Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis

S. C. Y. Ng [*,a] *and M. Bakhtiari*[b]

Advanced Informatics School, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra (Jalan Semarak), 54100 Kuala Lumpur, Malaysia

[*,a]*vader6869@gmail.com,* [b]*bakhtiari@utm.my*

Abstract – *Advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and remain undetected for as long as they can. The intention of an APT attack is to steal data and eavesdropping rather than to cause damage to the network or organization. The problem of APT is the techniques used are stealth oriented and detection of APT attack has been difficult and even almost impossible in the early stage of penetration by exploiting Zero Day Vulnerabilities. This research is aimed at different angles of perspectives in order to detect APT attack by focusing at different areas besides Zero-Day Vulnerabilities. The new approach will detect APT by analyzing the traffic in between attacker and victim in a controlled virtual environment. By analyzing the traffic, this research has collected some samples of evidence in order to aid in APT detection. The achievements of this research are the evidences of connection and traffic patterns of each attack function recorded in traffic monitoring tools. All data were collected to be analyze and patterns of communication were recorded in a graph form in order to provide a clear picture for the researcher to identify the common pattern as an evidence to be picked up when an attack is going on and able to alert the victim. The future work of this research is to implement proposed framework with the actual network of computers with real life networking peripherals and real computer system instead of virtual environment. Besides, this research aimed to analyze the "Knock On" technique used by hacker to contact the C & C Server on demand.* ***Copyright © 2016 Penerbit Akademia Baru - All rights reserved.***

Keywords: Advanced Persistent Threat, Zero Day Vulnerabilities, APT, Cyber Attack

1.0 INTRODUCTION

In our modern days, computers are used to store vital information for further process and to provide services for organizations and society. The information security which provides services is important issues in which the confidentiality, the integrity and the availability of information are core principles of the matter. These principles important and always gets close with the CIA Model. Policy, laws and local rules have been created to enforce these principles [1]. An example of such a law is the Malaysia's "Personal Data Protection Act 2012" which sets rules for the protection of personal information in information systems of any organizations in Malaysia [2].

A breach of one of these principles can be considered to be a security incident. An intentional breach of these security principles by an outsider is often considered a criminal offence by law. For example; in Malaysia this law is called "Computer Crimes Act 1997". Intentional breaches of security by electronic means are often called cybercrimes.

It can be devastating if any organization is targeted by cybercrimes either for political advantage or financial gain. Research shows that cybercrimes are preferable for criminals since they can operate internationally and not all countries have laws against cybercrimes [3]. Cyber criminals easily move

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

their operations to other countries and operate anonymously to avoid prosecution. Even when they are identified by local law enforcement they still run a low risk of being convicted by the local authority because of different country has different rules and laws [4]. Working in the cybercrime industry is even more attractive in countries with high unemployment rates and political unstable, like European countries and even in Malaysia.

Research has shown that criminals in Russia paying IT graduates ten times more than normal jobs would [3]. Economic motives are not the only motivators for cybercrimes but from purely fun and jokes to political motives are purpose which drives hackers to attack companies and even governments facilities and online systems [3]. The growth of the internet and the increased use of computers in society are followed by an increase in the number of attacks. As a result of the rising number of attacks security was tightened. The result is a rat race between cyber criminals and security expert leading to increasingly complex attacks and defences.

The most complex and advanced attacks are targeted attacks which are specifically aimed at companies or governments to reach a predetermined goal. The security company Symantec identifies targeted attacks as one of five recurring themes of cyber security threats in 2010. The other four are often part of a targeted attack [4]. Targeted attacks that received a lot of media attention where the Aurora Trojan, the Stuxnet worm in 2010 and the Diginotar hack in 2011. The Aurora Trojan was aimed at obtaining intellectual property of large corporations [4]. The Stuxnet worm was aimed at disruption of industrial systems in Iran [5].

The “Diginotar” hack was aimed at generating rogue signed certificates with the goal of spying on traffic to websites. The best known example of such a generated rogue certificate was for *.google.com [6]. Targeted attacks with political motives are often easy to detect since they aim to disrupt services to inflict visible damage which gives them publicity. This is often achieved by simple Denial of Service attacks. Targeted attacks with an economic purpose or espionage, like stealing trade or state secrets are executed with more stealth and Advanced methods. Such attacks are also called Advanced Persistent Threats (APT) in literature and by companies [7].

2.0 METHODOLOGY

2.1 Design Method

To accomplish the objectives of this research, the qualitative technique are to be adopted. Details of the qualitative research techniques, a qualitative research is designed to advise the researchers how the process is, and why things happen as they do. Qualitative research has its roots in social science and is more concerned with understanding why people behave as they do: their knowledge, attitudes, beliefs, fears and aims to achieve an in-depth understanding of the situation. This research involves analysis of data such as traffic, timing, or intervals of connection of the attacking traffic. Not only it provides valuable information to certain research questions in its own right but there is a strong case for using it to complement quantitative research methods. The main method for collecting data in this qualitative research methodology is analysing the traffic of an attack. The resulting data is usually transcribed and then analysed for conclusion. Thus, qualitative data are all about texts and data may contain transcriptions.

2.2 Research Framework

This project is to study and investigate the pattern of common Advanced Persistent Threat Attack by creating a real life attack scenario by using computer machines interconnected in a network. This study’s aim is to aid the effort of research in order to detect APT attacks. The framework presented in chapter two defined aspects of attacks related to detection of APT attacks. The attack related aspects describe the attacks and therefore what should be detected. The business aspects are driven by the

impact of the attacks and they give therefore the reason for detection. Detection locations are the places where attacks can be detected. A choice of detection location determines the input data for analysis. Detection and analysis methods determine how attacks are detected. The attack aspects also influence the business aspects and these in turn influence choice on detection aspects. Attack aspects also influence the network locations and these in turn influence the detection aspects. These direct and indirect relations determine the design space. According to [8], in a general level of a cyber-attack, there are 8 steps in common for hackers to launch a cyber-attack as shown in Table 1:-

Table 1: Common APT Attack Steps

Attack Steps	Attack Method	Attack Features	Detection Location	Detection Method	Analysis Method
External Reconnaissance	Attack Method Per Phase	Detectable Features of Attack Method	Network Location Where Aspect/Attacks	Attack Aspect Detected at Network	Analysis by Detection Method
Gaining Access					
Internal Reconnaissance					
Expanding Access					
Gathering Information					
Information Extraction					
Control Of Information Leak					
Erasing Track					

2.3 Operational Framework

The analysis of Advanced Persistent Threat in the literature review shows that the detection of the attack is hard to detect than multi-step attacks are caused by the nature of the exploitation and the effort of attackers to avoid detection at all caused by manipulating the vulnerabilities of operating systems and software [9]. This study will implement an investigation of elements of attacks and detection location where point or places where attacks can be detected. The choice of locations determines the input data for analysis and traffic monitoring. From the common attack step we see in Table 1, the investigation will be focusing on steps starts from the hacker's internal reconnaissance, expanding access, gathering target information and information extraction. An attack scenario will be created in a Virtual Environments using Virtual machines to be played as attacker and victims. During the attack scenario, all inbound and outbound traffic will be monitor while launching each attack in order to investigate the behavior of the attack and traffic pattern of the network when the victim's machine is being access remotely. Traffic analysis sensors of multiple instances shows that it has higher frequency [11]. Table 2 shows the attack methods and attack features and detect location of the Advanced Persistent Attack.

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

Table 2: Methods, Features and Detect Location

Internal Reconnaissance	Malware Rootkit Botnet	Change Network Usage Execution Commands	Server Client Traffic
Expanding Access	Malware Exploits Botnet	Different Traffic Pattern Traffic Content	Server Client Traffic
Gather Information	Malware Botnet	File Usage Pattern File Access Frequency	Server Client Traffic
Information Extraction	Malware Botnet	Volume of Traffic	Traffic

2.4 Methodology Phases

There are three phases involves in the research methodology in order to fulfill the objectives of this research. Phase 1 will be the data gathering on investigation and study about the attack structure, Phase 2 will be the model designing to detect the communication pattern of the attack focusing on the network traffic analysis. Lastly Phase 3 will be the Implementation and Testing of the proposed model design in order to generate result of the findings related to countermeasures of the research.

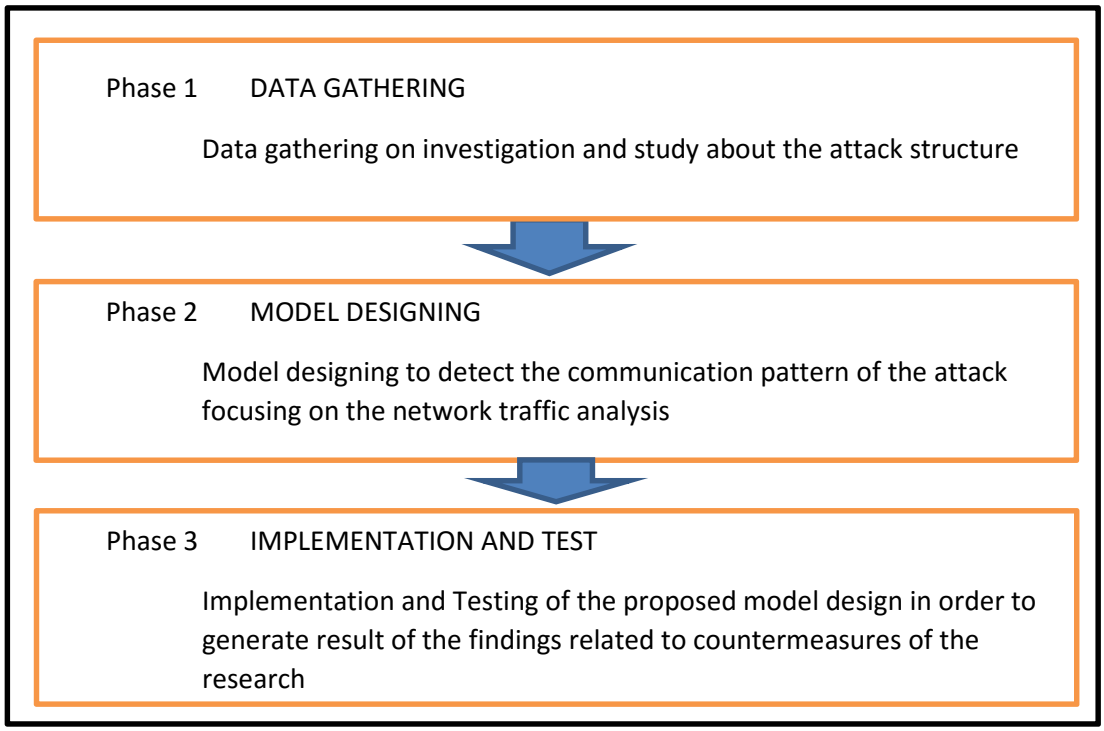


Figure 1: Methodology Flowchart

2.4.1 Data Gathering and Investigation

In the first phase we will be focusing on data gathering and investigate all the elements of Advanced persistent threat attack. This phase will be further split into 4 main elements which contains Low Level to High level Attack, Point of Exploitation, Impacts of Attack, and Elements of Detection. This investigation's purpose is to fulfill the first objective of the research, to study and investigation on vulnerabilities of a computer towards Advanced Persistent Threat and Remote Administrative tool Attack.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

2.4.1.1 Low Level to High Level Attack

The steps of attacks are classified as high level of attack. For examples are the scope we are focusing on including internal reconnaissance, expanding access, gathering information, and extract of information. These are called high level attacks and it's the real intention of the hacker's. In order to achieve success in high level attacks and to get to their goal, hackers need to conduct low level attacks in order to gain vital information either in a complete form or partial fragments. The examples of low levels attacks are sending phishing emails, sending malicious URL link with infected websites, tricking users to install malware, root kits, scanning network for security flaws and etc. Low level attack is vital in order for the hacker to gain as much information as possible and launch their attack to achieve high level goals. So from low level to high levels of attack, these are the steps we are investigating and look into in order to aid the detection of Advanced Persistent Threat attacks.

2.4.1.2 Point of Exploitation

After we are clear with what is the elements of the hacker's attack, we look into Where is the location of the attacks is going to take place. While launching attacks against a system or a network, hackers needs a platform, a location, a place to run their malicious codes or commands. This research is focus on the common and similarities if the hacker's move in order to aid in the detection and countermeasures. So, if a hacker is going to launch an attack (what), which location (where) will he start first? Network, open ports, infected USB sticks, public internet services and etc. This section will be the effort of investigating the location of the attack takes place and where it will be taken place.

The examples of attack location can be log files of operating system and network routers or switches, computer virtual memories, and network traffic. Attack comes from various form, steps and approach. By limiting our methods means limiting the attack steps of the hacker. Detecting only a small amount of attack without linking its relationship with other possible steps taken by the hackers will give a negative effect in detection of the attack, it will cause a false alarm, hence irritating the users, system administrator or whoever it may concern. The full research which involve high cost of intrusion detection by using multiple sensors will provide the most accurate result [11].

According to [10], it requires the colleration of results using methods for distributed system detection in order for the Intrusion Detect System tragetting the complex attack steps launched by the hackers over the network. From the literature review of this research, we stated that all Advanced Persistent Threat attacks where hackers launched remotely will definitely generate network traffic, therefor in research methodology, we are going to focus on the network traffic generated by the attacking steps by creating an attack scenario where attacker and victim both plays the role in the scenario. This is a logical theory where, by analyzing the network traffic, we are suppose to be able to find evidence of an Advanced persistent threat attack. In order to make it happen, we will deployed multiple probes and scanning multiple network protocol ports by using Wireshark as a network monitoring tool to capture as many data as possible and investigate upon it to find the evidence of the attack.

This investigation will be anticipating the ports which will be used by the hackers for the attacks. Hackers used common ports such as HTTP-80/8080, SSL – 443 in order to launch commands upon the targetted victims' machine. This anticipation within the investigation will increase the effectiveness and lower the cost, time and man power to analyze the traffic captured by not scanning the non-common ports where normally network administrator will closed it if it's not nessasary to open for any network operations. This approach will result in reduction of the loads of individual who is doing the analysis work and maintaning the scalability.

2.4.1.3 Impacts of Attack

To answer this question, there's only one word, Impact. The impact of a cyber-attack is the main reason why a defense system and measure are required to be implementing in order for countermeasures and

by reducing the damage of the impact. For this investigation we are aiming at accuracy, effectiveness and economical to defend against cyber-attacks with minimal false alarm for the comfort of the user of the defense system. For an organization to invest in a comprehensive defense system, it depends on a lot of factors such as, cost, necessity, how crucial the information are to be protected and the value of the data. It usually scales down to cost, depending on how much money an organization or company are willing to spend money on defense system and how well their understanding about the impact of an full scale cyber-attack.

2.4.1.4 Elements of Detection

From the previous questions and explanation actually leads to the question on how we are going to detect Advanced Persistent Threat attacks launched by hackers with malicious intent. All the aspects discussed above shows that the attack features which are common and able to be detected can be located in the network traffic, system files, system logs, operating system registries and etc. The traditional signature effectively detects known attack but the concern of this research is about detecting unknown attack, hence, anomaly detection method was used to provide some chances of detecting the attack by analyzing network behavior. The best way so far for defending against unknown APT attacks are the combination of both traditional signature detection and anomaly detection method. This research will be focusing on discovering new elements and aspect in order to aid the detection system available today by study on a real attack scenario created and generate results in order to offer the finding as an aid to the defense system.

2.4.2 Model Design

This phase will focus on the design of the model in order to provide the best result in this research. The purpose of this phase is to fulfill the second objective of the research, to propose a new model of countermeasure for Advanced Persistent based on communication pattern to be able to alert Remote Administrative Tool Attack.

2.4.2.1 Evaluation Model

The focus on this investigation is on all the high level attack, which means that defense system, should be monitoring the organization's machine even after there were no attack has been detected. From the stealth nature of Advanced Persistent Threat Attack, the victim will never know when the attacker will launched their attack. A good defense system should provide all time monitoring in order to detect new unknown attacks, not just provide the client and users the false sense of security. Figure 2 show how the designed model is going to work and shows how and where data will be collected and what data will be collected.

Analyzing the system with too many rules to scan will heavily slow down the process, hence by having decision tree in the application of the rule for the purpose of reducing the time to analysis the traffic [12]. There are 2 enviroments involve in this model design, The Virtual Enviroment where the attack scenario is located and demonstrated. Another one is The Actual Enviroment where the researcher is monitoring the network traffic of the attack when it takes place. This model design are capable of providing the researcher enough information as evidence to investigate the attack pattern and all the elements of the attack. In the Model design itself consist of 3 parties which are the Attacker, Victim, and the Researcher all playing their role in order to make this research a success. The suggestion to the implementation of the learning rule will be the next approach of this study. The example porposed will be a fuzzy rule-based inside the model of the design [7]. The approach to investigate the attacking traffic will be SNORT and Wireshark. Wireshark records the traffic and will be saved in a .cap file. Investigation can be made upon the information recorded in the file where attack took place. This investigation will further generate a report to show evidence of the study.

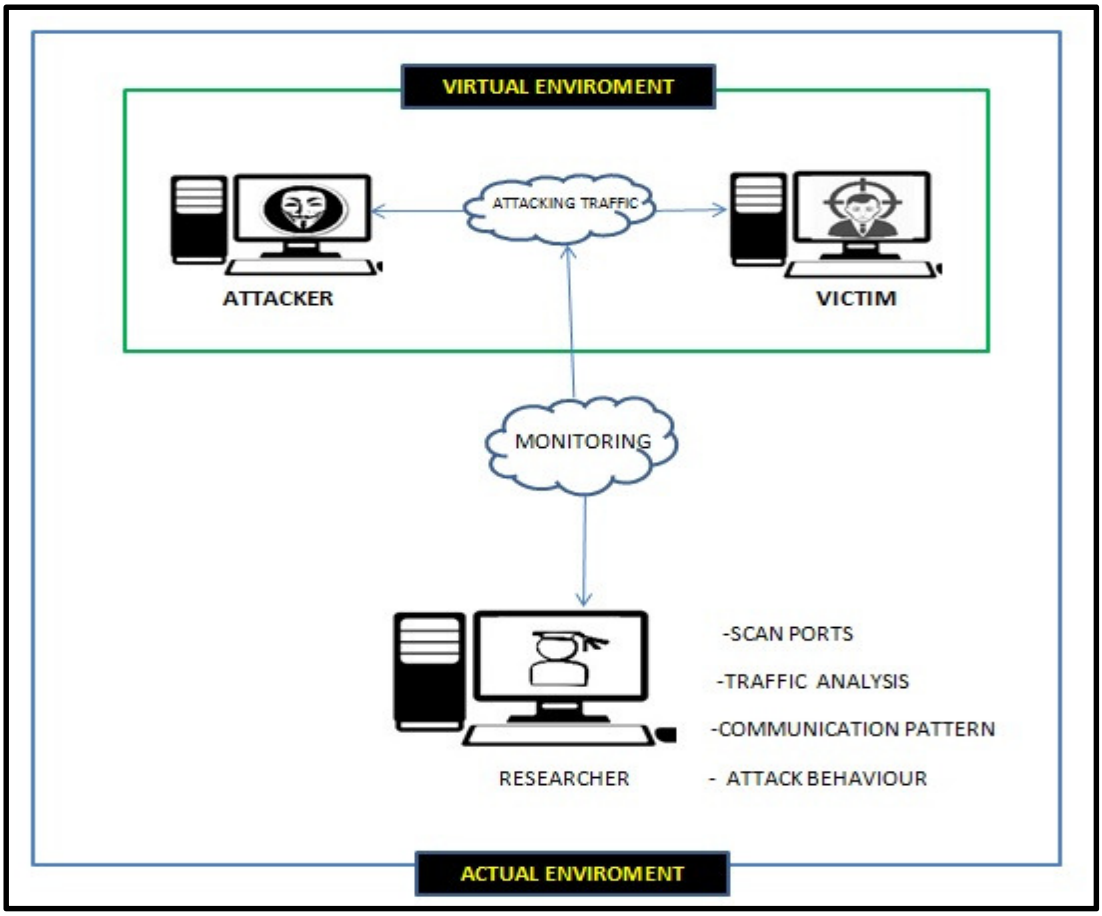


Figure 2: Framework Model

From the research of the related topic, the knowledge of low level attacks were studied in order for the researcher to create attack scenario for the purpose of correlation of events [13] [14]. Shell software were not proposed because it provides no common communication standard and the protocol they created, IDMEF were never being test in the real life scenario and only being tested in the laboratory [15].

2.4.3 Implementation and Test

This phase will focus on the implementation and the testing of the model in order to proof the theory of the model design. The purpose of this phase is to fulfill the third objective of the research, to implement and test the proposed countermeasures for Advanced Persistent Threat based on communication pattern against RAT attack.

2.4.3.1 Phases of High Level Attack

As we describe in data gathering and investigation of phase 1, we will be focusing mainly the 4 phases of an APT attack which consist of internal reconnaissance, expanding access, gathering information, and extracting information. The main reason we choose this 4 phases of high level attack very much related to the design of our model in phase 2. The reason this 4 steps is focused because during the implementation of this phases, the hacker and the victim generates the most traffic in between the 2 parties[15], hence, giving the researcher the availability of evidence flow through the network and can provide the effectiveness of the evidence collected through the network monitoring tools.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

2.4.3.2 Internal Reconnaissance and Expanding

Once the hacker gain access into the victim's computer or network, usually by multiple steps of low level attacks in order to achieve in to this step, they will start to scan the machine, network, computer manufacturers, software versions, and other related juicy information to look for potential exploits. It is during this point of attack hackers will generate the most noise in the network because each step the take for the purpose of reconnaissance, the send out commands to the victim's machines and the C & C server will respond to it and reply with information the hacker needs. This is the time where the researcher can collect the most evidence and proof of intrusions in order to aid the detection of unknown attacks.

Once the hacker found the slightest or any flaw in the operating system or the software vulnerabilities, he will start creating possibilities for further expansion of his access to other parties such as network clients and servers. The attacker will start performing active reconnaissance on the computer system and network itself by implementing its backdoor malware for a convenience of a call back functions whenever he needs it again. The model design we proposed is targeting on the noise generated by the hacker during this phase. The noise of the attack will largely affect the network communication behavior because when the hacker is doing internal reconnaissance, he is doing trial and error by testing all the possibilities and whatever it takes to get as much information as possible. By this trial and error, he is actually breaking the network behavior and the pattern of the communications. The anomaly detection technique is based on traffic inbound/outbound frequencies to identify unusual traffic between server and client and unusual traffic will be identified as a suspicious event. This might not be very useful because the inbound/outbound traffic a lot depends on the behavior of the user of the machine. This will lead to more false alarms which is unnecessary.

2.4.3.3 Gathering and Extract Information

Once the attacker done his internal reconnaissance, by this stage the hacker should be already have a hold of the information's location he is looking for. Information such as technical documentation, financial report, management letters and media files like video, photos and images are consider the most valuable information within an organization because it holds all the important and decision making data for the high level of management people. Before they can extract the information, the will make it look legitimate in a file storage application in the public internet in order for the extraction to look very normal. They will then continue to snoop around for other juicy information which is valuable for other organizations.

When the hacker starts to manipulate the C & C server and issue command for it to download the valuable information from the victim's machine back to the hacker's machine, this will create the most noise in the network as a uncommon connection has established in between the attacker and the victim over the C & C server which have been deployed by the hacker by manipulating the vulnerabilities of the system and exploitation of the system flaw.

This is where the Researcher will monitor the traffic, open ports, connection information, IP and other crucial information needed to generate the result in order to aid detection. The communication between the C & C server from the victim's machine back to the attacker may seem legitimate because they use normal ports such as HTTP-80/8080. SSL-443. So as for this research, the monitoring will start with a non-attack scenario and recorded to be a base line and standard for a clean environment without any hacking activities. This standard will then be compared to the attacking scenario generated traffic and result. Hence, the difference between the attacking scenario and the Non attacking clean state scenario will be the uncommon behavior of the unknown attack and provide enough information to aid in intrusion detection.

3.0 RESULT AND DISCUSSION

This section below will be the implementation and test of traffic data collection of our proposed detection method after an Advanced Persistent Threat already took place. All inbound and outbound traffic will be monitored by "Wireshark" and all network connection link will be monitored by "TCPView". "DU Meter" will be used as well to calculate the total output and input data of the attack as well, it will be filtered out to record only IP address of Attacker and Victim only to avoid any confusion with normal operating system's service traffic. This section below will go through all 5 common functions of Remote Administrative Tool named "NjRAT v0.7".As we mentioned about the Framework Model, this section below will demonstrate the in-depth of what is actually happening in the monitoring scenario. The attacker's environment is shown in Figure 3.

Figure 3: Attacker's Environment

As you can see from the Figure 3 and Figure 4, the attacker is running a RAT called NjRAT v0.7 which is capable of running all common functions of a Remote Administrative Tool to demonstrate the hacker already gain access into the victim's system by exploiting known vulnerabilities and unknown zero-day vulnerabilities. In this research we will monitor the attacker's traffic to see how much data they require to send out to command the C & C server which has been installed in the victim's computer. From the victim's side, you can see Wireshark running IO Graph function to record all TCP traffic in between the hacker's machine (192.168.118.128) and Victim's machine (192.168.118.140). Our research has shown that both attacker and victim are communicating with each other mostly with TCP protocol.

3.1 Data Collections Based on RAT functions

In this section, this research will look in-depth into each function of Remote Administrative tool. We will collect data based on how a RAT works.

3.1.1 C&C Server and Victim "KeepAlive" Signal

In this test and implementation, we have already installed the C&C Server on victim's machine (192.168.118.140) generated by NjRAT 0.7d and connect through an uncommon port which is Port 5552 to avoid any interference with other legitimate traffic. This isolation of port usage will make our

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

result more accurate without interfering with other legitimate operating system service traffic and software traffic. In this section we are testing the "KeepAlive" signal in between the attacker's machine and the C & C Server installed in the victim's machine. From our research, based on our data collection from the inbound and outbound traffic monitoring, the Attacker (192.168.118.128) will send a TCP [PSH, ACK] every 15 to 18 seconds to the Victim (192.168.118.140). The victim's C&C server will then reply with a [PSH, ACK] packet as well to respond to attacker's RAT. Attacker will then reply with a [ACK] packet to notify the victim's C&C server that the attacker has acknowledge of its existence on the network that connection has established as shown in Figure 5 and Figure 6.

From the IO graph of "Wireshark", we filter out only TCP connection which only contains the traffic in between Attacker (192.168.118.128) and Victim (192.168.118.140) only and the connection pattern of "KeepAlive" signal are as shown in Figure 7.

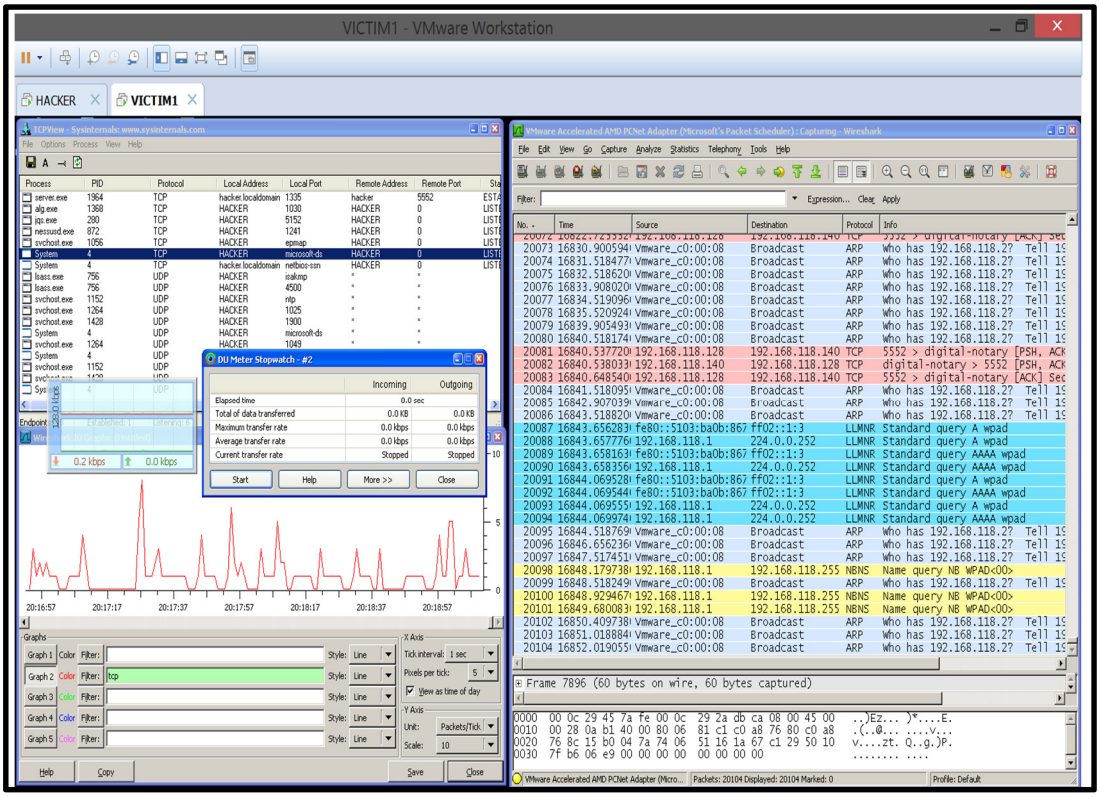
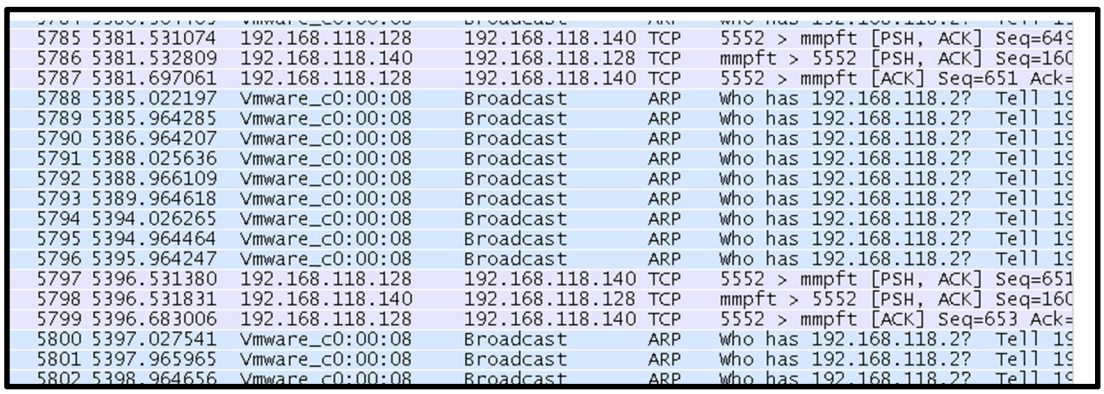


Figure 4: Victim's Environment

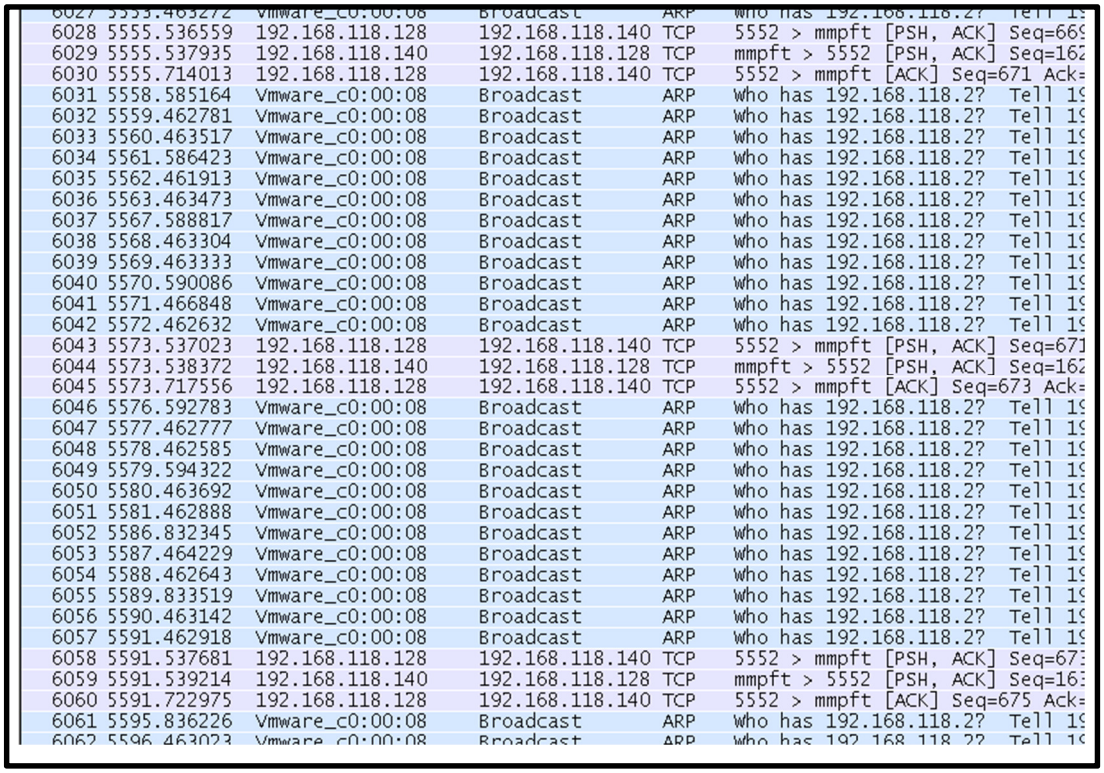


5785	5381.531074	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [PSH, ACK] Seq=649
5786	5381.532809	192.168.118.140	192.168.118.128	TCP	mmpft > 5552 [PSH, ACK] Seq=160
5787	5381.697061	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [ACK] Seq=651 Ack=
5788	5385.022197	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5789	5385.964285	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5790	5386.964207	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5791	5388.025636	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5792	5388.966109	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5793	5389.964618	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5794	5394.026265	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5795	5394.964464	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5796	5395.964247	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5797	5396.531380	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [PSH, ACK] Seq=651
5798	5396.531831	192.168.118.140	192.168.118.128	TCP	mmpft > 5552 [PSH, ACK] Seq=160
5799	5396.683006	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [ACK] Seq=653 Ack=
5800	5397.027541	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5801	5397.965965	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
5802	5398.964656	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19

Figure 5: 15 Seconds Interval Connection Sample

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016



6028	5555.536559	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [PSH, ACK] Seq=669
6029	5555.537935	192.168.118.140	192.168.118.128	TCP	mmpft > 5552 [PSH, ACK] Seq=162
6030	5555.714013	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [ACK] Seq=671 Ack=
6031	5558.585164	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6032	5559.462781	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6033	5560.463517	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6034	5561.586423	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6035	5562.461913	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6036	5563.463473	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6037	5567.588817	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6038	5568.463304	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6039	5569.463333	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6040	5570.590086	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6041	5571.466848	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6042	5572.462632	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6043	5573.537023	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [PSH, ACK] Seq=671
6044	5573.538372	192.168.118.140	192.168.118.128	TCP	mmpft > 5552 [PSH, ACK] Seq=162
6045	5573.717556	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [ACK] Seq=673 Ack=
6046	5576.592783	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6047	5577.462777	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6048	5578.462585	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6049	5579.594322	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6050	5580.463692	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6051	5581.462888	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6052	5586.832345	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6053	5587.464229	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6054	5588.462643	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6055	5589.833519	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6056	5590.463142	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6057	5591.462918	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19
6058	5591.537681	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [PSH, ACK] Seq=673
6059	5591.539214	192.168.118.140	192.168.118.128	TCP	mmpft > 5552 [PSH, ACK] Seq=163
6060	5591.722975	192.168.118.128	192.168.118.140	TCP	5552 > mmpft [ACK] Seq=675 Ack=
6061	5595.836226	Vmware_c0:00:08	Broadcast	ARP	Who has 192.168.118.2? Tell 19

Figure 6: 18 Seconds Interval Connection Sample

As you can see from the IO graph above, the connection in between Attacker and Victim are constantly connected via a TCP connection and it has scaled down into a very predictable time interval gap of 15 seconds. The total data transfer in between the 2 machines are kept very minimal to avoid detection. This research has monitored the traffic in between both machine and we have found that it's only less than 128 kilobyte for both incoming and outgoing data transferred over a more than 11 hours and 33 minutes of monitoring as shown in Figure 8.

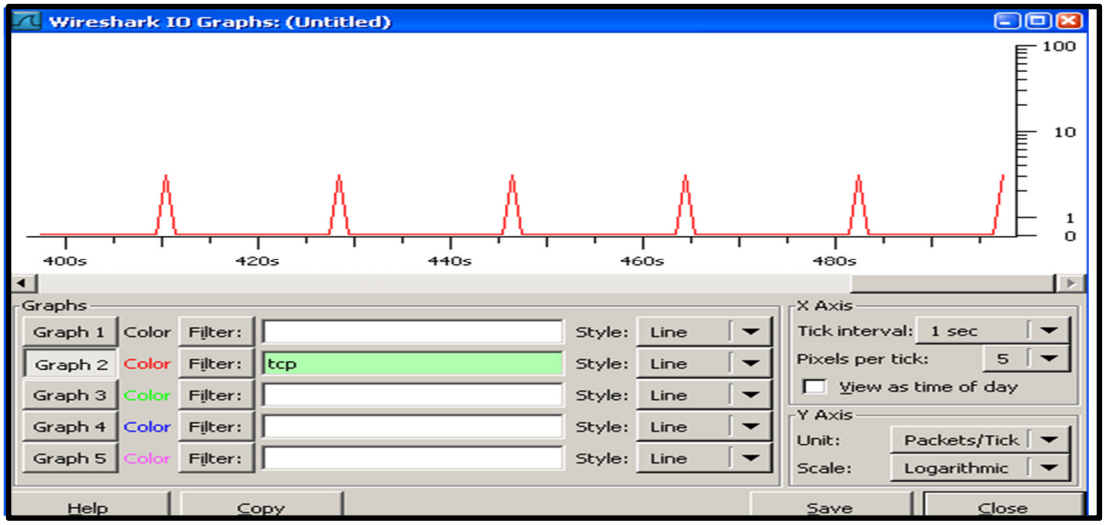


Figure 7: Connection Pattern of RAT

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

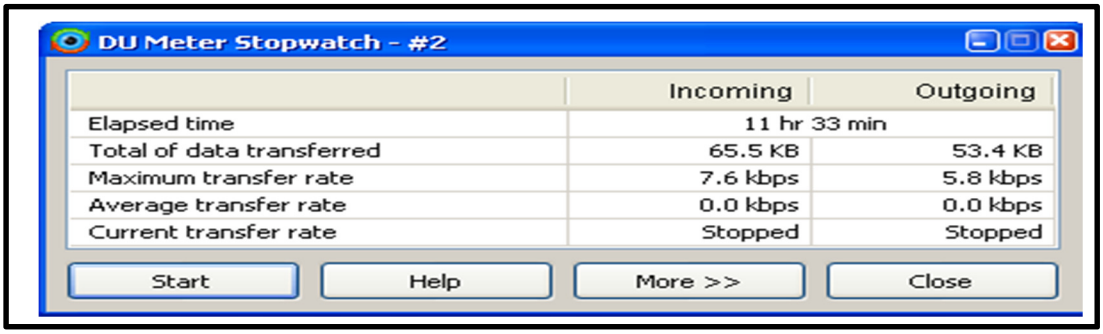


Figure 8: Total Data Transfer of KeepAlive

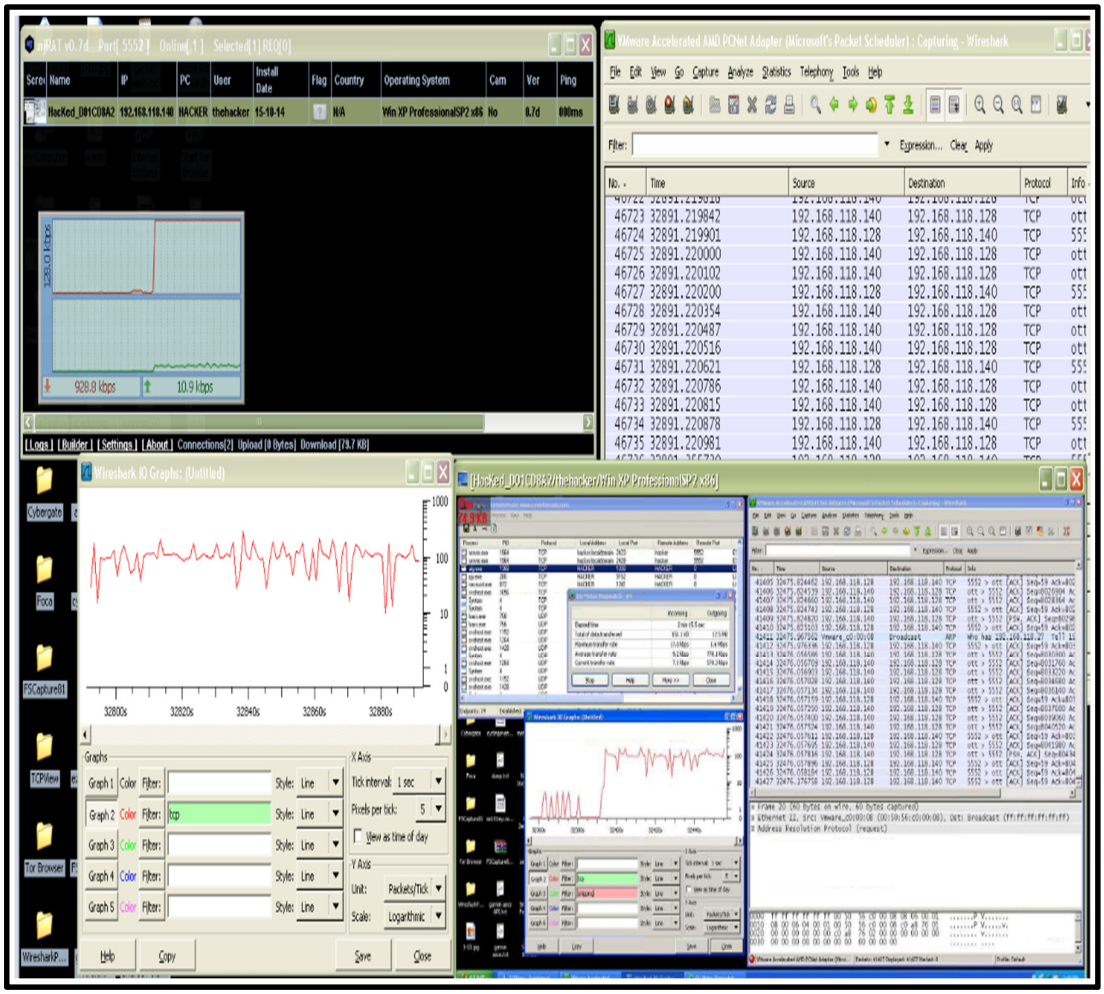


Figure 9: Attacker's Side Remote Desktop

As a result from this monitoring, we can conclude that the communication in between the attacker and victim via a RAT tool are actually predictable with actual data and analysis collected from this research. The pattern of communication actually exist and it can be picked up. This information can actually aid anti-virus software and firewalls to detect and alert the user/victim about an Advanced Persistent Threat is actually happening in the organizations computers/network.

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

3.1.2 Remote Desktop

Remote Desktop is one of a common function exist in almost all RAT available in the dark market including PoisonIvy, Cybergate, Dark Comet and Etc. This function enable hacker to view exactly what the victim is doing in their computer. It's a live video feed and it captures the screen and can even record as a video file. This feature normally generate a big amount of noise in the network and it should be easily aid in detection of any Advanced Persistent Threat exploiting Zero-Day Vulnerability from the initiation of the attack from the attacker machine (192.168.118.128), this research has found that there is a network traffic spike from an Average traffic of 0.5 kbps into a noticeable and easily traced big amount of traffic of 800 kbps in average. The data recorded are shown as Figure 9.

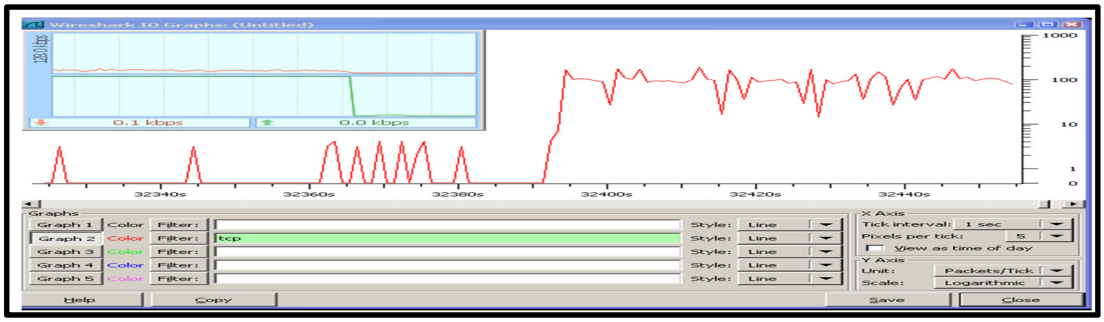


Figure 10: Remote Desktop Traffic Spike

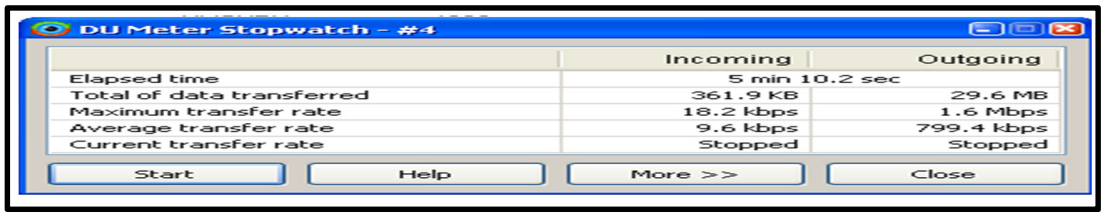


Figure 11: Remote Desktop Data Transfer rate

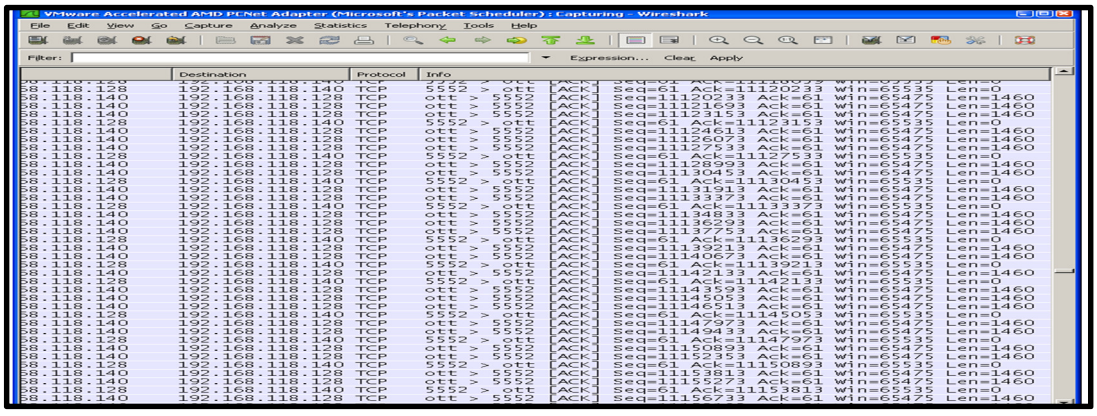


Figure 12: Data Length Remote Desktop

This is the screen from the attacker's side, as you can see the attacker can clearly see what is going on in the victim's screen. This has generate a continuous TCP traffic in order for the attacker to have a live video feed of the victim's screen. The noise generated by this attack is very loud in the network and should easily picked up by monitoring the network and shall be presented as an evidence of the existence of RAT attack is taking place in the victim's computer. The network spike can indicate the attack and

should be able to alert the victim that someone is looking at their screen. The network spike recorded are as Figure 10.

From the analysis and study on the monitored traffic of RAT remote desktop function by the attacker towards the victim, a set of Data length remain constant at Len = 1460 bytes. That can also be an evidence to pick up to determine a RAT attack exist in the system. The analysis also shows that by just a short period of time which we recorded for only a little time over 5 minutes, a total of 29.6 MB of data already uploaded out from the Victim to be sent over the network to the attacker with each packet data length of 1460 bytes as shown in Figure 11 and Figure 12.

3.1.3 Remote Microphone

Remote Microphone is a common function in all RAT. This function enables hacker to remotely turn on the build in microphone of the victim's computer and listen to whatever conversation the victim is talking about. This can be very dangerous as it involves privacy, and secrecy of an organization such as important business meetings and even government and military top secret meeting. This functions is as useful as not only to listen, it can be recorded remotely if they infiltrate the system beforehand. In the initial stage of remote microphone being activated, there is a spike of the network traffic as well, but from the research, the traffic volume is much lesser compare to Remote Desktop Live Video Feed, the result of the research observation are as shown in Figure 13:

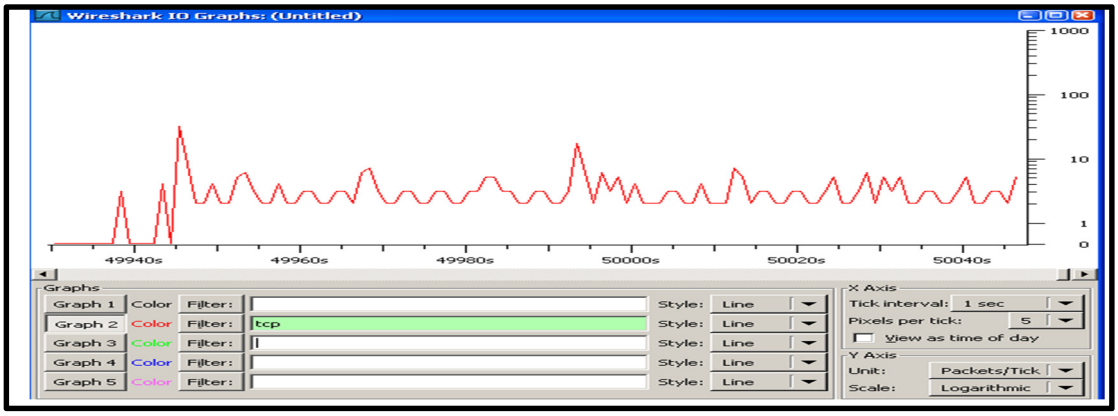


Figure 13: Remote Microphone Traffic Spike

From Figure 13, besides the traffic spike, there are a specific pattern of the communication when the attacker is listening from the victim's microphone. It generates a significant noise in the network which can be an evidence to lead the researchers to detection of an Unknown attack.

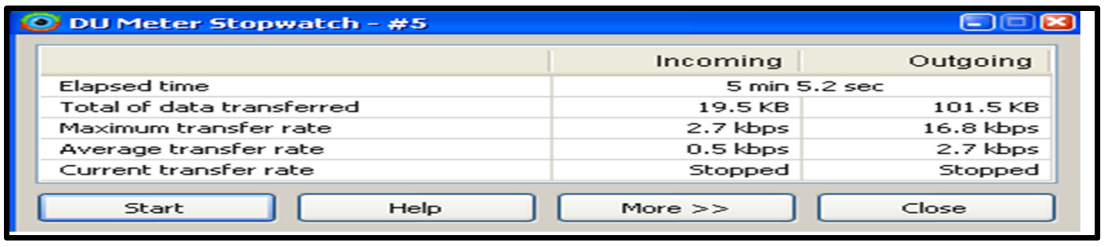


Figure 14: Remote Microphone Data Transfer Rate

Figure 14 shows that Data rate of transfer are kept at minimum in order to avoid detection and loud noise in the network traffic. Compare to Remote Desktop Video Feed of 800 kpbs, Remote Microphone only averages about 16.8 kbps to be fully operational. The total data transferred over 5 minutes of monitoring only clocked about 101.5 KB. Besides that, the data length of each packet are at a constant rate of 233 byte per packet of transfer over the network which can be identify as an evidence to aid detection of an attack towards a victim's machine as shown in Figure 15.

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

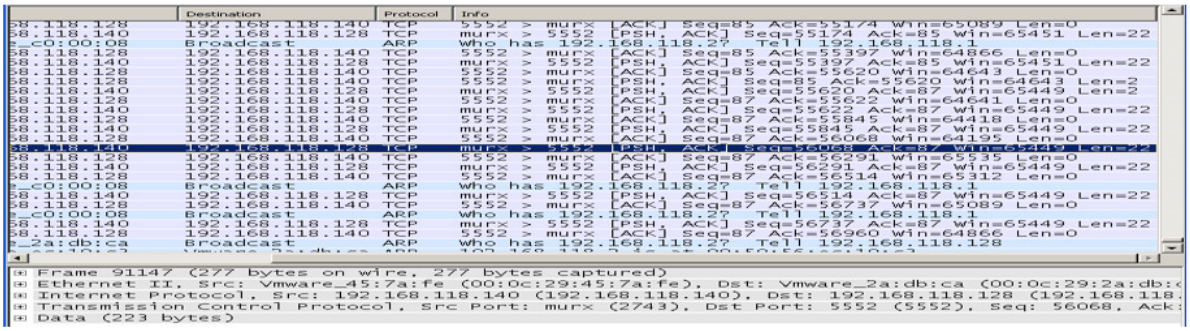


Figure 15: Data Length Microphone

3.1.4 Keylogger

Keylogger is a very basic function of a RAT. It helps hacker to obtain passwords and as a monitoring functions to monitor what the victims are up to. This function enable the hacker to record whatever the victim is typing through their keyboard. This is normally use to steal password when the victim is typing their password into the web browser. This attack is hard to detect because it only generates a small amount of noise in the network traffic when executed. This is Shown in Figure 16:

Figure 16: Keylogger On Attacker's Side

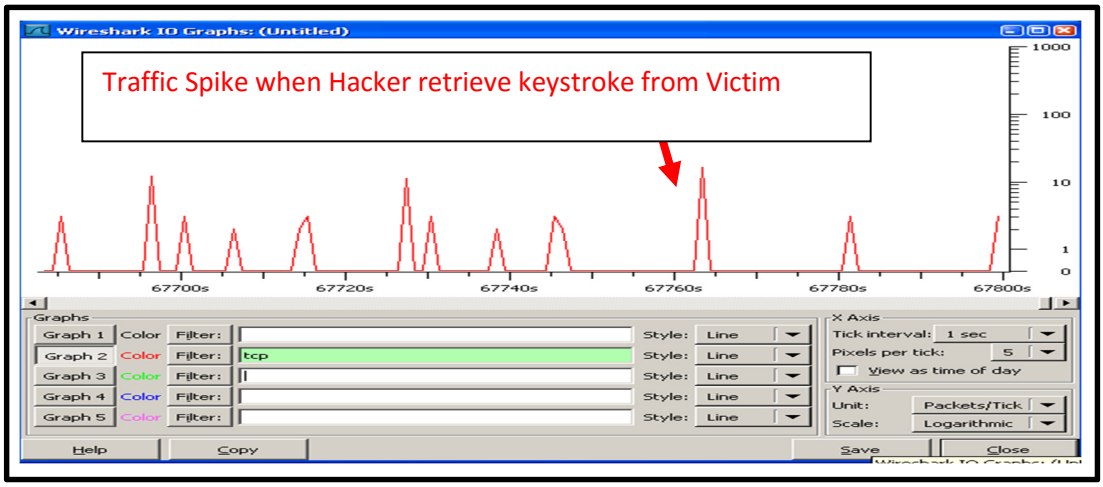


Figure 17: Keylogger Traffic Spike

The traffic spike when the hacker retrieve the keylogged data can dramatically help in detection. The unusual TCP connection creates noise in the network and can be identify as evidence of an RAT attack if monitored from the victim's machine. This research has captured the keylogger attack traffic for 5

minutes and the data flow in between the attacker and victim is at a very minimal rate. This data captured cannot be justify as evidence for RAT detection because unlike other RAT attack, it doesn't generate big chunks of data to be appeared as suspicious activity to be able to aid in detection of RAT attack.

3.1.5 Remote File Download

This is a function which exist in all RAT in order to steal files by remote download from the victim's computer. It basically includes File Explorer to browse around all the file structures of the victim. It can also browse into the victim's restricted system folder as if it already obtains the administrative privileges. Once the RAT is deployed via the exploit of zero-day vulnerability, hacker can view, download, and upload whatever files they want into victim's computer remotely. If hacker uses this functions, it will generate a huge amount of noise to be able to be picked up for detection. The larger the file the hacker steals, the louder the noise will be generated in the traffic to be picked up as an evidence to be detected as RAT attack exist in the system. This research has picked up the noise in the implementation and test of the method proposed.

Figure 17 in this research has look in to the traffic spike during the attack, and the observation was interesting and the noise is so loud in the traffic and it can be a very clear indicator to be identified as an evidence of a RAT Attack.

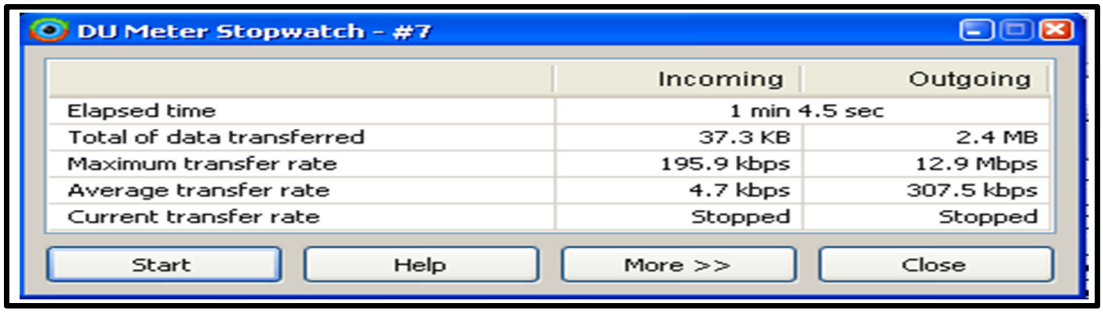


Figure 17: Data Collection of Remote Download

Based on the traffic data recording in Figure 3.19, this research has monitored the remote file explorer for only less than 120 seconds for the initiation of the attack and transfer a 2.4 MB Docx file from victim to the attacker. Amazingly when it takes a very short period of time to transfer the file over to the attacker because from the study it actually triggers the maximum transfer rate of the network can offer. It spikes up to 12.9 MBps in 4 seconds and drop back down to 0.2 kbps in less than a second after closing the TCP connection. This shows a very huge spike was created and the noise in the network can be easily picked up. In a nutshell, it only takes less than 5 seconds to transfer a 2.4MB file from the victim to the attacker, the noise is so loud that it should be easily picked up by any traffic monitoring software and be used as an evidence. The noise and traffic spike is shown in Figure 18.

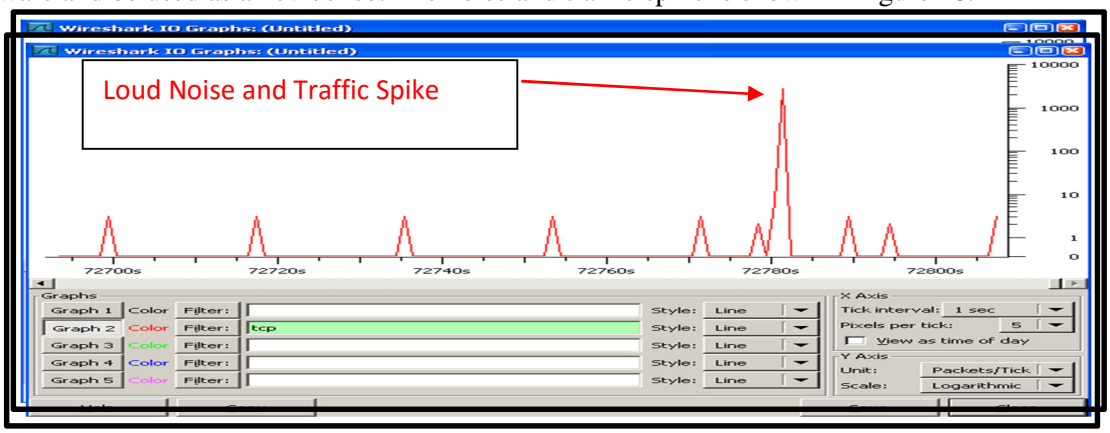


Figure 18: Traffic Spike of Remote Download

4.0 CONCLUSION

This research went through all common functions of Remote Administrative Tool named "NjRAT v0.7" and was filtered out to record only traffic from IP address of Attacker and Victim only to avoid any confusion with normal operating system's service traffic. As we mentioned in the Framework Model, this test and implementation demonstrated the in-depth of what is actually happening in the monitoring scenario. All data was collected to be analyse and patterns of communication were recorded in a graph form in order to provide a clear picture for the researcher to identify the common pattern as an evidence to be picked up when an attack is going on and able to alert the victim. The main idea of this research is that every cyber-attack involving Advanced Persistent Threat with or without zero-day vulnerabilities, known or unknown attack will definitely generate traffic in between the attacker's machine and victim's host. This research is about analysing the traffic in between the attacker and victim's machine by creating a virtual environment. Every outbound and inbound traffic of the attack will definitely leave evidence in real time. So the virtual environment will demonstrate the activity of the attacker and from the traffic they generate, we will look into the common pattern in the traffic to pick up traces of the existence of attack. This research aimed directly at the traffic pattern of each attack function of Remote Access Tool after they have exploit using known or unknown attack. The traffic data collection will be on the victim's side because victim's machine is the one obeying the attacker's command via RAT and that being said, most evidence will be at the victim's side. This research is limited to time constraints, the proposed framework will contribute to the antivirus, network intrusion and prevention, as a reference when developing a control framework for preventing Advanced Persistent Threat attack by exploiting zero-day vulnerabilities. The proposed framework was developed based on past research that were conducted through the duration of this project. Therefore it is still pending for implementation by the detection based organization to provide the actual implementation result.

ACKNOWLEDGMENT

The author would like to thank for the support given to this research by Malaysia Ministry of Defense (MINDEF) and Universiti Teknologi Malaysia (UTM) for providing an opportunity and necessary facilities to support this research work.

REFERENCES

[1] A. K. Sood, R. J. Enbody, Michigan State University (2013).

[2] A.B. Munir, S.H.M. Yasin, Personal Data Protection in Malaysia. Sweet & Maxwell Asia (2012).

[3] Advanced Persistent Threat: A Decade in Review, Command Five Pty Ltd, June, 2011

[4] C. Iheagwara, A. Blyth, T. Kevin, D. Kinn, Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation, Information and Software Technology 46 (2004) 651-664.

[5] C. Kruegel, T. Toth, Using Decision Trees to Improve Signature-Based Intrusion Detection, in *RAID 2003*, Pittsburgh, 2003

[6] Govcert.Nl, Stuxnet - eengeavanceerde en gerichteaanval, Govcert.Nl, The Hague, (2011).

[7] Fox-IT, Interim Report, DigiNotar Certificate Authority breach, Fox-IT Business Unit Cybercrime, Delft (2011).

[8] C. Tankard, Persistent threats and how to monitor and deter them, Network security 2011 (2011) 16-19.

[9] D.R. Cooper, P.S. Schindler, Business Research Methods. McGraw Hill, International Edition (2008).

[10] D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, MetasploitableThe Penetration Tester's Guide (2011).

[11] C. Zhou, C. Leckie and S. Karunasekera, A survey of coordinated attacks an collaborative intrusion detection, Computers & Security 29 (2010) 124-140.

[12] FireEye 2014, Zero Day Vulnerabilities, white paper survey of 2013.

[13] Frankie Li, Anthony Lai, DdlDdl Valkyrie-x Security Research Group {ran2, drakfloyd,dll}@vxrl.org (2011)

[14] N. Gaud, A. Deen, S. Silakari, Architecture for Discovery of Context-Aware Web Services Based on Privacy Preferences. In 2012 Fourth International Conference on Computational Intelligence and Communication Networks, IEEE (2012).

[15] H. Debar, F. Telecom, D. Curry, Guardian, B. Feinstein and I. Secure Works, The Intrusion Detection Message Exchange Format (IDMEF), The IETF Trust, Network Working Group, 2007.