Journal of Computer Science

Original Research Paper

Advanced Persistent Threats (APT)-Attribution-MICTIC Framework Extension

Pedro Ramos Brandao

Instituto Superior de Tecnologias Avançadas-Lisbon (ISTEC) Coordinator Professor, Portugal

Article history
Received: 28-02-2021
Revised: 06-05-2021
Accepted: 07-05-2021

Email: pb@pbrandao.net

Abstract: Analysis of one of the fundamental parts of the Advanced Persistent Threats (APT) Attacks. The phases of the APTs, their framing with the identification of criminals. Type of attack that normally requires resources only available to the State-State hacking. The importance of Attribution in the analysis of APTS. The unique and differentiating characteristics of this type of attacks compared to traditional cyber-attacks. Development of an extension for one of the few Frameworks applied to Attribution in APTs, the MICTIC.

Keywords: APT, Advanced Persistent Threat, Cyber Security, Cyberwar, Cyber Espionage, Malware, Virus, Network Security, Cyber Terrorism

Introduction

Nowadays, companies face a severe issue in terms of Cyber Security and that is Advanced Persistent Threats (APT).

APTs are highly sophisticated threats and attacks against computer networks which are extremely difficult to detect and once intrusive remain within the infrastructure for a long time. APTs break all the conventional rules of Cyber Security attacks, typically adopting their techniques on data and information, taking users as an entry point and concealing their tracks with extreme caution and care, so many traditional security measures are not effective in addressing this threat.

Many organizations are focusing all their energy on a perceived threat, but if that' s the wrong threat, they will still be compromised. This is the case for APTs.

Taking a brief look at APT, the advanced nature of the opponent means that they will usually find a way into the organization. Unfortunately, many companies can't understand all of their exposure points and if the attack gets to know more than the defense we will lose. Furthermore, the invader is quite persistent.

The major reason for APT's success is that it' s a new threat that many organizations are not prepared to deal with. The old threat was visible, it could be detected if the security devices were well configured, if it failed, it would move on to the next target and was mitigated. Most of the security we currently have in place is prepared to handle that level of attacks, not APT. Whilst some of APT attacks are automated, we are dealing with a sophisticated attacker who carries out part of the attack with manual intervention, it' s not just the attack that is sophisticated the attacker also has quite sophisticated knowledge. Once a human is involved in the planning and potentially in executing the attack, the adversary can adapt and use human intelligence to extract information from a target. It' also common for organizations not to recognize APT is a silent killer.

Advanced Persistent Threat is used to describe an adversary, usually a foreign government that will target an organization, without ceasing until they successfully compromise the entity, with the goal of data extraction and long-term access. The key words for APT are stealthy, targeted, adjustable and focused. Although APT isn't new, the large-scale nature in which it attacks systems and the fact that more organizations are noticing that their current form of defense against traditional attackers needs to change is new.

To investigate the perpetrators behind criminal cases, the term investigation is commonly used. In reverse, the assignment is usually reserved for tracking APTs, i.e., Cyber Espionage. A key premise is that APT groups are directly embedded in, or at least led by, intelligence agencies. Therefore, the term state-sponsored attacks was coined and is more or less used as a synonym of APT attacks nowadays. The affiliation to governments by hackers is obvious. Several other reports also contained names and even photos of individuals believed to be the likely perpetrators and to be working for the military. In particular, the US Department of Justice has unveiled a remarkable number of charges against hackers from North Korea Russia as China and Iran (Wendt *et al*., 2013).

Considering the fact that governments traditionally publicly deny their involvement in cyber attacks and protect their own assets from prosecution, it is a valid point for attributions to matter.

In the Cyber Security community, there is the often-repeated opinion that it is irrelevant who is behind an attack because the security measures are always the same, regardless of the origin of the perpetrators. But that' s not true for APTs. In practice, there is hardly a company or organization that can implement all existing and recommended security measures and because in APTs unique, attack-specific tools are built.

Therefore it' s critically important to know to whom the authorship of the APT attacks can be attributed.

So this paper will focus on this aspect and in practice will propose an extension of the MICTIC Framework.

Literature Review

According to De Vries (2012), traditional security defenses cannot be applied to APTs, these types of attacks incorporate several simultaneous attacks. One of the main challenges related to APTs is that one can never know where the attacks begin, that is, where the point of infection starts.

According to Levine (2013), APTs are successful because they are highly specialized and always untraceable. These are one of the greatest Cyber Security threats of our time. Having high rates of success.

According to Moon *et al*. (2014), APTs are the most advanced and complex Cyber Attack of our time. They are able to bypass traditional security mechanisms. They require a new defense technique.

According to Lima (2015), the main difference between this threat and all others, old viruses are not a sophisticated problem and it' s easy to discover their signature and it' s possible to detect malware running on a system. Not in the case of APTs.

According to Wendt *et al*. (2013), One of the techniques used by APTs is Spears phishing and the malware may not remain on the machine in which it' s activated, this type of attack easily gains control of machines on a network.

According to Adelaiye *et al*. (2018), this type of attack is highly invisible and sophisticated and it can provide attackers with the ability to be in a system for months without being detected. It states that it is impossible to detect this type of attack with conventional approaches. They use multiple attack vectors which makes them highly effective. The effectiveness of these types of threats is also due to a number of human vulnerabilities. According to the author, traditional computer security systems are ineffective against these types of threats.

According to Alkan (2018), APT-type attacks are highly effective and cause enormous damages.

According to Ghafir and Prenosil (2014), the use of zero-days technology creates an inability for conventional detection and security mechanisms to find evidence of these attacks. The fact that they do not use known signatures makes them even undetectable by traditional and conventional means.

According to Wagner *et al*. (2017), APTs require a greater understanding and holistic approach, which means that traditional systems do not detect them, he states they are a very significant threat to current systems.

According to Khan (2020), traditional security solutions are not applicable to APTs.

According to Li *et al*. (2018), APTs are a new type of attacks characterized by difficulty in detection and with a serious problem in traditional Cyber Security defense processes.

According to Stalling (2018), it states that APTs are all successful mainly due to the fact that they use "zero-days exploits."

According to Joloudari *et al*. (2020), traditional detection systems do not work with APTs. One of the reasons pointed out is the use of totally unknown signatures.

According to Mustafa (2013), the sophistication of these types of attacks is increasing and it is essential to study new ways to address the problem.

According to Virvillis (2014), these types of attacks go completely unnoticed by traditional detection mechanisms.

Also, according to Virvillis (2014), current security solutions have been systematically failing on all fronts in defending against APTs. It is required, according to the filing, to find new forms of mitigation for APTs.

According to Mirza *et al*. (2014), he regards APTs as the most fearsome threats in technical terms. It also states that the use of intrusive technologies without known signatures allows attacks to go undetected by traditional mechanisms and that a new approach is require\ed.

According to Wang *et al*. (2014), APTs are characterized by using unknown signatures, this leads to them being undistinguishable within the internal network traffic. Thus undetectable by traditional technological processes.

According to Quader (2021), these types of attacks are among the most dangerous.

According to Ussath *et al*. (2016), traditional attack detection methods are not applicable to APTs. It' s necessary to create a new methodology.

According to Chandra *et al*. (2016), APTs are undetectable by their own nature and nowadays they have increased their sophistication exponentially. It is necessary to create multifaceted approaches to deal with the problem.

According to Min *et al*. (2017), APTs are difficult to detect and cause huge losses of information, new techniques are required to address the problem.

According to Zhang *et al*. (2017), APT attacks are different from traditional Cyber Security attacks and present enormous challenges.

According to Yang *et al*. (2018a), compared to traditional malware APTs do not intend to cause destruction on systems but to steal data. Therefore, they must be undetectable. Thus, traditional detection systems are not the current solutions to solve this type of threat and other more integrative and original solutions need to be developed.

According to Yang *et al*. (2018b), APTs always manage to avoid traditional Cyber Security defenses.

According to Khosravi-farmad *et al*. (2018), one of the greatest challenges for large computer networks is fighting back against the new challenges presented by APTs. This type of attack, according to this author, cannot be prevented by traditional mechanisms, including technological ones, of Cyber Security defense. Other approaches are required.

According to Yan *et al*. (2019), APTs are currently considered the most sophisticated cybercrime weapons that exist.

According to Joloudari *et al*. (2020), APTs use a diversified set of methods, simultaneously, so defense must also constitute an integrated set of defense methods, not exclusively a technology-centric one. Current solutions do not detect APTs in their early stage.

According to Zou (2020), it' s extremely difficult to trace APTs with currently existing solutions.

According to Tankard (2011), APTs are not detectable in their early stage, one of the solutions is to develop a solution consisting of several differentiated elements that added together can cover all the characteristics of APTs.

According to Auty (2015), a change in mindset is needed to come up with a solution to APT-type attacks.

According to Cheng *et al*. (2020), APTs are a specific class of multi-attacks different from traditional attacks and as such the traditional methods now in place do not solve this type of problem. They are undetectable by conventional technological means as they use "zero-days" technology.

According to Cheng *et al*. (2020), even in IoT it is difficult to manage detecting APTs with conventional mechanisms.

According to Chen *et al*. (2018), APTs cause too much damage before they can be detected, when they are detected. Current Cyber Security mechanisms are a very far from being able to solve the problem.

According to Lv *et al*. (2019), conventional Cyber Security defenses do not work with APTs.

According to Friedberg *et al*. (2015), current Cyber Security attack protection mechanisms are insufficient for APT-type attacks.

According to Berrada *et al*. (2020), traditional security systems do not solve the problem of APTs, they are among current undetectable systems.

According to Ghafir *et al*. (2018), as APTs are directly linked to Cyber espionage the goal is to steal data, so they are equipped with mechanisms that make it impossible to be detected by conventional methods.

According to Prenosil (2014), APTs are an issue for current detection systems, it's not possible to come up with a solution that goes exclusively through technology, it has to be an integrated set of several solutions.

According to one of the world's leading experts on Advanced Persistent Threats (APTs), (Cole, 2012), an author recognized as such by the entire scientific community, APTs are a completely different issue from all others. APT breaks all the rules of attackers, usually adapting its techniques to files, targeting users as an entry point and hiding its trail very carefully; therefore, many traditional security measures are not effective in dealing with this threat. Unfortunately, many companies fail to understand all their exposure points and if the offense is always much more sophisticated than the defense, we will usually lose. Moreover, it' s quite persistent. The main reason for APT's success is that it' s a new threat that many organizations are not prepared to deal with. Because each APT attack is unique and different, there are many variations and thus hard to identify. APT is a cybernetic cancer. There is no visible sign of a problem until the impact is so severe for an organization. APT is a completely different issue from the ones most organizations are used to dealing with. According to the author we need a new way to approach the issue. Still according to the author, there is no single solution to protect ourselves from APTs (Cole, 2012).

In late 2020, Microsoft reported that it was the subject of one of the largest ATO-type attacks, from Russia. 41 This is one of the largest software companies in the world, which invests millions of dollars a year in security, yet I could not detect the attack. The attack was carried out by writing lines of code in an update to the third-party Solar Winds security software that Microsoft uses. When an update was made to that software all Microsoft systems became infected. The main problem, however, is that Microsoft was unable to detect the attack. The attack was detected by a third company, FireEye, which detected anomalies in the Solar Winds software and after investigating these anomalies concluded that it was a malicious change to the code and then warned all customers using that software, including Microsoft (itnews, 2021).

From the literature review the major conclusion that can be drawn without much doubt is that everyone considers APS to be the most serious of all Cyber Security risks, that this type of attack can get through the traditional defenses and that it has a high degree of sophistication. These factors lead us to conclude with a relatively high degree of certainty that a large portion of TPAs are orchestrated by government entities or large global corporations.

Within this context it is extraordinarily important to have mechanisms to try to know to whom the actual authorship of the attack can be attributed (not who operated it, but who ordered it).

According Rid and Buchanan (2015), the MICTIC model focuses exclusively on technical issues and should also focus on issues of a political nature and human actions.

According Fraser *et al*. (2019), the analysis made by the MICTIC Framework should be more refined, including the investigation of different activities on the social networks of hypothetical authors or sponsors of the attacks.

Typical Phases of an APT Attack

APT attacks usually have a pattern (in fact the only pattern they possibly have) in terms of execution phases.

First phase or recognition phase: Gathering information on the target, looking for specific areas that can be focused on to achieve a long-term commitment with the minimum amount of energy or effort. This usually involves finding an individual who can be targeted for use in phase two.

Second phase or initial intrusion phase: Determine and find some way into the organization to establish an internal attack position. This usually does not require exploitation and is most commonly accomplished by convincing a user to open an attachment or click on a link that should not be opened on the computer within the network.

Third phase or backdoor creation phase: Theoretically, the APT is intended to be able to communicate with the target network. After the initial intrusion has been executed and implemented, a remote way in is established so that the attacker can continue to move around the compromised network and usually in a lateral manner.

Fourth phase or credential acquisition phase: An attacker aims to control the entire network and keep long-term access for current and future use. This usually requires obtaining, cracking or hijacking administrator credentials and the related administration privileges.

Fifth phase or utility installation phase: At this point, the attacker wants to establish persistence and full control of the network. This is usually achieved by installing tools to create a complete command and control communication with the compromised network.

Sixth phase or data exfiltration phase: The final step is to steal and extract the critical information from the network in a stealthy way. This is usually done by enrolling and masking data to make it look like legitimate traffic (Cole, 2012).

Seventh phase or trail clearing phase: The last phase is to fully clear the attack trail of the entire system. Make sure no one finds anything related to the attack.

The Authorship Attribution Process

The assignment can be performed at various levels of granularity. The step of assigning attacks to a group is very easily done if threat intelligence is available. Even if data is not provided in the normal way. The level of granularity of attribution is much more complex and is usually not performed by the security teams of an affected company, but by intelligence analysts or security firms. A single attack usually does not provide enough data for the analysis effort. Another level of attribution is routinely performed by analysts and covers the question of whether an attack is state-sponsored or criminally motivated (Hartley, 2014).

The most advanced level of attribution is the identification of specific organizations and individuals. This is only possible in rare cases, as in the case of Chinese PLA officers who were convicted of computer espionage in a US court. They were found guilty of hacking networks and stealing trade secrets as part of an APT1 group (USDJ, 2014).

The names obtained by the various security companies are totally inaccurate with regard to the assignment, as can be seen from Table 1. Of all the attacks listed, it was not possible to clearly assign the one responsible for the attack. Which demonstrates the difficulty in terms of traditional techniques to obtain more objective data. This is also one of the reasons why we propose the addition of two more layers to the MITIC Framework, that is, to strongly consider the aspect of the human actor.

Table 1: Examples of the difficult to make the correct Attribution by only names (Wang *et al*., 2014)

Kaspersky	CrowdStrike	FireEye	Symantec
Unknown	Commentpanda	APT1	Comment Crew
MSUpdater	PutterPanda	APT2	Junebug
Unknown	GothicPanda	APT3	Buckeye
Sykipot	Maverick	APT4	Hornet
Sofacy	FrancyBear	APT28	Sofacy
Turla	VenomousBear	Snake	Epic
Newscaster	CharmingKitten	Newsbeef	Unknown
CloudAtlas	Unknown	Unknown	Inception
RedOctober	Unknown	Unknown	Ricra
Project Sauron	Unknown	Unknown	Strider

Table 2: MICTIC Framework (Haq and Gomez, 2013)

	Aspect	Example Evidence
_M	Malware	e.g., language settings, timestamps, strings
_I	Infrastructure	e.g., WHOIS data, links to private websites
_C	Control Server	e.g., source code or logs on seized hard drives
_T	Telemetry	e.g., working hours, source IPs, malware generation
_I	Intelligence	e.g., intercepted communication
_C	Cui bono	Geopolitical analysis of strategic motivation

Table 3: Extension of the MICTIC Framework to MICTICSI Framework

	Aspect	Example Evidence
_M	Malware	e.g., language settings, timestamps, strings
_I	Infrastructure	e.g., WHOIS data, links to private websites
_C	Control Server	e.g., source code or logs on seized hard drives
_T	Telemetry	e.g., working hours, source IPs, malware generation
_I	Intelligence	e.g., intercepted communication
_C	Cui bono	Geopolitical analysis of strategic motivation
_S	Social Engineering	Behavioral analysis through data leakage or patterns
_I	Internal Leaks	Analysis of data obtained from internal collaborators

Allocation Phase

Phase One: The first step is to access and analyze something that the IT department has or knows about. Nowadays the standard is to buy an Anti-Virus or an anti-malware program and gradually update it to adapt it to the new dangers. In the process the companies that provide these products collect huge amounts of malware and cybercrime artifacts that they share and eventually come to the attention of IT departments. The actual Anti-Viruses act as sensors and send information to the companies that produced them. This data after being treated and structured can be one of the starting points to achieve an attribution process, not exclusively, but in correlation with other data. In many cases customers are also the ones who inform security companies of the existence of an APT, this information is or should be shared.

Phase Two: Regardless of how the data about APT malware and attacks was found, the next step of the assignment is to divide the data into intrusion sets. At first, attacks, malware and control servers are just unconnected data points stored in customer databases and reports. In order to refine the intrusion sets, the analyst collected all malware samples discovered on the affected customers' systems. One example is the concrete manifestation of malicious artifact in the form of a file.

Phase Three: The nature of the stolen data was clearly favorable to the latter, since it was not easily monetizable information, such as credit card data in online banking credentials. The gigantic scale of Hacking activity can be indicative of the fact that a government is behind the attack, so the scale of the attack and its complexity are also key indicators for attribution.

Phase Four: State-sponsored activity requires identifying the country from which the attackers work - thus linking the attack to a specific government. The perpetrators do not connect their own computers directly to the victim's networks, but instead use hacked servers from uninvolved third parties or rented anonymous servers as jump servers. They often move from one of these servers to the other before connecting to the control servers.

Phase Five: Is one of the most complex because it is about establishing relationships between the organizations that have been involved. As well as their public identification. It was achieved through many processes including the correlation of traces and signatures of technologies from previous attacks and the artifacts used in the attack under study, there can always be patterns, humans are programmed to act by patterns and hackers are not outside this rule, often unconsciously use the same patterns both technological and behavioral and this can serve to establish a correlation.

Phase Six: The last phase of the assignment is the presentation and communication of the results. As a rule, these are hypotheses and probabilities, in APTs we never work with absolute certainties. However, the hypotheses and probabilities have to be consistent and based on strong evidence. The language to be used should always be "probably impossible", "unlikely", "probable", "almost certain", with regard to a theory terms should be used to describe its degree of certainty: "Low", "medium", "high", "very high".

Investigation: An Extension to MICTIC Framework

The issue of attribution is being taken very seriously by large companies, non-governmental organizations, government agencies, yet there is no real Framework that implements Attribution. Obviously, many government agencies and companies will have action templates and even Frameworks, yet they don't publicize them or share them with the academic community.

We are familiar with the Q Model by (Rid and Buchanan, 2015), these authors focus on policy issues related to Attribution and the impact they can have on the public, they rarely address the techniques for achieving Attribution itself.

Steffens (2020), proposes a Framework for Assignment called MICTIC (Table 2), our research has led to an extension of this Framework and is presented here, the intent is to improve complementarily the initial Framework, the Assignment process.

Cyber espionage always has several aspects and in order to analyze Attribution, this set of aspects must be understood and analyzed. These aspects are not phases, as (Steffens, 2020) states, but rather isolated yet coherent artifacts, as well as activities correlated with these artifacts.

The acronym used by Steffens (2020), MICTIC, is derived from the following terms: _Malware, _ Infrastructure, _Control Servers, _Telemetry, _ Intelligence in _Cui Bono. Each of these items represents a source or type

of data to be used in the Assignment, you can also analyze these divisions through subgroups of analysis.

Let's have a look at the meaning of each of the artifacts, _Malware, encompasses anything to do with back doors, Trojans, viruses, exploit software, etc. In other words, these are artifacts that are the responsibility of programmers and software engineers; _Infrastructure, are related to appropriation, use of server platforms where the malware is going to be deposited, there are members specifically for these tasks; _Control Sever, are very specific individual servers from which there is the ability to manage certain tasks, this is possible through appropriation of privileges; _Telemetry, data on the activities of operators within a victim network, which security companies can analyze; _ Intelligence, additional resource coming from knowledge obtained from government agencies; _Cui Bono, these are tasks related to the attack but not from the technical group.

We now propose an extension to this Framework to make it more robust and more comprehensive. The APTs, practically the entire scientific community agrees on this (having been proven in the bibliography study) cannot be understood and analyzed solely and tendentially from the technological perspective, there is another fundamental component to understand them, unlike the traditional attacks that can usually be analyzed with technology. APTs elude conventional analysis, the border has to have components that accommodate these non-technological analysis needs.

It is in this perspective that it is proposed to add two more layers to the MICTIC Framework and to extend it under the name MICTICSI (Table 3).

Justification for the Inclusion of these two New Artifacts

Social Engineering is the ability to gain access to confidential information or important areas of an institution or group of people through persuasion skills. In opposition to the mysticism attributed to the technique, it' s not required to use any technological equipment to perform this activity. An analysis in this context can be started with small pieces of data. Self-confidence, ease of communication, professional aptitude and great persuasive ability are characteristics of a social engineer. Many attacks victims claim that they hardly know they passed on information they shouldn't have because of the talent of the person they talked to and this case is not as unlikely as we think. Now, it is possible that the attackers use these techniques, so after the attack all those who were (hypothetically) in contact (physical or non-physical) with the attackers should be surveyed. The obtained data can be crucial for Identification and Attribution. It' s about using one of the attacker's own techniques against them.

In terms of insider data leaking, the problem has never been as serious as it is today, it's cheaper to corrupt a company employee to attack the company than to develop technological processes to attack it exclusively from the outside.

Therefore, this factor is relevant nowadays, in the Attribution processes, the company must be scoured to find side information on the APT attackers and try to find out by all means who collaborated and what these employees know about the attackers.

Thus, the extension of the MICTIC Framework is justified, as it now encompasses new non-technological techniques consequent to the unique characteristics of APS itself.

The type of attacks that we are referring to, that is, the Advanced Persistent Threats (APT), usually have a truly robust and sophisticated typology and as we have already mentioned, they can easily bypass conventional security defenses, in practice defenses of the type security systems. intrusion and protection or endpoints cannot achieve the desired effect TEC, 2019.

Recent studies agree that the approach must be different and broader (Virvillis, 2014). Research must also move to the area of social networks and social engineering (Micro, 2014).

Jasek *et al*. (2013) suggest, for example, the use of a new concept, Social Honey Pots, to detect APT-related activities and sources of attribution.

Recent research (Kemp, 2017) indicates that about 74% of users are online and about 92% of those who may be connected to APT may also be online ISAC, 2013. Thus, the information obtained from social networks, all of them, can provide important information about those responsible for certain attacks (Ahmad, 2015). Especially because APT attacks that in their initial phase also use social networks, to build networks and trust, have a digital footprint on the Internet and these footprints must all be analyzed.

Obviously, social engineering through its tools plays an important role here.

Methodologies and Tools for Applying the Extension

Attribution is the task by means of which a researcher tries to obtain more information about an actor or sponsor of an APT who carries out a certain action in cyberspace. The very changing nature of the evidence obtained on the web makes this work a complex activity that forces the analyst to work in a manipulable and changing scenario. For this reason, it is necessary to know the limits that we must face when evaluating the evidence obtained during an investigation with ramifications in cyberspace.

The proposal to create two more layers in the MICTIC Framework, has as main objective to complement the same, introducing a new paradigm in the model. It is intended to introduce the human factor in a more objective and more intensified way, in technical language we can say that we must use tools that are currently used by cyber espionage. this is because a large part of the APT are in the context of cyber war and cyber espionage, so the tools

to be used for the Attribution must be identical tools or of the same typology as those used by cyber spies or spy or security agencies and intelligence.

Thus, in this topic we present a set of tools that can be used in the context of the two additional layers proposed for the MICTIC model, however what is proposed is not invalid that other tools can or should be used.

OSRFramework

It is a package of applications for obtaining information in open sources programmed in Python and distributed under the AGPLv3 license. The set of integrated applications includes tools to facilitate the research process in open sources to facilitate the identification of users in the network.

Its main characteristic is the ability to search for users in more than 200 different platforms that speed up the collection activities and could serve as a starting point for the identification of information related to the investigated or even for carrying out targeted attacks depending on the sensitivity of the person. exposed information (Rubio, 2020).

This suite has five main tools. The USUFY, this tool makes requests to different platforms present in the network for a specific username and will try to identify the text that indicates the NO presence of the user in said network: A 404, an image, a message of "the user does not exists", etc. The alias_generator, in certain situations, may not have a specific alias as only some data of the profile under study is available. For these cases, a script has been configured that generates a list of possible aliases from the information provided by the user and using a series of transformations already observed in the past by the authors as common practices for the generation of new aliases. This application has several utilities to modify the generated aliases. MAILFY, allows us to investigate an email, performs different verifications: Identify if the email exists; if the mail has been used to register accounts; It was used in key servers; attempts to use the HaveIBBeenPwned payment API to detect security breaches; uses the DeHashed platform to identify email leaks; uses the reverse lookup of ViewDNS.info to identify domains registered with that email (Neekman, 2019). The SEARCHFY, with this tool you can make inquiries against the search services of users of different platforms. This functionality extends the capacity of usufy by allowing the existence of profiles in different search engines to be brought together under the same query. In this case, instead of searching by username, broader searches can be made using names and names or whatever term is considered relevant. The DOMAINFY, is a tool that has also evolved a lot over time. With its default behavior, it allows identifying main domains that resolve using a nickname or brand. PHONEFY, allows to identify possible cases of telephone spam associated with a telephone number using the application. CHECKFY, in case we have evidence of an email pattern, we could try to find out the email that hides behind by relying on a list of aliases generated by alias_generator.

Tinfoleak

It is an open source tool that automates the extraction of information from and facilitates its subsequent analysis for the generation of intelligence. It is included in multiple security-oriented Linux distributions: Kali Linux, CAINE, BlackArch, but it can also be downloaded directly from the official website. Metadata analysis face: Metadata associated with the profile photos or images published by users is shown (https://www.isecauditors.com/herramientas-tinfoleak).

Recon-ng

It is a web recognition framework written in Python. Its main features include independent modules, database interaction, construction with comfortable functions, interactive help and command completion. It looks like the Metasploit Framework.

TheHarvester

It is an application in Python and released with a GLP 2.0 license that facilitates the identification of corporate accounts and subdomains thanks to the different wrappers it has for different search engines. The installation process can be carried out using Git against the official repository itself and solving the necessary dependencies.

Maltego

It is a tool distributed under a private license by Paterva oriented to the collection and visualization of information in a visual graphical interface. It works with the concept of transforms, which are small applications that perform specific tasks on the entities represented graphically. It is one of the most recognized tools in the field of Internet research to the point that the Community Edition has been included in distros such as Kali Linux.

Namechk

It has a similar approach to usufy, in a simple way we can check if a user is busy in certain social networks or domains on the Internet.

Socialbearing

It is a platform from which we can extract information about various networks in a simple way. However, the option to extract information about a user is the one that usually provides more context information.

Conclusion

The identification and Assignment process is extremely important, at all levels. Information on APTs is always very scarce and difficult to acquire. It's important

to develop technological and non-technological techniques to identify and attribute the origin of APTs. This function can sponsor the development of other techniques for the defense and mitigation of APTs, as we can begin to create patterns, patterns are the best weapon against APTs.

There are very few Frameworks, or very few known Frameworks, applicable to Attribution. One of them is MICTIC and we start from this and created an extension to it, making it more complete as well as more comprehensive. Allowing you to easily accomplish the assignment.

Acknowledgements

We are grateful for the support given to research by Prof. António Chaves Fidalgo and the Higher Institute of Advanced Technologies (ISTEC).

Ethics

This article is original and contains unpublished material. The author has read and approved the manuscript and no ethical issues are involved.

References

Adelaiye, O. I., Showole, A., & Faki, S. A. (2018). Evaluating Advanced Persistent Threats Mitigation Effects: A Review. International Journal of Information Security Science, 7(4), 159-171.

Ahmad, I. (2015). How Many Internet and Social media Users are fake? Infographic, 04.

Alkan, M. (2018). A Study on Advanced Persistent Threat. 3rd International Conference on Computer Science and Engineering. https://www.researchgate.net/publication/329612289_A_Study_on_Advanced_Persistent_Threat

Auty, M. (2015). Anatomy of a advanced persistent threat, Network Security. https://www.researchgate.net/publication/275219292_Anatomy_of_an_advanced_persistent_threat

Berrada, G., Cheney, J., Benabderrahmane, S., Maxwell, W., Mookherjee, H., Theriault, A., & Wright, R. (2020). A baseline for unsupervised advanced persistent threat detection in system-level provenance. Future Generation Computer Systems, 108, 401-413. https://doi.org/10.1016/j.future.2020.02.015

Chandra, J. V., Challa, N., & Pasupuleti, S. K. (2016, March). Advanced persistent threat defense system using self-destructive mechanism for cloud security. In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 7-11). IEEE. https://ieeexplore.ieee.org/abstract/document/7569181

Chen, J., Su, C., Yeh, K. H., & Yung, M. (2018). Special issue on advanced persistent threat. https://doi.org/10.1016/j.future.2017.11.005

Chen, W., Helu, X., Jin, C., Zhang, M., Lu, H., Sun, Y., & Tian, Z. (2020). Advanced persistent threat organization identification based on software gene of malware. Transactions on Emerging Telecommunications Technologies, 31(12), e3884.

Cheng, X., Zhang, J., Tu, Y., & Chen, B. (2020). Cyber situation perception for Internet of Things systems based on zero-day attack activities recognition within advanced persistent threat. Concurrency and Computation: Practice and Experience, e6001.

Cole, E. (2012). Advanced persistent threat: understanding the danger and how to protect your organization. Newnes. ISBN-10: 1597499552

De Vries, J. A. (2012). Towards a roadmap for development of intelligent data analysis based cyber attack detection systems. https://repository.tudelft.nl/islandora/object/uuid:090446d3-7562-41ce-94d3-ab7153cd05d5

Fraser, N., Plan, F., OLeary, J., Cannon, V., Leong, R., Perez, D., & Shen, C. (2019). APT41—A dual espionage and cyber crime operation. FireEye Blog.

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security, 48, 35-57.

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: an overview. International Journal Advance Computer Network Security, 4(4), 5054. https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview

Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359. https://doi.org/10.1016/j.future.2018.06.055

Haq, T., & Gomez, J. (2013). LadyBoyle Comes to Town with a New Exploit. FireEye Blog.

Hartley, N. (2014). Hat-tribution to PLA Unit 61486. CROWDTSRIKE Blog, June, 9, 2. https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/

itnews. (2021). Microsoft breached in suspected Russian hack using SolarWinds.

Jasek, R. O. M. A. N., Kolarik, M. A. R. T. I. N., & Vymola, T. O. M. A. S. (2013, August). APT detection system using honeypots. In Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press (pp. 25-29). http://www.wseas.us/e-library/conferences/2013/Valencia/ACIC/ACIC-02.pdf

Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137. https://ieeexplore.ieee.org/abstract/document/9214817

Kemp, S. (2017). Digital in 2017: Global overview. https://wearesocial.com/special-reports/digital-in-2017-global-overview

Khan, M. (2020). "Advanced Persistent Threat: Detection and Defence", University of Bradford, 2020. https://www.researchgate.net/publication/340859787_Advanced_Persistent_Threat_Detection_and_Defence

Khosravi-Farmad, M., Ramaki, A. A., & Bafghi, A. G. (2018, October). Moving Target Defense Against Advanced Persistent Threats for Cybersecurity Enhancement. In 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE) (pp. 280-285). IEEE. https://ieeexplore.ieee.org/abstract/document/8566531

Levine, C. (2013). Conceptualizing financial loses as a result of advanced persistent threats. https://digitalcommons.pace.edu/honorscollege_theses/122/

Li, P., Yang, X., Xiong, Q., Wen, J., & Tang, Y. Y. (2018). Defending against the advanced persistent threat: An optimal control approach. Security and Communication Networks, 2018. https://www.hindawi.com/journals/scn/2018/2975376/

Lima, A. J. C. (2015). Advanced persistent threats (Doctoral dissertation). https://repositorio.ul.pt/handle/10451/20168

Lv, K., Chen, Y., & Hu, C. (2019). Dynamic defense strategy against advanced persistent threat under heterogeneous networks. Information Fusion, 49, 216-226. https://doi.org/10.1016/j.inffus.2019.01.001

Micro, T. (2014). Custom Defense Against Targeted Attacks, TrendMicro.

Min, M., Xiao, L., Xie, C., Hajimirsadeghi, M., & Mandayam, N. B. (2017, May). Defense against advanced persistent threats: A Colonel Blotto game approach. In 2017 IEEE international conference on communications (ICC) (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/7997103

Mirza, N. A. S., Abbas, H., Khan, F. A., & Al Muhtadi, J. (2014, August). Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms. In 2014 International Symposium on Biometrics and Security Technologies (ISBAST) (pp. 129-132). IEEE. https://ieeexplore.ieee.org/abstract/document/7013108

Moon, D., Im, H., Lee, J. D., & Park, J. H. (2014). MLDS: multi-layer defense system for preventing advanced persistent threats. Symmetry, 6(4), 997-1010. https://www.mdpi.com/2073-8994/6/4/997

Mustafa, T. (2013, April). Malicious data leak prevention and purposeful evasion attacks: an approach to advanced persistent threat (APT) management. In 2013 Saudi International Electronics, Communications and Photonics Conference (pp. 1-5). IEEE. https://ieeexplore.ieee.org/abstract/document/6551028

Neekman, V. (2019). Python-emailnow3, POSIX. https://docs.python.org/3/library/posix.html

Prenosil, V. (2014). Advanced Persitent Threat Attack Detection: Na Overview, International Journal of Advancements in Computer Networks and Its Security, Vol. 4, Issue 4, 2014.

Quader, F. (2021). "Persistent Threat Pattern Discovery", Baltimore University.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37. https://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

Rubio, Y. (2020). OSRFramework, i3Visio, Madrid. https://github.com/i3visio/osrframework

Stalling, W. (2018). Computer Security, Pearson. l

Steffens, T. (2020). Attribution of Advanced Persistent Threats. Springer Berlin Heidelberg. https://link.springer.com/book/10.1007%2F978-3-662-61313-9

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network security, 2011(8), 16-19. https://doi.org/10.1016/S1353-4858(11)70086-1

USDJ. (2014) US charges five Chinese military hackers for cyber espionage against US Corporations and a Labor Organization for commercial Advantage. United States Department of Justice. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016, March). Advanced persistent threats: Behind the scenes. In 2016 Annual Conference on Information Science and Systems (CISS) (pp. 181-186). IEEE. https://ieeexplore.ieee.org/abstract/document/7460498

Virvilis, N., & Gritzalis, D. (2013, September). The big four-what we did wrong in advanced persistent threat detection?. In 2013 international conference on availability, reliability and security (pp. 248-254). IEEE. https://ieeexplore.ieee.org/abstract/document/6657248

Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013, December). Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing (pp. 396-403). IEEE. https://ieeexplore.ieee.org/abstract/document/6726235

Virvillis, B. (2014). Changing the game: The Art of Deceiving Attackers, in Proc. 6th Int. conf. IEEE, 2014. https://ieeexplore.ieee.org/abstract/document/6916397

Wagner, R., Fredrikson, M., & Garlan, D. (2017). An advanced persistent threat exemplar. Carnegie-mellon univ pittsburgh pa pittsburgh United States. https://apps.dtic.mil/sti/citations/AD1086847

Wang, Y., Wang, Y., Liu, J., & Huang, Z. (2014, November). A network gene-based framework for detecting advanced persistent threats. In 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 97-102). IEEE. https://ieeexplore.ieee.org/abstract/document/7024564

Wendt, J. D., Suppona, R. A., Wilson, A. T., & Doak, J. E. (2013). Can we identify spear phishing targets before the email is sent? (No. SAND2013-3821C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). https://www.osti.gov/servlets/purl/1115637

Yan, D., Liu, F., & Jia, K. (2019, May). Modeling an information-based advanced persistent threat attack on the internal network. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/8761077

Yang, L. X., Li, P., Yang, X., & Tang, Y. Y. (2018a). A risk management approach to defending against the advanced persistent threat. IEEE Transactions on Dependable and Secure Computing, 17(6), 1163-1172. https://ieeexplore.ieee.org/abstract/document/8417919

Yang, L. X., Li, P., Zhang, Y., Yang, X., Xiang, Y., & Zhou, W. (2018b). Effective repair strategy against advanced persistent threat: A differential game approach. IEEE Transactions on Information Forensics and Security, 14(7), 1713-1728. https://ieeexplore.ieee.org/abstract/document/8565986

Zhang, Q., Li, H., & Hu, J. (2017, July). A study on security framework against advanced persistent threat. In 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 128-131). IEEE. https://ieeexplore.ieee.org/abstract/document/8076527

Zou, Q. (2020). An Approach for Detection of Advanced Persistent Threat Attacks. Computer, IEEE Computer Society, 2020. https://www.researchgate.net/publication/347261373_An_Approach_for_Detection_of_Advanced_Persistent_Threat_Attacks