International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

A Data Driven Anomaly Based Behavior Detection Method for Advanced Persistent Threats (APT)

Ezefosie Nkiru[1], Ohemu Monday Fredrick[2]

[1]Department of Computer Science, African University of Science and Technology, Abuja, Nigeria

[2]Department of Electrical and Electronics Engineering, Air Force Institute of Technology, Kaduna, Nigeria

Abstract: ***Advanced Persistent Threats (APT), represents sophisticated and enduring network intrusion campaigns targeting sensitive information from targeted organizations and operating over long period. These types of threats are much harder to detect using signature - based methods. Anomaly - based, which consists of monitoring system activity to determine whether an observed activity is normal or abnormal, according to a heuristic or statistical analysis, can be used to detect unknown attacks, but despite all significant research efforts, such techniques still suffer from a high number of false positive. Detecting APTs is complex because it tends to follow a "low and slow" attack profile that is very difficult to distinguish from normal, legitimate activity. The volume of data that must be analyzed is overwhelming. One technology that holds promise for detecting these kind of attack that is nearly invisible is Big data analytics. In this work, we propose a data driven anomaly based behavior detection method which aims to leverage big data methods, capable of processing significant amounts of data from diverse or several data sources. Big data analytics will significantly enhance or improve the detection capabilities, enabling to detect Advanced Persistent Threats (APT) activities that are passing under the radar of traditional security solutions.***

Keywords: Big data, Advanced Persistent Threats, Big data analytics, network intrusion, Hadoop

1. Introduction

With the rapid development of computer networks, new and a sophisticated types of attacks has emerged which require novel and more sophisticated defense mechanisms. Advanced Persistent Threats (APTs) are one of the fastest growing cyber security threats that organizations face today [12]. They are carried out by knowledgeable, very skilled and well - funded hackers, targeting sensitive information from specific organizations. The objective of an APT attack is to steal sensitive data from the targeted organization, to gain access to sensitive customer data, or to access strategic or important business information that could be used for financial gain, blackmail, embarrassment, data poisoning, "illegal insider trading or disrupting an organization's business" [30]. APT attackers target organizations in sectors with high - value information, such as national defense or military, manufacturing and the financial industry.

The technologies and methods employed in APT attacks are stealthy and difficult to detect, for instance they can employ "social engineering which involves tricking people into breaking normal security procedures" [13]. In addition, the APT intruders constantly change and refine their methods, in addition, insiders who abuse legitimate access rights to manipulate and steal data.

Once hacking into the targeted network is successful, the intruder would install APT malware on the victim's system. The attacker would now be able to monitor and control the spread of malware and also remotely control the infected systems. This opens channel through which they steal sensitive information from the victim's system unknowingly to the owner over a long period of time except if the malicious activity is detected. After the information of interest has been found the attacker gives command to exfiltrate the information. That is usually done through a channel separate from the C & C channel. To maintain access to the network the attacker continuously rewrite code and employ sophisticated evasion methods. The frequency or the rate of such attacks and breaches highlights the fact that even the best IT network perimeter defenses or traditional security solutions, including proxy, firewall, VPN, antivirus, and malware tools are unable to prevent the intrusions [Craig Richardson (http: //data - informed. com/use - data - analytics - combat - advanced - persistent - threats)]. The data breach investigation report stated in [14] confirmed that, in 86% of the cases, evidence about the data breach was recorded in the organization logs but the traditional security solutions failed to raise security alarms. This is a signal that will need another form of security solution in addition to the existing once that can be able to detect the activities of APTs. Detecting APTs is complex because it tends to follow a low and slow attack profile that is very difficult to differentiate from normal, legitimate activity. Thus, detection of this kind of attacks relies heavily on heuristics or human inspection.

The best way to achieve this detection is by examining communication patterns over many nodes over an extended period which is better than micro - examination of specific packets or protocol patterns for malware which tends to generate too many false positive. Though as pointed earlier differentiating normal, legitimate activity from APT malicious is difficult, nevertheless, certain aspects of APT behavior, can be detected by observing treads over periods of time (days or weeks) to spot unusual patterns.

An approach that can connect different low level events to each other to form an attack scenario can possibly detect APTs attack [15] [16] and reduce false positives. The correlation of recent and historical event of network traffic logged data from many number of diverse data sources can help detect APT malware. According to Jared Dean [31] "Anomaly detection should detect malicious behaviors including segmentation of binary code in a user password,

stealthy reconnaissance attempts, backdoor service on a well - known standard port, natural failures in the network, new buffer overflow attacks, HTTP traffic on a nonstandard port, intentionally stealthy attacks, variants of existing attacks in new environments, and so on". Accurate Anomaly detection of these malicious behaviors suffers several challenges due to the huge volume of data that must be analyzed. Big Data storage and analysis techniques can be a solution to this challenge. The advantage of big data tools are they can assist to handle the large volumes and semi structured data formats involved in monitoring large networks [32]. Big data helps to collects and analyzes terabytes of data collected from diverse sources and in addition, such correlation helps to lower false positive alerts. It helps to increase the quantity and scope of data over which correlation can be performed. Big data analytics will significantly enhance the detection capabilities, enabling to detect APT activities that are passing under the radar of traditional security solutions.

This work presents an intelligent distributed Machine Learning System that detects APT activities based on examining communications patterns registered in Network traffic and logs over multiple nodes over an extended period. The proposed system leverages big data Machine Learning methods to identify the necessary features to identify APT command and Command channel and with the extracted features a model is created to detect malicious traffic. Classification method was used to create the models and the detection accuracy of the created model was evaluated. The evaluated results show that the models are capable of detecting malicious attack with high accuracy and with low false positive rates.

2. Related Works

This section presents some of the work done in this area and their outcomes

Ping Chen; Lieven Desmet; Christophe Huygens; (2014), "**A study on Advanced Persistent Threats**" APTs are sophisticated, specific and evolving threats, yet certain patterns can be identified in their process. In this paper, the writers focused on the identification of these commonalities. Traditional countermeasures are needed but not sufficient for the protection against APTs. In order to mitigate the risks posed by APTs, defenders have to gain a baseline understanding of the steps and techniques involved in the attacks, and develop new capabilities that address the specifics of APT attacks [5].

Bhagyashree S Jawariya; (2014), "**Detecting Unknown Attacks Using Big Data Analysis**" In this paper a Big Data System Model for reacting to previously unknown cyber threats is proposed. Big data analysis techniques that can extract information from a variety of sources to detect future attacks.

Xiaohua Yan; Joy Ying Zhang; (2013), "**Early Detection of Cyber Security Threats using Structured Behavior Modeling**" In this paper, the writer proposed an effective early intrusion detection system called Structured Intrusion Detection (SID) system based on structured modeling of cyber - attack behavior, which aims to discover the underlying high - level behavioral patterns within network traffic that are likely to be early signs of cyber - attacks [1].

3. Methodology

In this work we leveraged big data methods to detect APT malware Command and Control Channels.

We leveraged Big data analytics machine learning algorithm to design a high level architecture for an intelligent distributed machine system for the classification and prediction of Command and Control traffic flows generated by APT malware, this system uses Spark as its core Computation Engine.

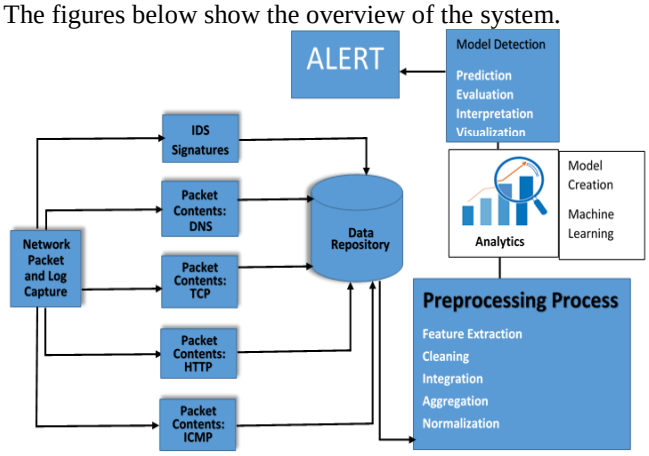
The advantage of big data tools - they assist to handle the large volumes and unstructured data formats collected from multiple source in monitoring large network without having challenges of discarding some of them because of not having proper technology to handle them which has always been the challenge. This is necessary in order to have the holistic view of the infrastructure which enables the defenders to correlate low and slow events as a result of APT attack.

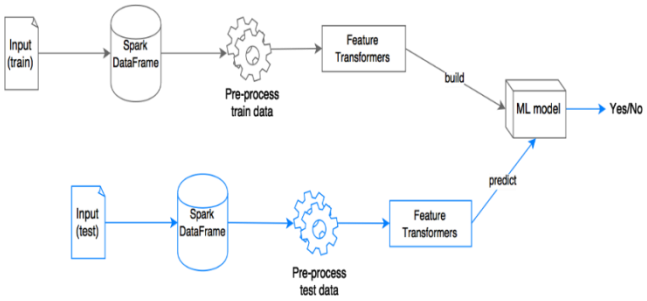
The proposed method detects APT activities based on the correlation of recent and historical event of network traffic logged data from many number of diverse data sources in the network.

The focus of this is to collect the whole network traffic packets and log data from various sources for the Implementation. The feature extracted is based on both packet header information and payload information. The technique combines both protocol analysis and content analysis. Machine learning techniques are effective, and automatically learns from labeled training data by taking intelligent hints from the data and with this predicts accurately.

The machine learning technique is divided into learning phase and testing phase. In the learning phase, the training datasets are analyzed and trained. The input given to the system is network traffic packets and logged data. Then a model is created in the learning phase. In the testing phase, new test data is given as input to the system. The system performs the task and applies the learned knowledge to classify unknown data.

The figures below show the overview of the system.





A. Data Collection
The input given to the system is network traffic packets and log event data from various sources. They collected dataset was properly labeled normal or malicious traffic. The dataset is collected and stored in Hadoop HDFS.

B. Data preprocessing
At this stage the data was preprocessed; we first filtered the data that is needed to build the model and cleaned it up. We filled the missing values.

C. Feature Extraction
The features extracted from the dataset are:

1) Start time: it defines the start time of each flow.
2) Stop time: it marks the time a particular flow end. The start time and Stop time can be used to find out the regularity of a connection.
3) Duration: it indicates the total time taken to complete the particular flow.
4) Byte rate per second: It defines the amount of byte that was transferred by a particular connection every second.
5) Packet rate per second: It defines the amount of packets transferred by a particular connection every second.
6) Total Source Byte: Defines the total bytes of data sent from the source
7) Total Destination Byte: Defines the total bytes of data sent from the Destination
8) Total Source packet: Define the total packets sent from destination.
9) Total Destination packet: Define the total packets sent from destination.
10) sourcePayloadAsBase64: This describes the full packet payloads for the source in base64.
11) Destination Payload As Base64: This describes the full packet payloads for the destination in base64.
12) Destination Payload As UTF: This describes the full packet payloads for the destination in as UTF.
13) Source Payload as UTF: This describes the full packet payloads for the source in as UTF.
14) Direction: this defines the direction of the flow.
15) Source TCP flag: It defines the Source TCP flag.
16) Destination TCP flag: It defines the destination TCP flag.
17) Protocol: It defines the protocol used for that flow.
18) Source Port: It defines the port used for that particular flow.
19) Source IP address: It defines the source IP address.
20) Destination IP address: It defines the destination IP address.
21) Service or application name: It defines the application used by the flow.

D. Model Creation via classification
The classification model is built with Random forests which is a supervised learning algorithm. The model is created based on selected features. Random forest performs well with large dataset.

E. Model Detection
Finally, we will carry out the model detection stage by giving the model a new data set it has not seen before, this data set is referred to as a test data.

4. Implementation and Evaluation of Results

A. Data collection
The Datasets used in this work are ISCX 2012 Intrusion Detection and Evaluation dataset and UNB ISCX Botnet Dataset both was obtained from Information Security Centre of Excellence University of New Brunswick Canada. The distribution of botnet types in the training dataset are shown in figure below.

Botnet name	Type	Portion of flows in dataset
Neris	IRC	21159 (12%)
Rbot	IRC	39316 (22%)
Virut	HTTP	1638 (0.94 %)
NSIS	P2P	4336 (2.48%)
SMTP Spam	P2P	11296 (6.48%)
Zeus	P2P	31 (0.01%)
Zeus control (C & C)	P2P	20 (0.01%)

The distribution of botnet types in the test dataset are shown in figure below:

Botnet name	Type	Portion of flows in dataset
Neris	IRC	25967 (5.67%)
Rbot	IRC	83 (0.018%)
Menti	IRC	2878(0.62%)
Sogou	HTTP	89 (0.019%)
Murlo	IRC	4881 (1.06%)
Virut	HTTP	58576 (12.80%)
NSIS	P2P	757 (0.165%)
Zeus	P2P	502 (0.109%)
SMTP Spam	P2P	21633 (4.72%)
UDP Storm	P2P	44062 (9.63%)
Tbot	IRC	1296 (0.283%)

B. Evaluation results and analysis
The overall implementation process was implemented using Spark and Python programming language and a Machine Learning (ML) pipeline.

We evaluated our proposed work using machine learning algorithms to identify whether the given new test data is malicious or not. The final classification model is created based on features described in section III.

The ML Pipeline API is a new DataFrame - based API developed under the spark. ml package. That was used for the model creation.

The detection rate of the model was evaluated using Spark ML inbuilt library for Evaluation known as Evaluation Metrics. During evaluation, for each data point, the predicted values is compared with the actual values and the results for each data point is assigned to any of this as we have mentioned before:
True Positive (TP)
True Negative (TN)
False Positive (FP)
False Negative (FN)
In Spark the Evaluation Metrics available are:

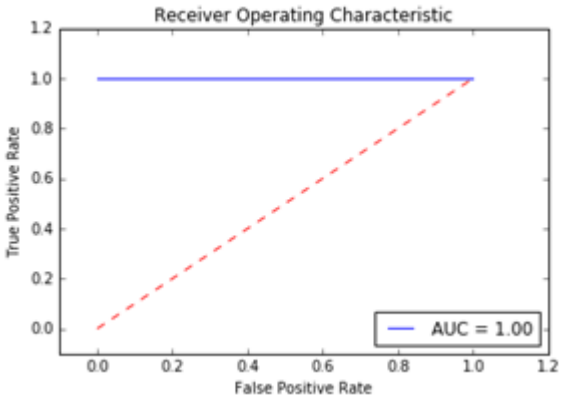
Available metrics

Metric	Definition
Precision (Postive Predictive Value)	$PPV = \frac{TP}{TP+FP}$
Recall (True Positive Rate)	$TPR = \frac{TP}{P} = \frac{TP}{TP+FN}$
F-measure	$F(\beta) = (1+\beta^2) \cdot \left(\frac{PPV \cdot TPR}{\beta^2 \cdot PPV + TPR}\right)$
Receiver Operating Characteristic (ROC)	$FPR(T) = \int_T^\infty P_0(T)\,dT$ $TPR(T) = \int_T^\infty P_1(T)\,dT$
Area Under ROC Curve	$AUROC = \int_0^1 \frac{TP}{P} d\left(\frac{FP}{N}\right)$
Area Under Precision-Recall Curve	$AUPRC = \int_0^1 \frac{TP}{TP+FP} d\left(\frac{TP}{P}\right)$

ROC (Receiver Operating Characteristics) curve is a plot of the true positive rate against the false positive rate. It reaches its best value at 1 and worst value at zero.

To determine the detection capabilities of the model, a cross - validation experiment is performed based on the training data. The optimal model with the best evaluation metric result was selected and finally fit over the entire data set.

The obtained results from the experiments are presented in the table below:
Metrics Scores
ROC Curve 0.9998823480575615.
True negative rate 80.930348817%
False negative rate 0.0428497097442%
False positive rate 0.002550577996097%
True Positive rate: 19.0242508953%



5. Conclusions

5.1 Summary

APTs are sophisticated and difficult to detect because of their slow and low manner of operation, yet certain patterns can be identified in their process. The best way to achieve detection is by examining communication pattern across many nodes over an extended period. Thus, correlation of recent and historical events of network traffic logged data from diverse data sources can help detect APT malware activities as well reduce false positive. Considering the volume of data that is required to be analyzed both structured and unstructured data, Big data analytics is only solution to the problem. Big data analytics is a good technique to analyze such volume of network traffic datasets because it provides a distributed environment. So from the result obtained from the analysis we can conclude that Big data analytics can significantly enhance the detection of APT command and control channels.

5.2 Challenges

We faced the following challenges in the course of this work:
1) Unavailability of dataset: Getting a good data set was a big challenge to this work.
2) Computing environment: We needed a distributed environment for the training and testing of the data set.

5.3 Future Work

We suggest that the analysis should be carried out with real APT malware real life data set and real time detection with the trained model.

References

[1] Xiaohua Yan; Joy Ying Zhang; (2013), Early Detection of Cyber Security Threats using Structured Behavior Modeling.
[2] Cloud Security Alliance; (September 2013); Big Data Analytics for Security Intelligence.
[3] Randy Franklin Smith; Brook Watson; (2013), 3 Big data security analytics techniques you can apply now to catch advanced persistent threats
[4] Judith S. Hurwitz, Alan F. Nugent, Fern Halper, PhD, Marcia A. Kaufman; (2013), Big data for dummies.
[5] Ping Chen, LievenDesmet, and Christophe Huygens; (2013), A study on Advanced Persistent Threats.
[6] What is advanced persistent threat (APT) ? Definition from whatis. com http: //searchsecurity. techtarget. com/definition/advanced - persistent - threat - APT
[7] Intrusion detection system - Wikipedia, the free encyclopedia. htm
[8] a b c d e f g h i j k nitin.; Mattord, verma (2008). Principles of Information Security. Course Technology. pp.290–301. ISBN 978 - 1 - 4239 - 0177 - 8
[9] Eric Hutchins, Michael Clopper, and Rohan Amin.; (2011). Intelligence - Driven Computer Network Defense Informed by Analysis of Adversary

Campaigns and Intrusion Kill Chains. In 6th Annual Conference on Information Warfare and Security.
[10] Bhagyashree S Jawariya; (2014). Detecting Unknown Attacks Using Big Data Analysis
[11] Labrinidis, A., &Jagadish, H. V.; (2012). Challenges and opportunities with big data. Proceedings of the VLDB Endowment, 5 (12), 2032–2033.
[12] Paul Giura, Wei Wang, AT&T Security Research Center, New York, NY; (2012). Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats
[13] http: //searchsecurity. techtarget. com/definition/social - engineering.
[14] Verizon; (July 2010).2010 Data Breach Investigations Report
[15] P. Ning, Y. Cui and D. Reeves, "Constructing attack scenarios through correlation of intrusion alerts, " in Proceedings of the 9th ACM conference on Computer and communications security, New York, 2002.
[16] S. Cheung, U. Lindqvist and M. Fong, "Modeling Multistep Cyber Attacks for Scenario Recognition, " in Proceedings of the DARPA Information Survivability Conference and Exposition, Washington, 2003.
[17] J. A. de Vries; (July 5, 2012). Towards a roadmap for development of intelligent data analysis based cyber - attack detection systems.
[18] Dr. Sam Musa.; (March 2014). "Advanced Persistent Threat - APT" https: //www.academia. edu/6309905/Advanced_Persistent_Threat_ - _APT.
[19] Command Five Pty Ltd.; (Retrieved 2011 - 03 - 31). Are you being targeted by an Advanced Persistent Threat?
[20] Command Five Pty Ltd.; (Retrieved 2011 - 03 - 31). The changing threat environment. . .
[21] "What's an APT? A Brief Definition". Damballa. January 20, 2010. Archived from the original on 11 February 2010. Retrieved 2010 - 01 - 20.
[22] Malware - Wikipedia, the free encyclopedia. htm
[23] Peter Gregory; (2013). Advanced Persistent Threat Protection For Dummies®, Seculert Special Edition Published by John Wiley & Sons, Inc.2013 by John Wiley & Sons, Inc., Hoboken, New Jersey
[24] http: //www.webdevelopersnotes. com/articles/ebay_phishing_email1. html
[25] https: //en. wikipedia. org/wiki/Antivirus_software
[26] https: //antivirus. comodo. com/how - antivirus - software - works. php
[27] http: //searchsecurity. techtarget. com/tip/How - antivirus - software - works - Virus - detection - techniques
[28] http: //searchsecurity. techtarget. com/definition/webfilter
[29] What is spam filter? - Definition from whatis. com
[30] Nikos Virvilis, CISA, CISSP, GPEN, Oscar Serrano, CISA, CISM, CISSP, Luc Dandurand; (2014). Big Data Analytics for Sophisticated Attack Detection Isaca Journal Volume 3, 2014
[31] Datamining and machine learning in cybersecurity. Page 86
[32] Command & Control: Understanding, denying, detecting QinetiQ Ltd 2014
[33] https: //nigesecurityguy. wordpress. com/2014/04/03/apt - detection - indicators - part - 3/
[34] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel. A view on current malware behaviors. In Proceedings of the 2nd USENIX conference on Large - scale exploits and emergent threats: botnets, spyware, worms, and more, pages8–8. USENIX Association, 2009.
[35] F. Giroire, J. Chandrashekar, N. Taft, E. Schooler, and D. Papagiannaki. Exploiting temporal persistence to detect covert botnet channels. In Recent Advances in Intrusion Detection, pages326–345. Springer, 2009.