Detecting Advanced Persistent Threats In The Network

Sheetal Dash
Queen's University of Belfast

Abstract- *An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. In this paper, we discuss how an APT works, we see that the attacker performs reconnaissance of the target for long period of time with an intention to spot security flaws that can be exploited. Further, we discuss what avenues the attacker uses to get into the network,the most common means being Social Engineering. There are other very successful methods such as SQL injection, Exploiting Zero Day vulnerabilities and so on.The malware uses various obfuscation techniques to stay under the radar and starts to capture intelligence over time to finally send the data out in encrypted form. We also discuss, how we can defend our networks against such attacks and in the eventuality of the bug creeping through how to detect it. Many advanced means of detection and mitigation have also been devised. In this paper we go on to discuss new research trends on this subject. It is important to understand that there is no silver bullet solution to stop APT attacks, but if we know enough about how they work and their intentions we can both defend and detect better.*

Keywords- APT, Artificial Intelligence, Firewalls, Internet, Intrusion Prevention System, Network security.

I. INTRODUCTION

HE use of internet has become so prevalent in today's world that the percentage of threat has also continued to expand proportionately. Nowadays there has been a large number of companies, industries and organizations which are working on the internet and the main threat to them is the threat named 'Advanced Persistent threats(APT)'. This type of a threat steals the data rather than causing damage to a network or organization. APT attacks the target organization in sectors containing high value of data, especially in manufacturing, defense and financial industries (including IT sectors).These type of attacks, generally get access to the database or the system of the victim without getting identified for a long time. In order to maintain such kind of an access the intruder must continuously rewrite code and employ sophisticated evasion techniques or sometimes maybe in requirement for a full-time administrator.

II. ILLUSTRATIONS

One of the most notable threats that had been traced in the 1980s was '**The Cuckoo's Egg**'[11] (see figure 1). This describes the discovery and hunt for a hacker who had broken into Lawrence Berkeley National Laboratory. In this attack the hacker had been engaged for several years in selling the results of his hacking to the Soviet KGB. These extraordinary techniques and hacking for a long period of time marks it as a classic early APT.

Now, in the 21st century, the techniques for the attacks have become more complicated and includes a large number of Command and Control(C2) hosts of computers. **Titan Rain,** in 2003 began in China with a series of far ranging cyber-attacks against US Govt. These had targets with the aim of stealing sensitive state secrets in an operation. The focus of the hackers was on military data and included APT attacks on high end systems of organizations such as NASA and the FBI. These attacks caused some friction between the US and Chinese governments and security analysts pointed fingers at the Chinese military as the source of the attacks.

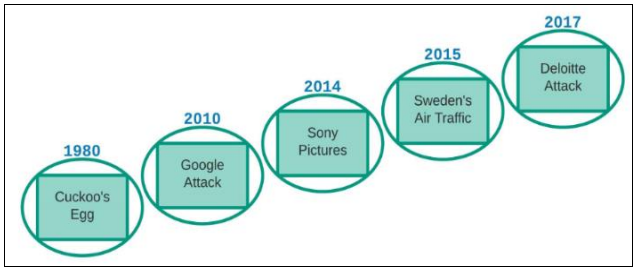

FIGURE 1. Chronological depiction of major APT attacks

Again in 2006, an attack named '**Sykipot**'[2] leveraged vulnerabilities in 'Adobe Reader and Acrobat'. These were a part of a long running series of cyberattack campaigns aimed primarily at US and UK organizations. These attackers consistently used targeted emails containing either a link or malicious attachments containing zero-day exploits. The point of entry method explained above here is

commonly called as Spear Phishing, playing a major role in APT attacks.

There were a few other real-world instances where APT attacks were detected [6]. It was a Chinese attack on **Google** in the year 2010, which targeted the source code alone. In 2011, RSA, the security division of **EMC Corp**. that had SecurID product data was stolen in a sophisticated cyber-attack against the company. This attack targeted mainly the intellectual property. More recently in 2014, **Sony Pictures** Entertainment incident has been described as the perfect APT attack. The Sony attack targeted mainly the personal identifying info stored on the network.Again in 2015, a cyber-attack launched by a **Russian APT group** jammed Sweden's air traffic control capabilities. In this attack, it was suggested that the operations at the Warsaw Chopin Airport hub were disrupted by what the carrier said was a cyber-attack on its flight planning computers. As a result, around 10 flights were cancelled and many others delayed. It was found that the problem was probably caused by what is known as the distributed denial of service attack(DDoS). In Sept 2017, **Deloitte** [10] announced the detection of a breach of the industries global email server via a poorly secured admin email in March. These attackers most likely had control of the server since Nov 2016. This means that, when a hacker deluges an organizations system with so many communication requests, it overloads the server and it can no longer carry out its normal functions. Above all we can clearly believe that the APT attacks can target specific organizations' specific data, which would differ and can have various motives.

III. HOW AN APT WORKS

Before we go and research how to detect and possibly avoid APTs, we need to understand how they work. APT attacks can best be described as a vicious circle of events.

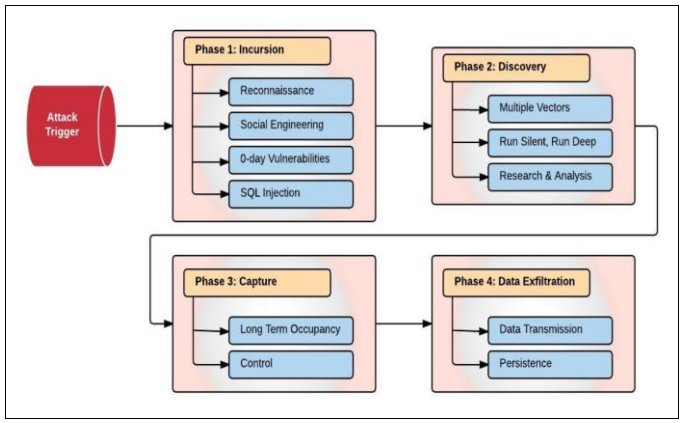

FIGURE 2. Steps of an APT Attack

These events can broadly be divided into four phases [12] (as per Figure 2).

Phase I: Incursion

To initiate an attack, the hackers would decide on a target and then plan to break into the systems/network. There are various ways of doing the same.

1. ***Social Engineering*** – People being weakest link in any organization, techniques such as inducing unsuspecting employees click on links or open attachments that appear to come from legitimate sources. An attacker attacking by means of Apt, generally uses **Spear Phishing,** which is a type social engineering. In one of the more recent attacks using Social engineering, in June 2015 there was a resume social engineering attack[15]. Attackers sent batches of email to enterprises and retailers, each containing a message which is quite commonly sent by job seekers in hope of landing a job. These spam emails had a ransomware-laden email attachment (Cryptowall 3.0 ransomware family), which locks down the infected system and demands a Bitcoin ransom.

2. ***Reconnaissance***[4]–This involves surveillance and monitoring of the target network with an aim to familiarize themselves with the target systems, processes and people, including partners and vendors. This could happen both online and offline. This activity could take months (maybe even years) and continues as the next steps occur.

3. ***Zero-Day Vulnerabilities*** – The Zero Day vulnerabilities are the ones, the defender is unaware of and therefore are extremely beneficial for the attacker. Considering the fact that finding such vulnerabilities are extremely difficult, it takes the most sophisticated attacker to exploit them. The Sony Pictures Entertainment[6] attack of 2014 mentioned earlier was an example of leveraging a zero-day vulnerability, where a team of hackers going by the name Guardians of Peace gained access to nearly 100TB of data.

4. ***SQL Injection*** - This method of incursion involves passing malicious code into a poorly designed application, which finally finds way to the backend database [16].To be able to find such applications, attackers usually employ what is called as a '**Spray and Pray Phishing**'. Large amounts of automated spam are released in hope that some will either click the links (Social Engineering) or will find way to the

databases of applications that have such vulnerabilities exposed.

Phase II: Discovery

Once in, the attackers stay low and try to gauge the system, its defenses and plan an attack.

1. ***Multiple vectors*** – Once the APTs have access to the internal network, they use various methods such as port scanning, downloading various tools to explore the software, hardware and network vulnerabilities.

2. ***Run Silent, Run Deep*** – The goal of an APT is to remain hidden and therefore avoid detection. Therefore, it makes use of numerous obfuscation techniques to make analysis and detection of malware more difficult.

3. ***Research & Analysis*** – Research and analysis of all the data mined from the network gathers the required intelligence (such as network topology, user IDs and so on) to launch stealth attacks.

Phase III: Capture

Capture phase involves accessing unprotected data, installing rootkits on target systems and network access points to capture data and instructions as they flow through the organizations.

1. ***Long Term Occupancy*** – APTs are designed to capture information in a stealth for a long period of time while staying unbeknownst to the victim organization.

2. ***Command & Control(C&C)***[1] – Once inside the network,C & C communication is used to instruct and control the malware to exploit the compromised machines. As they try and gain capability to also re-program those machines, potential for mayhem becomes much higher.

Phase IV: Data Exfiltration

After establishing the required control and having captured enough information, it continues to stay there and the following phases occur meanwhile.

1. ***Data Transmission*** – After the capture phase, the data is transmitted back to the Attacker systems either in clear text or more commonly in encrypted form to avoid detection. Once the data is received, it is consumed by the relevant parties either to wreck mayhem or sell them off in the market to give competitive advantage over the victim.

2. ***Persistence*** – Finally, persistence is what is of paramount importance in an APT attack. Even after data is exfiltrated out of the target, the malware continues to stay there for future use for a long period of time.

IV. CHALLENGES IN DETECTING APTS

Security analysts have been looking at the issue of APT attacks and its preventions for quite some time, but with little success. Though solutions for preventive measures have been introduced continuously, the detection gap remains alarmingly long. This is because, sometimes the common security solutions fail to detect the actual APT infection. The main reason behind the APT detection gap[5] is the sophistication of the infection methodologies used by the attackers. Most infections occur beneath the infected operating system, and as such, cannot be seen in real-time by common detection technologies like Anti Malware applications and software.

V. WAYS TO DETECT APTS

The ideal situation would be, to be able to thwart such attacks and if we are unable to do so, detect them – the soonerthe better. Below are a few ways in which we can do so:

To be able to defend against Social Engineering attacks below measures can be employed:

- Sharing of information with employees on a need to know basis – Permissions need to set in granular fashion and access to sensitive data should be given to only those whose job function requires it.
- Usage of a good security software that filters emails well.
- Addition of Email certifications and encryptions to the email client.
- Creating awareness about Social Engineering attacks and ways to deal with Phishing attacks.
- Asecurity layered approach should be taken in organizations for better protection.

To prevent against APTs in their Reconnaissance stage, we would need the help of a good firewall and intrusion prevention system(IPS).

- The firewall controls which ports are exposed and to whom they are visible.

- The IPS can detect port scans in progress and shut them down before the attacker can map the entire network.
- Computer OS Fingerprint Probe: The agent or appliance detects an attempt to discover the computer OS.
- Other TCP checks for abnormal flags on the packets.

Monitoring the volume and frequency of data transmitted over the network – During Data Exfiltration stage, the malware would be attempting to send the captured information back to the attacker by various means. Monitoring the data flow in and out of the network, would enable us to identify anomalies and therefore detect the malware. This can be done by using network rules, identity and access management(IAM), and bastion hosts.

- Retaining a list of usual email addresses/machines data is being sent so that the nature and scope can be identified.
- Using logging to keep track of data movement in the network.
- Enforce further scrutiny when the recipient (whether email address or a machine) is outside the organization.

Certain tools like Security Analysis or Analytics software are very useful to detect APTs in a network.

- These tools and software can be easily deployed in order to collect, filter, integrate and link different types of security event information.
- This also helps to get a more comprehensive view of the security infrastructure.
- These tools help in correlating the events that occur in different places in order to detect the suspicious activity that occurs through a large number of devices in an organization.
- This software analyzes logs and data of different events from different applications, network defenses, controls etc.
- They also help the industries in implementing the real-time monitoring of the servers, network traffic and controls, consolidating and coordinating diverse event data from the applications, logs etc.
- In addition, it also performs forensic analysis in order to understand the techniques and system vulnerabilities of the attack in a better way.

As a result, these would help the security controllers to figure out how systems were compromised and which all were affected if the attack would still persist.

Few of the below methods can also be used to detect APTs:

- Usage of common anti-malware products like Client Applications, gateways, sandboxes and cloud services, which tries to detect and prevent 'Penetration'.
- Also, there are few anti-APT solutions which focus on the 'APT Activity' in the infected machine by discovering and monitoring the most outbound traffic of the APT.

APT detection is very much at a nascent stage and a lot of research is underway to find faster ways to detect APTs.

Intrusion Prevention System (IPS)

Intrusion prevention is a preemptive approach[8] to network security where this system sits in line between source and destination actively analyzing and taking automated actions based on what it sees.

IPS can be considered as a successor of Intrusion detection system(IDS). This is considered more active in the sense that post detection, it both notifies the administrator and also blocks access. The actions that an IPS carries out include the below:

- Notifying Administrator
- Dropping malicious packets
- Blocks traffic from the attacker
- Resets the connection

Various detection mechanisms used by IPS are:

1. Statistical anomaly-based detection
2. Signature detection
    a. Exploit facing signatures
    b. Vulnerability facing signatures

It is noteworthy that IPS do not help us handle massive port scans on their own. We need to either rely on Snort (or similar tools) or add rules on IPS to drop connections from the IP identified.

VI. MITIGATION MEASURES

APTs are one of the most sophisticated and dangerous real-time threats that can be encountered in a network. It affects as many hosts as it can, which means the mitigation is a real challenge.

But there are few mitigation strategies which when implemented would be helpful for potentially blocking 85% of the targeted attacks in the network. Few of them can be described as follows:

1.) ***Application Whitelisting***– This will be the technique of creating the whitelisting of the allowed application, help identifying and stopping unknown executables from attacking the system.
2.) ***Application Patches***– Every application needs to be updated in order to reduce the likelihood that they might be exploited.
3.) ***OS Patches***– Patching of the operating system needs to be carried out as and when necessary in a prompt manner. Clearly, the OS software as well could be compromised if it is not updated regularly.
4.) Minimize Administrative privileges – Accounts with administrative privileges are usual targets for APT attacks as they allow bypass traditional security barriers of a network. Minimizing the number of such accounts keeps the risk levels also to a minimum.
5.) Prevent usage of insecure channels –Secure channels must be preferred over insecure ones such as https instead of http. Any attempts to override that should be reported to IT security personnel.
6.) Data storage in single data lakes should be avoided. Instead the data should be compartmentalized, to mitigate the loss per attack.
7.) Maker-Checker functionality in system administrator workflows must be added to increase accountability and restrict easy overriding of approvals.

VII. ADVANCED MITIGATION/DETECTION TECHNOLOGIES

A. SIEM

Security Information and Event Management(SIEM) stores a baseline of how normal state of affairs should be and then compares it with real-time logs and traffic to register any anomalies. What this basically means is, this is a work in progress at all times and requires frequent fine tuning. Incorrect calibration could result in either a lot of false alarms or missing genuine alerts.

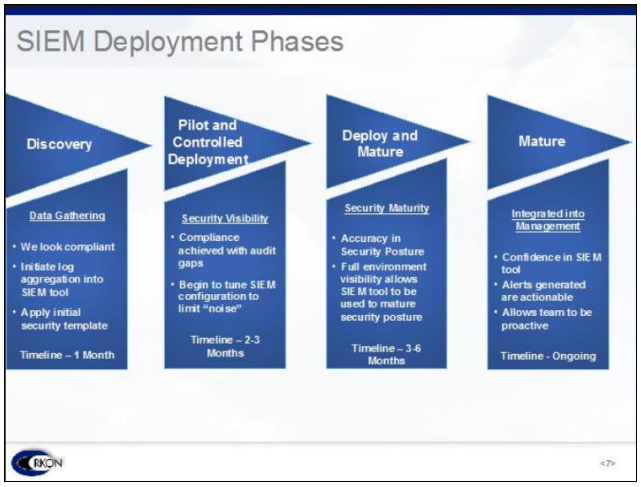

FIGURE 3. SIEM Implementation Steps [13]

SIEM implementation can be broadly divided into 4 phases(see figure 3), starting with the "Discovery". In this phase, the idea is to lay the groundwork in terms reviewing the organizations security posture and the business case for SIEM. Also, the current controls that currently in play will need to be identified. Log accumulation is initiated based on an initial template. Based on the knowledge, from the Discovery phase, in the "Pilot" phase the template is extended to further technologies, the assumptions made in the Discovery phase are tested in real time. After the pilot implementation, the final implementation happens in the "Deploy" phase in which controlled deployment/initial production test run happens. After the final deployment, the system is calibrated and recalibrated to "Mature" the model developed. The confidence in the results give rise to actionable alerts.

B. Vulnerability Assessments

Vulnerability Assessments(VA) take a laundry list of known security defects, analyze the network and report any misgivings. This is like an internal audit based on the list which is regularly updated.

C. Versive Security Engine

Versive Security Engine(VSE) is an automated threat hunting system built on an Artificial Intelligence platform. The engine distills the most valuable practices used by professional threat hunters and makes then machine-scale and automatic. It exposes ongoing adversary campaigns automatically by connecting suspicious or malicious activity, from across the network and over time, into coherent, contextualized and actionable Threat Cases.

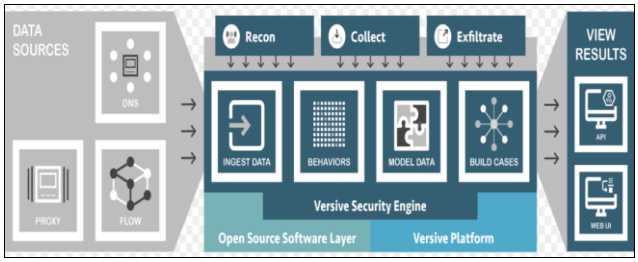

FIGURE 4. Versive Security Engine [14]

The VSE as shown in figure 4, works by first baselining the normal behavior using various data sources from the network using other supplemental security tools. Based on that information, the VSE models the behavior that strongly correlates to advanced adversary campaigns. The VSE compares the results across the network and across time, with an aim of building threat cases. Finally, all the results are displayed on a UI in the form of reports or using an API exposed for use.

VIII. DISCUSSION

This section discusses the proactive measures to defend against an attack and the reactive steps to tackle attacks after they are in effect. As discussed in SIEM [13], this is a model of making sure everything is running fine. It is a diagnostic tool that checks system health to find anything that is anomalous in terms of the way the network/system is functioning. Whereas Vulnerability Assessments, are a check on the various controls in place to prevent an attack, find out security flaws or loopholes that could be exploited for an attack. While it is important for us to detect an attack as soon as it intrudes into the network, what is even more important is the proactive ways of defending against them which is provided by such assessments. Essentially for sound functioning we would want a two-layered protection consisting of both the above-mentioned measures. Another reason, why VA and SIEM need to work in conjunction is, the baseline that SIEM is going to be based on, should not be one with security flaws in it.

With VSE [14]we get sound baseline developed after a lot of groundwork in terms of numerous vulnerability assessments,a mature model of system health check by way of comparing current health with the previous baseline saved(updated regularly).Coupled that with the Artificial Intelligence and the machine learning platform, gives us a model that is able to effectively identify security threats and raise necessary threat cases.

IX. CONCLUSION

We have seen that with the exponential rise in data volumes and the number of big and smaller players in the market also increasing rapidly, the weak links are also increasing proportionately and making the APT attacks more plausible and more effective. In this paper, we have seen how dangerous the APTs can be if left undetected. Here we propose two-pronged defense technique to protect our data and the sanity of our systems, in which we have strong security principles enforced by automated and frequent audits of the system for security holes that can be exploited. We also need to have a solution in place that would constantly monitor our systems, events, logs to capture any anomalies to finally report them and filter/block any suspicious activities. While there are more than a few tools in the market to achieve these, ideal ones are those which use a fine comb while performing their tasks with minimum manual intervention.

X. ACKNOWLEDGEMENT

This research paper was supported by Queen's University, Belfast. I wish to thank the ECIT department for the opportunity of performing research, and therefore providing the basis of this article. I am indebted to an anonymous reviewer for providing insightful comments and providing directions for additional work which has resulted in this paper. Without the anonymous reviewer's supportive work this paper would not have been possible.

REFERENCES

[1] Detecting theenemyinside the network How Tough Is It to Deal with APTs? Trend Micro Inc. [Online], Available: https://www.trendmicro.co.uk/media/wp/apt-primer-whitepaper.pdf

[2] N. Villeneuve and J. Bennett. (2012). Detecting apt activity with network traffic analysis. Trend Micro Inc. [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf, accessed Oct. 31, 2013.

[3] GUODONG ZHAO, KE XU, LEI XU1, AND BO WU1, ''Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis,'' in Proc. IEEE Global Telecommun. Conf. (GLOBECOM), vol. 3. 2015, pp. 1132–1142

[4] (Feb 2017)Ed Koehler," How Do You Detect an Advanced Persistent Threat in Your Network?"[Online]. Available: https://www.avaya.com/blogs/archives/2017/02/apts-part-

4-how-do-you-detect-an-advanced-persistent-threat-in-your-network.html
[5] AvishaiZiv, Detecting and dealing with Advanced Persistent Threats to embedded systems [Online]. Available: http://www.newelectronics.co.uk/electronics-technology/detecting-and-dealing-with-advanced-persistent-threats-to-embedded-systems/61636/, May 2014
[6] InfoSec Institute, [Online]. Available: http://resources.infosecinstitute.com/current-trends-apt-world/#gref
[7] Bejtlich, R.: What Is APT and What Does It Want (2010), http://taosecurity.blogspot.be/2010/01/what-is-apt-and-what-does-it-want.html
[8] Himanshu Arora, 'Introduction to intrusion prevention systems', IBM Developer Works March 19, 2013 [Online], Available: https://www.ibm.com/developerworks/library/se-intrusion/
[9] A. K. Sood, and R. J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," Security & Privacy, IEEE 11.1 (2013): 54-61.
[10] William Tsing,"Deloitte breached by hackers for months", Malware bytes Labs blog Sep 2017 Article [Online], Available:https://blog.malwarebytes.com/security-world/2017/09/deloitte-breached-by-hackers-for-months/
[11] Simon Heron, "Five notable examples of advanced persistent threat (APT) attacks", Get Safe Online 19 Aug 2015 Article [Online], Available: https://www.getsafeonline.org/business-blog/five-notable-examples-of-advanced-persistent-threat-apt-attacks/
[12] Symantec. (2012). Advanced Persistent Threats: A Symantec Perspective [Online]. Available:http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf
[13] Irma Garcia, "A Step-by-Step Guide to a Successful SIEM Deployment", Ingram Micro Advisor, [ONLINE]. Available http://www.ingrammicroadvisor.com/security/a-step-by-step-guide-to-a-successful-siem-deployment
[14] Versive. (2017). How the Versive Security Engine Works [Online]. Available: https://www.versive.com/product/
[15] JP Buntinx, "Top 3 Social Engineering Attacks Of 2016", The Merkle, [Online], Available: https://themerkle.com/top-3-social-engineering-attacks-of-2016/
[16] Techopedia. SQL Injection [Online], Available: https://www.techopedia.com/definition/4126/sql-injection

Sheetal Dash received her B. Tech degree in Computer Science from SOA University, India, in 2013. She is currently pursuing the master's degree in Applied Cyber Security with Queen's University, Belfast, United Kingdom. Her research interests include Network Security and NexGen threat detection.