Review of the Defence Against Advanced Persistent Threats

Abstract

In this literature review Advanced Persistent Threats (APT) will be reviewed in order to better understand the defence mechanisms against such threats. Defence against APT's is a very important issue due to the large amounts of data being exploited by long term events. By writing this review more people will be aware of the severity of this issue, however the work done in this review is merely a snapshot of the evolving field of APT's.

Introduction

APT is a type of advanced malware, used in order to collect data and gain access to a system. APT's are still very relevant, as these attacks continue to be a threat to companies and notably government organisations. By reviewing defense systems, the hope is that we will be able to better mitigate these types of attacks. This review will be conducted by presenting background information of APT's at the start of the review followed by answering each research question, which will be presented in chronological order. Thorough analysis of 3 pieces will then be conducted. Research questions on this topic are listed below:

How are we able to communicate APT attacks more effectively to cyber analysts?

How are we able to reduce data consumption decrease runtime on defence systems?

How are we able to decrease the number of false positives and false negatives?

This review aims to provide more intensive analysis on defence systems against APT's and answer the research questions provided. It also aims to provide ways in which defence systems may improve moving forward.

During the Overview section of my review, I aim to give more insight on defensive systems as well as go over some common challenges developers of such systems must consider when defending against APT's. I will also go over the sourcing of my information. During the Review of Literature I aim to provide a detailed analysis of APT's and the defence systems listed [3][4][5]. The aim for the Discussion section is to answer my research questions as well as provide any improvements that may need to be done, whether that be an improvement in testing and data collection on defensive systems or an improvement for a system feature. The conclusion will conclude the review.

Overview

Defence against APT's is challenging due to the slow and delayed approach that an APT virus usually takes, leading to thousands or even millions of audit logs which need to be analysed and indexed by a Cyber Analyst. Over the last decade, a push for more efficient detection has been requested with the launch of multiple APT campaigns. Common Challenges of APT's include data reduction, effective communication of attack logs to Cyber analysts and reducing the number of false positives and negatives.

The Review of Literature will be in Methodological order, through each research question, where information on each question will be tackled by the 3 conferences. These will all be separated into their own paragraphs. Before the research questions are answered, there will also be background on prior APT attacks, in order to get a better idea on the types of patterns which arise and how to stop them.

All citations and references within this literature review published are no older than 2015, so that problems and information reviewed will not be in any way outdated. I have also only referenced from some of the highest ranked conferences and most trusted sites to ensure that the information I provide details on are accurate.

Review of Literature

In order to better understand APT attacks and what to do when faced against such attacks, frameworks have been given in order to promote defensive measures against such attacks. One of these frameworks is known as the Cyber Kill Chain [1] which characterises and gives APT attackers seven phases in order to be successful in an attack. Of course, an APT attacker does not follow these phases themselves and attack phases may vary and some repeated over again [6]; however generally APT attacks do follow this framework and from a defensive point of view, in order to stop an APT attack, you must break part of the chain as the attacker is only deemed successful if and only they are able to pass through all seven phases.

To get a better understanding of APT's, the knowledge of prior and known attacks can be vital in an APT defence systems success. This is due to attack patterns that occur. In a 'survey of publicly available reports on advanced persistent threat actors' [2] published in 2017, details some of the most well-known APT attacks. One of them being APT17 which was conducted against multibillion dollar search engine Google. The hacking group 'Aurora Panda' used malicious URLs to lure users to malicious sites where the APT would then be installed. Interestingly, after this advanced threat attack, with the 'actors' successfully identified, the group has had to "retool". Through this retooling stage, the group went from using a tool known as HIKIT, reportedly as a rootkit to hide processes and network connections in order to conceal the presence of malware within the system [7][8], to another well-known tool, known as BLACKCOFFEE, used by multiple Chinese groups [9] and uses a reverse shell to exploit vulnerabilities within their victims machines. The tools that well known hacking group Axiom chooses are currently publicly known and can be defended against if cyber analysts abroad are able to recognise these attack patterns and act accordingly to break the 'cyber kill chain'[1]. However, as attacks become more sophisticated, development of new tools and modifications of old tools have arisen, making simple pattern detection obsolete and the fight against advanced persistent threats more complicated.

APT attacks are known to be prolonged attacks designed to be passive in order to remain undetected for a number of years. The main objective of an APT attack is to collect data and information, which is why government organisations are the ones who are mainly affected.

Achieving Effective Communication to Cyber Analysts:

In order to correctly identify whether an attack is happening, Cyber Analysts need to look through over 3 million low level audit logs, making communication of APT alerts an important step in order to pinpoint these attacks as fast and efficiently as possible. The Holmes defence systems [4] main approach to defence against APT's is to generate 'alerts of significance', that is, allowing cyber analysts to find potential attacks much faster by decreasing the number of events found within an audit whilst also keeping false positives and false negatives down to a minimum. As stated earlier in the review, hosts generate numerous events, however, only a small number of events relate to the events of an APT attack. It is hard to detect rare events in these situations without a high rate of false alarms. Stealthier attacks make it increasingly difficult when attacks occur in the main server, executed in the main memory which doesn't leave any traces of possible downloaded files, etc.

A paper published in 2006 from work done at NEC labs in America titled "High Fidelity Data Reduction for Big Data Security Dependency Analyses" [3] uses System Event Trace paired with System Dependency Analysis, to record sequences among multiple objects, for example, the timing, type of operation and the direction of flow of information. This process assists in reconstructing the causal events by looking at patterns in these events. Event Aggregation is a powerful technique used which simplifies the process of finding malicious events that may have occurred in the system. It follows a rule of determining whether 2 events are aggregable by whether they share the same attributes. They must also have the same 'source' and 'destination' entity. By decreasing the number of events present, Cyber Analysts are more able to effectively go through the system log data and pick out events that may be potentially malicious. These techniques however also tie into data reduction which will be covered more in depth during that section.

The ATLAS (A Sequence-based Learning Approach for Attack Investigation) system by USENIX [5] uses a different approach compared to the other systems discussed. Like the other 2 systems discussed ATLAS maintains audit logs made by the system and uses these logs for thorough analysis. However, ATLAS uses "Model Learning" in order to compare and recognise attack sequences and patterns. Furthermore, the ATLAS system launches an 'attack investigation phase' where it analyses nodes through a constructed causal graph where optimisations in order to reduce data consumption are put in place. A 'learning phase' will also be implemented for future references in order to memorise attack and non-attack sequences. One of the ways that the ATLAS system uses to tackle the issue of audit log analysis, is through techniques of balancing data using under sampling and oversampling. Unbalanced data is inevitable in APT attacks. USENIX measures that on average, attack entities, that is, entities that have been recognised by ATLAS as malicious on average are numbered at 61, whereas non attack entities, that is, entities that have not been recognised as malicious are around 21 thousand.

Under sampling uses a Levenshtein Distance[10] in order to compare similarities between sequences, to do this ATLAS[5] has allocated a maximum number of similarities in which if exceeded will be filtered out.

Oversampling uses

Data Reduction:

Data consumption is a big issue within APT defence systems and a big aim of modern defence systems is trying to reduce the amount of data consumed, as it is incredibly wasteful. The Holmes defence system [4] estimates that attacks constitute for less than 0.001% of audit data volume collected. This, along with the fact that cyber analysts must go through logs and index them, make it incredibly time consuming and work heavy as well as the data itself being difficult to interpret. Low level audit data from a system is estimated to reach 0.5 to 1 gigabyte per host[3], however big companies with over 200,000 hosting computers, which is where APT actors often target more frequently, would have to store around 17 petabytes of data which is unreasonable and incredibly wasteful[3]. To successfully be able to detect such attacks, a cyber analyst must successfully weave through normal activities and analyse any forms of malicious activity which would be very tough and time consuming especially with the potential ‘false positives’ that can be accidentally acquired. “High Fidelity Data Reduction for Big Data Security Dependency Analyses” [3] similar to Holmes [4] collects low level system events from servers, however the system mechanism used to reduce data volume is quite different. This system allocates POI events (Point of Interest) where the POI is an event that must be examined to see whether or not it is malicious by finding the root cause of such an event. To do this, the system allocates timestamps to events that have occurred in similar time frames and neighbouring nodes. Any event that has happened after this event will be disregarded, as the root cause of the event could not have happened after the event had actually occurred. Shadowed events will also be ignored as they are also irrelevant. A shadowed event is when the same event has occurred at a later stage, there is no reason to analyse the same event twice, instead the system merges the event information together.

Event aggregability [3] occurs within this system when 2 events have the same source and destination nodes and are completely equivalent. Disregarded events along with Event Aggregation will decrease the amount of logs and events stored within a database. We will see later on in the review how different algorithms within this defence database will lead to different optimisations.

The Holmes system [4] however, checks audit log data to view where the initial compromise is. Once identified, Holmes checks IP addresses where it refers to a table, where it is split up into trusted and untrusted IP addresses. If the IP address is seen and viewed as trusted, it will view it as a low security threat. If the IP address is untrusted, then Holmes will check if files have been accessed and compromised. This system therefore achieves data reduction through IP address ruling.

ATLAS [5] reduces data through the elimination of nodes that are not reachable by attacking nodes on the causal graph created. ATLAS labels an attacking node on whether all the events of the node are attacking events. The causal graph constructed is only for non-repeating edges(eg; P1 or process because there is only 1 process) they also combine actions that are repeating, into one node (eg; s1,s2,s3 nodes being combined into 1 big entity) making the graph simplified and more data efficient by 81.81%[5].

Reduction in False Positives:

A big part of APT defence systems is the reduction of false positives and false negatives. Too many false positives may lead cyber analysts to be hardened to such alerts causing them to not act as quickly as they should or even not checking whether an alert is really signalling an APT threat or not. Too many false negatives also poses the problem of not being able to see the broader scope of an APT attack. If some events are getting flagged as negative it could even delay the knowledge that the machine has been compromised in the first place, therefore delaying action against the threat.

In order to reduce false positives ATLAS first identifies through Lemmatisation [5] whether a hostname is malicious or not. Furthermore, ATLAS looks at non attack sequences to identify them as non-threatening for future reference, this allows ATLAS to distinguish between threatening and non-threatening attacks allowing it to flag attacks more accurately, reducing data and reducing false positives.

The “High Fidelity Data Reduction for Big Data Security Dependency Analysis” [3] paper uses 3 available approaches used to deal with APT’s all with its very own positives and negatives. The first approach is an algorithm known as the CPR algorithm and improves “big data systems” by up to 3.4 times and has very few false positives with a rate of 0.2%. The PCAR algorithm however improves “big data systems” by up to 5.6 times and also has a low false positive rate. The naive approach however has a false positive rate of 13.9% which is very large.

To reduce false positives Holmes [4] uses a combination learning patterns that have little to no effect but may produce false positives and use shortcuts that assign weights to nodes and paths in the graph(HSG graph) based on their severity so that the graph can be ranked and then the highest ranked getting presented to the analyst.

Discussion

The Holmes system [4] does a good job with communication of Cyber threats to Cyber Analysts however Holmes lacks heavily within the data reduction and false positives fields. This is since attempts made in data reduction may lead to vulnerabilities within the system that attacks are easily able to exploit. An example of this would be the trusting of IP addresses. IP spoofing [11] can be used which would not only be used to conceal the identity of the attacker but will also allow the attacker to get trusted access. A solution to this feature would be to look at the locations of the IP addresses as well to make sure the people behind the address are actually trusted.

False positives are also able to be manipulated within the Holmes system as kernel and operating system data is not logged and therefore automatically assumed to be trusted. If an APT attack gets into the kernel operating system. The APT will not be detected throughout the rest of its lifecycle. A way around this is to either have 2 separate systems, one monitoring the kernel operating system with Holmes monitoring the outside, or for further optimisations to be made to be able to fit kernel auditing into the scope of the Holmes model.

ATLAS approaches data reduction and through their over and under sampling can communicate attacks effectively, however ATLAS has noted that if there were a large number of attacking entities, the entity subsets may become exponential. Although APT attackers try to keep a low profile by having a low amount of attacking nodes, if they were able to find out information about the user and the user was using the ATLAS defence system, they would be able to then exploit that vulnerability which can lead to false negatives and the system may have trouble coping.

High Fidelity Data Reduction for Big Data Security Dependency Analyses approach to data reduction is the best out of the 3 systems discussed and has no known vulnerabilities, however the scope of this defence model does not go into how to better communicate attacks to cyber analysts and barely touches on false positives and how to reduce it. This system is therefore recommended that it be used alongside other machines as it covers a very broad issue of APT analysis. A way this can be improved is with a full integration of one of the systems talked about above with this system in order to effectively reduce data whilst also being effective in the other 2 problems discussed making a system with improvements all round.

Conclusion

To conclude, cyber-attacks and malware detention is a very important and concerning threat that governments and major corporations must be on the lookout for. Holmes, ATLAS and High-Fidelity Data Reduction are all systems that try to stay ahead of APT threats, however APT threats is an evolving situation, and these systems will eventually be outdated. New systems and research must be done on a regular basis in order to keep ahead of APT's and keep data systems safe and out of reach from intruders.

Bibliography

[1] Lockheedmartin.com. 2015. *Gaining the Advantage*. [online] Available at: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>

[2] Antoine Lemay, Joan Calvet, François Menet, José M. Fernandez

2018. pp. 26-59 | *Survey of publicly available reports on advanced persistent threat actors*

https://doi.org/10.1016/j.cose.2017.08.005.

(https://www.sciencedirect.com/science/article/pii/S0167404817301608)

[3] Xu, Z., Wu, Z., Li, Z., Jee, K., Rhee, J., Xiao, X., Xu, F., Wang, H. and Jiang, G., 2016. *High Fidelity Data Reduction for Big Data Security Dependency Analyses | Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. [online] Dl.acm.org. Available at: <https://dl.acm.org/doi/abs/10.1145/2976749.2978378>

[4] Ieeexplore.ieee.org. 2019. *HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows*. [online] Available at: <https://ieeexplore.ieee.org/document/8835390/>

[5] Alsaheel, A., Nan, Y., Ma, S., Yu, L., Walkup, G., Celik, Z., Zhang, X. and Xu, D., 2021. *{ATLAS}: A Sequence-based Learning Approach for Attack Investigation*. [online] Usenix.org. Available at: <https://www.usenix.org/conference/usenixsecurity21/presentation/alsaheel>

[6] Meinel, C., Cheng, F., Jaeger, D. and Ussath, M., 2016. *Advanced persistent threats: Behind the scenes*. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/abstract/document/7460498>

[7] Novetta.com. 2021. *Hikit Analysis*. [online] Available at: <https://www.novetta.com/wp-content/uploads/2014/11/HiKit.pdf>

[8] Glyer, C., 2017. *Hikit, Software S0009*. [online] Attack.mitre.org. Available at: <https://attack.mitre.org/software/S0009/>

[9] Attack.mitre.org. 2017. *BLACKCOFFEE, Software S0069*. [online] Available at: <https://attack.mitre.org/software/S0069/>

[10] Cuelogic Technologies Pvt. Ltd. 2017. *The Levenshtein Algorithm*. [online] Available at: <https://www.cuelogic.com/blog/the-levenshtein-algorithm>

[11] Internetsociety.org. 2015. *Addressing the challenge of IP Spoofing*. [online] Available at: <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf>