State of the Art Analysis of Defense Techniques against Advanced Persistent Threats

Jeslin Thomas John
Supervisor: Dr. Holger Kinkelin
Seminar Future Internet SS2017
The Chair of Network Architectures and Services
Faculty for Informatics, Technical University of Munich
Email: jeslin.john@tum.de

ABSTRACT

Advanced Persistent Threats (APT) have become one of the most serious IT security issues in the recent times, owing to reasons of its complexity, duration and inability of proper tracking. The threat posed by APTs have turned out to be a major concern not just for IT Firms, but also for industrial establishments, governments, military organizations etc. Although different research proposals exist in the academia, many of those are not yet reflected in existing solutions in the market. The following paper attempts a state of the art analysis of the different works from academic research and commercial solutions available in the market, compares their benefits and consequences to arrive in to a taxonomic illustration of the defense mechanisms. In addition, the paper also proposes a novel approach for APT Defense based on theoretical computational methods.

Keywords

APT Detection, APT Defense, Cyber Attacks, Attack Pyramid, Attack Trees, Fractal Analysis, Machine Learning, Intrusion Kill Chains, Command & Control Communication

1. INTRODUCTION

The sophisticated, targeted, persistent and well planned cyber attacks targeting specific organizations, governments, military groups etc. are collectively referred as *Advanced Persistent Threats (APT).* [10] These attacks are mostly complex, stealthy and generally involve multiple stages that span over a long period of time. This makes APTs tough to detect, defend and mitigate.[11] The stages of an APT process are quite easily mistaken to be independent events that occur in unrelated slots of time. In this context, the static attack detection techniques prove to be ineffective and blacklisting and malware signature based techniques fail.[5]This clearly marks that the traditional approaches are inefficient in handling the sophistications of APT threats and novel approaches for detection and mitigation are required. As a result, innovative and proactive methodologies, that can provide security with an insight to continuously monitor the systems under protection, detect vulnerabilities and security breaches are being sought for. This would aid in minimizing the impacts caused to the target system, in cases of an attack. Various research proposals discussed in this paper makes use of a wide range of approaches for APT detection, depending upon the nature of the system under consideration.

In the next section, a background of the APT attacks are briefed which aids in better analyzing the approaches discussed further. Section 3 lists out the major works from the research world while section 4 details on some of the prominent industrial solutions available. Finally, the author discusses his own thoughts for the proposal of an APT detection system, based on theoretical computational methods, that can lead to better detections and defense.

2. BACKGROUND KNOWLEDGE

APTs are well planned security attacks, aimed at exploring the known vulnerabilities of a system, to get unauthorized access, by overriding the security and defense mechanisms in place. The attack goal in most cases would be to infiltrate in to the system, learn the internal activity flows and access confidential information. This demands a great deal of passiveness in attack operations, to go on undetected for a greater extent of time. It is *Advanced*, as the attacker makes use of a complex mix of diverse attack methods targeted and adapted to the vulnerable system, *Persistent*, as the attack life cycle is lengthy and can span over a long period of time without being detected as the attacker slowly goes on to acquire control over the target system, *Threat*, as the attack can cause damage of intellectual property that incur loss of money and reputation.[2]

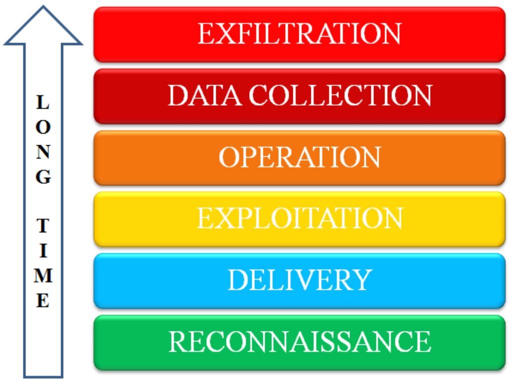

Figure 1: Typical stages of an APT

Figure 1 shows the typical stages of an APT with the possible attack strategies adopted in each stage described. APT attacks mostly begin by choosing an attack target, which normally would be a vulnerable spot inside the system that

doi: 10.2313/NET-2017-09-1_09

can let the attacker in. Once the target is fixed, the attacker normally loads a malware in to the secure network, which will establish a stealthy connection to a server outside the network. This helps him to learn more of the system and explore weaknesses by constant passive monitoring, minimizing attack footprints.This stealthy mode of communication is called a C&C, or *Command & Control* which taps the secure network details to an external system. [1]

3. ANALYSIS OF ACADEMIC PROPOSALS

A variety of proposals from the academic researches were analyzed to classify and compare the major approaches that are employed in the detection and defense of APTs. The benefits and demerits of these approaches were compared and contrasted to provide the reader a broader picture of the defense mechanisms and their applicability. As an outcome, a taxonomy of the various approaches was also generated, based on the underlying techniques used, which gives a neatly classified reference for further studies.

3.1 Detection using Fractal Dimension based Machine Learning Classification

The major idea behind most of the APT prediction methodologies is to identify some unique feature in the whole behavior of the system under consideration, and to track this uniqueness. The unique feature is then used to identify any possible deviations from intended behavior and efficient defense mechanisms are formulated. One major approach for APT defense using this unique property feature is the use of machine learning based techniques for fractal analysis.[1] Fractals are infinitely scaled and iterated abstract patterns often emulated in nature. Fractal analysis is a contemporary method of applying nontraditional mathematics, to patterns that defy understanding with traditional Euclidean concepts.[1]

The proposed system aims at representing the network level Command and Control (C&C) communications of the APT processes as fractal dimensions and implementing a fractal based machine learning algorithm, which compares it's output with a standard machine learning algorithm. Any significant deviation observed in the comparison can possibly suggest the presence of a valid APT attack.[1]

On a brief note, the defense system starts itself by extracting feature vectors after building a data set by combining the packet capture (PCAP)[15] files from various online sources. Noise reduction is performed on this data set and is presented as an input to an anomaly classification algorithm. The major algorithms employed for anomaly detection are the K- Nearest Neighbors and the Correlation -fractal dimension based algorithm. At any instance, one of these algorithms are chosen based on the intended performance specifications such as accuracy, sensitivity, specification or precision. The algorithm thereby predicts the possible valid inputs from the given data set that qualify for an APT.[1]

One successful implementation making use of this idea, based on TCP attributes, was proven to be efficient in the research set up.[1] In any case the accuracy of predictions always depends up on the quality of the training data that are fed in to these machine learning algorithms. So the data extraction and the prehistoric standard data must be clean and inclusive so as to produce the most accurate prediction results.

3.2 Defense using System and Attack Intelligence

APT attacks are posing major threats not only to IT Infrastructure, but also to the Industrial control systems in critical functional domains such as oil and gas manufacturing, refineries and nuclear plants. The recent well known attacks in this domain includes the Stuxnet[14], which was targeted on destroying Iran's nuclear plans and Aurora[13], which was aimed at stealing Googles Intellectual property documents.

One work from academia aiming on detection of APTs in Industrial control systems introduces tools such as *Tofino*[12] and *Defender*[17] as the backbone. The use of *Tofino* enables Deep Package Inspection (DPI) with convenient and easy configuration steps, offering a standard network monitoring solution. It also runs in compatibility with the standard industrial control systems such as PLC(Programmable Logic Controllers), SCADA(Supervisory Control And Data Acquisition) and DCS(Distributed Control Systems)[4]

The detection approach monitor all the events that can occur in the system, records and projects the relevant items that may qualify for a sequence, in a succession of APT events. The recorded events are then matched with the already known attack behavior patterns and alarms are generated whenever a match is found. Though this seem to be a straight-forward and simple approach, the prediction can be fairly accurate and useful, provided the attack behavior database is well updated and inclusive.

As the detection approach is based on pattern matching between behaviors and events, techniques similar to formal method approaches for language recognition can be made use of. One possibility of such a technique will be the use of state machines that can predict an APT attack based on sequential event matching, with events as input symbols and patterns as transitions. One such implementation demonstrates a state table based approach enabling reduced space complexity, for detection of attacks similar to StuxNet.[4]

3.3 Detection using a Context-Based Detection Framework

APT threats can be also identified using a framework that can produce inferences based on context information. A conceptual model based on the *Attack Tree* concept is extended here to form an *Attack Pyramid*, which has the attack goal at the top of the pyramid and the event environments as the lateral planes. [2]

3.3.1 Attack Trees

An *Attack Tree* is a means to represent threats in a tree structure based on the work by Bruce Schneier[8] which originally uses the *Threat Tree* concept from Edward Amoroso[9]. The tree is constructed by positioning the goal of the attack as the root of the tree, and the various methods by which the goal can be reached, as children of the root. The child

[1] https://imagej.nih.gov/ij/plugins/fraclac/FLHelp/Fractals.htm

nodes in the tree can be connected by either *AND* rules, if both the nodes together should be present to reach the goal, or *OR* rules, if either of them can serve the purpose. On iteration, each of the child nodes are considered as a goal of the attack and subtrees are created with the goal as the root.

Attack trees help security administrators in an organization to create the hierarchy of vulnerable elements and the path of an attack, giving a big picture of the security architecture.

3.3.2 Attack Pyramid

The researches here modifies the attack tree concept to form a pyramid structure, called as an *Attack Pyramid*, which positions the attack goal as the root of the tree and the lateral planes as the environment where the attack evolves. The idea here is to map the APT stages to the planes of the pyramid namely physical plane, user plane, network plane, application plane and so on.[2]

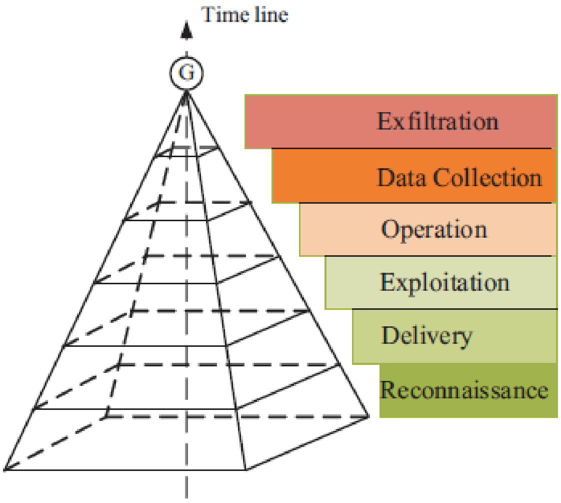

Figure 2: The Attack Pyramid. [2, Page 71]

The planes differ from system to system, depending up on the attack goal and the security architecture. Every attack in this kind of a model is viewed as a crawl along the planes to reach the goal, with multiple attack trees spanning the pyramid planes. The detection system aims at find relations between the occurrence of different events in the planes and building the attack crawl.[2]

3.3.3 Events

All the events that can occur in the system is classified here, inorder to associate events to system activities. Events can be *Candidate Events* which includes all logged events, *Suspicious Events* that are reported as an abnormal activity or *Attack Events* that are detected by the security tool as a valid attack activity.

The system records all the events that occur in the system and classify them to fit in to one of the event set. These events are then mapped to the pyramid planes using predefined mapping rules. The detection rules in this case can be based on signatures, policies or profiling. Mathematical correlations are then made by using correlation rules that finds the relations between independent events, to trace the attack path in the pyramid planes.[2]

The detection framework makes inferences taking in to consideration the context, the correlation rules, historical information, the confidence level and risk levels to arrive in to valid conclusions.

Figure 3 depicts the unfolded attack pyramid which clearly depicts the pyramid planes, and the corresponding APT stages. The crawl of a possible attack is marked with pointed arrows, as multiple attack trees to reach the goal G of the attack pyramid.

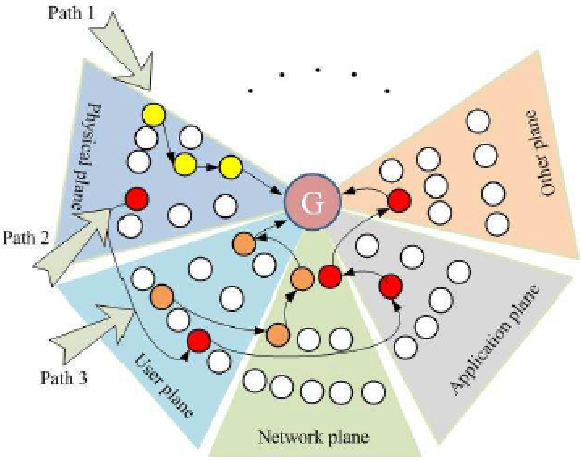

Figure 3: The unfolded attack pyramid. [2, Page 71]

3.4 Detection using Honeypots

Honeypots are computer systems devised as a decoy to mimic the real setup to deceive cyber attackers to detect, deflect and gain information on the methods employed by the attackers. The placement of honeypot traps in IT systems helps to enable an inexpensive detection of cyber attacks at an earlier stage including the ones missed by traditional intrusion detection systems.

The key idea in this kind of an APT detection approach is to tie up an alarming system to the honeypots devised, so that an early detection or warning on a intrusion can be made available. A properly configured honeytrap can be proven efficient in placing the attacker on a greater risk of getting identified, as a single mistake from the attacker side can alert a detection leading to an alarm. In addition, provided a low number of false positives, the defense team can timely devise counter measures while the attack advances.[3]

One successful implementation of such a honeytrap makes use of the *KFSensor*[3] tool, which is based on a Windows architecture and by writing a suitable Perl based alerting module.

Table 1: Taxonomy of APT Defense Techniques

Defense Technique	**Applicability**	Implementation Available
Fractal Analysis	IT Systems	Yes, Psuedo Code
Context Based	IT Systems	Yes, Psuedo Code
System & Attack Intelligence	Industrial Control Systems	Yes, State Table Based
Honeypots	IT Systems	Yes, Perl Script
Intrusion Kill Chains	IT Systems	Yes, Using Hadoop FS
Distributed Computing Based	IT Systems	Yes, Using Hadoop

3.5 Detection of Multi- Staged attacks using Intrusion Kill Chains

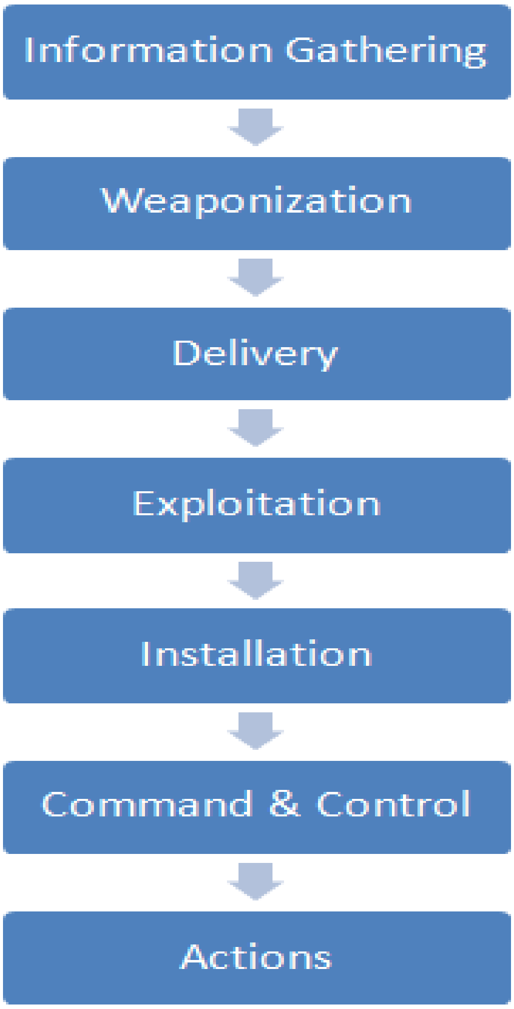

Figure 4: The Intrusion Kill Chain.

Multi-staged cyber attacks are always hard to detect and defend due to their dynamic nature and the fairly unpredictable time frame that encompasses the course of events. While some APT detection methods aim at using the traditional malware detection mechanisms and blacklists, multi staged attacks usually tend to be a hard nut to crack. One notable research in this field proposes a system that makes use of the properties of an IKC(Intrusion Kill Chain)[20] that can suitably model the attack and enable early detection. IKC is a seven stage model that any attacker should inevitably follow to execute a successful APT attack[5]

The system evolves itself by proposing a layered security architecture that adapts to a multi staged attack model and then by collecting and analyzing the security events. The analysis of the security events includes logging the outputs from various sensors such as host intrusion detection system (HIDS), network intrusion detection system (NIDS), firewalls and so on, which are later processed by a Hadoop based log management module. The Hive queries on this distributed file system are analyzed by an Intelligence module which correlates it to a possible IKC. There also custom tools inside the system that performs code analysis and behavioral analysis for malware detection.[5]

The intelligence module predicts the possibility of an IKC primarily by analyzing the Hive query outputs from the HDFS system that contains the sensor logs. The analysis maps each of the suspicious event identified to one of the seven stages of the attack model formerly devised and then a defense plan is formulated which contains attack mechanisms and the possible defense strategies. Once the defense line is identified, it is mapped to an IKC phase, where from an IKC is rebuilt and the multistage attack is predicted.[5]

The research also demonstrates a real world implementation of the concept using commodity hardware running Hadoop clusters and with Apache Sqoop and MySQL.[5]

3.6 Taxonomy of APT Defense Methods

A straightforward classification of the APT defense methods available is depicted as in Table 1 above. The approaches are marked with information, if a valid implementation of the solution is available.

3.7 Analysis of approaches

The defense approach using honeypots are simple, straight forward and less resource intensive compared to the sophisticated ones proposed using fractal analysis, but is limited to the application domain with the dependency to the system behavior. Fractal analysis on the other hand proves to be better efficient as it involves thorough analysis of all network and host related data flows and mined data of relevant events and their consequences. Intrusion kill chains and Attack pyramids propose efficient means to track and alert on APTs alongwith valid predictions on the further progressions.

4. ANALYSIS OF INDUSTRIAL SOLUTIONS

In light of the various approaches discussed, various solutions available in the market for APT Defense are worth to

Table 2: Comparison of Industrial Solutions

Feature	THOR	TrendMicro	Kaspersky	Symantec
Network Flow based	Yes	-	-	-
NIDS	-	-	-	Yes
Threat Intelligence	-	-	Yes	-
Automatic Correlation	-	-	Yes	-
Deep Package Analysis	-	Yes	-	-
Sandboxing	-	-	Yes	-

be analyzed. For the matter of analysis, couple of well known solutions were handpicked, compared and contrasted. It was observed by the author that only limited precise information on the product architecture and technology is provided by most of the vendors, which makes it hard to analyze the quality of the tool.

4.1 Defense Solutions based on Network Flow Analysis

Network flow analysis includes various approaches to collect and process network traffic, and all related data items that can be used for studying the behviour of the network, record activities and generate inferences. This evidence can be used for determining network features such as security, performance, integrity, capability etc. The following tools presented are based on flow analysis to detect discrepencies in a network.

4.1.1 THOR

One prominent implementation available in the market from BSK Consulting GMBH[16] that employs the concept of network flow based prediction is THOR.[16] The solution claims to implement deep system scanning for APT detection. THOR can be configured in a complete off-line operation mode, that leverages the flexibility by making it possible to merge logs from different network segments off-line. The solution makes use of the signatures maintained by security analysts and claims to have custom attack related patterns for enhanced detection capabilities. The solution also supports multiple output formats, ranging from text log to ArcSight CEF, which enables easier integration with SIEM systems. In addition, the solution claims to have an unknown malware detection feature, that uses a file scoring mechanism, based on attributes, contents and meta data.

THOR runs in three major use cases namely,

- Triage Sweep
- Single System Live Forensics
- Image Scan in Lab

The tool also can quarantine samples via network, using BiFrost[16] and can detect deleted elements by a disk surface scan, using DeepDive[16]

4.1.2 Symantec Endpoint APT protection

One of the well known players in the industry, Symantec uses an End point APT protection[2] using multi-layered approach. The strategy devised there is to use a combination of their products array to enable the APT protection, among which the Key player is an intrusion prevention system.

4.1.3 Kaspersky Security Operation Center

Kaspersky SOC from Kaspersky Labs claims to use a centralized threat monitoring approach using the so called *Security Operation Centers*[18], which is a team of cyber defense engineers and resources who can act upon the alarm of a security incident. In addition, the solution provides support for threat intelligence and automated correlation. The firm also provides a *Security Network* tool that is supposed to be an instant reactor to APT threats and a *Automatic Exploit Prevention Technology* with their Kaspersky lab protection solutions, that is supposed to block exploits in targeted attacks. This tool also supports standard white-listing modes which is aimed at reducing the attack surface.

4.2 Defense Solutions based on Deep package analysis (DPI)

4.2.1 TrendMicro DeepSecurity

One noteworthy solution found in the market employing DPI Analysis is *Trend Micro Deep Security*[19] which provides a *Deep Discovery Inspector and Advisor*[7] that claims to be equipped enough to filter malicious content by sandbox simulation of suspicious files, by means of a passive non-intrusive mechanism. The tool also provide destination analysis and communication fingerprinting for tracking C&C The standard here is to follow a Rule based heuristic analysis and perform a Deep packet inspection for protocol detection. To add on, the solution extends itself with a handful of threat scan engines for threat detection and makes use of correlation techniques.

The tool is claimed to be equipped with dedicated threat engines and multi-level co-relation rules, that aids in the detection of threats with minimal false positives. The sandbox analysis is done using a *Virtual Analyser* which provides a quarantine for safe explosion of the threat to perform an in depth forensic analysis. One necessary feature of these tools is the compatibility it should have with standard SIEM(Security Information and Event Management) consoles. SIEM systems are used to analyze secuirty events collected from various sensors residing in the network.This solution facilitates compatibility with standard SIEM platforms, enabling Enterprise wide threat management from a single SIEM console.[7]

[2] https://www.symantec.com/content/dam/symantec/docs/data-sheets/atp-endpoint-en.pdf

4.3 Other Solutions

One another solution available in market for APT Defense is the *WildFire*.[3] The solution claims to be performing Sandbox analysis for secure and controlled execution of the threats and DNS based intelligence to track any C&C activity that might reflect an APT process.

4.4 Analysis of industrial solutions

On analysis of available implementations, the gap between academic research and solutions is pretty wide. Most of the vendors are aiming to promote their business based on the strategy of selling their product ranges as a whole rather than showcasing a single product that can cater to the problem. As most of the solutions don't expose their internal implementations, its hard for a naive customer to assess the efficiency of each of them.

The proposal for a better industrial product swill be to use a hybrid system that encompasses the features of honey pots for early detection and misleading for systems which are regularly monitored by a security team, fractal analysis for IT infrastructures involving heavy traffic flows and globally distributed network by backing up with a distributed multi staged detection system, system and attack intelligence for industrial systems and intrusion kill chains clubbed with context behavior in case of middle-sized implementations.

5. PROPOSAL

As an inference from the analysis of existing solutions and the academic research, the author have a theoretical proposal for a better efficient self-learning defense system, which relies on the principle of artificial intelligence and context sensitive computational methods. The current research works its way on by identifying relevant events from the noise created by an APT attack and aims at correlating this to one of the identified stages in an APT life cycle. Later on, an alert is generated and the system administrators are informed of a possible APT attack. This doesn't appear to be highly effective, as the systems mostly generate independent alerts which needs manual intervention to correlate between events to recreate the attack flow.

An alternative approach would suggest the use of a mechanism similar to that of context sensitive automatons, to create an APT life cycle generator as a context sensitive machine with each of the possible APT cycles, as a language generated by the machine. On each step when an APT qualified event is encountered, a context sensitive transition is performed by the life cycle generator, with the event as an input symbol and the APT stage associated with the successful completion of the preceding event as the previous state of the machine. The idea here is to try and match every new event with an existing APT generator if a valid transition is present, or else to spawn a new machine with its current state corresponding to the event. A transition table is constructed from the input events and the stages, that will contain the permutation of all possible event occurrences from every stage, and the stage changes that can happen.

The APT generator machine introduced above can be mathematically represented as follows :

$M_{APT} = (Q,\ \Sigma\ ,\ \Gamma\ ,\ \delta\ ,\ q_0,\ Z,\ F)$ where

Q : Q is a finite set of APT life stages.

Σ : Σ is a finite set of relevant input events

Γ : Γ is a finite set called the stack alphabet.

δ : δ : (Q $\times$ ($\Sigma \cup \{\epsilon\}$) $\times \Gamma \times$ Q $\times \Gamma^*$) , is a finite subset of all possible decision moves.

$q_0 \in$ Q, is the start stage

Z$\in$ Γ is the initial stack symbol

F$\subseteq$ Q is the set of accepting stages.

On encountering a new event, the system will try to find a machine among the ones available to perform a possible transition that will lead to the creation of a portion in the APT life cycle.This approach will prove really efficient with APTs, as the time - variant, long spanning independent events can be easily correlated and further stages can be predicted with greater accuracy. The system will also train itself using a machine learning approach, to expand is transition table so as to match with the threat database.

6. CONCLUSION

Advanced Persistence Threats as discussed in this paper are mostly complex, stealthy and sophisticated. It generally involve multiple stages that span over a long period of time. Detection methods for these threats are not straight forward due to it's complexity and longer duration. Nevertheless, standard security measures based on blacklisting and malware signatures are ineffective. These situations naturally call in the need for innovative systems that enable continuous monitoring of the network and all associated interactions to the system. A handful of such approaches were analysed in this paper.

Different approaches exist in research for APT detection, but only a few have successful working implementations. A proposal would be a hybrid of many approaches, which would work better than just one. The industrial solutions available in market incorporate many of the research concepts described in this paper. In addition to the approaches analyzed, the author proposes a detection system based on formal methods which is efficient to identify and track associated events in an APT attack.

7. REFERENCES

[1] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens and Witold Kinsner: *Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification*, In Proceedings of IWSPA'16, pages 64-69, , ACM, March 11 2016, New Orleans, LA, USA

[2] Paul Giura and Wei Wang: *A Context-Based Detection Framework for Advanced Persistent Threats*,

[3] https://www.paloaltonetworks.com/features/apt-prevention

In Proceedings of the 2012 International Conference on Cyber Security, pages 69-74, IEEE, 2012

[3] Zainab Saud and Dr M Hasan Islam: *Towards Proactive Detection of Advanced Persistent Threat (APT) Attacks using Honeypots*, Islamabad, Pakistan, In Proceedings of SIN '15, The 8th International Conference on Security of Information and Networks, Pages 154-157, ACM 2015

[4] A. Redondo, Aitor Couce-Vieira and Siv Hilde Houmb: *Detection of Advanced Persistent Threats Using System and Attack Intelligence*, In Proceedings of EMERGING 2015 : The Seventh International Conference on Emerging Networks and Systems Intelligence, pages 91-94, IARIA, Hamar, Norway, 2015

[5] Parth Bhatt, Edgar Toshiro Yano and Dr. Per M. Gustavsson: *Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks*, In IEEE 8th International Symposium on Service Oriented System Engineering, April 2014

[6] Paul Giura and Wei Wang: *Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats*, In Proceedings of the ASE 2012, [Online]. `http://web2.research.att.com/export/sites/att _labs /techdocs/TD _101075.pdf`

[7] *Trend Micro DEEP DISCOVERY Data Sheet*, [Onine]. www.trendmicro.de/media/ds/deep-discovery-inspector-datasheet-en.pdf, Deep Discovery 3.2 NY, Trend Micro, 2012

[8] B. Schneier : *Attack Trees - Modeling Security Threats*, Dr. Dobbs Journal, December 1999

[9] E. G. Amoroso : *Fundamentals of computer security technology*, Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1994.

[10] RSA : *RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats* , http://bit.ly/gaf8hj, February 2011.

[11] Vries, J.D. and Hoogstraaten H. and Berg, J.V.D. and Daskapan S : *Systems for Detecting Advanced Persistent Threats CyberSecurity*, 54-61, IEEE Computer Society 2012

[12] E. B. E. Schweigert and M. Thomas : *Securing ethernet/ip control systems using deep packet inspection firewall technology*, Tofino Security, 2014. [Online]. Available: https://odva.org/Portals/ 0/Library/Annual20Meeting202014/2014 ODVA Conference Byres Schweigert Thomas Securing EtherNetIP with DPI FINAL.pdf.

[13] M. Zeller, *Myth or reality-does the aurora vulnerability pose a risk to my generator?*, in Protective Relay Engineers, 2011 64th Annual Conference for. IEEE, 2011, pp. 130-136.

[14] M. Kenney, *Cyber-terrorism in a post-stuxnet world*, Orbis, vol. 59, no. 1, 2015, pp. 111-128.

[15] PREDICT. (2009) *DARPA Scalable Network Monitoring(SNM) Program Traffic.*

[16] *THOR*, [Online]. Available: https://www.bsk-consulting.de/apt-scanner-thor/

[17] M. Brian : *Industrial defender solutions*, Lockheed Martins, 1996, retrieved: May, 2015. [Online]. Available: http://www.wurldtech.com/.

[18] *Kaspersky SOC* [Online]. https://www.kaspersky.com/enterprise-security

[19] *TrendMicro DeepSecurity*, https://www.trendmicro.com/en_ca/business/products/network/deep discovery.html

[20] Hutchins Eric M., Cloppert Michael J., Amin Rohan M, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, ICIW2011