A Study on APT in IoT Networks

Bruno Carneiro da Rocha[a], Laerte Peotta de Melo[b] and Rafael Timóteo de Sousa Jr.[c]
National Science and Technology Institute on Cyber Security, Electrical Engineering Department, University of Brasılia (UnB), P.O. Box 4466, Brasılia–DF, CEP 70910-900, Brazil

Keywords: Advanced Persistent Threats (APT), Internet of Things (IoT), Middleware.

Abstract: Many companies are being targeted by attacks called Advanced Persistent Threats (APT). These are difficult to be detected because espionage and important information stealing are the main tecniques instead of trying to crash the system by causing a denial of service (DoS) attack, for example. With the popularization of the Internet of Things (IoT) and knowing that these devices do not always have a high level of security, this type of attack can be more efficient and further compromise the security of associations. A study containing the main attacks and a proposed defense model will be presented in this work.

1 INTRODUCTION

With the advancement of internet technologies, information security has become a major concern for organizations. In the last decade, many companies have been the target of a new type of attack, called Advanced Persistent Threats (APT).

(Ghafir et al., 2018) found that the volume, complexity and variety of cyber attacks are growing exponentially. This growth trend is being driven by the cyber war and the emergence of the Internet of Things (IoT).

According to (Kumar et al., 2019), on the Internet of Things (IoT), devices interact with us to answer our explicit or implicit needs. And every day we see new devices emerging and bringing a long-term view of IoT closer to reality. However, there are still many challenges related to the reliable and efficient development of applications.

In this work, a research on the main APT attack and defense techniques will be presented, in addition to addressing some known attacks and defenses in IoT devices. Based on this, a defense middleware will be proposed to increase security in networks with IoT devices that can be a gateway to APT attacks.

[a] https://orcid.org/0000-0002-8705-732X
[b] https://orcid.org/0000-0002-2075-6601
[c] https://orcid.org/0000-0003-1101-3029

2 THEORETICAL REFERENCES AND RELATED WORKS

2.1 Advanced Persistent Threats (APT)

(Zhang et al., 2018) states that the term APT Attack was first proposed by the USAF (United States Air Forces) in 2006. According to the NIST (US National Institute of Standards and Tecnology), the definition of APT is: Attackers with technology proficiency use a variety of intrusion programs (networks, physical and fraud) with valuable resources to achieve the objective of the attack. According to (Ghafir and Prenosil, 2014), APT is a cyber threat based on ”one-day exploits” where the attacker can still have other attack objectives even with the critical system breached.

2.1.1 APT Attacks

In (Yang et al., 2020), the authors report a generic APT attack in four steps, namely: Preparation, Infiltration, Lateral Movement and Data Exfiltration.

The ”preparation” phase consists of researching which company will be the target, which company has digital assets that have a certain importance. Then, an analysis of the employees is made and a generic email is created to send malware.

The ”infiltration” phase consists of sending the email with the malware to the selected employees who would be potential targets to run the backdoor.

Rocha, B., Melo, L. and Sousa Jr., R.
A Study on APT in IoT Networks.
DOI: 10.5220/0010615201600164
In *Proceedings of the 18th International Conference on e-Business (ICE-B 2021)*, pages 160-164
ISBN: 978-989-758-527-2

When executed, the attacker has command and control with the target server.

The ”lateral movement” phase consists of installing other backdoors on other nodes in the network to propagate access by the company.

And finally, ”data exfiltration” phase from the organization's network nodes.

In (Zou et al., 2020), a more specific example of an APT tactic on Windows networks is shown. The tactic consists of five steps. The attack is separated into two phases, the first phase being an attack on the Domain Controller and the second phase a direct attack on a Windows machine in the domain. In this tactic, the attack begins with the use of software or malicious hardware. To gain privileges, the attacker can try to circumvent the UAC (User Account Control). With the necessary privileges, the attacker can act without being noticed. After that, the attacker can try to perform cryptanalysis on the passwords of users that are stored in the Account Database File. In case of success, the attacker will have access to other machines on the network and thus obtain the necessary data.

2.1.2 Detection of APT Attacks

To perform the detection of an APT, the first action to be taken is to know the main characteristics of this type of attack. (Zou et al., 2020) cites the following characteristics:

1. **Multiple Attack Stages:** The attack typically has several phases and each phase has a specific objective. Example: First, the attacker tries to gain remote access and then tries to do a cryptanalysis.
2. **Control and Data Dependency:** Each attack has prerequisites and subsequent conditions. Example: For an attacker to access a server, he first has to install malicious software and after accessing the server, he must erase his trail.
3. **Malware:** Malware is the most widely used technique for successful APT attacks.
4. **Data Exfiltration:** Here, the goal of attackers is to know what data will be obtained and how it will be done. After that, it is important to erase the entire trace.

The authors in (Zou et al., 2020) presented a detection method by identifying the techniques used and then relating it to a specific and already known tactic of APT. Machine learning techniques were used to detect the technique and relate to the tactic already known. (Ghafir et al., 2018) also used machine learning techniques to assist in detecting APT attacks. The authors (Chandel et al., 2019) have proposed a community for smart sharing of known threats. In this way, organizations share knowledge about cyber attacks. In (Zhang et al., 2018), a study and proposal for a security framework is carried out.

2.2 Internet of Things (IoT)

With the recent technological advances made in the Internet of Things (IoT), there is an exponential growth of smart devices that help to build increasingly interactive scenarios that help people in their daily lives. (Kumar et al., 2019) cites 14 (fourteen) types of IoT devices, which have been classified by Avast Software's Wifi Inspector tool:

1. **Computers in General -** Example: Macbook, NetBook, Intel PC
2. **Network Nodes -** Example: Router, Hub, Switch
3. **Mobile Devices -** Example: iPhone, Android
4. **Wearable Items -** Example: Fitbit, Apple Watch
5. **Videogames -** Example: PlayStation, XBox
6. **Home Automation Items -** Example: Nest Thermostat
7. **Storage Devices -** Example: Home NAS
8. **Surveillance Items -** Example: IP cameras
9. **Work Devices -** Example: Printers and Scanners
10. **Domestic Virtual Assistants -** Example: Alexa
11. **Cars -** Example: Tesla
12. **Media and TV Items -** Example: Chromecast
13. **Appliances -** Example: Smart Refrigerators
14. **Other Generic Items -** Example: Toothbrush

In recent years, there have been many advances in this area. In (Hua et al., 2019), the authors carried out an automation study in this area. The authors of (Lee et al., 2017) have created new authentication methods through a stateless restful webservice system. The authors at (Ferreira et al., 2013) also conducted a study using RESTApi for intercommunicating IoT devices.

2.2.1 IoT Attacks

The authors at (Kumar et al., 2019) found that many popular IoT devices on the market have weak security. This allowed several attackers to attack these devices using known techniques, such as DDoS (Distributed Denial of Service) attacks, identity theft, man-in-the-middle attacks and compromised local networks. Even with the due concern to protect the IoTs from these attacks by companies specializing in security,

many devices have relatively weak firmware (with low power and power) and the adoption of security measures is still unfeasible.

There are several techniques for exploiting vulnerabilities in IoT. (Kalita and Kar, 2009) describe in their article some attacks on IoT devices:

1. **DDoS Denial of Service Attacks** - Prevents normal use of the network by excessive traffic and increased latency.
2. **Sybil Attacks** - Several malicious devices make use of the identity as if they were theirs.
3. **Wormhole** - The attacker redirects incoming messages over a low-latency link to another part of the network.
4. **Sinkhole or BlackHole** - Make a node that has already been compromised as more attractive and receive all network traffic on that node.
5. **Hello Flood** - Sending many HELLO messages broadcast on the network in order to trick other nodes that the compromised node is also part of the network
6. **Traffic Analysis** - Traffic analysis allows you to see who is interacting on the network, in addition to identifying communication patterns.
7. **Espionage** - After entering the network, it is possible to spy and obtain confidential information and even authentication credentials.

In (Kumar et al., 2019), Avast Software's Wifi Inspector software was used to scan the local network for devices that accept weak credentials or have vulnerabilities that can be exploited remotely.

It was related in (Koupaei and Nazarov, 2020) that several IoT devices have resource limitations. Performing computer analysis with low information storage resources left the devices defenseless as they were not designed to have successful security metrics. In order to increase security on devices, it is necessary to implement cryptographic algorithms in addition to guaranteeing authentication on chips and firmware. The authors also cite 5 (five) challenges for the implementation of security:

1. **Devices with limited CPU and low memory**
2. **Vulnerable network options**
3. **Devices that need high performance must have lightweight encryption algorithms in order not to interfere with operation**
4. **Strong passwords are not enough**
5. **Enable security updates are not always possible**

We can also mention other attacks on IoT devices that can cause more serious damage. For example, (Vaishnavi and Sethukarasi, 2020) describes how the Sybil attack can interfere with IoT devices that use sensors on the body and report the patient's health status to medical centers.

2.2.2 Detection of Attacks in IoTs

In the past few years, several researchers have conducted IoT attack detection studies. The detection process becomes more complicated because the devices are heterogeneous in nature and each has a different hardware infrastructure (Vaishnavi and Sethukarasi, 2020). (Rana et al., 2018) made a systematic review of several types of IoT security frameworks. The authors concluded that there are still several security holes in this IoT world.

(Pacheco et al., 2020) developed an intrusion detection system for fog computing or fog computing. Mist computing is the equivalent of "cloud computing" or cloud computing, but for IoT devices. This system was built based on artificial neural networks. In (Pacheco et al., 2018), another study was developed to perform detections in several types of attacks. In 2017, a study was carried out for the intelligent water system, because according to the author, there are several cyber attacks on the water distribution system (Pacheco et al., 2017). A host-based intrusion detection system (HIDS) by signature for IoT devices was proposed in (Dutra et al., 2019). This proposed system prevents vulnerables IoT devices to be infected and join botnets. It is also able to notify the IoT middleware about potential failure indicators.

A security analysis of UIoT middleware using metrics was proposed by (Ferreira and de Sousa Junior, 2017). The purpose of this analysis was to provide privacy, authenticity, integrity and confidentiality when exchanging data between network participants, including IoT devices. A framework for detecting vulnerabilities in each layer of home networks was developed by (Pacheco and Hariri, 2016). An architecture based on Intrusion Prevention Systems (IPS) was proposed by (Gonçalves et al., 2019). This proposed system allows the network to be able to block attacks, reducing the volume of malicious traffic and isolating the affected device from the rest of the network.

3 MIDDLEWARE PROPOSAL AS AN EXTRA LAYER OF SECURITY

3.1 Methodology

To carry out this work, a bibliographic research was first carried out using the so-called exploratory methodology. This analysis provided a theoretical basis for both APT and IoT.

The study made it possible to reflect on a new middleware where the main attacks and defenses were analyzed so that our main objective is the privacy of all devices and users of the network under study.

3.2 The Proposed Middleware

The middleware must be located between the internal network containing the IoT devices (in addition to the rest of the network) and the internet. The middleware will be in a DMZ, so that any external user does not have direct access to the internal devices on the network, but will only have access to the exposed services. See figure 1.

For access to middleware, and to avoid invasion attempts, the suggestion is to configure the DMZ firewall and allow access only from previously registered MAC addresses. Other MAC devices that try to connect to the middleware and are not previously registered may be redirected to a Honeynet.

All requests and responses must go through middleware. This will record in the database all requests and all responses, as a way of further analysis. Requests and responses must be made via REST calls, using the HTTPS (secure) protocol, that is, encrypted.

The middleware should not allow users to log in with standard credentials (example: admin, password). In addition, it should require users to create strong authentication on each IoT device that is connected to the network. The middleware should check for updates to IoT devices. If so, it will not be possible to proceed with the connection. If an IoT gateway exists, it must also be checked continuously to verify that the firmware is out of date and has secure encryption.

Alerts will also be generated when new devices connect to the network. A check of open ports on the network can also be done by the middleware to aid intrusion detection.

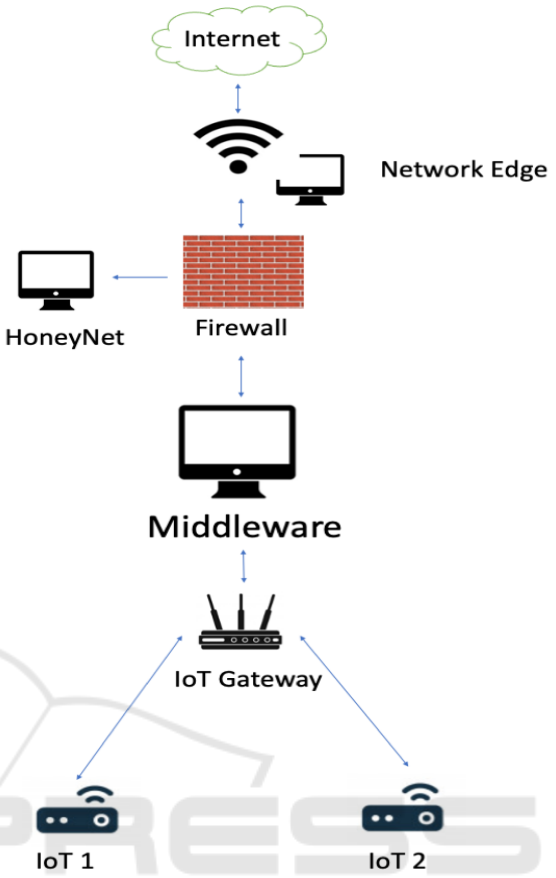

Figure 1: Proposed Middleware.

4 CONCLUSION AND FUTURE WORK

After analyzing several APT attacks, it was found that phases like ”preparation”, then ”infiltration”, followed by lateral movement and, finally, data exfiltration are very common in most invasions.

As much as studies are done to increase the security of IoT devices, they don’t support a more robust security implementation because of the simple hardware or firmware. Detection methods are more effective in this case, but the security of these devices still depends mainly on the action of their users. Security measures are: keep the firmware updated and create passwords that are difficult to be cracked by the most common attacks on the market.

In order to solve this problem, a middleware is being developed in such a way that it is able to check firmware information to help the final user. Intrusion detection systems and machine learning will also be incorporated into this middleware, in order to avoid the greatest possible number of attacks.

ACKNOWLEDGEMENTS

This work was supported in part by CNPq - Brazilian National Research Council, Grant 312180/2019-5 PQ-2, Grant BRICS 2017-591 LargEWiN, and Grant 465741/2014-2 INCT in Cybersecurity, in part by CAPES - Brazilian Higher Education Personnel Improvement Coordination, Grant 23038.007604/2014-69 FORTE and Grant 88887.144009/2017-00 PROBRAL, in part by the Brazilian Ministry of the Economy, Grant 005/2016 DIPLA and Grant 083/2016 ENAP, in part by the Institutional Security Office of the Presidency of Brazil, Grant ABIN 002/2017, in part by the Administrative Council for Economic Defense, Grant CADE 08700.000047/2019-14, and in part by the General Attorney of the Union, Grant AGU 697.935/2019.

REFERENCES

Chandel, S., Yan, M., Chen, S., Jiang, H., and Ni, T. (2019). Threat intelligence sharing community: A countermeasure against advanced persistent threat. *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*.

Dutra, B. V., de Alencastro, J. F., de Caldas Filho, F. L., e Martins, L. M. C., de Sousa Jr., R. T., and de O. Albuquerque, R. (2019). Hids by signature for embedded devices in iot networks. *V Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)*.

Ferreira, H. G. C., Canedo, E. D., and de Sousa Junior, R. T. (2013). Iot architecture to enable intercommunication through rest api and upnp using ip, zigbee and arduino. *1st International Workshop on Internet of Things Communications and Technologies (IoT'13)*.

Ferreira, H. G. C. and de Sousa Junior, R. T. (2017). Security analysis of a proposed internet of things middleware. *Cluster Comput 20*.

Ghafir, I., Hammoudehc, M., Prenosilb, V., LiangxiuHanc, Hegartyc, R., Rabiec, K., and Aparicio-Navarrod, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*.

Ghafir, I. and Prenosil, V. (2014). Advanced persistent threat attack detection: An overview. *International Journal of Advancements in Computer Networks and Its Security– IJCNS*.

Gonçalves, D. G. V., de Caldas Filho, F. L., e Martins, L. M. C., de O. Kfouri, G., Dutra, B. V., de O. Albuquerque, R., and de Sousa Jr., R. T. (2019). Ips architecture for iot networks overlapped in sdn. *Workshop on Communication Networks and Power Systems (WCNPS)*.

Hua, J., Liu, C., Kalbarczyk, T., Wright, C., Roman, G.-C., and Julien, C. (2019). riot: Enabling seamless context-aware automation in the internet of things. *IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*.

Kalita, H. K. and Kar, A. (2009). Wireless sensor network security analysis. *International journal of computer science & information Technology (IJCSIT)*.

Koupaei, A. N. A. and Nazarov, A. N. (2020). Security analysis threats, attacks, mitigations and its impact on the internet of things (iot). *Synchroinfo Journal*.

Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R., and Durumeric, Z. (2019). All things considered:an analysis of iot devices on home networks. *28th USENIX Security Symposium*.

Lee, S., Jo, J.-Y., and Kim, Y. (2017). Authentication system for stateless restful web service. *Journal of Computational Methods in Sciences and Engineering*.

Pacheco, J., Benitez, V., Félix-Herrán, L., and Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. *IEEE Access*.

Pacheco, J. and Hariri, S. (2016). Iot security framework for smart cyber infrastructures. *IEEE 1st International Workshops on Foundations and Applications of Self-* Systems*.

Pacheco, J., Ibarra, D., Vijay, A., and Hariri, S. (2017). Iot security framework for smart water system. *IEEE/ACS 14th International Conference on Computer Systems and Applications*.

Pacheco, J., Tunc, C., and Hariri, S. (2018). Security framework for iot cloud services. *IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*.

Rana, K., Singh, A. V., and Vijaya, P. (2018). A systematic review on different security framework for iot. *Fifth International Symposium on Innovation in Information and Communication Technology (ISIICT)*.

Vaishnavi, S. and Sethukarasi, T. (2020). Sybilwatch: a novel approach to detect sybil attack in iot based smarthealth care. *Journal of Ambient Intelligence and Humanized Computing*.

Yang, L.-X., Huang, K., Yang, X., Zhang, Y., Xiang, Y., and Tang, Y. Y. (2020). Defense against advanced persistent threat through data backup and recovery. *IEEE Transactions on Network Science and Engineering*.

Zhang, Q., Li, H., and Hu, J. (2018). A study on security framework against advanced persistent threat. *7th IEEE International Conference on Electronics Information and Emergency Communication*.

Zou, Q., Sun, X., Liu, P., and Singhal, A. (2020). An approachfor detection ofadvanced persistent threat attacks. *THE IEEE COMPUTER SOCIETY*.