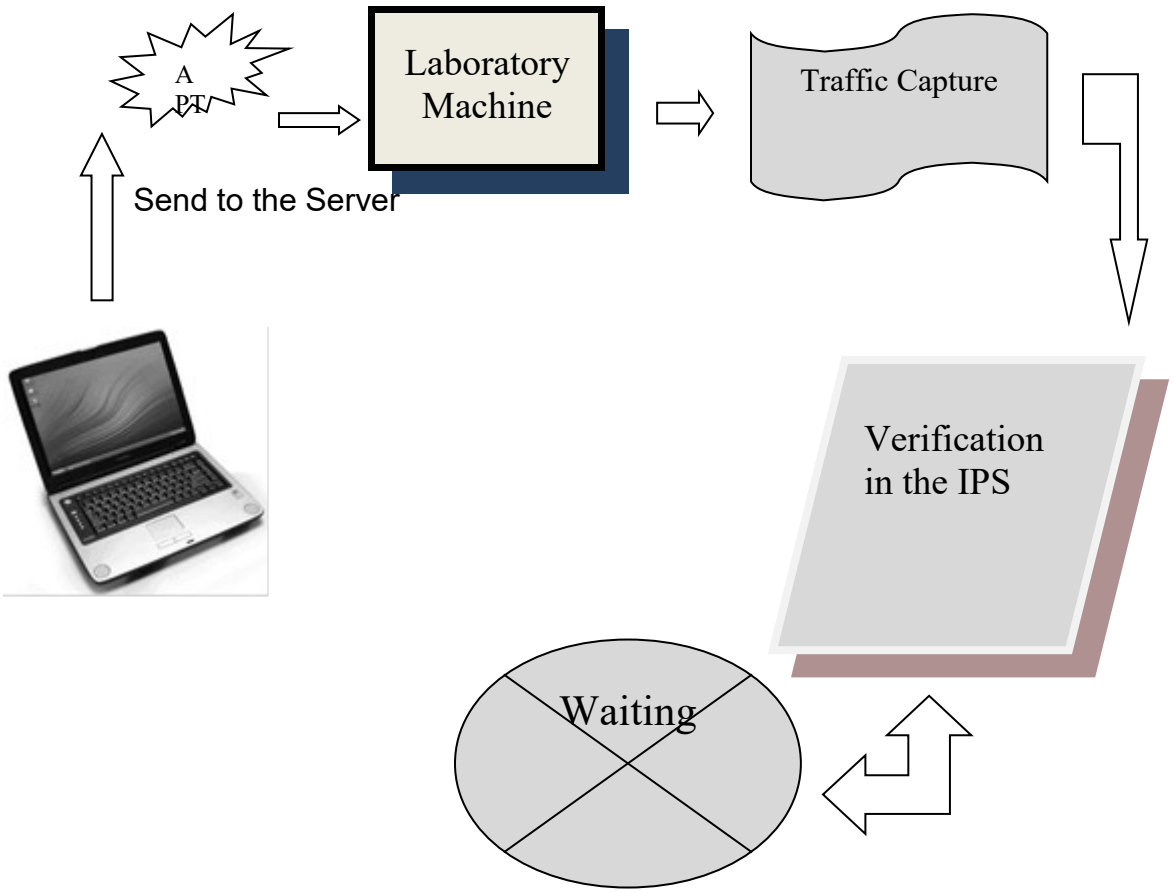

Figure 4. Flowchart proof number 1. Source: own.

It is observed that the machine continues its operation without generating any unavailability, not see any change, apparently as if nothing had happened. They are also reviewed as if it is carrying traffic capture through the SSH protocol with the program PUTTY, running the command tcp dump (Figure 5)

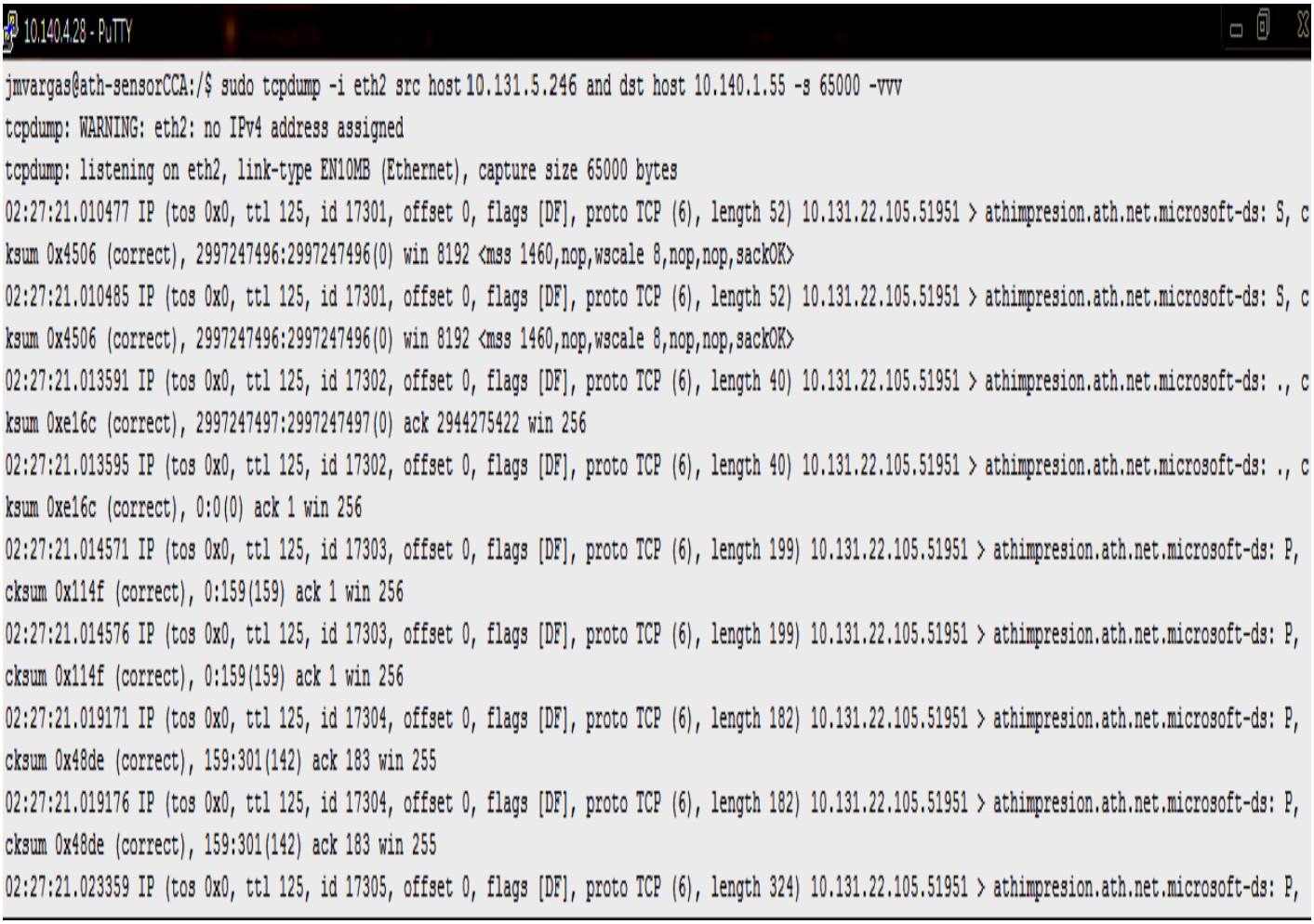

Figure 5. Traffic capture. Source: own.

It was observed that it begins to make important information capture team as credentials, even though you have antivirus and antimalware, which detected this unusual traffic.

Then the next phase is to verify from IPS If you find this traffic (Figure 6), in which also it notes that it detects no signature attack, this allows us to see the magnitude and the risk of this threat.

Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

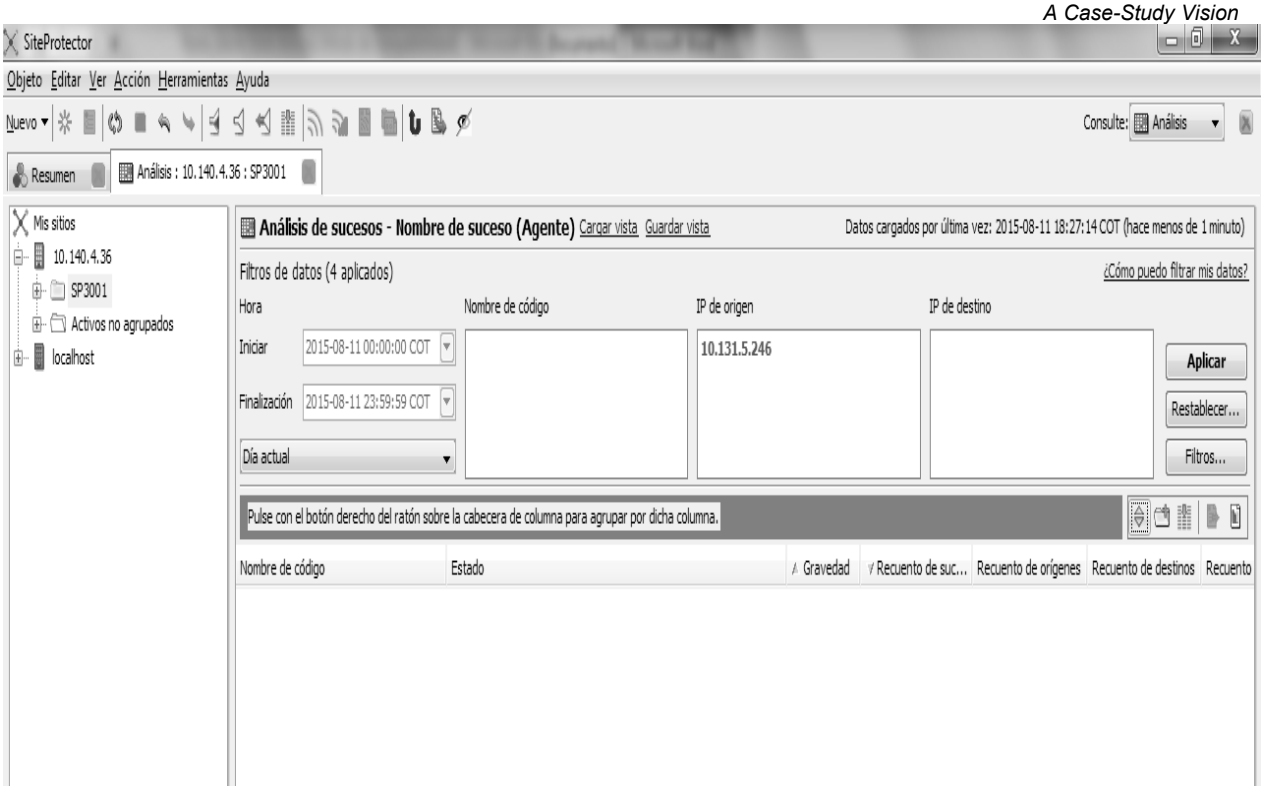

Figure 6. Verification in the IPS. Source: own.

To finish and to perform the containment of the threat is from blocking firewall preventing the entity IP traffic from the source to the server making, if no longer institutions implement methods of detecting APT.

The second proof: looks to verify containment mechanisms and are effective in eradicating this threat. It again installs an ATP testing machine, it proceeds to generate blocking traffic IP source from the entity firewall and again carry traffic capture and verification to confirm that the IPS is blocking effectively (figure 7).

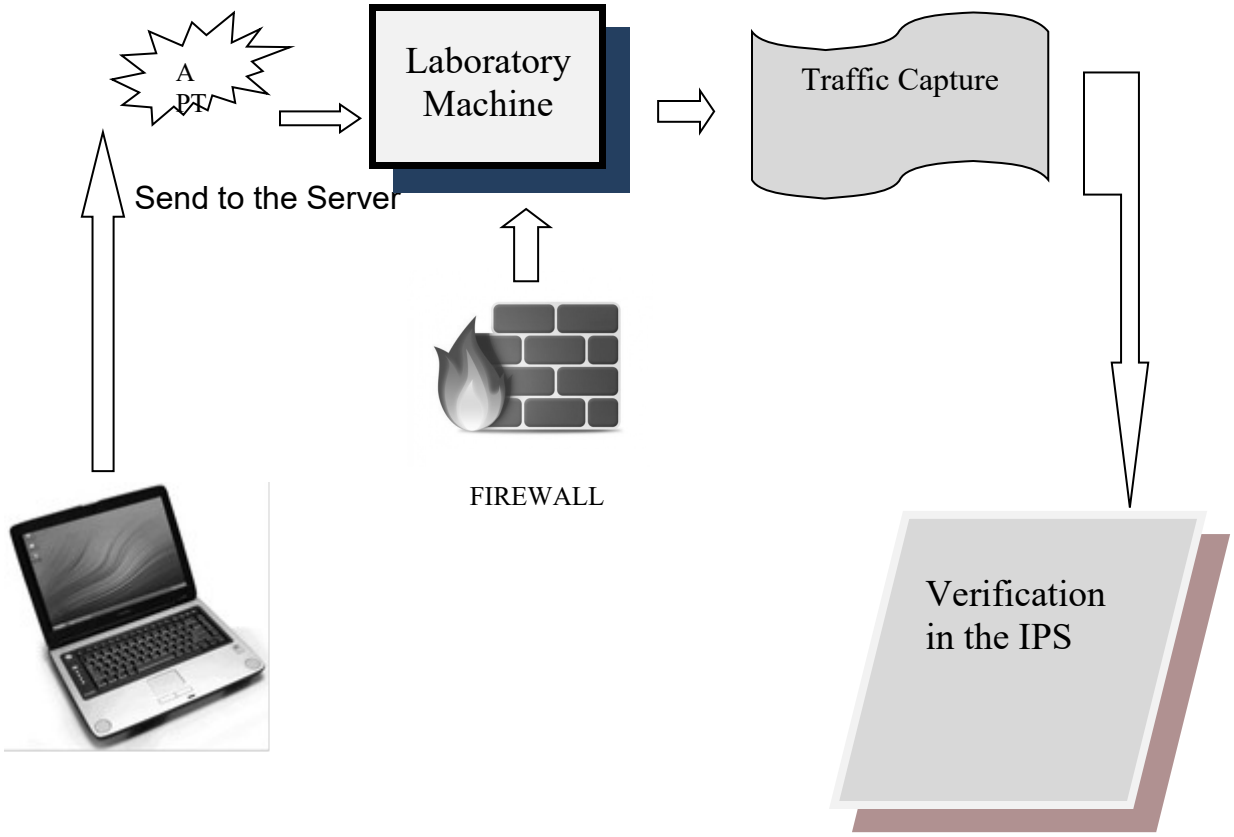

Figure 7. Flowchart proof number 2. Source: own.

With the firewall capture carried, traffic blocking is performed again (Figure 8) in which it is observed that there is not traffic capture but after several hours time capture it shows that there are some small time periods where there are leaks of information, for this reason it is necessary to perform proof blocking traffic from de IPS too.

```
jmvargas@ath-sensorCCA:/$ sudo tcpdump -i eth2 src 10.131.5.246 and dst 10.140.1.55 -s 65000 -vvv
[sudo] password for jmvargas:
tcpdump: WARNING: eth2: no IPv4 address assigned
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 65000 bytes
```

Figure 8. Capture of traffic 2. Source: own.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

The third proof: (Figure 9) It is to use the two defense mechanisms the firewall and IPS to ensure total security and eradication of APT Lock is from the firewall and IPS and proceeds to capture and verify. For several days it is captured therefore getting to work satisfactorily without any leaks of information. No evidence of traffic capture and see that the threat is eradicated.

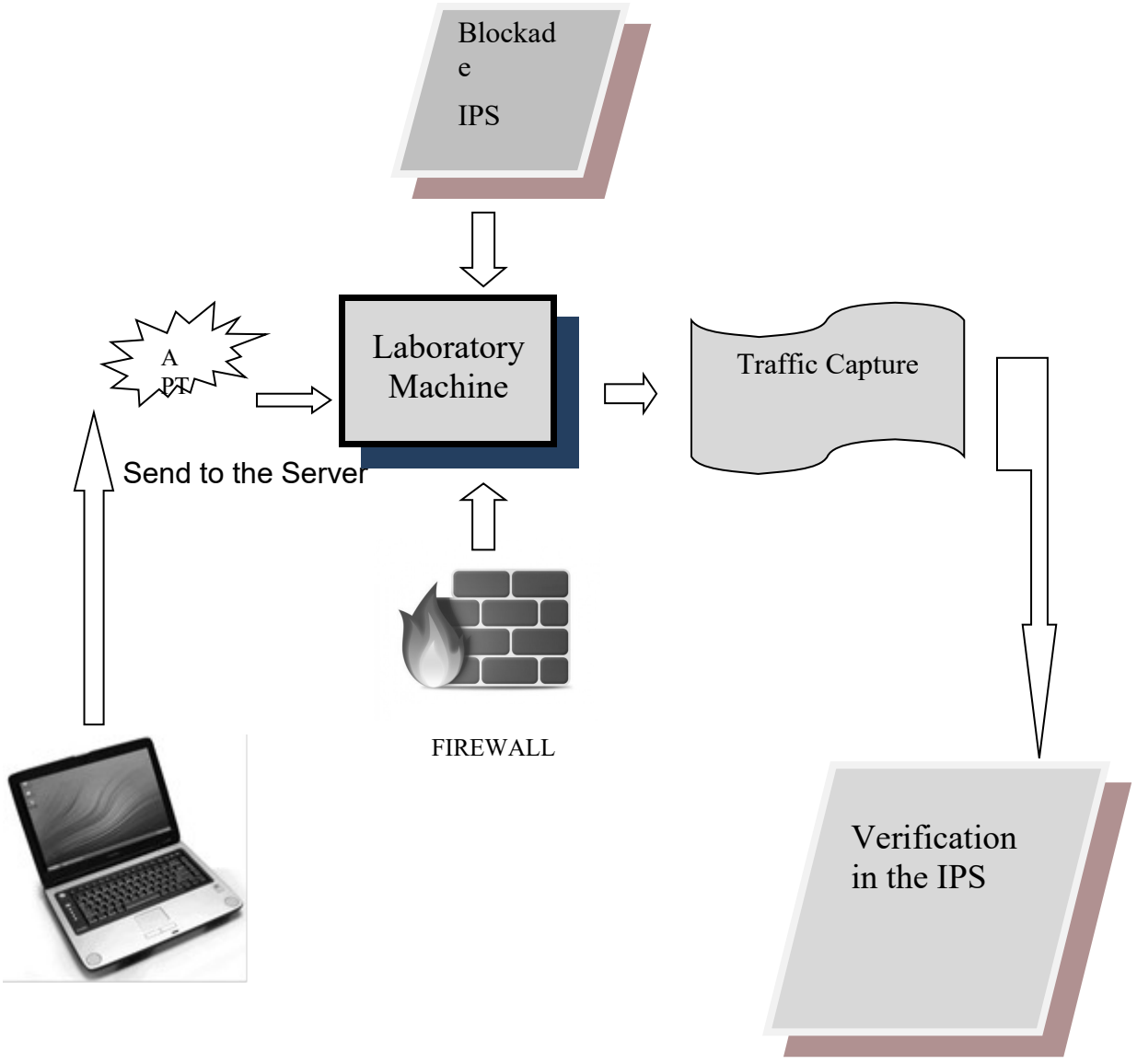

Figure 9. Flowchart proof number 3. Source: own.

6. APT detection

There are many detection methods that can be used with in organizations which provide real-time information registered anomalies within each method specializes in a special type of detection.

Among detection methods is HIDS (host based intrusion detection), by installing the agent on computers that allows detection of events that occur on a computer, as configuration changes, all abnormal types of connections that are attempted from the host to one or more networks you can perform to block traffic to malicious sites, exploiting vulnerabilities detection.

IOC (indicators of compromise), the indicators of commitment detect patterns of behavior registered when they have been compromised by an APT raid systems, using XML Schemes in detailing the behavior of APT.

SIEM (security information and event management), platforms are correlated and can generate alarms when anomalies are detected or specific events, monitoring previously defined for different types of information sources (hids, fw, ids, ips, content filters, among others) organizations Settings can be performed on these platforms to perform correlation between one or more sources of information at once in order to detect unauthorized connections attempts scanning of different teams, attempts scanning of different equipment, APT distribution network of the organization.

Fecha de envío: 13 marzo 2016
Fecha de recepción: 09 abril 2016
Fecha de aceptación: 22 agosto 2016

7. Conclusions

The Organizations must integrate their specialized security staff payroll who knows the use of tools and technologies that enable it to perform the detection and analysis of anomalies that occur inside the organization, in order to detect, contain and eradicate APT and document lessons learned in managing security incident.

It is necessary to train employees to make them aware of the risk to the company because of the APT, It is necessary to know how to detect these abnormalities and prevent important information leaks at the hands of their attackers.

It is important that companies implement a screening method in order to perform blocking these threats and protect organizational information.

The APT that is currently being used by cyber-crime endangers us all because we might be falling victim to these scams on the net.

It is necessary to use various methods to ensure the security of the information is 100% if not they may have some information leaks in some time periods.

Grateful to.

A million thanks' to ATH SA company who allowed us to perform the necessary tests and use their equipment detection and containment of threats and being able to take the necessary evidence and making the application in a real organization.

References

[1] Colombia Digital, “¿De qué manera el IoT impacta en cómo protegemos nuestros dispositivos?” [Online] available in: https://www.colombiadigital.net/actualidad/noticias/item/8756-de-que-manera-el-iot-impacta-en-como-protegemos-nuestros-dispositivos.html

[2] Colombia Digital, “¿Cuáles son los amenazas de seguridad financiera más populares en Colombia?” [Online] available in: https://colombiadigital.net/actualidad/noticias/item/8365-cuales-son-los-amenazas-de-seguridad-financiera-mas-pop ulares-en-colombia.html

[3] Red seguridad, “¿Por qué tienen éxito los 'Advanced Persistent Threat'” (APT)? [Online] available in: http://www.redseguridad.com/opinion/articulos/por-que-tienen-exito-los-advanced-persistent-threat-apt

[4] “Apts: una ¿nueva? amenaza”. [Online] available in: https://www.s21sec.com/es/sobre-s21sec/news-a-events/articulos/774-apts-una-inueva-amenaza

[5] “Defiéndase contra las APT con análisis de seguridad de big data”. [Online] available in: https://www.s21sec.com/es/sobre-s21sec/news-a-events/articulos/774-apts-una-inueva-amenaza

[6] Welivesecurity, “Guía definitiva para entender y protegerte de las APT”. [Online] available in: http://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/

[7] CSIRT – CV. (2013) “Deteccion de APTs”. [Online] available in: http://cert.inteco.es/exfrotinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf