Detecting C&C Server in the APT Attack based on Network Traffic using Machine Learning

Cho Do Xuan[1], Lai Van Duong[2]
Information Assurance Dept
FPT University,
Hanoi, Vietnam

Tisenko Victor Nikolaevich[3]
Systems of Automatic Design
Peter the Great St. Petersburg Polytechnic University
Russia, St.Petersburg, Polytechnicheskaya, 29

***Abstract*—APT (Advanced Persistent Threat) attack is a form of dangerous attack, it has clear intentions and targets. APT uses a variety of sophisticated, complex methods and technologies to attack on targets to gain confidential, sensitive information. Currently, the problem of detecting APT attacks still faces many challenges. The reason is APT attacks are designed specifically for each specific target, so it is difficult to detect them based on experiences or predefined rules. There are many different methods that are researched and applied to detect early signs of APT attacks in an organization. Today, one method of great concern is analyzing connections to detect a control server (C&C Server) in the APT attack campaign. This method has great practical significance because we just need to detect early the connection of malware to the control server, we will prevent quickly attack campaigns. In this paper, we propose a method to detect C&C Server based on network traffic analysis using machine learning.**

***Keywords*—Advanced Persistent Threat (APT); abnormal behavior; network traffic; machine learning; APT detection; Control Server (C&C Server)**

I. Introduction

The publication [1, 2] presented the characteristics, procedures and life cycle of APT attack. From the characteristics of the APT attack, it shows that the APT attack has specific, clear objects and goals. Any organization, individual, business or governmental agency can become victims of this attack. In the past, APT attack groups often operated for personal purposes. However, most APT attack groups are now financially supported by government or financial institutions in order to implement political motives. Due to this change, ATP attack groups are increasingly equipped with not only modern attack, hide and cover tracks tools, but also a team of warlike, elite hackers. In the publication [3], the authors have presented some of the characteristics of the attack scenario makes APT attack detection becomes much more difficult than any other threats, such as advanced attack tool, lack of public data, and using standard encryption protocols. From the above presentations, we can see the dangers as well as difficulties in detecting APT attacks. In fact, many APT attacks have taken place over the years, exploiting large amounts of data without the victim's knowledge.

However, although APT attacks are advanced and sophisticated with completely new attack ways, they are all separated into four main stages [3, 4, 5]: spying (collecting information), attacking and escalating privilege, stealing information, and covering tracks. All four stages have the same role and importance, they support each other in the entire offensive campaign.

In the attacking and escalating privileges stage and stealing information stage, all of these are performed by commands from the C&C Server to the malware that has been exploited in the target machine. Therefore, if the system can detect abnormalities in the connection, it can quickly and accurately detect the signs of APT in the system. To detect the connection to the C & C Server, studies often focus on the issue of monitoring the anomaly of network traffic or rely on a list of C & C Server that has been built before. However, APT malware often easily bypass these traditional approaches. Therefore, in order to improve the ability to detect abnormal connections to a C&C Server, in this paper, we propose a method to analyze abnormal behavior in network traffic based on machine learning techniques. Accordingly, firstly the network traffic data will be analyzed and extracted behaviors relying on domain name or IP address, then these behaviors will be built into a feature vector. Finally, we use a machine learning algorithm to classify them in order to detect the abnormal connection of the C & C server. The science of our paper includes recommending some abnormal features of C&C Server based on Network traffic and using the Random Forest algorithm to detect abnormal connections. The paper is organized as follows. Section II reviews some recent works in the literature on C&C Server detection. The proposed C&C Server detection system using machine learning is presented in Section III. In this section, the new features for the C&C Server detection process are also described in detail. Experimental results and discussions are provided in Section IV. The paper is concluded in Section V.

II. Related Works

A. Several Methods of Detecting APT are based on Abnormal Connections

In [3], the authors proposed a method for APT attack detection based on the analysis of abnormal behaviors of flow in Network Traffic. This method includes the process of extraction, normalization, and analysis of abnormal values of three groups of signals in flow, which are numbytes, numflows, numdst. Andrew Vance et al. [6] used measures non-signature based traffic and involved flow based measurements and applied a statistical for detection APT attack. Weina Niu et al.

[7] introduced a method for APT attack detection based on Mobile DNS Logging using four sets of features, which are DNS request, answer-based features; Domain-based features, Time-based features, Whois-based features. With the selected feature sets, the authors used a number of machine learning methods such as Global Abnormal Forest, k-Nearest Neighbor to detect APT Malware. G. Zhao et al. [8] used five sets of features: Domain-based features, Time-based features, Whois-based features, DNS answer-based features; Active probing features and used J48 decision tree algorithm to detect APT malware command and control domains (C&C Domain). In [9], the authors used three sets of features to detect the domain APT, which are Domain name lexical features; Ranking features; DNS query features and Random Forest machine learning.

B. Detecting APT Attack using Big Data Technology

The publication [10] listed a number of APT attack detection tools based on analysis and correlation calculations among events such as Splunk, LogRapse, and IBM QRadar. Jisang Kim et al. [11] proposed a method to detect APT attacks based on the process of collecting and processing collected data sources consisting of the network packets are collected; Email logs are traced to accept; the privilege increase logs (Syslog) are traced to accept; Call-back domain blacklist; Internal DNS server; SSL port. However, in this paper, the authors didn't present the technical solutions and the big data processing technology used. Besides, Sung-Hwan Ahn et al. [12] proposed the idea of applying big data technology to APT attack detection. Accordingly, the authors proposed the architecture of big data analysis system consisting of the following stages: collecting data from firewall and log, behavior, status information (date, time, inbound/outbound packet, daemon log, user behavior, process information, etc.) from anti-virus, database, network device and system; preprocessing data; analyzing data; and giving warning results for signs of APT attacks. However, in this paper, the authors didn't present the solution or technology used in bigdata to support the model proposed by the authors. In the paper [13], the authors proposed the APT attack detection model on the big data platform with two main processes: Behavior Rule Generation and Abnormal Behavior Detection. In this proposed model, the authors use the Hadoop MapReduce framework.

C. Some Commercial Software Detecting APT Attacks

The document [14] introduced a number of commercial products and technologies that support APT attack monitoring and detection, including Symantec, Forcepoint, McAfee, Kaspersky Lab, Fortinet, Cisco, Palo Alto Networks, and FireEye.

McAfee Advanced Threat Defense is designed to detect APT malware and zero-day vulnerability by combining static analysis with dynamic analysis through sandboxing techniques. The analysis results will be provided to the system to detect and alert from within the network to the terminals. However, the disadvantage of this solution is the inability to analyze attachments on emails.

Kaspersky Anti Targeted Attack Platform (KATAP) is a solution that combines machine learning algorithms with sandbox technology to handle information about threats collected from inside systems and terminals in order to detect signs of APT malware (including known, unknown and APT malware) at any stage in the APT attack's life cycle. However, the disadvantage of the KATAP solution is not providing the monitoring and troubleshooting function after APT attack campaign, and the weakness in preventing data leakage.

FireEye's APT attack prevention solution is a set of solutions that analyze data from multiple sources such as Web, Email, File, Central Management and Malware Analysis. Accordingly, all suspicious files, attachments, files, and URLs are automatically scanned and monitored through the rule sets, then all suspicious signals will be transferred to the sandbox environment to be executed.

Advanced Malware Protection (AMP) solution of Cisco is the solution to detect APT attacks at the stage of spreading or hiding in the system or all 3 phases (consist of before APT attacks, during APT attack, and after APT attack). In Before APT attack phase, AMP uses information about threats worldwide gathered from Cisco's Collective Security Intelligence, Talos Security Intelligence and Research Group, and AMP Threat Grid to prevent known malware attacks.

In During APT attack phase, AMP uses information obtained from known attacks (signature), combined with AMP Threat Grid technology with the ability to automatically analyze malware in order to identify and prevent suspicious, dangerous files that are trying to gain access to the network. In After APT attack phase, AMP not only checks and monitors at the time of the attack, but continues to monitor and analyze all operations and paths of the data (though it was previously considered to be “clean”), and look for signs of dangerous behavior. When detecting a file containing malicious code, AMP provides visual information about the activity in the network, in each terminal of malicious code, AMP also allows quick response and troubleshooting through a simple web interface. However, AMP doesn't provide a function to prevent data leakage.

WildFire is Palo Alto Networks’ APT attack detection solution, providing full visibility of all traffic, including APT threats from Web traffic, email protocols (SMTP, IMAP, POP), FTP (regardless of whether it is encrypted or not). The weaknesses of the WildFire solution is that it only focuses on monitoring the network layer, with little interest in the application layer and only focuses on detecting and preventing attacks but doesn’t provide troubleshooting.

III. C&C Server Detection Model Development

A. Model Overview

Fig. 1 presents the proposed C&C server detection system using machine learning. The model consists of the following components:

- Network Traffic: Network data that is checked here can be taken directly in real-time from the network card or can be taken from the pcap file.
- Extract features: In this paper, we use the Bro IDS tool to assist in analyzing network traffic into network components. Bro IDS Tool is a network security monitoring tool with fast processing speed. It detects

intrusion based on rule sets and helps to separate features from network traffic at high speed.

- Training: After extracting the necessary information based on Bro IDS log files, the features will be saved in the CSV file. Random Forest algorithm will be used to classify from those features

B. Select and Extract Features

Table I lists the features of network traffic we use. All features marked "*" in Table I are newly extracted and selected in this research.

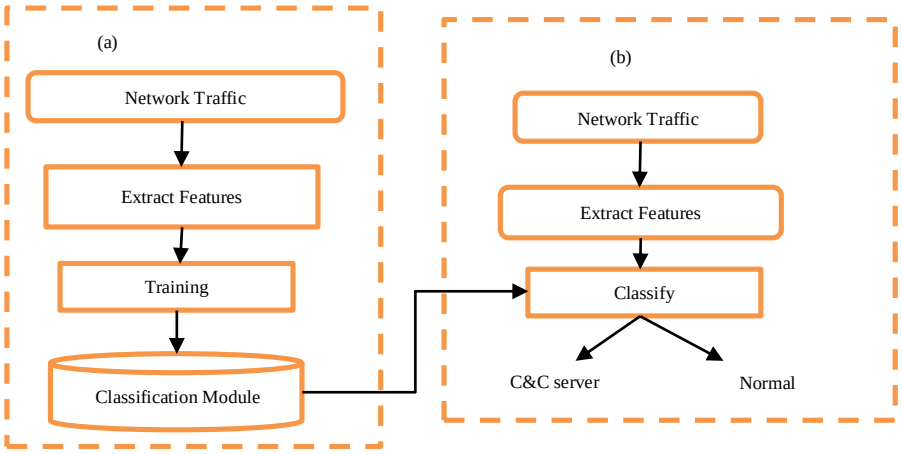

Fig 1. Overview Model.

TABLE I. LIST OF FEATURES USED TO DETECT A C&C SERVER

No	Feature	Type
1	Anomaly Port and Protocol	Bool
2	Ratio of number of packets OUT/IN *	Integer
3	Ratio of number of Bytes OUT/IN *	Integer
4	Ratio of inter-arrival times OUT/IN *	Integer
5	Number of three way handshakes	Integer
6	Number of connection teardowns	Integer
7	Number of complete conversation	Integer
8	Anomaly Data *	Float
9	Number of packets per time *	Integer
10	Number of bytes per time *	Integer
11	Percentage of TCP SYN packets	Float
12	Percentage of TCP SYN ACK packets	Float
13	Percentage of TCP ACK packets	Float
14	Percentage of TCP ACK PUSH packets	Float
15	Command and File System *	Bool
16	Data to computer in LAN	Bool
17	Tor Network *	Bool

The features in Table I are defined as follows:

- Anomaly Port and Protocol: In order to find abnormal ports, which don't run properly service according to the Internet standard, the first step is extracting the strange IP address that the server queries to in the DNS packet. From there, we find the queries that server queries to that IP address. From those records, we extract the protocols and service ports from the server, consider whether they are suitable or not, otherwise, the protocol and the port are abnormal. We define this because when a server provides service out with a specific port, it always listens to requests and returns responses through that port. For example, web services with the HTTP protocol have a default port of 80. Thus, the webserver always listens to requests and responds via port 80.
- Ratio of number of packets OUT/IN: is the ratio of the number of OUT and IN packets.
- Ratio of number of Bytes OUT/IN: is the ratio of the number of bytes of OUT and IN packets.
- Ratio of inter-arrival times OUT/IN: is the ratio of inter-arrival times OUT and IN.
- Number of three way handshakes: is the number of three way handshakes.
- Number of connection teardowns: is the number of the failed connection. Table II shows some cases that occur when a connection fails.
- Number of complete conversation: is the number of successful connections.
- Anomaly Data: The first step is identifying strange IP addresses through DNS records. Then, we take the value of the tcp.len field of all records that their destination IP is a strange IP address. From there, we find the maximum size of the packet and calculate the average size of the packets
- Number of packets per time: is the number of packets in a period such as hours, minutes, seconds, days, weeks, months and years.
- Number of bytes per time: is the number of sizes of packets in a period such as hours, minutes, seconds, days, weeks, months and years.
- Percentage of TCP SYN packets: is the percentage of the SYN flag in the TCP protocol of packets.
- Percentage of TCP SYN ACK packets: is the percentage of SYN ACK flags in the TCP protocol of packets.
- Percentage of TCP ACK PUSH packets: is the percentage of ACK PUSH flags in the TCP protocol of packets.
- Command and File System: The commands that the C&C server sends to malware are always command line, so if traffic has the system command line that is transmitted to any machine in the system from the external internet, it is very likely from C&C server. In addition, recent attacks such as Sofary Group's Parrallel Attack [15], which is organized by APT 28 in February 2018, the malware will save the data that the malware obtained into the file in the % APPDATA% folder and transfer directly to C&C Server. Similarly, other attacks, the malware also hide information in directories like% TEMP%, etc. and send it directly to the C&C server. Thus, if the network traffic has command lines and system files, it is certainly attacked by APT.
- Data to computer in LAN: In recent attacks, the first computer on the LAN that is hacked will be used to gather all data from other computers on the LAN and data from that machine will be sent to C&C Server via VPN. Typically, the APT15 attack on the US Navy on June 14, 2018 [16].
- Tor network: In order to encrypt the operations and commands of malware when it accessed to the victim machine, APT organizations often use the Tor network to encrypt and to avoid detecting C&C Server addresses.

C. C&C Server Detection Method

To detect connections from within the network to the C&C server, in this paper, we use the Random Forest algorithm. Random Forest is an ensemble classification method [17]. This algorithm is based on an ensemble of classifiers, which normally are Decision Trees to make the final prediction. The theoretical foundation of this algorithm is based on Jensen's inequality [18]. According to Jensen's inequality applied to the classification problems, it is shown that the combination of many models may produce less error rate than that of each individual model. In the study [19, 20] has proven Random Forest algorithm has many advantages compared to other machine learning algorithms. In this paper, we use the Random Forest algorithm with the number of decision trees of 10 in order to classify and test connections.

TABLE II. THE FAILED CONNECTION CASES

Packet sent	Packet received
Send TCP SYN	TCP Reset
Send TCP SYN or UDP Packet	ICMP unreachable
Send TCP SYN or UDP Packet	Do not receive the packet for 120 seconds

IV. EXPERIMENTS AND EVALUATION

A. Dataset and Experiment Environments

In this paper, we collected 61 network traffic files of APT attacks from [21-26]. Table III lists in detail the components of the experimental dataset.

TABLE III. THE COMPONENTS OF THE EXPERIMENTAL DATASET

Source	[21-24]	[25, 26]
The number of PCAP files	28	33
The number of DNS queries	985,595	272
Domain name	50 domain names (consisting of 26 domain names related to APT attacks, and 24 clean domain names)	45 domain names (consisting of 18 domain names related to APT attacks, and 27 clean domain names.)
IP address	921 IP addresses (including 581 public IP addresses, and 71 IP addresses related to APT attacks)	105 IP addresses (including 75 public IP addresses, and 25 IP addresses related to APT attacks)

B. Metrics

To evaluate machine learning models, in this paper we use the following metrics:

Accuracy: the percentage of correct decisions among all testing samples

$$acc = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

where: TP (True Positive): is the number of network flows which the model correctly predicts is the APT attack network flow; FN (False Negative): is the number of network flows which the model incorrectly predicts is normal; TN (True Negative): is the number of network flows which the model correctly predicts is normal; FP (False Positive): is the number of network flows which the model incorrectly predicts is the APT attack network flow.

Precision: is the ratio of the number of APT attack network flows that is correctly predicted among those classified as APT attacks network flows.

$$precision = \frac{TP}{TP + FP} \times 100\%$$

Recall: is the ratio of the number of APT attack network flows that is correctly predicted among those that are actually the APT attack network flows.

$$\mathrm{Re}call = \frac{TP}{TP + FN} \times 100\% \quad (3)$$

TPR (True Positive Rate): is the rate of network flows which the model correctly predicts is the APT attack network flow.

$$TPR = \frac{TP}{TP + FN}$$

FPR (False Positive Rate): is the rate of network flows which the model incorrectly predicts is the APT attack network flow.

$$FPR = \frac{FP}{FP + TN}$$

TNR (True Negative Rate): is the rate of network flows which the model correctly predicts is normal.

$$FNR = \frac{FN}{TP + FN}$$

FNR (False Negative Rate): is the rate of network flows which the model incorrectly predicts is normal.

$$TNR = \frac{TN}{FP + TN}$$

C. Experimental Results

Synthesizing APT attack malware data from data set that is divided by the ratio of 70% for training and 30% for testing and obtaining model. Tables IV and V describe the results of APT attack detection using the Random Forest algorithm.

TABLE IV. EXPERIMENTAL RESULTS OF C&C SERVER DETECTION MODEL TRAINING

Precision	Recall	Accuracy	TPR	FPR	FNR	TNR
0.925	0.998	0.955	0.998	0.095	0.002	0.905

TABLE V. EXPERIMENTAL RESULTS OF C&C SERVER DETECTION MODEL TESTING

Precision	**Recall**	**Accuracy**	**TPR**	**FPR**	**TNR**	**FNR**
0.9996	1	0.9998	0.9996	0.0004	1	0

Through the experimental results in Tables IV and V, we can see that C&C server training and detection model brings good results. This shows that the Random Forest classification algorithm and the features that are selected and extracted in the paper have brought good effect. In particular, the experimental part of detecting C&C server is absolutely accurate, which showed that the training model created a very good model for detection. Therefore, from the experimental results in this paper, we can see that the features, which represent the abnormal connection behaviors and are selected and proposed by us, present exactly the difference between normal connections and APT connections. This is very important because most APT attacks will be difficult to detect without the events-stringing system.

V. CONCLUSION AND FUTURE DIRECTION

The APT attack has been and will be a dangerous attack and a challenge to information security systems. In this paper, based on the Random Forest machine learning algorithm and the unusual behavioral features of network traffic, we successfully detected and alerted C&C servers early. The results of this research can be used in intrusion detection and prevention systems to look for abnormal signs of the network. In the future, we will improve the features of network traffic in order to detect the signs of an APT attack when this attack uses encryption techniques to transmit information

REFERENCES

[1] Adel Alshamrani; Ankur Chowdhary; Sowmya Myneni; Dijiang Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities" IEEE Communications Surveys & Tutorials, 2019, 1, 1–29.

[2] Eric Code. “Advanced Persistent Threat. Understanding the Danger and How to Protect Your Organization,” 1rd ed.; Elsevier, Amsterdam, 2012; 309.

[3] Mirco Marchetti, Fabio Pierazzi, Michele Colajanni, Alessandro Guido, “Analysis of high volumes of network traffic for Advanced Persistent Threat detection,” Computer Networks. 2016: 109; 127-141.

[4] Combating Advanced Persistent Threats – “How to prevent, detect, and remediate APTs , Tech. rep,” McAfee Inc. (2011).

[5] Ivo Friedberg, Florian Skopik, Giuseppe Settanni, Roman Fiedler. “Combating advanced persistent threats: From network event correlation to incident detection,” Computers & Security, 2015, Volume 48, Pages 35-57.

[6] Andrew, V, “Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing,” In: 2014 First International Scientific-Practical Conference Problems of Info Communications Science and Technology, pp 173-176, Kharkov, Ukraine, 14-17 Oct. 2014.

[7] Weina, N., Xiaosong, Z., GuoWu, Y., Jianan, Z., Zhongwei, R, “Identifying APT Malware Domain Based on Mobile DNS Logging” . Mat. Pro. in. Eng. 2, 1- 9 (2017).

[8] Zhao, G., Xu, K., Xu, L., Wu, B, “Detecting APT malware infections based on malicious DNS and traffic analysis,” IEEE Access. 3, 1132–1142 (2015).

[9] Do Xuan Cho, Ha Hai Nam, “A Method of Monitoring and Detecting APT Attacks Based on Unknown Domains,”. Pro. Com. Sci. 150, 316-323 (2019).

[10] The Radicati Group, Inc. Advanced Persistent Threat (APT) Protection-Market Quadrant 2018. An Analysis of the Market for APT Protection Solutions Revealing Top Players, Trail Blazers, Specialists and Mature Players. February 2018. Pp48.

[11] Jisang Kim, Taejin Lee, Hyung-guen Kim, Haeryong Park, “Detection of Advanced Persistent Threat by Analyzing the Big Data Log,” Advanced Science and Technology Letters Vol.29 (SecTech 2013), pp.30-36.

[12] Sung-Hwan Ahn; Nam-Uk Kim; Tai-Myoung Chung, “Big data analysis system concept for detecting unknown attacks,” In the 16th International Conference on Advanced Communication Technology. 16-19 Feb. 2014. Pyeongchang, South Korea.

[13] Hyunjoo Kim, Jonghyun Kim, Ikkyun Kim, Tai-myung Chung, “Behavior-based anomaly detection on big data,” In the 13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015, Edith Cowan University Joondalup Campus, Perth, Western Australia. pp. 73-80.

[14] Advanced Persistent Threat (APT) Protection - Market Quadrant 2019. An Analysis of the Market for APT Protection Solutions. The Radicati Group, Inc. April 2019. Pp53. https://www.symantec.com/content/dam/symantec/docs/reports/2019-radicati-apt-protection-market-quadrant-en.pdf [access date 3/1/2020]

[15] Sofacy Attacks Multiple Government Entities. https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/ [access date 3/1/2020]

[16] MirageFox: APT15 Resurfaces With New Tools Based On Old Ones. https://intezer.com/blog/research/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/ [access date 3/1/2020]

[17] Leo Breiman, “Random Forests,” Machine Learning, vol. 45, no. 1, pp. 5- 32, 2001.

[18] Thomas G. Dietterich, “Ensemble Methods in Machine Learning”, in Proceedings of the International Workshop on Multiple Classifier Systems, (MCS 2000), pp 1-15, Cagliari, Italy, 21–23 June 2000.

[19] R. Markus., et al., "A survey of network-based intrusion detection data sets, ". Computers & security, vol. 8, no. 6, pp. 147–167, 2019.

[20] Cho Do Xuan, Hoa Dinh Nguyen and Tisenko Victor Nikolaevich, “Malicious URL Detection based on Machine Learning” International Journal of Advanced Computer Science and Applications(IJACSA), 11(1), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110119.

[21] The CTU-13 Dataset. A Labeled Dataset with Botnet, Normal and Background traffic. https://www.stratosphereips.org/datasets-ctu13. [access date 3/1/2020].

[22] APTNotes - Github Repo. https://github.com/kbandla/APTnotes. [access date 3/1/2020].

[23] APTNotes - Website https://aptnotes.malwareconfig.com/ Targeted. [access date 3/1/2020].

[24] Cyber Attacks Logbook (Kaspersky) https://apt.securelist.com/. [access date 3/1/2020].

[25] DeepEnd Research: List of malware pcaps, samples, and indicators for the Library of Malware Traffic Patterns. https://contagiodump.blogspot.com/2013/08/deepend-research-list-of-malware-pcaps.html. [access date 3/1/2020].

[26] Malware dump. https://contagiodump.blogspot.com/. [access date 1/4/2020]