 doi:10.20944/preprints202106.0621.v1

Advanced persistent threat detection and defence (APT)

Hassan Adeyoola
Computer Science (Cyber Security)
University of Bradford
Bradford

hadeyool@bradford.ac.uk

***Abstract*—as the growth and popularity of technology has become simultaneous ascend in both impacts and numbers of cyber criminals thanks to the web. For many years, the organization has strived in ways of preventing any attacks from cyber-criminal with advanced techniques. Cybercriminals and intruders are developing a more advanced way to breach the security surface of an organization. Advanced Persistent Threats are also known as APT are new and a lot more sophisticated version for multistep attack scenarios that are known and are targeted just to achieve a goal most commonly undercover activities. this report, there will cover everything I know that tells us about APT with more word and brief explanations**

Keywords—cyber-criminal, organization, Advanced Persistent Threat, undercover activities (keywords)

I. Introduction

Since the invention of the internet, we have been relying on networks and servers to help function our lives of 1.4 billion people (and counting) on the planet earth. Unfortunately, in the world we live in many malicious activities are going on, some report the lately and their damage has a massive effect on their victim's lives. From stealing information to masquerading as someone authentic, these are cybercrimes, and they are a danger in our daily lives and this report, I will go profoundly on a topic that correlates to this type. I will adhere to research that I have found on the internet about this topic. This will also include the common types of mitigating cyber-attacks which means the detections and defense that are used. What is also included in this report will show how some sites progressions on extracting data malware that cybercriminals use including their location just to show insight on how the world is fighting back against cybercriminals.

II. What is Apt

"An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data." (What is APT (Advanced Persistent Threat) | APT Security | Imperva, 2020)

In the cyber security business, an APT is s broad term that is used to describe an attack campaign especially when an intruder or a group of intruders, set up an unlawful long-term bearing on a network for the sake of mining highly important data.

III. Types of APT attacks

The most crucial thing to comprehend about APTs is their flexibility. Although they are capable of infiltrating attacks of tremendous and sophistication, they can also indulge in a very basic attack. Rivals are concerned about the ROI also known as the return of investment and the efficiency just like everyone in an organization and it is quite often that a single attack is successful. Below are some of the most common vectors for the attacks and they are:

A. Phishing

This is known to be a type of social engineering which mostly consists of stealing user data, which includes the user's credit card numbers and login credentials. It happens when an attacker, masquerades themselves as a trusted or authentic entity, then deceives the victim into opening a text, email, or instant message.

B. DNS modifications

Also known as dns hijacking. It consists of manipulating transactions and user will be deceived since they are not aware of the activity of their servers especially during an internet session. Since it is malicious exploitation, this means users are being redirected with the help of DNS servers that are rouge and never change the IPS address of the user that is being redirected of their servers especially during an internet session.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 June 2021 doi:10.20944/preprints202106.0621.v1

C. Zero days attacks

Which is also described as Day Zero, is an attack that involves the exploitation of a possibly a serious software security weakness in which the developers or vendors are not aware of. This means that the vendors or security software developer must quickly resolve the weakness immediately when it has been discovered as this could limit the threat to those who uses the software.

D. Supply chain attacks

A supply chain attack also known as either third party or value chain attack, it happens when an intruder penetrates your system through a provider or an outside partner that can have access to an organisation system. This is known to have significantly change enterprises' attack surface for the past few years, since there have been more service providers and suppliers grabbing their hands-on important data more than ever before

E. Ransomware

First, ransomware is a type of mischievous software that is designed to stop the access to a computer files or even the computer until the victim paid the sum of money. Most ransomware alternatives are encrypting files on the computer affected, that will make them inaccessible, and demand a ransom payment to restore access to the computer.

F. Pirated software

Also known as software piracy, this is when an unapproved copying of a software that has been purchased. This means when you buy the software from a company it does not mean you are the owner of that software; all it means is that you are a licensed user.

IV. Risk and impacts

The victims of these types of APT that are especially the main target are being carefully researched and illegally monitored. They are mostly large industrial business or local networks. These are known to be mostly vulnerable and the impact it could are known to be following and they are :

A. Rational property theft

This known to include patents or the secrets for trading. The impact goes deeper according to this website it says that these sorts of situations keep chiefs up around evening time all things considered: Intellectual property (IP) which is one of the the essential part of the 21st-century organization, a basic engine driving improvement, intensity, including the development of organizations and the economy "Intellectual property can constitute more than 80 percent of a single company's value today.1 It's no surprise, then, that thieves—armed with means, motive, and opportunity—are in hot pursuit." (Gelinne, Francher and Mosburg, 2020) which briefly shows the fundamental of what the attacker wants to materialize.

B. Sabotaged critical organisation infrastructures

That means deletion of a database. As a result of this here is a brief explanation of the impact, according to the source I got from a website which says
"a bigger threat than foreign states targeting political party emails was "covert sabotage, by chucking a cyber spanner, as it were, into the now cyber-dependent critical infrastructure that we have". This could include the financial system or energy utilities." (Eyers, 2020)

C. Sites fully taken over

Gangs have taken steps to offer taken information to intruders; exploit taken information to assault casualties' colleagues; and plug casualties' "messy mysteries" based on reasonable research which can be viewed in websites especially local or government ones for instance "Some attackers took advantage of COVID-19 to coax people into opening malicious emails and attachments, while other ransomware groups agreed to an ad-hoc ceasefire on healthcare vendors." (Novinson, 2020)
In this scenario it could be that the attacker could be asking for ransom or else they could not release the site for the company until there is an agreement that needs to be done and that could cost the business a lot of money and time especially if the business is a marketing and financial industry.

D. Classified information compromised

Which includes employee of an organisation or a private user data a great example for this is when a person in the name of Harold T. Martin III, who was a worker at the N.S.A. cooperation personalized accessed the co-operation hacking unit, confessed his criminal activity, two years after his arrest in what may be described as the biggest breach of classified information in history. "F.B.I. agents who swarmed his modest home south of Baltimore in 2016 found stacks of documents and electronic storage devices stashed in his car, his home and even a garden shed." (Shane, 2020)

V. Dectection and defence

In the computing industry especially in the cyber security environment, there are requirements in how things should be before its being utilized. This case we must solve the APT and have a fully functioning plan to detect and defend users from APT. Which means it must have a multi-faceted approach on the role of network admins, individual users, and providers of security here are the activities during an APT session

A. Traffic monitoring

Now the best practice of preventing the instalment of stolen data extraction or something we call backdoors which is a malware that is known for negating normal authentication procedure for accessing a system. We are encouraged to use monitoring egress and ingress traffic, this because it does not only stop malware and stolen data extraction, inspecting the traffic inside the desired network can also aid in alerting security personnel to any strange behavior that may be a malicious activity.
There are examples of this types of process and one of this is a WAF which is a Web Application Firewall, and they are been installed into your network traffic that is inside the perimeter of your network filter traffic which are connected to your web application servers; therefore, it is protecting one of your weak attack sides. The other features that are included in a WAF is that it can clear out application layer attacks. This

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 June 2021 doi:10.20944/preprints202106.0621.v1

includes attack like SQL injections, Remote File inclusion also known as RFI as they are known for commonly used on a phase of an APT infiltration.
Network firewalls which are also known to be a service for network monitoring are different in this matter. This is because they are able to provide a rough view of how users are communicating within the network while aiding in finding an internal traffic abnormality (strange or unusual large data transfer, abnormal logins). The end could indicate an APT attack that is being performed. It is possible to monitor system honeypots or file sharing access

In conclusion the use of incoming traffic monitoring system could be helpful in terms of detection and the removal of malwares like backdoor shells. This can be discovered just by the interception of remote request from the operators or users.

B. *Access control*

As for criminals, the largest and the most vulnerable soft spot in your security perimeter is your employees especially the ones in organizations'. As common as it may be, this is potentially why intruders can view network users since it can be an easy entrance to penetrate your defence, as they are hold withing the organisations' security perimeter.
Here below are the likely mistakes or deliberates that these target or employee do that could open a gateway for intruders and they are:

- The carelessness of a user, especially those who fail to comply to the network security policies. This could grant access to unauthorized users and could lead to potential threats or attacks
- Users who negotiate with the intruder to have the network access by them since the rouge employee is able to access them, leaving them open for planned threat by him/her and the intruder
- Malicious insiders who deliberately took the advantage of their identity just to give the intruder access

The way to mitigate this type of problem is to develop an effective control that will require a thorough review of everyone in the organisations' especially the information that have been accessed. A great example is classifying data on a need-to-know basis, this known to be affective since its aids in blocking the intruder's ability to be able to infiltrate login credentials all from a low-level employee member, using it to gain access to classified materials.
The other things that are required in defence are to secure key network access point with a two-factor authentication also known as 2FA. In this process it requires users to use a 2nd form of authentication when they want to see the organisations' secretive materials, this usually done by sending a verification code to the users communicating devices, mobile phones, tablet and many more. This proven to being able to prevent intruders masking as an authentic user to being able to explore the organisations' network.

C. *Domain whitelisting and Application*

The method of whitelisting consists of controlling the domains that can be accessed from the organisation or your network, this includes applications which can be installed by users. This is an effective method as is well known for being able to reduce the accomplishment rate of APT attack all by reducing the attack surfaces that are available.
It is known that this type of security measure is not that deceiving, on the other hand it has been know that domains that are trusted can be compromised. Majority of security experts knows that malicious or strange files often arrive as a software that seems legitimate. To add into this, software that have old product version are vulnerable to compromisation and exploitation.
In order to have an efficient whitelisting, it is recommended to have a strict update policy. It must be enforced to reassure that your users or the organisations' employees are always running with the latest version of any application provided on the list

D. *APT diagram*

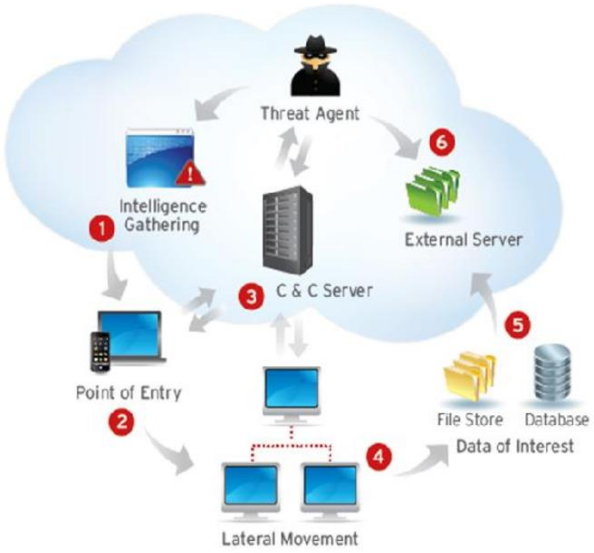

Fig. 1. Example of an APT attack (*figure caption*)

REAL LIFE CASES OF APT

In some areas of APT there are ways of measuring the attack and according to a research I found a site called fire eye, it clearly goes through a many case. here are the examples

"APT34
Suspected attribution: Iran

Target areas: This danger bunch has directed wide focusing across an assortment of businesses, including monetary, government, energy, compound, and broadcast communications, and has generally centered its activities inside the Middle East

the trust APT34 is engaged with a long-haul digital surveillance activity generally centered around observation endeavors to profit Iranian country state interests and has been functioning since 2014. Assessment made was proved that APT34 works was made for Iranian government based on details of infrastructure which contain mentions of Iran,

the utilization of Iranian infrastructure, and aiming the supports with nation-state interests.

The associated malware used are: POWBAT, POWRUNER, BONDUPDATER

“Attack vectors: In its latest campaign, APT34 leveraged the recent Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER.” (Platform et al., 2020)

"APT41

Suspected attribution: China

Target areas: APT41 has straightforwardly focused on associations in at any rate 14 nations going back to as right on time as 2012. The gathering's surveillance crusades have focused on medical care, telecoms, and the cutting-edge area, and have verifiably included taking protected innovation. Their digital wrongdoing interruptions are generally evident among computer game industry focusing on, including the control of virtual monetary forms, and endeavored sending of ransomware. APT41 operations against advanced education, travel administrations, and news/media firms give some sign that the gathering additionally tracks people and directs observation.
“Overview: APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Related malware: APT41 has been noticed utilizing in any event 46 diverse code families and apparatuses.

Assault vectors: APT41 frequently depends on lance phishing messages with connections, for example, aggregated HTML (.chm) records to at first trade off their casualties. Once in a casualty association, APT41 can use more complex TTPs and send extra malware. For instance, in a mission running close to 12 months, “APT41 compromised hundreds of systems and used close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits. APT41 has also deployed rootkits and Master Boot Record (MBR) bootkits on a limited basis to hide their malware and maintain persistence on select victim systems.” (Platform et al., 2020)
“APT31
Suspected attribution: China

Target areas: Numerous, including the government along with the transnational financial company, aerospace, and defense organizations, including high tech, construction along with the manufacturing, communications, media, and the insurance.
“APT30
Suspected attribution: China

Target sectors: Members of the Association of Southeast Asian Nations (ASEAN)

Overview: APT30 is noted not just for sustained activity over a long period of time but also for being able to successfully modify and adjusting the source code to sustain the same tools, methods, and structure ever since at least the year of 2005. Indication reveals that the group arranges targets, possibly works in shifts in a collaborative environment and builds malware from a coherent development plan. The group has had the capacity to infect air-gapped networks and this has been happening according to the report, since 2005.

All of the associated malware includes: SPACESHIP, SHIPSHAPE, FLASHFLOOD

“Attack vectors: APT30 uses a suite of tools that includes downloaders, backdoors, a central controller, and several components designed to infect removable drives and cross air-gapped networks to steal data. APT30 frequently registers its own DNS domains for malware CnC activities.” (Platform et al., 2020)

CONCLUSION

Throughout the research and the actions that have been taken to stop intruders, in the security industry. This defense strategy which includes the mentioned techniques clearly showed crucial importance on how companies always come up with plans to reduce the risks of problems that could take place on their surface.

Furthermore, the strict implementation of the company including education employees or users mostly focuses on the psychology of humans. The ability to distribute a workforce on requirements needed to not fall into the trap of social engineering. Those strategies mentioned are not technical and they deal with APT attacks taking the advantage of blind trusted individuals who have emails Personal or private accounts and attachments.

In the future, as companies or organizations are obtaining ideas and more defense systems to stop attacks like the APT, they should have an advanced team that is solely based on the APT attacks since it is a traditional attack, and it could be in a system unknown and undetected.
On the other hand, some employees cannot be trusted in making sure they can mitigate attacks like APT since they could work with the intruder. Organizations should have a way of finding these rough employees as it will reduce the risk of APT forming or even worse changing the industry reputations. Local users should always make sure that if the software they are using should be updated luckily most software will remind the users when it needs updating. Furthermore, there have been many cases of APT and there will be more cases rising and it is based on preparations that can be used to detections and defense to reduce the incident of APT.

REFERENCES

[1] Learning Center. 2020. What Is APT (Advanced Persistent Threat) | APT Security | Imperva. [online] Available at: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/> [Accessed 17 December 2020].

[2] Gelinne, J., Francher, D. and Mosburg, E., 2020. The Hidden Costs Of An IP Breach: Cyber Theft And The Loss Of Intellectual Property. [online] Deloitte Insights. Available at: <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html> [Accessed 17 December 2020].

[3] Eyers, J., 2020. Sabotage Of Critical Infrastructure A Growing Risk, Says Former Chief Spy. [online] Australian Financial Review. Available at: <https://www.afr.com/companies/financial-services/sabotage-of-critical-infrastructure-a-growing-risk-says-former-chief-spy-20170202-gu3xgu> [Accessed 17 December 2020].

[4] Novinson, M., 2020. The 11 Biggest Ransomware Attacks Of 2020 (So Far). [online] CRN. Available at: <https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-> [Accessed 17 December 2020].

[5] Shane, S., 2020. N.S.A. Contractor Arrested In Biggest Breach Of U.S. Secrets Pleads Guilty (Published 2019). [online] Nytimes.com. Available at: <https://www.nytimes.com/2019/03/28/us/politics/hal-martin-nsa-guilty-plea.html> [Accessed 17 December 2020].

[6] Berros, Y., 2020. 5 Most Common Types Of APT Attack Vectors | XM Cyber. [online] XM Cyber. Available at: <https://www.xmcyber.com/5-most-common-types-of-apt-attack-vectors/> [Accessed 20 December 2020].

[7] Platform, H., Forensics, N., Security, E., Security, E., Demand, D., Services, F., Systems, I., Intelligence, T., Validation, S., Defense, M., Response, I., Consulting, C., Demand, E., Training, C., Stories, C., Success, C., Portal, C., Support, C., Programs, S., Notices, S., Products, S., Portal, D., Overview, P., Resellers, F., Partners, T., Partners, C., Providers, G., Locator, P., Center, P., Partner, B., Reports, A., Reports, T., Industry, T., Groups, A., Blogs, R., Security?, W., Cloud, C., Validation, S., Magazine, T., Downloads, F., Market, F., Training, E., FireEye?, W., Honors, A., Directors, B., Relations, I., FireEye, C., Releases, P., Opportunities, J. and Groups, A., 2020. Advanced Persistent Threat Groups (APT Groups) | Fireeye. [online] FireEye. Available at: <https://www.fireeye.com/current-threats/apt-groups.html> [Accessed 21 December 2020].

[8] Ghafir, I. and Prenosil, V., 2020. Figure. 1. Typical Steps Of APT Attack.. [online] ResearchGate. Available at: <https://www.researchgate.net/figure/Typical-steps-of-APT-attack_fig1_305956804> [Accessed 21 December 2020].