Original Research Paper

Advanced Persistent Threats Campaigns and Attribution

[1]Pedro Ramos Brandao, [2]Henrique Sao Mamede and [3]Miguel Correia

[1]Department of Computer Science, Instituto Superior de Tecnologias Avançadas-ISTEC, Portugal
[2]Department of Computer Science, Universidade Aberta, Lisbon, Portugal
[3]Department of Computer Science, Instituto Superiror Técnico, Lisbon, Portugal

Article history
Received: 16-10-2023
Revised: 28-01-2023
Accepted: 13-05-2023

Corresponding Author:
Pedro Ramos Brandao
Department of Computer Science, Instituto Superior de Tecnologias Avançadas-ISTEC, Portugal
Email: pb@pbrandao.net

Abstract: The main objective of this study is to carry out a systematic review of the literature regarding Advanced Persistent Threats (A.P.T.) and A.P.T. Campaigns. The work is focused on campaigns with geographical origin in China and for this reason, the main A.P.T. campaigns from that region are analyzed. All types of documentation were used for the systematic literature review, including gray literature, such as reports from official and government agencies. The Attribution is one of the most important parts of the APT problem, this study tries to demonstrate that it was possible to make the Attribution in relation to certain Groups in China, groups that attacked many western countries via APT. The problem to be solved is to Assign these Groups, that is, to know who are the authors of the APT. The scope of work is specifically the APT attacks and their possible origin in China.

Keywords: Advanced Persistent Threats, A.P.T., A.P.T. Attribution, A.P.T. Campaigns

Introduction

Computer systems have become an important part of our society; most of the information we use in our day-to-day lives is in digital format. Unlike a physical document, a digital document is exposed to a broader range of threats, especially if it is somehow available on the Internet. Information is power, so it's no wonder that someone, somewhere, is trying to steal it, so it's a fact that adversaries already operate in this new world. Thieves, terrorists, and even mafias have started using the Internet as a means to achieve their ends. Cybersecurity tries to protect information and systems against these and other types of threats using anti-virus, firewalls, or intrusion detectors, among others. Unfortunately, the news continues to come out, millions of euros stolen from banks via computer, companies looted of their intellectual property, and governments embarrassed by their secrets being exposed to the world. Questions arise: Why are security systems failing? How is the opponent overtaking them? The truth today is that attackers have acquired not only advanced talent in the area but also highly sophisticated tools and will use them to succeed in their goals. Although information theft and unavailability are the most common threats and, therefore, the most discussed, this study emphasizes attacks against critical infrastructures. Advanced Persistent Threat (A.P.T.); is a term used to characterize sophisticated, organized attackers with resources to carry out computer attacks. Invented by the U.S. Air Force in 2006, the term discussed computer intrusions with non-military personnel. In its origins, the word threat indicates that the adversary is not an automatic piece of code; that is, the adversary is human and it is this human who controls part of the attack and contributes to its success, advanced because this human is trained and specialized in the use of the entire computer spectrum to achieve its objective and persistent better, as this objective is formally defined, that is, the attack is only concluded when it reaches the target in full. Unfortunately, the term has come to be used to describe many computer attacks and to have an extremely commercial connotation with the “anti-APT systems” that invaded the market shortly after the attack suffered by Google in 2010.

A.P.T.s are today one of the most complex and most feared types of cyberattacks (Virvilis and Gritzalis, 2013). However, little scientific data is published about the attribution of this type of threat, i.e., about who sponsors and is behind these attacks, unlike surveys on hypothetical proposals for detecting them. The published material available on this subject is seen mainly from government agencies or companies dedicated to cybersecurity issues. This study reflects an

investigation that seeks to identify the source of A.P.T. attacks and campaigns and the possible attribution. The article is based on a systematic literature review on this issue, i.e., based on reports focused on A.P.T.s originating in China. Focusing on that country is merely a way of reducing the scope of the study while keeping it relevant.

There are few scientific articles about A.P.T. campaigns, but reports from credible entities explain the campaigns and their possible attribution. This article uses scientific papers and reports to explain a set of A.P.T. attack campaigns. However, we start by presenting A.P.T.s and the valences of the so-called gray literature and its importance for the study of A.P.T. campaigns. This study does not aim to express the personal opinions of the authors but to be factual, based on analyzing and describing what the consulted reports affirm or objectively expose.

Materials and Methods

Much of this study and the systematic literature review use Gray Literature (G.L.). i.e., documentation not formally published. This fact justifies that the methodology that we will present focuses on the system used for the gray literature that supports the entire research.

In the mid-2000s Systematic Mapping studies (S.M.) and Systematic Literature Reviews (S.L.R.) were adopted from the medical sciences and since then, only a few S.L.R. studies have been published in Software Engineering (S.E.) (Garousi *et al*., 2019; Higgins, 2017). S.L.R.s are valuable as they help researchers and practitioners index gaps and evidence in a specific research area, consisting of several hundred papers. Unfortunately, S.L.R.s are less valuable when they review only the formally published literature, excluding the large bodies of (G.L.) that S.E. professionals constantly produce outside academic forums. As S.E. is field application and practitioner-oriented, the role of the G.L. should be formally recognized, as was been done, for example, in educational health and research sciences and management (Garousi *et al*., 2019).

For the use of gray literature in this research paper, we used the model proposed by Garousi *et al*. (2019).

In the early 1990s S.L.R. which includes both academic and G.L. was referred to as Multivocal Literature Reviews (M.L.R.) in educational research (Garousi *et al*., 2019). The major difference between an S.L.R. and an M.L.R. is the fact that while S.L.R. uses only peer-reviewed academic articles as input, M.L.R.s also use G.L. sources, e.g., videos, blogs, web pages, and white papers, M.L.R. recognize the need for "multiple" voices rather than building evidence from only knowledge rigorously reported in academic settings (formal literature). An M.L.R. definition: Multivocal literature comprises all accessible texts on a common topic, which is often contemporary. The texts have incorporated the voices or opinions of diverse groups of authors (policy centers, practitioners, journalists, academics, state offices of education, independent research and development firms, state agencies, local school entities and etc. Texts are appearing in different forms, which reflect various perspectives, purposes, and information sources, which address various aspects of the topic and incorporate or not different research logics (Garousi *et al*., 2019).

Many S.L.R. guidelines and recommendations, e.g., Cochrane (Higgins, 2017), do not FORBID the inclusion of G.L. in S.L.R. studies. On the other hand, they recommend considering G.L. as long as the sources of G.L. meet the exclusion/ inclusion criteria (Garousi *et al*., 2018). Nevertheless, almost all S.L.R. articles in the S.E. domain exclude G.L. in S.L.R. studies. This situation sets back both scientific and academic research with a complete scope.

According to (Garousi *et al*., 2019), the justification for using gray literature in a scientific investigation can be validated by answering a set of questions, shown in Table 1.

In terms of systematic literature review (classical, peer-reviewed scientific sources), no sources related to A.P.T.s Attribution were found.

This fact, plus the results from the test performed, represented in the right-hand side of Table 1, justify the use of gray literature in this research paper.

Shades of Gray Literature

The Shades of the Gray model, shown in Fig. 1, is consistent with Table 2, offering the spectrum of white, gray, and black literature of possible sources. The 'white' literature is visible in both Fig. 1 and Table 2 and is characterized by the authority where both the experiment and the output control are fully known. According to Table 1, the gray literature corresponds for the most part to the 2nd tier in Fig. 1, with moderate credibility and output control. Hence, tier 1 is more credible. Black literature finally corresponds to ideas, concepts, and thoughts. Because blogs, tweets, and emails refer mainly to concepts, ideas, or beliefs, they are in the 3rd tier. However, there are even "shades" of gray in the classification. Depending on the factual content, a specific type of gray literature may be in a different tier than shown in Fig. 1. For instance, if a presentation (or a video usually linked to a presentation) is about new ideas, it would fall into the third tier (Garousi *et al*., 2019):

Tier 1 (High Creditability): Books, journals, government reports, white papers
Tier 2 (Moderate Credibility): Annual reports, news articles, presentations, videos, etc.
Tier 3 (Low Credibility): Blogs, emails, Tweets, etc.

In this study, we are already creating a first-quality screen, seeing the 1st tier according to the model of (Garousi *et al*., 2019), to consider the contents of this tier as High Credibility.

Table 1: Validation test for gray literature usability (Garousi *et al*., 2018)

#	Questions	Possible answers	M.L.R.-autotest
1	Is the issue "complex" and can't be solved by considering only the formal literature?	Yes/no	Yes
2	Is there a lack of volume or quality of evidence or consensus on outcome measurement in the formal literature?	Yes/no	Yes
3	Are contextual pieces of information necessary to the subject under study?	Yes/no	Yes
4	Is the goal to validate or corroborate scientific results with practical experiences?	Yes/no	Yes
5	Is the purpose of challenging assumptions or falsifying results from practice using academic research or vice versa?	Yes/no	Yes
6	Would synthesizing perceptions and evidence from the technical/scientific and academic communities be helpful to either or even both communities?	Yes/no	Yes
7	Is there a large volume of professional sources showing high interest in this research paper?	Yes/no	Yes

Table 2: Spectrum of "White," "Gray," and "Black" literature (Garousi *et al*., 2019)

White literature	Gray literature	Black literature
Papers published in peer-reviewed journals	Preprints	Ideas
	e-Prints	Concepts
		Thoughts
Conference proceedings		Technical reports
Books		Data sets
Classes		Video and Audio (A.V.) media
		Blogs

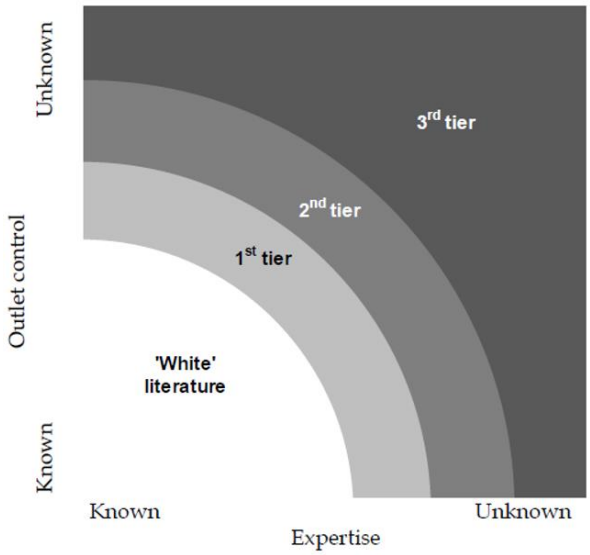

Fig. 1: Shades of grey literature (Garousi *et al*., 2018)

Source Quality Assessment

Assessing the quality of sources is about determining the extent to which a source is free of bias and valid. Contrary to formal literature, which usually is following a controlled review and publication process, the G.L. process is more diverse and with less control. In consequence, the quality of the G.L. is more varied and more often labor-intensive to assess. There are various models for evaluating the quality of G.L. sources. Some are only suitable for specific G.L. source types; for example, online comments exist only for open-source types for comments such as news articles, blog posts, or videos. Popularity can indicate a highly commented blog post, although, on the other hand, spam comments could skew the number of comments, therefore invalidating high popularity (Garousi *et al*., 2019). To present a synthesized approach to the quality evaluation of G.L. sources, we use a model in which one of our checklist criteria has strengths and weaknesses.

In theory for source selection, you can also use any item on the quality assessment checklist. For example, the publication date, methodology, or the number of backlinks could possibly be used as one of the selections of criteria. The advantage of this is that more sources can be excluded with a high degree of certainty. Based on a set of criteria, much less effort is required, therefore more time-consuming evaluation of study quality. In addition, using the "research method" as a set of criteria in a specific source, for example, a survey, case study, or experiment, allows for further evaluation of the quality of the research study (rigor). To investigate specific study types' quality (rigor) in detail, tailor-made checklists for specific study types are also possible in this template. Thus, we conceptually use the model provided in Table 3. The use of this model can be seen in Table 5 (which uses the elements listed in Table 4), where some of the selected papers are exemplified. Only papers whose normalization was higher than 0.5 were accepted; however, as there had been other previous quality filtering, in this quality check model, almost all papers tended towards a rating of 1 (Garousi *et al*., 2019).

Table 3: Gray literature quality assessment checklist (Garousi *et al*., 2019)

Criteria	Questions
Producer's authority	Is the publishing organization respectable? For instance, the Software Engineering Institute (S.E.I.)
	Is an individual author associated with a respectable organization?
	Has the author published other work in the field?
	Does the author have experience in the field? (e.g., principal software engineer of the job)
Methodology	Does the source have a clearly defined goal?
	Does the source have a stated methodology?
	Do authorized contemporary references support the source?
	Are there clearly defined limits?
	Does the work cover a specific issue?
	Does the work refer to a particular population or case?
	Does the work seem to be balanced in a presentation?
Objectivity	Is the statement in the sources as objective as possible?? Or is the statement a subjective opinion?
	Is there acquired interest? For instance, a tool comparison made by authors working for a specific tool vendor
	Do data support the conclusions?
Data	Is the item dated?
W.R.T.'s position compared to other sources	Was the related G.L. or formal sources linked/discussed?
Novelty	Does it enrich or add something unique to the research?
	Does it strengthen or refute a current position?
Impact	To normalize all of the following impact metrics into a single aggregate impact metric (whenever data is available): Number of citations, backlinks, social media shares, comments posted for a specific online entry such as a video or a blog post, number of paper or page views
Output template	1st G.L. tier (measure = 1): High output control / High credibility: Books, journals, theses, government reports, white papers
	2nd G.L. tier (measure = 0.5): Moderate output control / moderate credibility: News articles, annual reports, presentations, Q&A sites, videos (like StackOverflow), Wiki articles
	3rd G.L. level (measure = 0): Low output control / Low credibility: Blogs, emails, tweets

Table 4: Five G.L. sources randomly selected from the set of articles that were subjected to the MLR-autotest (Garousi *et al*., 2019)

I.D.	Reference
GL1	WikiLeaks, what did Equation do wrong, and how can we avoid doing the same? 2021
GL2	T. Weiner, The History of the C.I.A.: The 13th five-year plan for economic and social development of the People's Republic of China, National Development and Reform Commission (N.D.R.C.), 2010
GL3	N. Villeneuve, Investigating a Cyber Espionage Network, 2021
GL4	Timberg, C., Nakashima, E., Chinese hackers suspected in attack on The Post's computers, The Washington Post, 2021
GL5	The United States Department of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S Defense Contractors' Systems to Steal Sensitive Military Information, 2021

Table 5: Application example of the quality assessment checklist (Garousi *et al*., 2019)

Criteria	Questions	Examp. G.L. Source GL1
Producer's authority	Is the publishing organization respectable? For instance, the Software Engineering Institute (S.E.I.)	1
	Is an individual author associated with a respectable organization?	1
	Has the author published other work in the field?	1
	Does the author have experience in the field? (e.g., principal software engineer of the job)	1
Methodology	Does the source have a clearly defined goal?	1
	Does the source have a stated methodology?	1
	Do authorized contemporary references support the source?	1
	Are there clearly defined limits?	1
	Does the work cover a specific issue?	1
	Does the work refer to a particular population or case?	1
Objectivity	Does the work seem to be balanced in the presentation?	1
	Is the statement in the sources as objective as possible?? Or is the statement a subjective opinion?	1
	Is there acquired interest? For instance, a tool comparison made by authors working for a specific tool vendor	1
	Do data support the conclusions?	1
Data	Is the item dated?	1
W.R.T.'s position compared to other sources	Were the related G.L. or formal sources linked/discussed?	1
Novelty	Does it enrich or add something unique to the research?	1

Table 5: Continues

	Does it strengthen or refute a current position?	1
Impact	Normalize all of the following impact metrics into a single aggregate impact metric (when data is available): Number of citations, number of backlinks, number of social media shares, number of comments posted for a specific online entry such as a blog post or a video, number of page or paper views	1
Output template	1st G.L. tier (measure = 1): High output control / High credibility: Books, journals, theses, government reports, white papers	
	2nd G.L. tier (measure = 0.5): Moderate output control/moderate credibility: Annual reports, news articles, presentations, videos, Q and A sites (like StackOverflow), Wiki articles	1
	3rd G.L. level (measure = 0): Low output control / Low credibility: Blogs, emails, tweets	
Sum (of 20):		20
Normalization (0-1)		1 (*)

Advanced Persistent Threats (A.P.T.)

In 2006, United States Air Force (U.S.A.F.) analysts used the term Advanced Persistent Threat (A.P.T.) to facilitate the discussion of intrusive activities (Jeun *et al.*, 2012) with civilian entities. In this regard, military teams were able to discuss the characteristics of the attack without revealing their confidential identities. The components of the terminology, which are defined by the U.S.A.F. are these:

- Advanced: The enemy, which is familiar with intrusion techniques and tools, is capable of developing custom exploits
- Persistent: The enemy, which intends to fulfill a purpose, takes orders and attacks only specific goals
- Threat: The enemy, which is coordinated, motivated, and supported

A.P.T. attackers have goals and purposes which are different from ordinary cyber criminals because of their targeted nature. For example, espionage in various sectors, such as military and industrial property, technical, economic, financial, intellectual extortion, and political manipulation.

The authors Garousi *et al.* (2019) have summarized the differences between A.P.T. attacks and traditional threats. The characteristics considered are purpose, target, invader, and approach (Tables 6-7) (Chen *et al.*, 2014a).

A.P.T.s pose a real threat to private and public entities worldwide and will continue in the future (Müller, 2019). They are the biggest threat to those, whose main problem is the difficulty of early detection as attackers use various techniques to evade efficiently and stay as long as possible undetected. The differences between an A.P.T. and an ordinary cyberattack are significant. For example, the number of resources of all kinds needed to carry out the attack. A typical cyberattack can be directed toward entities or organizations with poor or no cybersecurity defenses.

The policies to steal data from customers or a company's financial activities (Chen *et al.*, 2014a). Those attacks are usually detected and the damage made is not so critical. Never less, an A.P.T. can focus on large industry sectors and organizations, causing great damage, such as theft of intellectual property, destruction of critical infrastructure, and failure of essential services. These attacks mostly go undetected and their caused damage can be vital. In last years, the quantity of reported cases of A.P.T. has increased (Garousi *et al.*, 2018; Jeun *et al.*, 2012) remarkably; one of the main goals of A.P.T. attackers is to remain undetected as long as possible.

One example of A.P.T. scope is for players to take advantage of existing issues that generate interest in the population. For example, the COVID-19 pandemic was a scenario for players to launch their attacks. In such cases, the bait has been advisory information about the health situation in various countries. Techniques like exploitation of remote access tools, spear-phishing, and ransomware have been widely used (T.I.T.M.L, 2020).

An A.P.T. is a targeted attack that gains unauthorized access to information and communication systems to exfiltrate confidential data or cause damage to a company, industry, or government organization (Jeun *et al.*, 2012; Chen *et al.*, 2014). Since the rise of Stuxnet (Falliere *et al.*, 2011), A.P.T.s have become more cautious and damaging, showing how easy it is to intrude into high-level systems, bypassing many of the more sophisticated defense tools used to protect the computing environment. Currently, many of these threats remain undetected. Many of them, once detected, reappear with modifications to achieve their goals. Examples are FIN6 APT10 (Pricewaterhouse, 2017) and APT41 (Fraser *et al.*, 2019) were attacks that caused significant money, confidential information, and intellectual property losses.

Table 6: Characteristics of an A.P.T. attack (Chen *et al*., 2014a)

Characteristic	A.P.T. Attacks
Definition	An A.P.T. is a sophisticated, targeted, and highly organized attack. (e.g., Stuxnet)
Attack	Government and organized crime players groups
Target	Diplomatic organizations, the information technology industry, and other sectors
Purpose	Filter sensitive data or cause damage to a specific target
Attack lifecycle	Keeps persistence possible using different mechanisms

Table 7: Characteristics of a typical malware attack (Chen *et al*., 2014a)

Characteristic	Common malware attacks
Definition	Malware is malicious software used to attack and disable any system. (e.g., ransomware)
Attacker	A cracker, i.e., (a hacker involved in illegal activities)
Target	Personal or business computers
Purpose	Personal Recognition
The attack lifecycle	Ends whenever detected by the security systems

A.P.T. Attack Processes

An A.P.T. is characterized by its approaches: Each A.P.T. campaign is different and all attacks are customized to the specific victim organization. Usually, the first step is to create a point to gain access to the user's network (Virvilis and Gritzalis, 2013). Next, the custom malware establishes a communication channel to maintain that access, allowing attackers to inject malicious code numerous times. Such malware moves laterally; the system (stealthily) detects vulnerabilities that it could exploit and infect other hosts on the same network. It as well duplicates itself to maintain persistence in the system. Eventually, A.P.T. malware is able to establish other outbound connections as it gets access to the system and obtains as much data as possible.

An example of a life cycle approach was described in FireEye's research on APT1. The cycle consists of eight stages: (1) Initial recognition; (2) Initial commitment; (3) Establishing support position; (4) Privileges with escalation; (5) Internal recognition; (6) Moving laterally; (7) Maintaining a presence and (8) Mission complete. The Stages between (3) and (8) Do not have to occur in this order; the order can be changed depending on the type of network of the target to attack (Mandiant, 2013). This report is quite relevant because it describes these types of threats in detail.

As A.P.T. campaigns are discovered, we observe that their anatomy is diverse and changes according to the specific purpose for which it was designed. The diversification of the attack into several vectors makes detecting these threats a complicated task.

A.P.T.s use various sophisticated methods and techniques, as noted above. The attack starts with a scan of the victim (most of the time a non-technological process); in most cases, emails or spear-phishing are used in conjunction with social engineering to help the victim download the infected file. Then the attacker compromises the computer and gets access to other computers within the same organization through the network (Mandiant, 2013).

The methods which characterize the more advanced A.P.T. groups use zero-day exploits (exploits against publicly disclosed vulnerabilities) and previously unidentified and unknown infection vectors. These methods can involve various governments and organizations in multiple countries to successfully steal confidential information for a long time undetected (Mandiant, 2013).

Depending on the attacker’s target, the techniques mainly used to carry out an A.P.T. attack are combined or adapted. Some examples of these techniques can be the following:

- Social engineering: Making a legitimate user compromise information system. Such technique targets people who have privileged access, manipulating them to disclose personal information to execute a malicious attack through persuasion and control rather than through random attacks involved in systems (Krombholz *et al*., 2015)
- Spear-phishing: A phishing campaign that primarily targets a specific organization to collect its user's credentials and financial or other sensitive data (Aleroud and Zhou, 2017)
- Watering hole: It resembles spear-phishing in cyber espionage. The attacks are tailored to the characteristics of the victims. To do this, attackers try to obtain information on the victim by considering the victim's interests (Symantec, 2019)
- Drive-by-download: This leads the victim to unintentionally downloads malicious software when visiting a compromised web page (Tanaka *et al*., 2017). The malware is downloaded stealthily, without the users' knowledge, by taking advantage of browser vulnerabilities and exploits or built-in plugins such as JavaScript, ActiveX, Java /, or Adobe Flash Player (Paganini, 2019a)

Attribution

Attributing a cyber-attack or a specific campaign to an actor might be a problem, which is more complicated when correlating an A.P.T. to a specific state or group. Experts are able to look at the evidence to identify attackers when they are analyzing these threats, for example as I.P. addresses, the malicious code used, or emails. These attackers mostly use the concept of a false flag, which contains impersonating a third party to camouflage their operations. In last years, attacks attributed to government players and organized groups have significantly increased.

The main players can be divided into two major groups: Government players and organized crime groups.

Government Players

Increasingly frequent becomes cyber-attacks carried out by governments and nation-states. Disruption of power supply in other countries or the suspected interference in elections is generating widespread public concern because of the high cyber capabilities of the players.

China: Chinese cyberattacks were focused mainly on industrial espionage and were aimed to steal intellectual property. APT1 has been this player's most persistent cyber threat (Mandiant, 2013).

United States: That player may have executed mostly sophisticated cyber-attacks. Attacks may have been very damaging and very advanced technologies were used, which means considerable resources were used for developing this type of attack. A.P.T. campaigns are being used mainly to enforce geopolitical interests. An example could be the world-famous Stuxnet operation (Falliere *et al*., 2011), which mainly targeted Supervisory Control and Data Acquisition (SCADA) systems to cause damage to Iran's nuclear program.

Russia: This player is active in state-sponsored A.P.T. activities. The groups have been involved in high-profile intrusions, subject to intense investigations (Lemay *et al*., 2018). An example could be, Microsoft recently detected spear-phishing attacks by APT28, targeting German government officials. This group tried to get access to employee credentials and infect their websites with malware (ThaiCERT *et al*., 2019).

Iran: In the Middle East, this player шы controlштп the most significant attack capability attributed to the country, with several incidents which were executed by various groups (Lemay *et al*., 2018). Some experts have monitored operations like APT33 as this group recently updated its infrastructure and changed its purposes. The main targets of this group have been the energy companies that have links to petrochemical production and the aviation industry. The latest malware campaigns had targeted organizations in the USA, the Middle East, and Asia (Paganini, 2019b).

North Korea: Cyber groups which are associated with this player had conducted many operations, including banking hacks, conventional espionage, and destructive attacks. For example, employed by this player is the WannaCry ransomware (Adams, 2018).

Israel: This player is being identified as one of the possible co-authors of the Stuxnet attack (Falliere *et al*., 2011). It is well known for the high potential of the intelligence services of this country; an example is its army's Unit 8200 (Cordey, 2019), the equivalent of the U.S. intelligence agency N.S.A. For example, The Duqu 2.0 attack (Kaspersky, 2015) has been attributed to this country. This attack was hypothetically sponsored by this state and has infected several systems in several countries in the last few years. Such malware uses zero-day vulnerabilities, sends data to command-and-control servers (C and C), and; uses different techniques to access computers.

Campaigns: Campaigns are the customized methods, actions, and techniques that attackers are performing against a target to execute an A.P.T. to extract highly sensitive data, for example, social network engineering, zero-day malware, and data extraction via C&C servers. Moreover, to the players mentioned above, privately funded, organized cybercriminal groups do not respond to government interests; such groups had run various campaigns. In the last years, new A.P.T. campaigns are being discovered; such campaigns are still mainly active and the number of affected targets is unknown. They use various methods of propagation, for example, infected files, exploits, and malware. Such campaigns are designed for cyberespionage and their main targets are the information technology industry and diplomatic organizations. It has the outstanding characteristic of being highly organized and involving many players.

Assignment

As a result, for state-sponsored espionage groups, A.P.T. agents are now a priority for companies producing security products. To develop anti-APT products, it is essential to know the structure and attribution of these attacks. Therefore, it is no surprise that the research topic of A.P.T. attribution is paramount and often secretive. The interest that this topic succeeds is on a large scale, but it is inversely proportional to the publicity of the research results.

The documentation needed to investigate ours is hard to find. And is no shortage of data, the information is in fragments into many Internet artifacts, such as industry reports, scarce publications, and blog posts by threat researchers or attack responses. As a result, much of our work will be based on reports from official state agencies and companies in the computer security

industry. That makes getting an image of the APT. APT attacks and much more of the assignment are time-consuming and extremely difficult.

China is probably the location of the most significant A.P.T. groups attributed to state-sponsored operations (Lemay *et al*., 2018). We state this based exclusively on the reports that are indicated in the references of this study and on the high number of evidence described in the referred reports that are all indicated and with a link to the websites where they can be consulted. No personal opinion is expressed, but an analysis of what appears in the consulted and duly referenced reports is presented. This section expresses the information and the shared infrastructure used by various Chinese A.P.T. players that used hypothetical locations in Chinese territory and therefore designated in this way.

APT16

The APT16 group is assigned to China by FireEye. FireEye has released two documents about APT16. One document is an analysis of the CVE-2015-2545 vulnerability in spear-phishing for attacks (Jiang *et al*., 2015). The other document Winters (2015) is a more sophisticated analysis of targeted attacks directed at Taiwanese enterprises, including the text of the spear-phishing bait, more details about the malware in use, and a description of the control and command connection. Such work identifies one of the sources of these attacks as the new APT16 group.

Below are some A.P.T. campaigns according to the references of the consulted reports.

APT17

Aurora Panda is the best-known A.P.T. group best documented in espionage cases, the Aurora attacks on Google. Their name, "the Beijing group," attests to this reality in relation to another Chinese group, "the Shanghai group." The first information about this group comes from analyzing the attacks on Google, in 2010. First, Varma provides a brief report (Varma, 2022) on the vulnerability used with spear-phishing targets designed to encourage users to visit malicious sites and malicious URLs. And, we have the reports from Symantec for the analysis of the attack range (Response Incident, 2014) and the reverse engineering analysis of the exploit on the Hydraq Trojan horse used in operation (Lelli, 2010) and also malware and spear-phishing investigation used in similar incidents (Selvaraj, 2010).

After this high-level attack, the group seems to have remained active. For example, at the R.S.A. 2016 conference Dennesen tells how APT players act themselves after the attacks are revealed to the public.

The stopping of the use of the Hikit tool has stimulated the use of new tools. The report (Intelligence, 2015a) about a new attack technique, using Microsoft TechNet to host command and control addresses encrypted for FireEye's BLACKCOFFEE / ZoxPNG Trojan horse, show this kind of retooling.

In its report about Hidden Lynx (Doherty *et al*., 2013), Symantec show a group of hackers that act like to be hired. The report shows two groups based on the Trojan used in the other stages of the attacks. The report also summarizes the attacks on the Bit9 company and the V.O.H.O. campaign.

APT1

The Comment Crew is a known A.P.T. group very dangerous. Like Aurora Panda, their pseudonym of "the Shanghai group" also prove the longevity of their notoriety.

Mandiant's APT1 report (Mandiant, 2013) is the first source of the notoriety of the group. This report is the first significant report on Chinese responsibility in hacking that provided issues to direct attribution. The report exposes the connection between this group of hackers and the Chinese Army (P.L.A.) unit 61398, providing long evidence. The report also gives a brief overview of cyber incidents involving the group for which Mandiant performed incident response to give an idea of the wide range of the cybercriminal team's operations. The report describes how the team operates and covers both the general lifecycle of the attack and specific details about the tools and infrastructure used. The report concludes by revealing the online identity of suspected team members who carried out the attacks.

The F.B.I. later confirmed some of these identities in its indictment of team members for commercial espionage (US Department of Justice, 2014).

Other documents give the activities of this group. The first one is McAfee's Operation ShadyRAT report (Alperovitch, 2022). This report doesn't provide many technical details. Still, it does provide an analysis of the attacks on the ShadyRAT Trojan horse, later revealed as part of the comment team's activity. McAfee's report provides the context for the more detailed Mandiant report.

The second report gives us the activities from Honeynet Supervisory Control and Data Acquisition (SCADA) (Wilhoit, 2013). In this investigation, Wilhoit locks the origin of attacks on SCADA systems. Although it was not explicitly designed to capture A.P.T. activity, he received a spear-phishing email from sources affiliated with the Comment Crew during his study. This provides exciting insight into the direction of critical infrastructure for this particular group.

More specialized investigations have also been produced on some of the tools used by the group. First, Hoglund describes the C, and C became the group's name (Hoglund, 2011). The tool is commonly associated with Comment Crew, in the distribution campaign targeting industry (Narang, 2013). A Symantec report by Coogan describes the use of WinHelp files to install malware

(Coogan, 2012), with an example of the capture tool used in the campaign and a detection heat map.

Shell Crew

The Shell Crew group is a Chinese group that became better known around 2014, especially after the highly publicized breach at insurer Anthem.

R.S.A. research (Johnson, 2010) is the source of the name Shell Crew. In their report on the A.P.T. group (Johnson, 2010), the researchers exposed the tendency of this A.P.T. group to install web shells as one of the main persistence techniques. At the same time, Crowdstrike released a report on a hacker named Deep Panda (Alperovitch, 2014a), targeting think tanks and other targets related to contexts of Southeast Asian politics. In their analyses, they present the attacker as favoring techniques designed to avoid uploading tools to the target machines, preferring the use of native scripts, such as PowerShell and W.M.I., and executing malware from memory, as well as shells, as a method to avoid detection.

In 2015, the breach disclosure at Anthem insurance company provided information about the Shell Crew group (Krebs, 2015). A timeline of events and a link to other victims were obtained. Nevertheless, Krebs (Krebs, 2015) says that the Shell Crew group is known as Axiom. As such, it isn't easy to assess the validity of this link. Other reports about the Anthem breach include a flash alert from the Federal Bureau of Investigations (F.B.I.) (Investigations, 2022) detailing the implication of the Shell Crew and a list of tools used as technical indicators. We should also consider a report from ThreatConnect (ThreatConnect, 2015) which systematically tracks and Attributes violations originating from China. This report delves into the infrastructure used in the breaches at Anthem, Premeva Blue Cross, V.A.E., and O.P.M. and aims to find commonalities. The report also exposes the role of a Chinese security firm and an academic institution in the attack. Dimaggio from Symantec (DiMaggio, 2015) has deepened its investigation into the group and they set out the results in their report on the cyber-espionage group. Including custom malware used by the group (DiMaggio, 2015). The report also documents links to other known players (Hackers), indicating that they also appear to have access to 0 days of the Elderwood project (DiMaggio, 2015). Finally, the R.S.A. report on Terracotta VPN presents an overview of the network used by the Shell_Crew group to anonymize the source of the attacks. In the report, R.S.A. details the inner workings of the tool used by attackers to redirect their traffic to disguise that the traffic originated in China. Shell Cew has previously used this service for attacks.

Emissary Panda

This group, labeled by Crowdstrike as Emissary Panda, was not analyzed in detail in a full report. However, some information has emerged about his activities. Dell SecureWorks produced this report regarding threats from the (Intelligence, 2015b), which has provided a high score of the group's capabilities and intentions. The report also summarizes the main tools used by this player (Hacker Group). Several tools used by various A.P.T. agents, such as Plug X and HTTP Browser, and custom tools, such as the Owa Auth web shell and the ASPX Tool web shell, were referenced. The report says by providing significant information about the group's preferences for each stage of the disposal chain (Intelligence, 2015a).

In the report on Operation Tiger, TrendMicro (Chang *et al.*, 2013) analyzed a specific campaign launched by Emissary Panda in detail. This presented a complete view of the inner workings of the A.P.T.s activity of this group located in China (Chang *et al.*, 2013).

APT3

The group referred to as APT3 is one of the lesser-known Chinese A.P.T. groups. However, this does not imply that they are less proficient than the more documented groups. The primary tool used by the group is the Pirpi backdoor which was documented back in 2010. The report presents packet capture from the exploration phase and early command and control communication. However, today there is no mention of this A.P.T. group. Another report by FireEye researchers from 2014 (Chen *et al.*, 2014b). The report also details the threat, confirming that this group first accessed several web browsers at the 0-days level in the past (Chen *et al.*, 2014b). A second report on the numerous attacks, dubbed Operation Clandestine Fox, by FireEye (Scott, 2022), provides more details about the spear-phishing techniques used and the attachments included in the emails. FireEye also documented another wave of attacks, called Operation Double Tap, in an article by Moran *et al.* (2014). The authors provide information about the spear-phishing email and the dropped downloader in this investigation. They also detail the types of commands available to attackers after command and control are established, which are the group's modus operandi (Moran *et al.*, 2014). They present the hypothesis for the change in behavior of this group as being that the requirements for a faster pace of attacks prevent them from relying exclusively on 0-day exploits.

FireEye investigated the details of Operation ClandestineWolf (Eng and Caselden, 2015). In this investigation, a spear-phishing campaign is detailed, using a 0-day Adobe Flash that they associate with APT3 (Eng and Caselden, 2015). This campaign compromised web servers hosting the exploit and distributed malware related to them (Eng and Caselden, 2015). A wave of

attacks in July 2015 spurred the production of several publications. First, an investigation by Lee and Falcone of Palo Alto Networks focuses on using an Adobe Flash vulnerability that was used by the group (Lee and Lewis, 2013). Straightforwardly, they compare the shellcode with the leaked HackingTeam shellcode and realize that there are significant overlaps, concluding that advanced groups, such as APT3, can quickly benefit from public disclosure of vulnerabilities. In the second place, W.P.W.C.'s Lancaster provides more details about how the group used a modified version of Scanbox in their attacks. The investigation discloses that the group has used the ScanBox framework to use the PluginDetect code for server-side identification of plugins in the exploitation phase. The research also provides the literal code for the PluginDetect component used by APT3. It lists the commonly used tools, including the options available for those tools, creating a pattern identifying this group and its Attribution in China (Response Incident, 2014).

Hurricane Panda

Hurricane Panda is a group primarily associated with a specific campaign that used Hurricane Electric DNS servers. The campaign, dubbed Operation Poisoned Hurricane by FireEye, was the subject of a publication by Moran *et al*. (2014). He explained how a type of malware used by A.P.T. was configured to use Hurricane Electric's DNS servers.

Crowdstrike further documents Hurricane Panda's activities in a series of reports, discussing how best to respond to this group's incidents. The reports mainly focus on how Crowdstrike products allow customers to fight off attackers. Still, they all include only partial information on how this A.P.T. operates, such as its complexity. For example, the first report (Alperovitch, 2014b) discusses using a local privilege access exploit by the group to gain access to the administrative level, which is necessary to install rootkits at the kernel level or obtain passwords. The second report (Schworer and Liburdi, 2015) discusses Hurricane Electric's use of servers to control well-known URLs, such as GitHub and Pinterest, and avoid detection at the network's internal perimeter. Finally, the third report (Alperovitch, 2015) analyzes the persistent group.

Icefog

Icefog is another lesser-known Chinese group that has targeted Kaspersky's investigation. The primary information on the group comes from a detailed report from Kaspersky (K. L. Z.A.O). Finally, the report summarizes the infection data and the characteristics used to attribute these attacks to China (K. L. Z.A.O).

Raiu and Golovkin (2015) conducted a follow-up investigation. They report how investigating a specific command and control domain led them to discover a Java-based version of the Icefog backdoor.

Ke3chang

Very few known studies and reports about this group and no known scientific articles exist. However, as Scott and Summit (2016) group the two operations and assign them to the A.P.T. Vixen Panda/APT15 group, this fact creates even more doubt than certainty regarding Ke3chang. SecureWorks' report on the Cutler Mirage campaign (Cutler, 2012) is this group's first published analysis. FireEye's report on Operation Ke3chang was published later but covered a more extended period. This report analyzes a series of breaches discovered during the investigation of attacks against foreign ministries in European countries. The group has not ceased operations, as explained in an article by Yates *et al*. from palo alto networks (Yates *et al*., 2016). This article shows that this group used the new Tidepool malware and attributes it to the malware used on Ke3chang. The article briefly overviews the Tidepool malware's vulnerability and compares it with the BS2005 malware used in one part of the Ke3chang operation (Yates *et al*., 2016).

NetTraveler

The NetTraveler group took its name from the malware it used in one of its operations. They mention that the group members speak and write native Chinese (Global Research and Analysis Team, 2004). The main report describing the activities of the NetTraveler group was published by the Global Research and Analysis Team (GReAT) at Kaspersky Labs (Global Research and Analysis Team, 2004). Finally, the report provides an overview of the infection statistics and how you can remediate the attack. It has an appendix with a detailed description of the malware's functionality and features. Raiu (2013), from Kaspersky, reports another attack using NetTraveler this attack, which occurred after the publication of Kaspersky's previous report, demonstrates a change in tactics by the group by using a Java exploit hosted on a watering hole site instead of sending documents containing exploits by email.

Night Dragon

The primary source of information on Night Dragon is a report by McAfee Foundstone and McAfee Labs, (McAfee, 2022) which explains how the attacker, through web compromise using SQL injection, spear phishing, and VPN access abuse, launched an espionage campaign targeting the energy sector. Next, the report lists the additional tools widely available on Chinese hacker sites and the R.A.T.s used in the attacks. Finally, the report goes into a little more depth

on the main tools used and further analyzes R.A.T.'s network communication. However, the appendices provide more information about zwShell R.A.T. and limited attribution (McAfee, 2022).

Putter Panda

Putter Panda is another A.P.T. group that has been directly assigned to players located in China. The primary documentation for this A.P.T. group is an extensive dossier produced by the Crowdstrike Global Intelligence Team. The report begins with the assignment to the P.L.A.'s 12th Bureau Unit 61486 through an investigation of online identity copying. This investigation also details the group's targeting interest in aerospace, satellite, and communications companies. The report also provides technical details of the various Putter Panda tools, such as the 3PARA Remote Access Tool, PNGDOWNER, HTTP client, and RC4 and XOR-based droppers. Finally, the report also provides a list of artifacts left behind by Putter Panda that can be used for detection purposes.

In 2016, presented a closer look at Putter Panda's activities, investigating an attack involving the group. The investigation provides a detailed analysis of the malware's low-level functionality that was not detected by anti-virus software at the time of infiltration. Additionally, they could leverage the evidence they found to identify other instances of this malware and present information about similar infections.

Hellsing

The activity of the Hellsing group was from Kaspersky. The report provides the email exchanges used to set up the attack. The last email message contained a customized backdoor. Further investigations in Kaspersky's telemetry database showed government and diplomatic targets attributed to this group. The report lists several campaigns and their respective command and control servers. And an overlap analysis with the infrastructure of other Chinese A.P.T. groups, including Ke3chang and Cycldek / Goblin Panda.

NAIKON-APT 30

FireEye has published a report on APT 30, FireEye threat intelligence group, which characterizes this group in detail. The report details the remote control software panel used by the attacker to manage these direct connections. The report also demonstrates the data exfiltration capabilities of the backdoors, which include the ability to target air-gapped networks, and shows that the tools are not designed to extract data of financial value, such as credit card numbers. This report analyzes the targets of this group and concludes that the objectives are consistent only with Chinese national interests. The report's authors highlight that this group makes intensive use of social engineering.

Table 8: Systematization of the analyzed A.P.T. campaigns

Name	Attribution year
APT16	2015-2020
APT17	2010-2020
APT1	2007-2013
Shell Crew	2014-2020
Emissary Panda	2010-2020
APT3	2010-2014
Hurricane Panda	2015-2019
Icefog	2011-2020
Ke3chang	2010-2020
NetTraveler	2004-2019
Night Dragon	2006-2016
IXESHE	2009-2019
Putter panda	2016-2020
Hellsing	2014-2020
NAIKON – APT 30	2017-2020

Table 8 shows us the APT campaigns from 2015-2020 that achieved Attribution.

From Kaspersky corroborate the FireEye report with a report. Finally, an overview of an anonymous operation against a country is presented. In another report, these authors, from Kaspersky, document some of Naikon A.P.T.'s previous campaigns. The authors mention the attackers' preference to use specific toolkits customized for the victim's country. Some of the toolkits are reported to come from the Chinese underworld. They also mention the effort invested in recognition to personalize spear phishing attempts. Several social engineering tricks implemented by this group, such as names with double extensions or right-to-left substitution techniques, are described in detail. The report lists several shared components (exploits, command and control, and malware) used to create an assignment against this group. The authors propose that the decoys used would provide information about the victims. This report thoroughly discusses backdoor and lateral movement tools, emphasizing capabilities and indicators. The authors note that some components appear to be shared with APT 30, a group associated with China. Based on the HDoor tool, a second-stage custom backdoor is also discussed in great detail, which provides information about lateral movement capabilities.

Results

The main results obtained from this study is the contact that there are many organized groups that have been attributed with the orchestration of APT activities, mainly against the West.

Discussion

APT Attribution is an extremely difficult technique, in order to obtain an Attribution it is necessary to have objective and unequivocal data on the exact origin of the

person responsible for the APT attack. Geographical origin is sometimes easier to obtain, but that alone is not enough for full Attribution. In the case of our work it was found that it is possible to Attribute many APT attacks originating in China, and it was also found that it is possible to make the complete Attribution to many truly Chinese Groups that even maintained long-term activities of attacks in relation to western countries.

It is concluded that there were many APT campaigns originating from Chinese Groups, some of them even outside Chinese territory, but the majority in Chinese territory.

Conclusion

As we have already mentioned, APTs A.P.T.s are the most complex and dangerous cyber threats. Although the number of academic publications on the topic of APT A.P.T. players is relatively low, the industry has provided a lot of information about these attacks that is a must-have source for understanding the problem and mitigating it. The large volume of publications shows interest in the topic and the magnitude of the problem.

There are no scholarly articles that explore the issue of awarding A.P.T.s. However, there are reports from security companies and government agencies, mainly from the United States of America.

Based on credible technical documentation, it has been shown that there is a pattern of groups using A.P.T.s that connect to Chinese territory.

On the other hand, the complexity of the modus operandi of these players, IXESHE who are said to have originated in China, suggests that these are not isolated or individual acts but possibly properly orchestrated campaigns with significant technological and financial support.

There are orchestrated campaigns with significant technological and financial support.

The main results unequivocally point to a large number of APT type attackers originating in China. This implies a greater need to implement anti-APT security measures in Western countries.

As APTs are extremely difficult to detect by conventional means, holistic measures and behavior analysis must be implemented to minimize and detect APTs.

The current status in the field is the verification that APT attacks originating in China have increased significantly in recent years.

The analysis in this study used many technical reports from security organizations and government agencies.

Acknowledgment

We would like to thank the three institutions that supported the authors: Instituto Superior de Tecnologias Aberta, Universidade Aberta, Instituto Superior Técnico.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

All authors equally contributed in this study.

Ethics

The article complies with all ethical principles.

References

Adams, C. (2018). Learning the lessons of WannaCry. *Computer Fraud & Security*, *2018*(9), 6-9. https://doi.org/10.1016/S1361-3723(18)30084-8

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160-196. https://doi.org/10.1016/j.cose.2017.04.006

Alperovitch. D. (2022). "Operation shady R.A.T." https://icscsi.org/library/Documents/Cyber_Events/McAfee%20-%20Operation%20Shady%20RAT.pdf

Alperovitch, D. (2014a). Deep in thought: Chinese targeting of national security think tanks. *Crowdstrike, Sunnyvale, CA, USA, Tech. Rep*, *772014*. https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/

Alperovitch, D. (2014b). CrowdStrike discovers the use of a 64-bit zero-day privilege escalation exploit (CVE-2014-4113).

Alperovitch, D. (2015). Cyber Deterrence in Action? A story of one long Hurricane Panda Campaign. *CrowdStrike, Executive Viewpoint, Entry Posted April*, *13*.

Chang, Z., Lu, K., Luo, A., Pernet, C., & Yaneza, J. (2013). Operation iron tiger: Exploring Chinese cyber-espionage attacks on United States defense contractors. https://www.erai.com/CustomUploads/ca/wp/2015_12_wp_operation_iron_tiger.pdf

Chen, P., Desmet, L., & Huygens, C. (2014a). A study on advanced persistent threats. In *Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15* (pp. 63-72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

Chen, X., Scott, M., & Caselden, D. (2014b). New zero-day exploit targeting internet explorer versions 9 through 11 identified in targeted attacks. *Fireeye Blog*, *26*.

Coogan, P. (2012). Targeted attacks make WinHelp files not so helpful. https://www.symantec.com/connect/blogs/targeted-attacks-make-winhelp-files-not-so-helpful

Cordey, S. (2019). *The Israeli Unit 8200–An OSINT-based study: Trend Analysis*. ETH Zurich. https://doi.org/10.3929/ethz-b-000389135

Cutler, S. (2012). The Mirage Campaign. *SecureWorks, Inc, Atlanta, GA Sept*, *18*. https://www.secureworks.com/research/the-mirage-campaign

DiMaggio, J. (2015). The black vine cyberespionage group. *Symantec Security Response*.

Doherty, S., Gegeny, J., Spasojevic, B., & Baltazar, J. (2013). Hidden Lynx–Professional Hackers for Hire. *Symantec Security Response Blog*, *112*. https://www.infopoint-security.de/medien/Symantec_hidden_lynx.pdf

Eng, E., & Caselden, D. (2015). Operation clandestine wolf–Adobe flash zero-day in APT3 phishing campaign. *FireEye. June*, *23*.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, *5*(6), 29. https://pax0r.com/hh/stuxnet/Symantec-Stuxnet-Update-Feb-2011.pdf

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

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*, 101-121. https://doi.org/10.1016/j.infsof.2018.09.006

Garousi, V., Felderer, M., Karapıçak, Ç. M., & Yılmaz, U. (2018). What we know about testing embedded software. *IEEE Software*, *35*(4), 62-69. https://doi.org/10.1109/MS.2018.2801541

Higgins, J. P. (2017). "Including unpublished studies in systematic reviews," in Cochrane Handbook for Systematic Reviews of Interventions.

Hoglund, G. (2011). Inside an APT covert communications channel. *Fast Horizon*, *16*. http://fasthorizon.blogspot.ca/2011/08/inside-apt-comment-crew-covert.html

Intelligence, D.S.C.T.U.T. (2015a). "Threat analysis – threat group 3390 cyberespionage." https://

Intelligence, F. T. (2015b). HAMMERTOSS: Stealthy tactics define a Russian cyber threat group. *Milpitas, CA: FireEye, Inc*. https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

Investigations. (2022). "FBI liaison alert system #A-000049-MW." http://krebsonsecurity.com/wp-content/uploads/2015/02/FBI-Flash-Warning-Deep-Panda.pdf

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. In *Computer Applications for Security, Control and System Engineering: International Conferences, SecTech, CA, CES 3 2012, Held in Conjunction with GST 2012, Jeju Island, Korea, November 28-December 2, 2012. Proceedings* (pp. 144-152). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-35264-5_21

Jiang, G., Caselden, D., & Winters, R. (2015). The EPS awakens. *FireEye Threat Research*, *16*. https://www.mandiant.com/resources/blog/the-eps-awakens

Kaspersky. (2015). Frequently Asked Questions. DUQU 2.0: "The Duqu," Technical Report, https://media.kaspersky.com/en/duqu-2-0-frequently-asked-questions.pdf

Krebs, B. (2015). Anthem breach may have started in April 2014. *Krebs Secur*. https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Lee, M., & Lewis, D. (2013). Clustering disparate attacks: Mapping the activities of the advanced persistent threat. *Last accessed June*, *26*.

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26-59. https://doi.org/10.1016/j.cose.2017.08.005

Lelli, A. (2010). The Trojan. Hydraq incident: Analysis of the Aurora 0-day exploit. https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit

Mandiant. (2013). "APT1 Exposing one China's Cyber Espionage Units," Technical Report Mandiant. https://www.hsdl.org/c/apt1-exposing-one-of-chinas-cyber-espionage-units/

McAfee, M. L. (2022). Foundstone Professional Services. "Global energy cyberattacks: “Night Dragon”."

Monnappa. (2022). "2nd meetup-reversing and decrypting the communications of A.P.T. malware." https://cysinfo.com/sx-2nd-meetup-reversing-and-decrypting-the-communications-of-apt-malware/

Moran, N., Scott, M., Oppenheim, M., & Homan, J. (2014). Operation Double Tap. *FireEye. November*, *21*.

Müller, M. (2019). Cyber security report 2019. *Die Aktiengesellschaft*, *64*(19), r283-r284. https://doi.org/10.9785/ag-2019-641919

Narang, S. (2013). Backdoor. Barkiofork Targets Aerospace and Defense Industry. *Symantec Official Blog*. https://www.symantec.com/connect/blogs/backdoor barkiofork-targets-aerospace-and-defense-industry

Paganini, P. (2019a). Turla APT Group's Espionage Campaigns Now Employs Adobe Flash Installer and Ingenious Social Engineering.

Paganini, P. (2019b). Iran-Linked APT33 Updates Infrastructure Following Its Public Disclosure. https://securityaffairs.com/87784/apt/apt33-updates-infrastructure.html

Pricewaterhouse, C. (2017). "Operation Cloud Hopper," Technical Report. https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf

Raiu, C. (2013). NetTraveler Is Back: The'Red Star'APT Returns With New Tricks. *Kaspersky Labs*, *3*. https://securelist.com/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/57455/

Raiu, C., & Golovkin, M. (2015). The chronicles of the Hellsing APT: The empire strikes back. *Kaspersky Lab) Retrieved April*, *21*, 2018. https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/

Johnson. A., L. (2010). "Hydraq – an attack of mythical proportions." https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions

Response Incident. (2014). RSA. Incident response: Emerging threat profile shell_crew. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/h12756-wp-shell-crew.pdf

Schworer, A., & Liburdi, J. (2015). Storm chasing: Hunting hurricane panda. https://www.crowdstrike.com/blog/storm-chasing/

Scott, J., & Summit, W. (2016). Rise of the machines: The dyn attack was just a practice run december 2016. *Institute for Critical Infrastructure Technology, Washington, DC, USA*.

Scott. M. (2022). "Clandestine fox, Part deux. FireEye", FireEye Report.

Selvaraj, K. (2010). Hydraq (Aurora) Attackers Back. https://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back

Symantec, (2019). Internet Security Threat Report, Technical Report 2. https://docs.broadcom.com/doc/istr-24-2019-en

Tanaka, Y., Akiyama, M., & Goto, A. (2017). Analysis of malware download sites by focusing on time series variation of malware. *Journal of Computational Science*, *22*, 301-313. https://doi.org/10.1016/j.jocs.2017.05. 027

Global Research and Analysis Team. (2004). "The NetTraveler (aka Travnet')."

ThreatConnect. (2015). "The anthem hack: All roads lead to China." https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

ThaiCERT, (2019). "Threat Group Cards: A Threat Actor Encyclopedia," Report, 2019. https://apt.etda.or.th/cgi-bin/aptgroups.cgi

T.I.T.M.L, (2020). "APT36 Jumps on the Coronavirus Bandwagon," R.A.T. 2020.

US Department of Justice. (2014). US charges five Chinese military hackers for cyber espionage against US corporations and a labor organization for commercial advantage. *The US Department of Justice*.

Varma, R., M. (2010). Labs. Combating Aurora. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Combating%20Threats%20-%20Operation%20Aurora.pdf

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://doi.org/10.1109/ARES.2013.32

Winters, R. (2015). The EPS awakens—part 2. *FireEye Threat Intell*.

Wilhoit, K. (2013). The SCADA that didn't cry wolf. *Trend Micro Inc., White Paper*.

Yates, M., Scott, M., Levene, B., Miller-Osborn, J., & Keigher, T. (2016). Operation Ke3chang Resurfaces with New TidePool Malware.