Future Generation Computer Systems 79 (2018) 243–246

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Editorial

# Special Issue on Advanced Persistent Threat

Jiageng Chen [a], Chunhua Su [b], Kuo-Hui Yeh [c], Moti Yung [d]

[a] School of Computer Science, Central China Normal University, Wuhan, China
[b] University of Aizu, Fukushima, Japan
[c] National Dong Hua University, Taiwan
[d] Columbia University, USA

ARTICLE INFO

*Keywords:*
APT
Zero-day vulnerability
Data driven security
Behavior based detection
Encrypted traffic

ABSTRACT

Recently, a new type of attack called Advanced Persistent Threat (APT) headline the news frequently. Different from other type of attacks, APT often has specific targets given sufficient fund support, and the attack can exist for a long period of time without being discovered. No single current protection approach alone can efficiently defeat APT, and thus research effort is required to further investigate this area. In this paper, we discuss the concepts of APT as well as the newest trends on how to efficiently detect and neutralize these hidden threats. A brief overview of eight accepted papers in our Special Issue on Advanced Persistent Threat is presented. Finally, we conclude this paper by highlighting the key points and summarizing the paper.



## 1. Introduction

Cyber security breach now has become a nightmare for companies and governments, who are struggling to protect their digital assets. Especially, the personal information and intellectual property assets are treated as the most valuable information in most of the agencies. Massive loss will follow once those data results in the wrong hands. Many researchers have raised concern about the further outbreak of the cyber security breaches. And in order to address the issue, enterprises must have continued focus on cybersecurity risk so they can achieve resilience when an incident does occur. According to the survey by ISACA, 61% of the IT department would like to increase budgets over their cybersecurity team in the near future, which includes increased pay for skilled workers, skills development training, awareness programs and response planning.

Huge investment in the area of cyber security however did not even slow down the damage caused by the new powerful attacks. In 2016, several government agencies and companies are hacked and sensitive information are leaked including the US department of Justice, Linkedin, YAHOO! and etc. In the first half year of 2017, we have already seen global outbreak of WannaCry ransomware, and attacks on organizations including Honda, Arby's, Intercontinental Hotels Group, Saks Fifth Avenue, the U.S. Air Force, over 60 universities and U.S. federal government organizations.

The fast-changing IT infrastructures such as cloud computing and virtualization have brought a big challenge to the traditional cyber security protection. More recently, the attacks have become more and more sophisticated which have the "highly targeted" and "long-term" characteristics. These long term, and sometimes state-sponsored attacks are usually known as Advanced Persistent Threats (APT) [1]. APT is not one sophisticated attack as most people would understand at the beginning, instead, it is a sophisticated combination of a wide known techniques to achieve a specifically targeted and highly valuable goal. Currently, no single technology can guarantee to block the APT attack, and more importantly, it is already too late when the attack is discovered.

To protect from APT attack is not an easy job which requires efforts by combining different technologies from different areas, as well as the effective integration of them. In this paper, we provide an overview of the APT in Section 2. Then in Section 3, we give some insights on how APT may be prevented by using the cutting-edge technology. We summarize the papers accepted in this special issue in Section 4 followed by Conclusion in Section 5.

## 2. Definition of APT and current protections

According to the definition given by the National Institute of Standards and Technology, APT is defined as follows: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues

http://dx.doi.org/10.1016/j.future.2017.11.005
0167-739X/

its objectives repeatedly over an extended period; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives".

APT is thus a targeted attack which has the following properties according to the report by Symantec:

1. Tools used in the APT attack is usually customized regarding the targeted environment including zero-day vulnerability exploits, viruses, worms, and rootkits and so on.
2. Different from the traditional cyber-attacks which expect to gain immediate financial gain, APT attack can last for a long period of time. The attackers usually move slowly and are very careful not to be detected.
3. Usually APT target is of very high value, and the groups behind are well financially supported.

APT attack usually does not involve brand new technologies, instead the well-organized multi-layer approach makes it rather difficult to defeat. The primary activities of an APT attack usually have the following life cycle.

- **Infection.** Like other attacks, in this step the attacker tries to exploit the flaws of the target system or network and upload the customized program to collect further information. The attackers investigate the potential weaknesses of the system carefully and try to take advantage of one or two of them to gain access of the front door of the system, and no serious damages happen at this stage yet. Social engineering is the most widely used and effective way to break through the system. Others include zero-day vulnerability exploits, which has big advantage from the technology's point of view. But on the other hand, only well-funded groups are capable of the exploiting in a long term.
- **Discovery.** Once the first door is broken through, useful information will then be collected such as internal network topology, resources allocation, hardware vulnerabilities and so on. Since the goal is the long term, it is important to keep the malware under the radar so that it can survive for a long period of time. Often code obfuscation techniques are applied to make the detection more difficult [2].
- **Capture and Transmission.** Sensitive information can be accessed in this stage, and possibly rootkit may be installed on the target system as well. To occupy the system for a long time is again the priority of APT. According to the report by Symantec on APT, on average the amount of time that a host was actively infected by an APT was 145 days, with the longest infection span being 660 days. The data must finally be sent back to the adversary. Recently, secure channel over the SSL protocol is often used to add to the difficulty of the detection analysis.

APT attacks given the above characteristics are even capable of threatening the industrial security. Company VirusBlokAda discovered a complicated malware called Stuxnet in 2010. Later in the same year, Iran reported that the state's nuclear power plants were attacked by Stuxnet, which caused serious national security issues. Unfortunately, there does not exist an all-in-one solution to efficiently defeat the APT attack. Multi-layer protection is still by far the most effective method which includes firewall, antivirus, intrusion detection system, web protection, email protection and sandboxing, and thus can greatly reduce the odds attacked by APT. Each one of these fields are being investigated by the researchers and new results are helping the industry to improve the security protection. Notice that recently most of the IT areas have already been benefitted from the booming technology such as big data analysis and machine (statistical) learning. Not surprisingly, cyber security will benefit from these technologies as well which is usually called data driven security.

## 3. Data driven security and APT

To totally prevent APT attack is nearly impossible given the current technology, and due to the property that APT can be hidden under the radar for quite a long time, it is very important to prevent from actual damage such as data theft. Data driven security can be utilized to help organizations neutralize cyber threats before they cause significant problems.

Security teams usually utilize logs to analyze the network threats. They often collect and analyze logs from critical systems, but this log-oriented approach to detect threats may leave space that sophisticated adversaries can exploit. In the data driven security scenario, deep packet inspection technique [3] is used to record, parsing, normalizing, analyzing, and reassembling all data traffic at every layer of the network stack instead of analyzing logs alone. Based on the anomaly detection theory [4], security anomalies can be detected and security incidents can be reconstructed much more efficiently.

Traditionally, firewall, antivirus and IDS systems largely adopt the signature based method to detect the threats, which relies heavily on comparing the discovered malicious patterns to the newly observed ones. Advanced attacker however can take advantage of the zero-day vulnerabilities to bypass the security protection, which cannot be efficiently detected by using the signature based approach. Furthermore, in the "Transmission" phase, the sensitive information could either be sent back bit by bit under the radar, or by taking the advantage of the encryption technique. Behavior based detection [5] is developed recently based on the statistical learning approach which can help to evaluate and predict the abnormal and suspicious behavior of the data pattern. Classification and anomaly detection will provide some advantage over the traditional signature based detection system once it is well trained in a relatively stable environment. Even the data is encrypted over the protocols such as SSL/TLS (NSS Labs, Inc. Predicts 75% of Web Traffic will be encrypted by 2019), by carefully examining the meta information, we are still able to classify the encryption traffic and get a deep insight about the behavior of the traffic, which can provide us with a better judgment on the long-term malicious malware [6]. Such techniques have already been applied from the attacker's point of view in web based application [7] and mobile based application [8] to infer user's privacy. While the privacy leakage is severe and troublesome, applying them in detecting APT may have an impressive result.

If the deep learning technology has already shown a great potential in the artificial intelligent area after the success of AlphaGo, then [9] is one of the leading results about the application of the neural network on the cyber security. It showed how the automatic and secure encryption and decryption can be achieved without specifying any concrete algorithms. The use of Generative Adversarial Nets (GAN) model [10] can be used to greatly improve the machine learning models, and thus can be considered to better defeat the APT attacks in the near future.

## 4. A brief review of accepted papers of this special issue

In this special issue, we have accepted in total 8 papers in the area of Advanced Persistent Threat (APT) covering the three stages (infection, discovery and transmission) from both adversary and protection's point of view. We give the summary as follows:

Christian J. D'Orazio et al. [11] proposed techniques to circumvent security mechanisms and facilitate collection of artefacts from cloud apps. SSL/TLS in iOS cloud apps can be circumvented which would allow forensic researchers and investigators to acquire evidential data from iOS devices. The goal of the attack can be successfully achieved by proceeding the following three stages: 1. The circumvention of security mechanisms; 2. The interception