ENSEMBLE OF CLASSIFIERS FOR DETECTION OF ADVANCED PERSISTENT THREAT

OKWARA JERRY CHIZOBA

A dissertationsubmitted in fulfilment of the
requirements for the award of the degree of
Master of Science Computer Science

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JUNE 2019

DEDICATION

This dissertation is dedicated to my dear wife Okwara Martina Bose and children (Okwara Gerald Ikechukwu, Okwara Dominica Chikaima) for their support and prayers which kept me afloat in the course of this Masters study.

ACKNOWLEDGEMENT

Reverence and all Glory be to the Almighty God, Most High, Good Shepherd and giver of live, wisdom, knowledge and understanding for the opportunity to learn.

I would like to appreciate my Supervisor Dr. Anazida Binti Zainal for her motivation, immense and untiring support during this journey. While preparing this dissertation, contacts were made with researchers, seniors, classmates (Dr. Nurudeen Mahmud Ibrahim, Juan Ramon Moya, Salma Hussein Omar, Rafeena Binti Mohamad Rabii) and their inputs made great impact; I appreciate you all.

I want to specially appreciate the Tertiary Education Trust Fund (TETFund) for sponsoring my Masters study, I am indeed very grateful. My profound gratitude also goes to my employer The Federal Polytechnic Ado-Ekiti, Dr. Akande Theresa Taiwo, Mrs. Adediran Stephania and Mr. Jimoh Abdul-Ganiyu Adetunji for their support and encouragement. Many thanks to the Skudai Catholic Centre (SCC) family, Rev. Fr. Christopher Lee, Mr. Krishna Ramoo and Ms. Sylvia Leicester for their hospitality, love and spiritual guidance.

In a special way I want to thank my siblings, Late father Mr. Andrew Okwara of blessed memories and my dear mother Mrs Edith Okwara for the instilled discipline, love and care which I find priceless.

ABSTRACT

The demand for application of technology in almost all walks of life is in the increase and can be seen to be geared by the paradigm changes in industrial revolutions (current 4.0), IoT/IoE (Internet of Things/Internet of Everything) concept, Internet 2.0, Artificial Intelligence (AI), BYOD (Bring Your Own Device) to mention a few but not without their increased inherent vulnerabilities and exposure to sophisticated and dynamic awaiting threats. Advanced Persistent Threats (APTs) among other malwares are some of the malicious attacks given serious attention as they have shown some level of complexities thereby causing defender solutions to poorly detect them. Poor APT attack tactics understanding, insufficient network traffic log analysis and poor classification are some of the problems identified for poor detection of these attacks. Network traffic logs are used by researchers to analyse the network and track attacks as packets move across network nodes. This research studies attack modelling in order to understand APT attack tactics and generate their dataset through simulation as well as a real dataset for normal operation. The experiment will be simulated on a virtual environment using dimensionality reduction technique on the network traffic log for improved log processing. To improve the APT detection accuracy flawed by their stealthiness, the ensemble of classifiers (Support Vector Machine, Random Forest, Decision Tree) with majority voting is used for better attack classification which resultantly gives a better detection accuracy of 90.47%.

ABSTRAK

Permintaan bagi teknologi aplikasi untuk hampir kesemua lapisan masyarakat telah meningkat dan boleh dilihat ianya dicetuskan oleh perubahan paradigma di dalam konsep revolusi perindustrian (terkini 4.0), IPB/IoE (Internet Pelbagai Benda/ “Internet of Everything), Internet 2.0, Kecerdasan Buatan, BYOD (Bring Your Own Device) tetapi bukan tanpa kelemahan mereka yang wujud dan pendedahan kepada ancaman yang sofistikated dan dinamik yang menunggu. Advanced Persistent Threats (APT) adalah antara serangan yang diberi perhatian yang serius disebabkan serangan itu memberikan kerumitan yang menyebabkan solusi pertahanan tidak dapat mengesan dengan baik. Pemahaman yang kurang tentang taktik serangan APT, analisis log trafik rangkaian yang tidak mencukupi dan cara klasifikasi yang kurang memberangsangkan adalah beberapa masalah yang dikenalpasti menyebabkan pengesanan yang kurang baik untuk serangan-serangan ini. Corak trafik rangkaian digunakan oleh penyelidik untuk menganalisa rangkaian dan menjejak serangan- serangan semasa paket bergerak merentasi node-node rangkaian. Penyelidikan ini mengkaji model serangan bagi memahami taktik serangan APT dan menjana dataset melalui simulasi dan juga data sebenar untuk operasi normal. Eksperimen ini akan disimulasikan di dalam persekitaran maya mengunakan teknik “dimensionality reduction” ke atas log rangkaian trafik bagi penambahbaikan pemprosesan log. Bagi memperbaiki ketepatan pengesanan APT yang cacat akibat sifatnya yang senyap, kumpulan pengelas (Support Vector Machine, Random Forest, Decision Tree) bersama pengundian majoriti di gunakan untuk pengelasan serangan yang lebih baik yang memberikan ketepatan pengesanan

Yang lebih baik 90.47%.

CHAPTER 1

INTRODUCTION

1.1 Problem Background

There is a growing demand for technology application and development in almost all walks of life leading to flexibility of platforms (hardware, software) that run their day to day operations. This has witnessed an increase in the use of mobile devices, cloud computing and company policies like BYOD (Bring Your Own Device) as a form of support or use for getting works done either onsite or from some remote locations (Rashid et al, 2014). These migrations and developments seems amazing but not without their increased vulnerabilities and exposure to attacks. Again, devices (Routers, Firewall etc.) that enable establishment of communication/access checks for these infrastructure are most times not properly configured, prone to vulnerabilities and or allows access due to trust thereby exposing its asset to possible threats (Randy, 2017; Rashid, et al, 2014). A typical example of how attackers exfiltrated data from their target stealthily would be to use among other means Internet Control Message Protocol (ICMP) echo request, Alshamrani et al (2019); Daniel (2018); Randy (2017); Singh et al (2003) which will evade scanning completely because it is considered benign (Shick and Horneman, 2014; Rashid et al, 2014). Over the years, computer networks have suffered from security setbacks owing to the incessant theft, destruction, sabotage, espionage to mention a few oriented attacks over its infrastructure (Brewer, 2014). Most of the severe cases are with targeted attacks on confidential and critical assets hosted on such infrastructures owned by governments, organizations and businesses, Alshamrani et al (2019) to mention a few. This type among other attacks is known for its use of increasingly advanced/sophisticated techniques, stealthy nature and die-hard persistence (Alshamrani et al, 2019). Today’s attackers are skilled at using a vast amount of sophisticated tools to garner information and attack their targets

(Alshamrani et al, 2019; Tankard, 2011). All these to mention a few have accorded them the nomenclature "Advanced Persistent Threats (APTs)".

As described by Nicho and Khan (2014) an "Advanced Persistent Threat (APT) is a term accorded to a new breed of insidious threats that use multiple attack techniques and vectors conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed, for long periods of time." In addition, the National Institute of Standards and Technology (NIST), (2011) describe the threat as:

"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, programme, or organization; or positioning itself to carry out these objectives in the future. The Advanced Persistent Threat:

(i) pursues its objectives repeatedly over an extended period of time;

(ii) adapts to defenders' efforts to resist it; and

(iii) is determined to maintain the level of interaction needed to execute its objectives."

The aftermath of these undesired activities is mostly huge losses and damages on the part of their target.

According to the Office of Cyber Security and Information Assurance, 93% of large corporations and 87% of small businesses reported some form of cyber breach in 2013 (Brewer, 2014). Furthermore, a Ponemon Institute study found that, in 2013, the average annual cost of cybercrime globally was $7.22m per organization, representing a 30% increase on the previous year's study (Brewer, 2014). As we move forward with more objects becoming Internet enabled and more services moving online, the cybercrime problem is only likely to worsen. In fact, an analyst firm Gartner recently stated that it is becoming impossible to prevent targeted attacks and organizations should instead focus their security spending on monitoring and response techniques (Brewer, 2014). With this in mind, analysts have predicted that, by 2020, 60% of security budgets will be spent on rapid detection and response approaches, up from less than 10% in 2013.

The aforementioned shows the level of effort and attention given to APTs as well as the intended deviation from the conventional detection/prevention approach to a more focused one regardless. There is need for network attack monitoring and response solutions for improved and focused defense against APTs.

APTs are undeterred, stealthy, targeted and sophisticated, Alshamrani et al (2019); Binde et al (2011) by nature and action therefore a call for serious concern for stakeholders of networked infrastructure defense. It is pertinent to note that most companies were not aware they have been compromised until it was brought to their notice (Auty, 2015). These attacks choose their target, profile them, design matching attack tools, deliver the tool to the target and remain persistent as they escalate privileges and propagate until they find the sort asset and carry out the required action. Due to the stealthiness, Binde et al (2011) of these attacks, there are challenges faced with detecting them and will be seen in the paragraph that follows.

Figure 1.1 shows the characteristic features of an APT that are hindering security solutions from detecting them. The identified features depict the stealthiness Binde et al (2011) of the attacks leading to their poor detection. Code obfuscation Binde et al (2011); Rashid et al (2014) is a stealthy and complex way of presenting malicious codes such that systems find them unclear, unreadable and therefore are not able to determine what they are meant for in some cases while in other cases they present as genuine code but are actually concealing malicious codes (Cert-UK, 2014; Binde et al, 2011). This increases the chance of the malware to propagate the system and span longer periods of time without being detected. As some solutions use known malware signatures to detect attacks, APTs use Polymorphic code tactics, a technique that allows their code to change while they replicate and propagate, causing concealment of trait thereby leading to scan misses from antivirus systems or Intrusion Detection Systems (IDS) and other signature based detection solutions (Cert-UK, 2014; Christodorescu and Jha, 2006). This technique is aided by the combined effort of code fragmentation, sophisticated encryption, encoding and decoding to defeat defender solutions (Cert-UK, 2014; Rashid et al, 2014). Again, they apply multi-staged attack vectors for confronting their target (Marchetti et al, 2016). While social engineering is being used, spear phishing, watering hole attacks can be launched simultaneously, disabling host protections with escalated privileges as they propagate (Christodorescu and Jha, 2006).

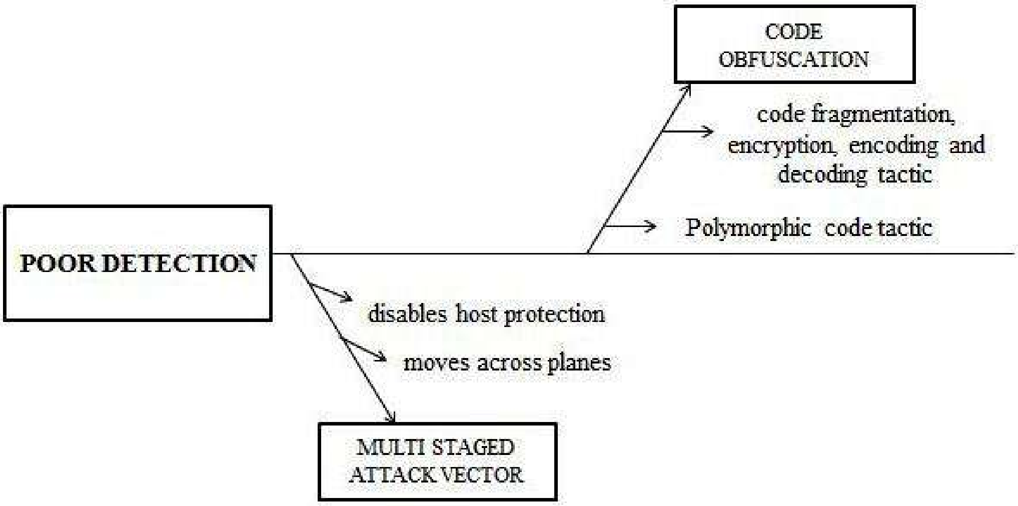

Figure 1.1: Poor detection of APTs aided by their Stealthiness

From the features discussed, it is obvious that the attack is technically organized and stealthy, using every available combination of complex techniques to evade detection through covering its track which accounts for their stealthiness and obscuring their codes such that they become unclear and concealed (Randy, 2017; Binde et al, 2011).

While there are existing works in APT detection, they have recorded their successes but not without setbacks. This section discusses some of the related research approaches of existing works in APT detection, their limitations, suggestions and the impact of the sophistication of APTs on detection solutions.

In order to improve or enhance detection of APTs, there is need to have a detailed understanding of their behavior and tactics (Cyber Kill Chain) and then come up with adequate solutions that can measure up with the attacks (Li et al, 2016). Machine learning techniques Ghafir et al (2018); Aburomman and Reaz (2017); Chandran et al (2015); Shah et al (2015) have been applied in researches for APT detection but not without their setbacks resulting from the changing attackers approach and sophistication especially (Nguyen, 2017). The following paragraphs briefly discusses some of these research approaches but are detailed in chapter 2 of this work.

Ng and Bakhtiari (2016) proposed for network traffic log analysis. This approach is taking noise patterns in network traffic into consideration and then plots some common patterns on graph which will be used to raise an alert based on some change in pattern. It used black listed known attack traffic patterns for the detection. However, APTs are polymorphic with ability to conceal their traits thereby causing the system to have false alarm tendencies which may result to poor detection accuracy. In order to reduce large volume network traffic log processing, they considered the use of decision tree to minimize rules that need to be processed for the logs in order to save processing time. A more rigorous choice for the network traffic log reduction would have been dimensionality reduction for efficient principal components selection instead of considering processing time alone (Nguyen, 2017; Ahmed et al, 2016; Sornsuwit and Jaiyen, 2015; Shyu et al, 2003).

APT attacks are getting more sophisticated by the day especially with the fact that they can now learn about the existing defense system and then rebuild their codes to measure up and beat the system. This calls for defenders to adopt relevant systems and by implication, machine learning techniques that will aid availability of information of changing attacker behaviors and tackle them accordingly (Parth et al, 2014). As APTs use multi-vectors for their attacks, Parth et al (2014) proposed for the use of Intrusion Kill Chain which is also CKC for modeling attacks to understand their behavior and propose for a framework that will take cognizance of these dynamic and multi-vectored attacks and then build appropriate solutions to tackle them. Their framework will combine Intrusion Kill Chain and behavior pattern of known attack that will be hypothesis based. The result of their framework will be a solution that will both describe the attack method and their anticipated effect. To achieve their objective, they proposed for a three (3) staged approach namely multi-staged attack, layered security architecture and security event collection and analysis system. The multi stage attack model reveals the behavior of the attacks, layered security architecture build a multi-layer of defense to frustrate attacks, while the security event collection and analysis system will use big data technology and a combination of five (5) modules to address large volume of logs from the network traffic that their sensors will capture. This work is commendable for the consideration of modeling the attack and using a layered security architecture meant to frustrate the effort of the attack. However, this system seems vague in terms of realistically setting up the framework and complex to be implemented especially with their modules that are expected to analyze the network traffic logs. It also seems not to have considered time therefore the tendency to take time in processing these logs following complex modules that will attend to the processing of the logs.

Ghafir et al (2018) proposed for APT detection with the application of correlation analysis on network traffic logs based on machine learning. Their work is three (3) phased namely:

i. Threat detection,

ii. Alert correlation and

iii. Attack prediction.

Threat detection will use eight (8) methods to detect a single APT attack stage (delivery stage); alert correlation framework is used to identify an APT attack by matching result from threat detection with related network patterns while attack prediction provides probability of an early alert based on machine learning inputs for anomalies in the network. This work is commendable for the consideration of the stealthiness of APT attacks attempting to go unnoticed during the delivery stage BITS (2011) of the attack as well the use of anomaly based techniques (Friedberg et al, 2015). However, it is only concerned with the second stage (delivery) of APT attack Hutchins et al (2011) not considering other stages.

From the discussions regarding the research approaches, Figure 1.2 shows the cause and effect of poor handling or processing of the network traffic as the issues to be addressed in this research while Figure 1.3 summarizes by showing the Scenario leading to the problem as well as the gap that lies within. Figure 1.2 indicates the poor consideration of the understanding of the behavior and tactics of APT attack. Again, it points out to the fact that network traffic logs are not properly managed and analyzed. Finally, it goes to show that there is inefficient logs correlation processing required for adequate detection accuracy (Wang et al, 2014; Ng and Bakhtiari, 2016).

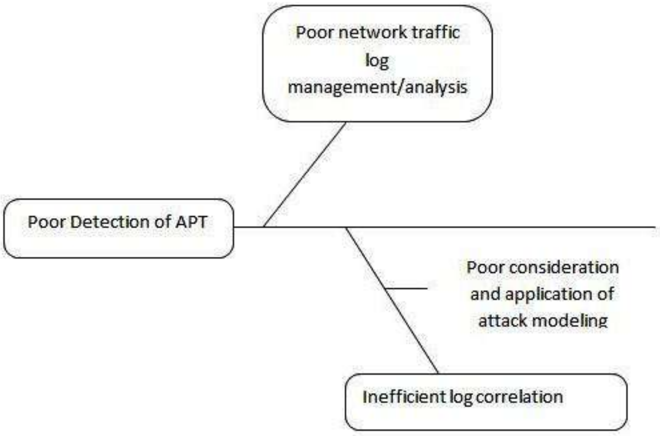
Poor network traffic log management/analysis
Poor Detection of APT
Poor consideration and application of attack modeling
Inefficient log correlation

Figure 1.2: Poor detection of APT resulting from poor network traffic log analysis

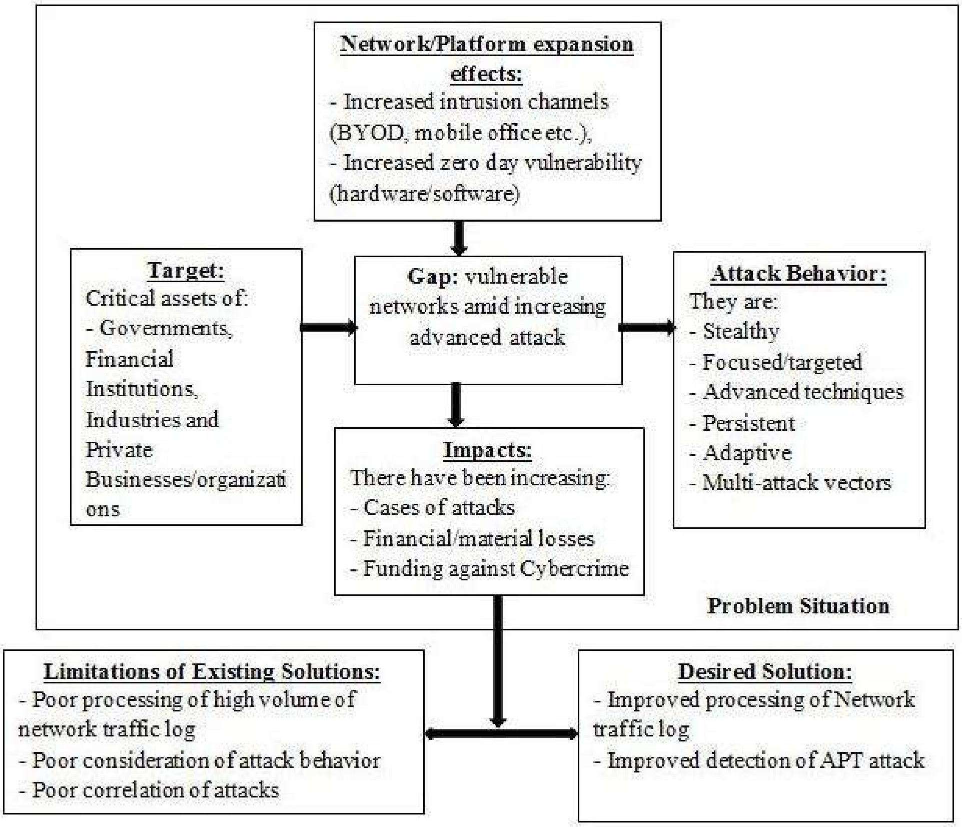
Network/Platform expansion effects:
- Increased intrusion channels (BYOD, mobile office etc.),
- Increased zero day vulnerability (hardware/software)
Target:
Critical assets of:
- Governments, Financial Institutions, Industries and Private Businesses/organizations
Gap: vulnerable networks amid increasing advanced attack
Attack Behavior:
They are:
- Stealthy
- Focused/targeted
- Advanced techniques
- Persistent
- Adaptive
- Multi-attack vectors
Impacts:
There have been increasing:
- Cases of attacks
- Financial/material losses
- Funding against Cybercrime
Problem Situation
Limitations of Existing Solutions:
- Poor processing of high volume of network traffic log
- Poor consideration of attack behavior
- Poor correlation of attacks
Desired Solution:
- Improved processing of Network traffic log
- Improved detection of APT attack

Figure 1.3: Scenario Leading to the Problem

It is pertinent to note that despite the contributions made by researchers in APT detection, they still stay ahead and continue to intrude systems. The network infrastructures still remain unprotected and have insufficient defense mechanism against APTs. This is therefore the impact of the sophisticated nature of APTs on research resulting to inappropriate solutions.

1.2 Statement of the Problem

Some of the existing approaches have considered known attack patterns, blacklist in order words signature based detection systems without considering the stealthy and polymorphic tactics of this attacks that have enabled them to conceal their known traits thereby beating detection. These attacks are stealthy and therefore require solution that puts these characteristic features into consideration. In addition, defender solutions are faced with poor detection accuracy resulting from false alarms rates and this is associated with poor log analysis and management.

The Research hypothesis is:

"*Detection of APT can be significantly improved by modeling the attack and appropriately processing and reporting the network traffic logs.*"

The following are the research questions that will be addressed in this work:

i. How to identify APTs and generate the attack?
ii. How can network traffic logs be efficiently processed and analyzed?
iii. How to properly identify APT attack with proper classification of attack?

1.3 Purpose of the Study

The purpose of this research is to develop a detection solution that is aimed at improving detection accuracy of APTs data exfiltration by improving the network traffic log processing and analysis using dimensionality reduction, improve detection accuracy using an ensemble of classifiers for better attack classification.

1.4 Research Objectives

The specific objectives of this work are:

i. To generate an APT attack and normal network traffic using simulated data from a virtual environment.

ii. To improve the analysis of network traffic logs by using the dimensionality reduction to increase its APT detection efficiency.

iii. To improve detection of APT attacks due to their stealthiness by using the ensemble technique.

1.5 Research Scope and Assumptions

The following are the scope and assumption for this study:

i. Based on the unavailability of an APT attack dataset for concerns of confidentiality of information they may contain, the dataset to be used will be a simulated one for APT attack against real data from a normal system. The simulated APT attack will be generated by injecting an APT trait connection (use of ICMP request to exfiltrate data) into the network traffic using Kali Linux as a penetration (using the "hping3" tool to convert a file into a series of ICMP packets) testing platform with Wireshark as a packet analyzer for capturing and logging events in the network traffic.

ii. As there are many stages of APT attack, this study will focus on detecting Data exfiltration Marchetti et al (2016) using ICMP protocol echo request Alshamrani et al (2019); Randy (2017); Singh et al, (2003) of an APT attack.

iii. This study will not look into any counter measures which are meant for post detection stage, it will only be concerned with the detection of an APT attack at the data exfiltration stage.

iv. The CKC model will be adopted for this work as a proof of concept for modelling attacks following the fact that it is widely referenced by researchers in that regard (Hutchins et al, 2011; Herlow, 2015).

1.6 Importance of the Research

The following are the motivations towards this research:

i. Cyber-attacks have cost governments and organizations losses running into billions of dollars and therefore curbing them cannot be overemphasized.

ii. Over 50% of victims of these attacks had no idea or clue to the fact that they were attacked. Therefore, the effective detection can help to cushion this effect.

iii. This research will make APT attack and detection information available for research and enlightenment purpose as there is a present shortage of such.

1.7 Organization of Thesis

This section briefly hints on the organization of the thesis which is sectioned into 5(five) chapters. Chapter 1 introduces the research with a discussion on the background of the problem. Chapter 2 reviews the background and what other researchers have done, therefore leading to the formulation of the objectives. Chapter 3 talks about the methodology to be used for achieving the objectives of this research. Chapter 4 discusses the data simulation and preprocessing while chapter 5 and 6 discusses ensemble technique results and conclusion respectively.

REFERENCES

Abadeh, M.S., Habibi, J., Barzegar, Z. and Sergi, M., 2007. A parallel genetic local search algorithm for intrusion detection in computer networks. *Engineering Applications of Artificial Intelligence*, *20*(8), pp.1058-1069.

Aburomman, A.A. and Reaz, M.B.I., 2017. A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security, 65,* pp.135-152.

Achleitner, S., La Porta, T., McDaniel, P., Sugrim, S., Krishnamurthy, S.V. and Chadha, R., 2016, October. Cyber deception: Virtual networks to defend insider reconnaissance. In *Proceedings of the 8th ACM CCS international workshop on managing insider security threats* (pp. 57-68). ACM.

Ahmed, M., Mahmood, A.N. and Hu, J., 2016. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, pp.19-31.

Ahmed, M. and Mahmood, A.N., 2015. Novel approach for network traffic pattern analysis using clustering-based collective anomaly detection. *Annals of Data Science*, *2*(1), pp.111-130.

Ahmed, M. and Mahmood, A.N., 2014, June. Network traffic analysis based on collective anomaly detection. In *Industrial electronics and applications (ICIEA), 2014 IEEE 9th Conference on* (pp. 1141-1146). IEEE.

Aljawarneh, S., Aldwairi, M. and Yassein, M.B., 2018. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science, 25,* pp.152-160.

Alshamrani, A., Myneni, S., Chowdhary, A. and Huang, D., 2019. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*.

Auty, M., 2015. Anatomy of an advanced persistent threat. *Network Security, 2015*(4), pp.13-16.

Avallone, S., Guadagno, S., Emma, D., Pescapè, A. and Ventre, G., 2004, September. D-ITG Distributed Internet Traffic Generator. In *Quantitative Evaluation of Systems, 2004. QEST 2004. Proceedings. First International Conference on the* (pp. 316-317). IEEE.

Binde, B., McRee, R. and O'Connor, T.J., 2011. Assessing outbound traffic to uncover advanced persistent threat. *SANS Institute. Whitepaper*, p.16.

Botta, A., Dainotti, A. and Pescapé, A., 2012. A tool for the generation of realistic network workload for emerging networking scenarios. *Computer Networks, 56*(15), pp.3531-3547.

Brewer, R., 2014. Advanced persistent threats: minimising the damage. *Network security*, *2014*(4), pp.5-9.

Brian,W,2017CyberKillChainMethodology,https://www.isaca.org/chapters3/Charlotte/Events/Documents/Event%20Presentations/12062017/Cyber_Kill_Chain_Wrozek.pdf

Brogi, G. and Tong, V.V.T., 2016, November. Terminaptor: Highlighting advanced persistent threats through information flow tracking. In *8th IFIP International Conference on New Technologies, Mobility and Security*.

Cert-UKCode-bfuscation:https://www.ncsc.gov.uk/content/files/protected_files/Guidance_files/Code-obfuscation.pdf.

Chandola, V., Banerjee, A. and Kumar, V., 2009. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), p.15.

Chandran, S., Hrudya, P. and Poornachandran, P., 2015, August. An efficient classification model for detecting advanced persistent threat. In *2015 international conference on advances in computing, communications and informatics (ICACCI)* (pp. 2001-2009). IEEE.

Chen, P., Desmet, L. and Huygens, C., 2014, September. A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer, Berlin, Heidelberg.

Christodorescu, M. and Jha, S., 2006. *Static analysis of executables to detect malicious patterns*.WISCONSIN UNIV-MADISON DEPT OF COMPUTER SCIENCES.

Cobb, S. and Lee, A., 2014, June. Malware is called malicious for a reason: The risks of weaponizing code. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)* (pp. 71-84). IEEE.

Daniel, M., 2018, Messaoud December. An ICMP Reference:Online source: https://danielmiessler.com/study/icmp/ (Accessed 20th March, 2019)

Dell Secure Works 2012: Lifecycle of an Advanced Persistent Threat. Counter Threat Unit research

D-ITG-Distributed-Internet-Traffic-Generation: ttp://traffic.comics.unina.it/software /ITG/ : (Accessed 12 March 2019)

Ford, V. and Siraj, A., 2014, October. Applications of Machine Learning in Cyber Security. In *Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering*.

Friedberg, I., Skopik, F., Settanni, G. and Fiedler, R., 2015. Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, pp.35-57.

Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K. and Aparicio-Navarro, F.J., 2018. Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, *89,* pp.349-359

Giura, P. and Wang, W., 2012, December. A context-based detection framework for advanced persistent threats. In *Cyber Security (CyberSecurity), 2012 International Conference on* (pp. 69-74). IEEE.

Gómez, S.E., Martínez, B.C., Sánchez-Esguevillas, A.J. and Callejo, L.H., 2017. Ensemble network traffic classification: Algorithm comparison and novel ensemble scheme proposal. *Computer Networks*, *127,* pp.68-80.

Haq, N.F., Onik, A.R. and Shah, F.M., 2015, November. An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA). In *2015 SAI Intelligent Systems Conference (IntelliSys)* (pp. 989-995). IEEE.

Hawkins, D.M., 1980. *Identification of outliers* (Vol. 11). London: Chapman and Hall.

Herløw, L. (2015). Detection and Prevention of Advanced Persistent Threats: Evaluating and Testing APT Lifecycle Models Using Real World Examples and Preventing Attacks through the Use of Mitigation Strategies and Current Best Practices. Denmark: DTU Compute: Department of Applied http://www2.imm.dtu.dk/pubdb/views/edoc_download.php/7057/pdf/imm 7057.pdf

Hutchins, E.M., Cloppert, M.J. and Amin, R.M., 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), p.80.

Ibrahim, N.M. and Zainal, A., 2018, July. A Model for Adaptive and Distributed Intrusion Detection for Cloud Computing. In *2018 Seventh ICT International Student Project Conference (ICT-ISPC)* (pp. 1-6). IEEE.

Kali Linux. Available at https://www.kali.org/ (Accessed 11 November, 2018)

Kaspersky:2012https://media.kaspersky.com/documents/business/brfwn/en/Advanced-persistent-threats-not-your-average-malware_Kaspersky-Endpoint-Control-white- paper.pdf

Kaur, H., Singh, G. and Minhas, J., 2013. A review of machine learning based anomaly detection techniques. *arXiv preprint arXiv:1307.7286*.

Keeping the UK safe in cyber space'. Gov.uk, 23 Jan 2014. Accessed Nov 2018.https://www.gov.uk/government/policies/keeping-the-uk-safe-incyberspace.

Kumar, G. and Kumar, K., 2013. Design of an evolutionary approach for intrusion detection. *The Scientific World Journal*, *2013*.

Li, M., Huang, W., Wang, Y., Fan, W. & Li, J. The study of APT attack stage model. Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on, 2016. IEEE, 1-5.

Li, Y., Wang, J.L., Tian, Z.H., Lu, T.B. and Young, C., 2009. Building lightweight intrusion detection system using wrapper-based feature selection mechanisms. *Computers & Security*, *28*(6), pp.466-475.

Lin, L., Zuo, R., Yang, S. and Zhang, Z., 2012, July. SVM ensemble for anomaly detection based on rotation forest. In *2012 Third International Conference on Intelligent Control and Information Processing* (pp. 150-153). IEEE.

Liu, Y., Corbett, C., Chiang, K., Archibald, R., Mukherjee, B. and Ghosal, D., 2009, January. SIDD: A framework for detecting sensitive data exfiltration by an insider attack. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Low, C., 2019. *"ICMP Attacks Illustrated"* SANS Institute Information Security Reading Room:https://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477 (Accessed 21st March, 2019)

L. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-Attack Graph Generation Tool," in Proceedings of the DARPA Information Survivability Conference & Exposition II, Anaheim, California, June 2001.

Mahmood, A.N., Leckie, C. and Udaya, P., 2008. An efficient clustering scheme to exploit hierarchical data in network traffic analysis. *IEEE Transactions on Knowledge and Data Engineering*, *20*(6), pp.752-767.

Marchetti, M., Pierazzi, F., Colajanni, M. & Guido, A. 2016. Analysis of high volumes of network traffic for Advanced Persistent Threat detection. *Computer Networks,* 109**,** 127-141.

Marchetti, M., Pierazzi, F., Guido, A. and Colajanni, M., 2016, May. Countering Advanced Persistent Threats through security intelligence and big data analytics. In *Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 243-261). IEEE.

Martin, L. (2015). Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense. Lockheed Martin CorporationManaging Information Security Risk: Organisation, Mission, and Information System View.

National Institute of Standards and Technology, Mar 2011. Accessed Nov 2018. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Mandiant. APT1 - Exposing One of China's Cyber Espionage Units.url:https:// www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Malware Risks and Mitigation Report. 1st ed. BITS- The Financial Services Roundtable; 2011. [Online]. Available at: http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf .

Meng, Y. and Kwok, L.F., 2013. Enhancing false alarm reduction using voted ensemble selection in intrusion detection. *International Journal of Computational Intelligence Systems*, *6*(4), pp.626-638.

Messaoud, B.I., Guennoun, K., Wahbi, M. and Sadik, M., 2016, October. Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges. In *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)* (pp. 1-6). IEEE.

Munro, K., 2012. Deconstructing flame: the limitations of traditional defences. *Computer Fraud & Security, 2012*(10), pp.8-11.

Minghui et al. 2018. Defense Against Advanced Persistent Threats in Dynamic Cloud Storage: A Colonel Blotto Game Approach: IEEE Internet of Things Journal 2018 DOI: 10.1109/JIOT.2018.2844878 https://arxiv.org/pdf/1801.06270.pdf

Mkuzangwe, N.N. and Nelwamondo, F., 2017, November. Ensemble of classifiers based network intrusion detection system performance bound. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 970-974). IEEE.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. *Journal of network and computer applications*, *36*(1), pp.42-57.

Moya, J.R., DeCastro-García, N., Fernández-Díaz, R.Á. and Tamargo, J.L., 2017. Expert knowledge and data analysis for detecting advanced persistent threats. *Open Mathematics*, *15*(1), pp.1108-1122.

Ng and Bakhtiari, 2016: advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis: Journal of Advanced Research in Computing and Applications ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

Nguyen, T.N., 2017. Attacking Machine Learning models as part of a cyber kill chain. *arXiv preprint arXiv:1705.00564*.

Nicho, M. and Khan, S., 2014. Identifying Vulnerabilities of Advanced Persistent Threats: An Organizational Perspective. *International Journal of Information Security and Privacy (IJISP)*, *8*(1), pp.1-18.

Oprea, A., Li, Z., Yen, T.F., Chin, S.H. and Alrwais, S., 2015, June. Detection of early- stage enterprise infection by mining large-scale log data. In *Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on* (pp. 45-56). IEEE.

Patcha, A. and Park, J. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12):3448–3470 (2007).

Pachghare, V.K. and Kulkarni, P., 2011, April. Pattern based network security using decision trees and support vector machine. In *2011 3rd International Conference on Electronics Computer Technology* (Vol. 5, pp. 254-257). IEEE.

Parth et al, 2014 Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks: 2014 IEEE 8th International Symposium on Service Oriented System Engineering

Peddabachigari, S., Abraham, A., Grosan, C. and Thomas, J., 2007. Modeling intrusion detection system using hybrid intelligent systems. *Journal of network and computer applications*, *30*(1), pp.114-132.

Ponemon Institute, Oct 2013 '2013 Cost of Cybercrime Study: Global Report'...\ www.Hpenterprisesecurity.com/collateral/report/Ponemon2013CyberCrimeReport_Global_1013.pdf

Prevention Is Futile in 2020: Protect information Via Pervasive Monitoring and Collective Intelligence'. Gartner, May 2013.

Prusti, D. and Jena S.K. 2015. *An Efficient Intrusion Detection Model Using Ensemble Methods*, Master of Technology Dissertation, Department of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, India

Puntney, G.T., 2016. *Chinese Cyber Economic Espionage: Motivations and Responses*. US Army School for Advanced Military Studies Fort Leavenworth United States.

Randy, F.S., 2017. *Detecting Compromised Systems Analyzing the Top Eight Indicators of Threat Traffic:* White Paper Commissioned by LogRhythm Oct. 2017: https://it-ecurityworld.com/assets/whitepapers/ Oct20170394.pdf (Accessed 18th March, 2019)

RapidMiner Available at: https://rapidminer.com/ (Accessed 3rd April 2019)

Rashid, A., Ramdhany, R., Edwards, M., Kibirige Mukisa, S., Ali Babar, M., Hutchison, D. and Chitchyan, R., 2014. Detecting and preventing data exfiltration.

Rivlin, A., Mehra, D., Uyeno, H. and Pidathala, V., FireEye Inc, 2016. *System and method of detecting delivery of malware using cross-customer data*. U.S. Patent 9,363,280.

Sanzgiri, A. and Dasgupta, D., 2016, April. Classification of insider threat detection techniques.In *Proceedings of the 11th annual cyber and information security research conference* (p. 25). ACM.

Schneier, B., 1999. Attack trees. *Dr. Dobb's journal*, *24*(12), pp.21-29.

Shah, A.A., Hayat, M.S. and Awan, M.D., 2015. *Analysis of Machine Learning Techniques for Intrusion Detection System: A Review*. Infinite Study.

Shick, D. and Horneman, A., 2014. Investigating advanced persistent threat 1 (apt1). SoftwareEngineering Institute (SEI) CERT Division Technical Report (CMU/SEI-2014-TR-001): https://resources.sei.cmu.edu/asset_files /TechnicalReport/2014_005_001_90523.pdf (Accessed 18th March, 2019)

Shyu, M.L., Chen, S.C., Sarinnapakorn, K. and Chang, L., 2003. *A novel anomaly detection scheme based on principal component classifier*. MIAMI UNIV CORAL GABLES FL DEPT OF ELECTRICAL AND COMPUTER ENGINEERING.

Singh, A., Nordström, O., Lu, C. and Dos Santos, A.L., 2003, July. Malicious ICMP tunneling: Defense against the vulnerability. In *Australasian Conference on Information Security and Privacy* (pp. 226-236). Springer, Berlin, Heidelberg.

Sipola, T., Juvonen, A. and Lehtonen, J., 2012. Dimensionality reduction framework for detecting anomalies from network logs. *Engineering Intelligent Systems*, *20*(1/2).

Sood, A.K. and Enbody, R.J., 2011. Malvertising–exploiting web advertising. *Computer Fraud & Security*, *2011*(4), pp.11-16.

Sornsuwit, P. and Jaiyen, S., 2015, October. Intrusion detection model based on ensemble learning for U2R and R2L attacks. In *2015 7th international conference on information technology and electrical engineering (ICITEE)* (pp. 354-359). IEEE.

Sorzano, C.O.S., Vargas, J. and Montano, A.P., 2014. A survey of dimensionality reduction techniques. *arXiv preprint arXiv:1403.2877*.

Sultana, N., Chilamkurti, N., Peng, W. and Alhadad, R., 2018. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, pp.1-9.

Symantec:https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

Tama, B.A. and Rhee, K.H., 2015. A combination of PSO-based feature selection and tree-based classifiers ensemble for intrusion detection systems. *Advances in Computer Science and Ubiquitous Computing* (pp. 489-495). Springer, Singapore.

Tan, P.N., 2018. *Introduction to data mining*. Pearson Education India.

Tankard, C., 2011. Advanced persistent threats and how to monitor and deter them. *Network security*, *2011*(8), pp.16-19.

Tsang, C.H., Kwong, S. and Wang, H., 2007. Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. *Pattern Recognition*, *40*(9), pp.2373-2391.

Van Acker, S., Nikiforakis, N., Desmet, L., Piessens, F. and Joosen, W., 2014, June. Monkey-in-the-browser: malware and vulnerabilities in augmented browsing script markets. In *Proceedings of the 9th ACM symposium on Information, computer and communications security* (pp. 525-530). ACM.

Virvilis, N. and Gritzalis, D., 2013, September. The big four-what we did wrong in advanced persistent threat detection?. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on* (pp. 248-254). IEEE.

Visumathi, J. and Shunmuganathan, K.L., 2012. An Effective IDS for MANET Using Forward Feature Selection and Classification Algorithms. *Procedia engineering*, *38*, pp.2816-2823.

Wang, Y., Wang, Y., Liu, J. and Huang, Z., 2014, November. A network gene-based frameworkfor detecting advanced persistent Threats. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on* (pp. 97-102). IEEE.

Weka. Available at: https://www.cs.waikato.ac.nz/ml/weka/ (Accessed 3rd April, 2019

Wireshark. Available at: https://www.wireshark.org (Accessed 12th November, 2018).

Yadav, T. and Rao, A.M., 2015, August. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication* (pp. 438-452). Springer, Cham.