Information **2015**, *6*, 183-211; doi:10.3390/info6020183

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Review

The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism

Gaute Wangen

Norwegian Information Security Laboratory, Center for Cyber and Information Security, Gjøvik University College, Teknologivn. 22, 2815 Gjøvik, Norway; E-Mail: gaute.wangen2@hig.no; Tel.: +47-907-08-338

Academic Editors: Qiong Huang and Guomin Yang

Received: 9 April 2015 / Accepted: 7 May 2015 / Published: 18 May 2015

Abstract: The recent emergence of the targeted use of malware in cyber espionage *versus* industry requires a systematic review for better understanding of its impact and mechanism. This paper proposes a basic taxonomy to document major cyber espionage incidents, describing and comparing their impacts (geographic or political targets, origins and motivations) and their mechanisms (dropper, propagation, types of operating systems and infection rates). This taxonomy provides information on recent cyber espionage attacks that can aid in defense against cyber espionage by providing both scholars and experts a solid foundation of knowledge about the topic. The classification also provides a systematic way to document known and future attacks to facilitate research activities. Geopolitical and international relations researchers can focus on the impacts, and malware and security experts can focus on the mechanisms. We identify several dominant patterns (e.g., the prevalent use of remote access Trojan and social engineering). This article concludes that the research and professional community should collaborate to build an open dataset to facilitate the geopolitical and/or technical analysis and synthesis of the role of malware in cyber espionage.

Keywords: cyber-espionage; advanced persistent threat (APT); review

1. Introduction

Spying is said to be the world's second oldest profession, as gaining the information advantage over competitors ensures competitiveness and increases the likelihood of survival. During the last two

decades, malware has really entered the scene of industrial cyber espionage with the recent occurrences of very sophisticated targeted information stealers, such as Flame, Gauss, Duqu and Regin. However, in cyberspace, there is quite a bit of both information and disinformation when it comes to cyber-attacks. The Snowden revelations have shown how the Internet can be subverted into a surveillance tool and, by extension, into an espionage platform. As more actors realize the potential of espionage in ICT infrastructures, this problem will keep increasing in the coming years. The reader can consider this article a step towards highlighting a growing problem that should be solved both technically and politically.

In this article, we therefore survey the state-of-the-art within known malware usage and attacks for intelligence gathering and espionage. These attacks usually present themselves in the shape of an advanced persistent threat (APT). Our review scope is limited to published material on types of known malware attacks against or made by larger entities, such as large organizations and nations. The emphasis is on what kind of and how malware is used for espionage and how it differs from malware in regular criminal activities.

The main contribution of this article is a taxonomy to document major cyber espionage incidents involving malware. In this taxonomy, we describe and compare cyber espionage impacts in the form of targets, origins and motivations and their mechanisms (dropper, propagation, types of operating systems and networks involved). This taxonomy provides a systematic way to document known and future attacks to facilitate research activities. Geopolitical and international relations researchers can focus on the impacts, while malware and security experts can focus on the mechanisms. The taxonomy is founded on our review of recent major cyber espionage events, and based on this, we discuss and generalize attack patterns for an industrial cyber espionage campaign. This article can aid the information security community by providing knowledge and awareness about state-of-the-art attack techniques and how APTs behave. This taxonomy has the potential to aid in the defense against cyber espionage by providing scholars a solid foundation of knowledge about the topic.

The remainder of this paper is as follows: First, we present the necessary background knowledge and related work for this paper. Then, we briefly discuss the methodology for choosing literature and the review scope. Further, we present the reviewed literature consisting of fourteen case studies. Then, we categorize our findings into the taxonomy. Lastly, we analyze, discuss and conclude about our work.

1.1. Background Knowledge and Related Work

The term "malware" is short for malicious software and is in short any type of software designed to do unwanted and malicious actions on a computer system [1]. Examples of malware include viruses, worms, Trojans, logical bombs, rootkits and spyware. These malwares exist in a variety of forms, from custom designed to attack a specific system, to generic self-replication probes that attack every available target.

There is also the so-called APT: this buzzword describes resourceful computer attackers who target and exploit specific entities, usually over a longer periods of time [2]. To a large extent, malware is what enables much of cyber espionage. Virvilis and Gritzalis [3] have published an article on what they call the big four: Duqu, Stuxnet, Flame and Red October, in which they outline the known technical details of these four APTs. Except for Red October, Bencsáth *et al.* [4] have also published an article on the same three APTs, where they call them cousins of Stuxnet.

There are many views on what cybersecurity is and is not; for this paper, we will use McGraw and Fick's [5] three distinctions:

- Cyberwar: It is not easy to distinguish an act of war performed in cyber space, as war is defined as a violent conflict between groups for political, economic or philosophical reasons. With this in mind, does defacing a website or infecting a computer with malware constitute an act of war? The authors argue that cyberwar requires a consequential impact in the physical world: to qualify as cyber war, the means may be virtual, but the impact should be real.
- Cyber espionage: This appears to be more easily defined as theft of intellectual property and company secrets in cyberspace. Cyber espionage is a means for intelligence gathering.
- Cybercrime: This is described as the most pervasive of the three, where criminal acts involving a computer or network are committed.

1.1.1. Difference in Malware for Crime and Espionage

Based on McGraw and Fick's definitions, how do we tell the difference between usage of malware in cybercrime and cyber espionage? In our opinion, the main difference is in the incentives. Based on the overview of incentives for creating malware provided in Felt *et al.* [6], we can summarize the main drivers behind malware production. Most of the Felt categories are driven by monetary gain, while the remaining incentives can be summarized as amusement, novelty, monitoring/information gathering, vandalism and fame/attention. Based on this, we assume that most cyber criminals produce and employ malware to make money. One of the traits that come with this is that they will attempt to maximize the profit of an attack, e.g., in phishing attacks, this translates into having as many targets as possible to maximize the probability that someone falls victim to the fraud. In contrast to this, an espionage attack is likely to be targeted, e.g., so-called spear phishing attacks. The incentives for espionage attacks also differs within the Felt categories, as monitoring and information gathering are the main drivers. The espionage attackers aim to steal valuable information for, e.g., future attacks, obtain industrial advantages or to gain the upper hand in a future negotiation. In addition, the attackers in an espionage attack will often be looking for specific information and know how to get it. This brings us to the role of expertise in cyber espionage, as a large-scale operation demands expert knowledge about the target. The operation must include more than the IT expert's knowledge of vulnerabilities to be successful. Among other things, a spear phishing email directed towards another country and culture requires expert knowledge about both language and political situations to succeed. Industry expertise is also required to mine and exfiltrate the correct information.

It is our opinion that the main differences are in the incentives; another difference is that it is the information stealers and stealth malware that are predominant in cyber espionage. We have summarized the differences in Table 1.

Table 1. Summarized overview of the general differences between cyber espionage and crime.

	Cyber Espionage	**Cyber Crime**
Main Incentives	Information Gathering	Monetary gain, Vandalism
Targets	Few	Many
Malware Design	Tailored	Generic
Knowledge Required	Industry specific, IT security, Culture and language	IT security
Resources Required	Many	Few
Engineering Complexity	High	Low

1.1.2. The Attribution Problem

Knowing who did what and determining who is responsible is not easy, especially on the Internet. We can trace computers and servers back to countries, but in most cases, we cannot be certain about who is sitting in front of the screen. It is also difficult to determine if a server is a root node in the cyber espionage network or just another stepping-stone (especially without physical access to the machine). It is common knowledge that security was not a main priority during the invention of the Internet. Deibert and Rohozinski [7] write that the Internet is full of loopholes, which allow the attacker to mask both his identity and location, e.g., online identities can be hidden, packet flows redirected and vulnerable machines used as proxies. In short, the "attribution problem" describes that there is a high level of uncertainty involved when determining who is doing what on a computer.

Deibert and Rohozinski also have a point in that cyber actions being committed that seem to benefit states may be the work of third-party actors operating under a variety of motivations. Unless a high integrity actor outright takes on responsibility for an attack, we can seldom be certain of who was involved.

Mandiant took a major step in terms of attribution with their report on APT1 [8]; they also comment on the necessity of attribution in terms of understanding the cyber threat landscape. We cannot ignore attribution, but we have exercised caution in doing so: when our review sources have suggested a cyber-espionage actor, we have taken this into our taxonomy. We judge that the security vendors value their integrity so much that they would not risk making false accusations. Furthermore, we have attributed actors that have claimed responsibility of an action, unless we found evidence to suggest otherwise. However, we do ask the reader to bear in mind the attribution problem and third party actors when using our taxonomy, as some of the alleged origins are more certain than others.

2. Methodology and Scope

The methodology for this article has been a theoretical literature review. Our main criterion for literature selection is documentation of major recent industrial cyber espionage attacks including malware. The breadth of this review includes all stages in an attack, from start until mission completed.

We review attack strategies and malware functionalities in-depth, but do not go into coding. In addition, reviewed literature must adhere to the following criteria in order to have been included:

- It must hold relevance to malware usage in industrial espionage and information gathering.
- The primary sources reviewed for this paper are technical reports from renowned security vendors and both peer reviewed journal and conference articles. A note on this is that most of the published literature within in this area is technical reports from security companies, and we therefore chose these as a primary source.
- Secondary sources reviewed include non-peer-reviewed sources, including other technical reports, subject books, white-papers and miscellaneous articles.
- The literature must describe attack vectors, malware function (information gathering) and targets.
- There is much exaggeration and (dis)information concerning APTs from different media. Therefore, the minimum requirement for an APT to be included in this report is that it is described in detail in a technical report from a renowned vendor.

Our main approach to non-peer-reviewed technical reports has been that as long as two independent security companies report on the same malware, we can validate the results for accuracy and truthfulness.

The main scope of this paper is industrial and political cyber-espionage using malware, where an actor digitally infiltrates a system and installs malware that transmits digital copies of secrets back to the attacker. However, there are also gray areas, e.g., when an attacker or malware first does reconnaissance (espionage) and then commits a crime. This paper for the most part addresses malware used for reconnaissance and information stealing purposes. Our review scope is limited to published material on types of known major APT incidents. This work is positioned in the intersection between espionage and the use of malware to collect data. With this article, we categorize the published data from technical reports and make it available to scholars and others.

3. Review of Published Industry Cyber Espionage Cases

In this section, we review literature on known cyber espionage attacks, including the background for the attack, where it took place, how the attack was conducted, the likely information it targeted and, if possible, the origin of the attack. For each malware, we give a brief introduction of reviewed literature before diving into the details. Although, not entirely within our scope, we also give an overview of W32.Stuxnet and Shamoon due to their significance.

3.1. Mandiant's APT1: PLA Unit 61398

Mandiant is an American security company that, in their report [9], first provided public proof of Chinese cyber espionage involving the Chinese government. The group that Mandiant describes as APT1 has origins in China and is described as the most persistent of China's cyber threat actors. The group has been conducting cyber espionage campaigns against several targets since 2006.

The only source we have available on this APT is the Mandiant APT1 report [9], and all of our information on this attack comes from this report. Mandiant reports to have backtracked APT1 back to an address in Shanghai, and estimates, based on the building's infrastructure, a staff of several

hundreds of people. The group had hacked at least 141 organizations spanning 20 major industries at the time of the report's publishing. Mandiant also found that China Telecoms provided special fiber optic communications infrastructure for the unit in the name of national defense.

Mandiant describes APT1's standard attack cycle using eight steps: (i) "initial recon" and (ii) "initial compromise". Further, the attackers (iii) "establish foothold" and move into a recursive loop with (iv) "escalate privileges", (v) "internal recon", (vi) "move laterally", and (vii) "maintain presence" until (viii) "complete mission". Mandiant reports spear phishing as the most commonly-used technique for compromising organizations, containing either malicious attachment or hyperlink to a malicious file. The attackers also had a technique of making malicious software appear as benign files, such as disguising an application to look like a pdf. The malware installs a remote access Trojan (RAT) on the system to establish a foothold. Mandiant describes two Trojans as standard for APT1: one simple, which allows the attacker to open a command shell, download and execute a file and sleep (malware remains inactive). The standard Trojan contains several components to both maintain command of the compromised system and for information stealing, e.g., execute programs, upload/download, list processes, keylogging/mouse movement logging, harvest network information, open a command shell and harvest passwords. APT1 in particular collects intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements and emails and contact lists. Harvested usernames and passwords are applied to escalate privileges within the compromised system. The attacker does propagation and lateral movement within the network manually. APT1's command and control (C&C) infrastructure spans over 900 severs, 849 distinct IP addresses, located in 13 countries.

On the origins of APT1, Mandiant presents a large amount of evidence that the threat comes from China, namely the People's Liberation Army (PLA) Unit 61398.

3.2. Red October

In 2013, the security company Kaspersky Labs published a technical report on a cyber-espionage network they named "Red October" [10]; the report is on different attacks in the period 2010 to late 2012. The main targets for this espionage network were various international diplomatic and governmental agencies.

In the previously-mentioned Virvilis and Gritzalis [3] article, the authors have performed four technical APT analysis, whereas one section belongs to Red October. However, the authors cite the Kaspersky Lab report [10] as one of their main sources of information, although one must assume that they have conducted their own analysis of the malware.

The general attack is described by Kaspersky as a classical scenario of specific targeted attacks, with two major stages: (i) initial infection and (ii) additional modules deployed for intelligence gathering. The attack was carried out using spear phishing e-mail, with the malware embedded in the attachment, as Microsoft Excel and/or Word files. Kaspersky was unable to retrieve e-mail used in the attacks, but based on indirect evidence, they claim to know that the phishing mails were either distributed using anonymous mailboxes from free e-mail providers or already compromised accounts from infected organizations. The malicious code was designed to exploit known vulnerabilities in Excel, Word or the pdf-viewer. All of

the analyzed attacks documented in the Kaspersky report show that the attackers employed already public exploit code with Chinese origins.

Upon infection, the malware initiated the setup of the main component, which, in turn, handled further communication with the C&C servers. The malware establishes a backdoor and connects to the C&C domains using a RAT.

Virvilis and Gritzalis [3] write that each malware build was unique for each target and each e-mail tailor-made. Virvilis further explain that due to its minimalistic architecture, it downloaded and executed specific modules, which allowed it to perform a wide range of tasks. For intelligence gathering purposes, the identified capabilities included the ability to steal information from Nokia phones and iPhones, SNMP brute force network devices and recover deleted files. The authors did not find any rootkit present, but express some uncertainty regarding this, as the analysis of all modules was not completed at the time of publication. The malware hid itself from security products by initially being minimalistic in its architecture and downloading encrypted modules, which it executed in memory. The malware also made use of encryption to pack its main executable for encoding and exfiltrate data.

Judging from the Kaspersky report, most targets were embassies (at least 30 infections), in addition to some government branches and industry. Kaspersky claims in the executive summary that the main objective of the attackers was to gather intelligence, which they reused in later attacks. They also report over 300 different infections reported from their security solutions. A strong hint of the origins of the attackers was found in the executable malware code, where the code contained a command to switch the code page of the infected system to be able to address Cyrillic characters. The report also mentions other artifacts, suggesting Russian-speaking origins [10].

3.3. Stuxnet

Stuxnet shook the ground when it was discovered back in 2010. Although probably not designed for espionage, the significance of Stuxnet as a targeted malware attack cannot be overstated. Ralph Langner describes Stuxnet as much more complex than any other malware seen before [11]. As the documentation surrounding Stuxnet is large enough to warrant its own review paper and Stuxnet being more utilized for sabotage than espionage [3], Stuxnet is in the grey area of our review. We review its history and functions due to its relevance for other advanced malware for espionage.

One of the most acclaimed sources on Stuxnet is Symantec's technical report "W32.Stuxnet Dossier, v 1.4 (2011)" [12], and therefore, we use this technical report to describe the target and the functionality of Stuxnet.

According to the authors from Symantec, one of the main things that made Stuxnet stand out was the difference between the dropper and the payload. The dropper targeted Microsoft Windows (MW) systems, while the payload was made for industrial control systems (ICS). What makes this stand out is that contrary to most malware, Stuxnet did no damage to the system that the dropper targeted, while the payload targeted and damaged another type of system. The complexity of the malware was another thing that made it stand out, as it included zero-day exploits, Windows rootkit, programmable logic controllers rootkit (the first of its kind), anti-virus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates and a command and control interface. The target

was, with a large degree of certainty, components of the programmable logic controls (PLC)-operated centrifuges in an enrichment cascade.

Stuxnet employed several methods for self-propagation, including several exploits: (i) self-replication through removable drives, (ii) spreading in a LAN, (iii) spreading through SMB and (iv) copying and executing itself on remote computers through network shares and remote computers running WinCC DB server. The malware also copies itself into Step 7 projects and automatically executes when the project is loaded.

The malware receives updates via peer-to-peer mechanisms within a LAN, which gives the attacker C&C and privileges to upload/execute code, while Langner [11] claims that Stuxnet used the C&C connection primarily for evidence of compromise. Upon infection, Stuxnet scans for a specific SCADA system fingerprint, namely the Siemens PLC. If it does not detect the specific PLC present on the system, it does not harm the system. However, when the fingerprint matched, the malware payload would be loaded. From our understanding, Stuxnet would first spy on the operations of the system and gather information. Further, it used the gathered information to take control of the PLC controlling the uranium centrifuges, making them malfunction by slightly changing the speed of operations, making them spin themselves to failure. The malware was conducted as a man-in-the-middle attack, feeding false data to the external controllers ensuring false measurements and avoiding the detection of the sabotage.

Although clearly within McGraw and Fick's definition of cyberwar, one of the things that makes Stuxnet interesting in the context of cyber espionage is its attack strategy, best described by Ralph Langner in the military terms of "fire and forget". The attack was indeed targeted, but the attackers distributed the malware "untargeted" on the Internet and hoping that it would eventually reach the target and activate, which it did [11].

3.4. Duqu

The malware "Duqu" was discovered in October 2011. Named after the property where it stores stolen data in file names starting with "DQ". Although not as famous as Stuxnet, they are described by several authors as similar [3,13–15], and Symantec believes that the same teams are behind the two malwares. Contrary to Stuxnet, Duqu seems to have been developed primarily for espionage reasons [13,14].

Bencsáth *et al.* [13] was the first to detect and publish an extensive analysis on Duqu (based on the first technical report [16]), and stands out as one of the most cited sources. A summary of this work is also found in Bencsáth *et al.* [4]. The Symantec technical report "W32.Duqu" [14] also stands out as an extensive source of information on Duqu, although probably not peer reviewed; while Virvilis and Gritzalis [3] primarily reference the work of Bencsáth *et al.* for their analysis.

Duqu uses much of the same code as Stuxnet, but the payload is different [14]. From our understanding, the attack method was also different to that of Stuxnet, where Stuxnet applied a "fire and forget" strategy, it seems that in one case, Duqu was delivered via targeted e-mails [14]. Duqu spread using an MS Word document with an embedded zero-day kernel exploit as the dropper. When the target opened the Word document, the exploit took advantage of an unknown bug in the handling of embedded fonts in the Windows kernel [13]. Duqu does not self-replicate, but can likely be commanded by the attacker to replicate through network shares; infected targets can also serve as peers in a

peer-to-peer C&C system [14]. In the local network infections, the original infection serves as a proxy to communicate with the C&C server.

Upon successful infection, the attackers were able to download additional executables, including a keylogger that could be used to steal passwords, save screenshots and steal other types of sensitive information [13,14]. Symantec believes that the malware gathers information to prepare for future attacks.

The lifespan of a Duqu infection was 30 days, in which the malware erased itself from the infected machine. It has been found that the attackers had the opportunity to extend this time period [13]. All known C&C servers turned out to be proxies and were wiped clean hours upon breaking the news of Duqu's detection, so nothing was retrieved from these servers [14].

The malware was detected and/or reported in few countries, very geographically dispersed (mostly Europe and Middle East), with very few infections (around twenty [13]). There is little information available regarding the targets of Duqu. What we can say based on the available literature is that they were likely corporations that possessed high value information to the attackers. We can also say that the information the attackers sought was highly specific, based on the low amount of detected attacks. Some sources indicate that Duqu gathered information on PLCs and industrial control systems for further attacks [17], but we cannot find confirmation of this from more credible sources.

3.5. Flame

Flame, also known as SKyWIper and Flamer, was also discovered in 2012. With its 20 MB [18], Flamer is arguably one of the largest malware ever engineered, consisting of about twenty modules. Flamer is an information stealer that was found in targeted cyber-espionage attacks conducted in Middle Eastern countries. Although having a high level of sophistication, Flame does not have any strong connection to Duqu or Stuxnet [3]. There is some discrepancy in the literature when it comes to how long Flame had been active: the previously-mentioned work of Bencsáthsath *et al.* from CrySyS Labs [19] and Virvilis and Gritzalis [3] suggested Flame to have been around for 5–8 years before being detected; the latter specifies the malware being active from May 2007. This does not match with other sources, such as Kaspersky Labs, suggesting the malware was created no earlier than 2010 [20]. However, Kaspersky Labs estimates the likelihood of earlier versions of Flame being out in the wild before 2010 as extremely high.

There exists some peer-reviewed literature on Flame, e.g., [3,4,18], technical reports [19,21] and white papers [20]. Analyzing Virvilis and Gritzalis's work, we see that they are both based on [4,19,21], which therefore represent our main sources to describe Flame.

One of the attributes that made Flamer stand out is its previously mentioned size of 20 MB; in comparison, Stuxnet was about 500 KB [12]. There are several reasons for not making such a large malware, one of the main being that it takes a long time to upload and download the malware, which, in turn, inhibits propagation. This reinforces the notion of controlled spread in the sense that Flame does not seem to have been written as an infect-as-many-as-possible malware. From the data provided by Kaspersky [20], Flame appears to be less targeted than, e.g., Duqu, as Flame has more infections in a

specific area (the Middle East). Kaspersky Labs [20] writes that victims range from individuals to certain state-related organizations and educational institutions.

The initial infection and the dropper are undocumented in the reviewed literature. Bencsáth *et al.* [4] state that no dropper component of Flame was available to the research community and further speculate on the possibility of no dropper being identified at all. Kaspersky Labs [20] hypothesizes about the initial infection, but does not provide any data to support the initial claims.

Bencsáth *et al.* [4] explain the propagation mechanism: Flame targets computers with MS Windows platforms and has many options for propagation within infected networks. The malware has worm-like capabilities and spreads through local networks by exploiting different vulnerabilities—the same print spooler exploit and LNK exploit as Stuxnet—and can also spread through removable devices. Notably, Flame can also turn an infected computer into a proxy for Windows Update, in practice compromising the function, which has several implications, such as Flame distributing itself in the local network to computers looking for Windows updates and subverting a basic security function to distribute itself. Without getting too deep into the details of how the attackers managed that, Bencsáth *et al.* [4] explains, "the attackers created a private signing key and a fake certificate for the corresponding public signature verification key that appears to be a valid certificate issued by Microsoft". Flame also attempts to evade security functionalities of the host system through its rootkit functionalities; it also contains a module for identifying programs that may be hazardous to Flame [4].

The information stealing capabilities are found in Flame's modules. Some of the more significant are [4,20]: Flame can record audio from the internal microphone from interesting applications, e.g., wiretapping VoIP calls; the malware can also take screenshots from interesting applications, such as instant messages; it also has the capability to sniff network traffic, log keystrokes, extract geolocations from images and perform Bluetooth functions, such as reconnaissance, to map devices in the vicinity and send/receive commands and data.

Flame stores all gathered in an SQL Lite database, before being encrypted (several encryption methods), compressed (zlib) and sent to the C&C periodically. Several C&C existed around the world; Kaspersky [20] speculates on this being about 80 different domains [3,20] and more than 15 IP addresses being used by the malware to contact the C&C, giving Flame the appearance of a botnet. Kaspersky estimates 1000 victims.

The peer-reviewed literature does not say much as for the origins of Flame. CrySyS Labs have published a comparison with Stuxnet and Duqu that shows many differences [19]. CrySyS Labs further deems it plausible that there was a different team behind Flame, but does not exclude the possibility that multiple independent development teams worked for the same purpose based on the similar requirements. Kaspersky Labs later confirmed a connection between the two teams by discovering identical code [22]; moreover, we do not know if this connection has been confirmed by others.

We find more information on the origins of Flame in the secondary literature. In 2012, the Washington Post published an article regarding the origins of Flame [23], where they claim that Flame was part of "Operation Olympic Games", in which they write that the U.S. (NSA and CIA) and Israel's military jointly developed Flame to collect intelligence in preparation for cyber sabotage of Iran's nuclear program (similar objectives as Stuxnet). They further claimed that the main purpose of the malware was to map and monitor Iran's computer networks, in preparation for a cyber-warfare campaign.

3.6. GhostNet

In 2009, Deibert and Rohozinski (Information Warfare Monitor) published a report on a cyber-espionage network they called "GhostNet" [7]. In addition, the same authors in collaboration with the Shadowserver Foundation published a technical report on a large-scale cyber espionage [24]. This report is also rooted in GhostNet. These two reports are the main source of information on GhostNet in this review.

The background for the discovery of GhostNet was the investigations of allegations of Chinese cyber espionage against the Tibetan community [7]. Upon investigating the incidents, the authors found GhostNet to include more than the offices of the Dalai Lama and Tibetan targets.

The main attack vector was spear phishing, containing contextual crafted emails and attachments. An example of an email in [7] shows the attackers masquerading as a "campaings@freetibet.org", with an attachment named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc". Both the email and its attachment show the extent of both the knowledge and craft the attackers possessed in this case. This attachment (and its likes) contained exploit code that directs compromised computers to download a Trojan known as gh0st RAT, which allows for real-time control of infected machines. From the Deibert and Rohozinski report [7], we gather that GhostNet also had a component for automatic propagation, where the malware gathered email contacts and forwarded the spear phishing email to them. Because of this, the authors believe many of the GhostNet infections to be "collateral damage".

The RAT enables the attacker to conduct what we by now can define as classical information gathering functionalities; search for specific files, log key strokes, wiretap microphones and web cameras. The malware targets and mines contact information for further spreading. Commercial Internet access accounts located on the Hainan Island in China enable real-time control of infected systems. Gh0st RAT also allows for exfiltration of information through the C&C infrastructure. The authors found evidence suggesting that GhostNet's C&C infrastructure design was complex and tiered and designed to maintain persistence. The top tier of the infrastructure leveraged cloud-based social media services to compromise computers and directed them to a stable core of C&C servers located in China. While investigating GhostNet, the investigators discovered insecure web-based interfaces to four C&C servers. By scouting these servers, the investigators discovered a network consisting of at least 1295 compromised computers in 103 different countries. The main bulk of known GhostNet servers were located in China (70%). In addition to having the main core of C&C servers located in China, the authors also found clear links between GhostNet and the Chinese hacking community. In particular, GhostNet was traced back to two individuals living in the Chinese city Chengdu.

3.7. Mahdi

Madi, or Mahdi, is a malware discovered in 2012 and contains a somewhat religious theme; the name Mahdi translates to something close to Messiah, and one of the two discovered droppers also had a religious theme. It infiltrated computer systems in Iran and Middle-Eastern countries, notably Israel.

We did not find any peer-reviewed literature on Madi; however, Kaspersky Labs and Seculert have published one technical report [25] (primary source for review) and three detailed descriptions of the malware [26–28] (secondary sources for review).

Researchers [25] believe Mahdi to have been active since 2011. There are at least 800 known infections in the Middle East, with the largest part in Iran, the second largest being Israel and the third being Afghanistan. This differs from the previous reviews in this paper, whereas targeted malware infections in the Middle East for the most part did not infect systems in Israel. Kaspersky and Securelist [26] describe the initial attack method as spear phishing. There were two such schemes employed: (i) use of e-mail attachments that contain what the authors describe as attractive images and confusing themes embodied in PowerPoint slide shows. These slides had embedded the Madi RAT downloaders, which would be enabled to run if the user had "active content" enabled in their PowerPoint program. (ii) The second initial attack method also employed e-mail attachments. The attackers sent out executables that were masked with, e.g., "harmless".jpg and .pdf extensions, leading the user to believe they had received a data file and not an executable. This dropper exploited a known vulnerability in the way Windows handles Unicode character sets. There were no zero-day exploits or unknown attack vectors involved in the attacks. Both droppers delivered remote access Trojans (RAT) into the infected systems. The backdoors were written in Delphi, and the Kaspersky and Securelist authors comment on this to be expected from more amateur programmer or developers in a rushed project [26].

Similar to previously reviewed espionage malware in this paper, the information stealing components include keylogging, screenshots at intervals, screenshots at specific events (e.g., from interesting applications), update backdoor, record audio, retrieve data and retrieve disk structures [25]. Madi thoroughly monitors for several keywords on the infected systems, ranging from mail and social media accounts to chats, documents and pictures, from which to steal information [28]. The malware also has a function to search for removable drives, search through files and copy interesting files. Mahdi's targets included critical infrastructure companies, financial services and government embassies, located in Iran, Israel and other Middle Eastern countries [29].

Further, Kaspersky Labs [25] explain that each type of stolen data is stored in special folders in the server, while files are exfiltrated to the Base64-encoded C&C servers. Further, the authors also comment on this communication as being messy. The literature does not describe any self-propagation methods for the malware. Security analyst Aviv Raff from Seculert [29] provides intel on the possible origins of Mahdi based on an analysis of C&C communication, which contained strings of Farsi and dates in Persian format. The location of the earliest C&C server was traced back to Teheran in Iran, which points the suspicion to Iranians.

A quote from the Kaspersky and Securelist authors [26] about Mahdi: "... most of the components are simple in concept, but effective in practice. No extended 0-day research efforts, no security researcher commitments or big salaries were required. In other words, attacking this set of victims without 0-day in this region works well enough."

3.8. Shamoon

Shamoon is a modular malware that targets the MW NT operating systems. As previously mentioned, Seculert discovered the malware in 2012 following a large-scale attack on the Saudi Arabian oil company "Saudi Aramco", where the malware reportedly infected around thirty thousand of the company's PCs and caused large damage to their IT systems. Shamoon's most discussed function is the wiper,

which targets and deletes documents and master boot records. It is also possible that Shamoon stole information; however, this is not confirmed, and thus, our review of this malware is brief.

There exists peer-reviewed literature on Shamoon. Zhioua [30] dissects Shamoon from a technical perspective. Dehlawi and Abokhodair [31] have published a case study of the Shamoon malware incident, and there are technical reports/blogs from Symantec [32].

Zhioua [30] writes that Shamoon consists of three main components; namely a dropper, wiper and a reporter. We cannot find documentation on the initial infection. However, once inside the local network, Shamoon self-propagates through network shares. The malware drops the reporter and the wiper components in the systems folder, creates a task to execute itself and creates a TRK service to start itself whenever the OS starts. The malware infects the computers, deletes documents and the master boot record and then reports the deleted files to an unknown C&C.

Zhioua [30] describes the wiper component as in charge of the destructive tasks. Shamoon first writes a list of all files for wiping and then goes on to wipe. Particular targets are files within any folders from Microsoft Windows' "My Documents" and "desktop" folders. The files are wiped using a JPEG image of a burning American flag. Shamoon then moves on to wiping the master boot record and the active partition, thus creating havoc in the local system. The reporter sends the collected information back to the attacker, thus giving the malware espionage capabilities. However, these were, as the literature points to, likely only utilized to send lists of deleted files back to the attacker.

According to a news article [33], the hacker-group "Cutting Sword of Justice" has assumed responsibility for the Shamoon malware. The group stated that the attack targeted Saudi Aramco, because it supported "oppressive measures" in the Middle East, thus indicating a political motive.

3.9. Gauss

In 2012, Kaspersky Labs discovered Gauss while conducting an in-depth analysis of unknown components of the Flame malware. Kaspersky [34] describes Gauss as a cyber-espionage toolkit based on the Flame platform, which is designed to steal as much information about an infected system as possible. Gauss got its name because of the platform's naming convention, which includes modules named after famous mathematicians, such as "Gauss", "Lagrange" and "Tailor". Again, the known infections seem to center on information systems in the Middle East, this time Lebanon being the country with the most reported infections.

Kaspersky Labs published the initial technical report(s) on Gauss [34,35], which provides a detailed description of the malware. In academia, Bencsáth *et al.* [4] provide a short description of Gauss and describe it as a relative of Stuxnet, Duqu and Flame.

According to Kaspersky Labs [34], Gauss was wide-spread, with over 1600 individual computers infected in Lebanon alone, while Israel was the second most targeted country, with around 500 infections, which makes it far more widespread than the similar Duqu and Flame. Reviewing the literature, we could not find any documentation on the original attack vector. Kaspersky Labs did not find any self-replication functionality in the malware modules. The malware targets several versions of the MW platform, including 7, XP and Vista.

As an information stealer, Gauss has numeral capabilities and is designed to collect as much information about the infected system as possible [34]:

- Hijacks browser sessions and steals password, cookies and browser history (Gauss module);
- Collects information about network connections, processes, folders, BIOS, CMOS RAM, local network and removable devices;
- Infects USB drives with a spy module in order to steal information from other computers;
- Interacts with C&C server, uploading stolen information and download additional modules.

Bencsáth *et al.* [4] explain that Gauss targeted information from banking systems, social networks, e-mail and IM accounts. The malware also contains commands to intercept data required to work with several Lebanese banks [34].

As previously stated, Gauss has not been found to self-replicate. However, upon infecting USB drives, the malware hides a spy module on the removable device and steals data from the system(s) into which it is plugged. The module uses a .LNK exploit to achieve this. An unknown mystery also surrounds Gauss; its encrypted payload in the Gödel module, which has not yet been decrypted. The payload is delivered onto USB drives and tries to decrypt when plugged into new systems. It is encrypted by a strong cipher; the key is not stored in the malware, and the malware tries to compute the key using strings from the path variable or the file names in the "Program Files" folder [35]. The module remains dormant until it decrypts and executes under the right conditions; thus, we do not know what it targets or what the payload is. The clear conclusion we can draw from this is that Gauss is highly targeted. However, besides the Lebanese banking industry, we do not know the specifics.

Gauss also installs a font called Palida Narrow on infected computers [4]. The purpose of installing this font remains unknown, but it allowed the security companies to devise a Gauss detector that checked the system if Palida Narrow was installed on it (for details on the detector, see [4]).

3.10. BundesTrojaner

The BundesTrojaner is a malware that has been around for a while and has reached several versions. This review is of the German BundesTrojaner discovered by Chaos Computer Club (CCC) in 2011 [36], which is a confirmed state-sponsored Malware mainly in Germany [37], "Bundes" meaning federal or nationwide.

Kaspersky Labs [38] and CCC [36] have both published technical reports on BundesTrojaner (Case R2D2) as the primary sources reviewed for this malware. Gregory and Glance briefly discuss the malware in their book [39], and F-Secure [40] briefly discusses the malware on their blog.

CCC [36] claims that the aim of the malware is to conduct "lawful interception" of data from suspects. From reviewing the related literature, we assume that the Trojan was manually installed on the targets' computers, with the purpose of spying on them. We cannot see mentioned any means for self-propagation or exploits and, thus, assume that such a feature does not exist in BundesTrojaner. Researchers should treat the CCC report carefully, as the group has obvious political motivations.

F-secure [40] and Kaspersky Labs [34] writes that BundesTrojaner targets MW platforms where it installs a backdoor (RAT). The malware installs a keylogger that targets specific applications, namely common web browsers (excluding Google Chrome), VoIP services, messenger services, ICQ and others.

BundesTrojaner includes features to wiretap, record and take screenshots of Skype conversations. In addition, the malware can switch on the computer's webcam and receive remote updates that could be used to install and run other programs [39].

CCC [36] comments on the legal issues of the Trojan's two C&C servers, where one is in U.S. and one is in Germany, where the former is configured as a proxy to protect the German server, thus trafficking all collected information outside of German jurisdiction.

3.11. Political Espionage in Hong Kong

Li and Lai [2] have published a paper on a case study of malware for political espionage. We do not know if this attack is part of a campaign from the other APTs reviewed in this article. We therefore report this as a standalone campaign. The attack used the spear phishing method to compromise targets. Using individually-tailored e-mail and attachments, the attackers attempted to lure the victim into opening them, thus, obtaining control of the target's computer. In this particular case, the e-mail senders were forged to appear from trusted sources. There are two instances of spear phishing mentioned by the authors. Both had relevant e-mail topics. One contained a meeting invitation, and the malware itself was contained in an attached document named "agenda.doc". The other contained local news on an incident, where the attached file containing the malware was supposed to contain additional information on the incident. An analysis of the "agenda.doc" showed, in short, that it was a binary file that modified several existing files, injected a malicious DLL file into explorer.exe and eventually started its own process and initiated encrypted communication with a foreign IP (C&C Server), thus allowing the attackers to steal data from the victim. The malware was programmed to capture a screenshots once every 1000 milliseconds and to collect all file system information. Thus, the authors speculate that if the target computers had virtual keyboards, that the motives were more financial. However, stealing all file system information suggested additional ulterior motives. The authors believe that the attacks were launched by a group that has local political interests in Hong Kong. They also find similar attack patterns with GhostNet and APT1, but do not attribute the attacker further.

3.12. Careto

In early 2014, Kaspersky Labs discovered an espionage malware they named "Careto" after one of the malware variations. Careto was discovered because it attempted to exploit a known vulnerability in Kaspersky's security software to hide itself. Researchers found that different versions of this malware had likely been around for about seven years, and in that time, it had targeted a relatively low number of victims, but from a vast span of both industry and government. The main cluster of infections was discovered in Morocco and Brazil. It has also been commented that the attackers were likely Spanish-speaking, as Careto translates to "Mask".

We found two technical reports as sources for our review, one from Kaspersky Labs [41] and one from McAfee Labs [42]. Careto is described by Kaspersky Labs [41] as a cyber-espionage APT that is likely to have been operative since 2007. Kaspersky reports to have observed 380 unique victims in 31 countries. The main targets of Careto was described as government institutions, embassies, energy industry, private companies, research institutions, private equity firms and activists.

Careto is described as a highly advanced malware that contains several tools (modules) for attack, where one of the more noticeable is a customized attack on older security products [41]. McAfee Labs [42] describes two known distinct variations of Careto, where the first one ("SGH") uses a kernel mode rootkit and data interception component, as well as user mode components to access the captured data and upload it to the external server. The second variation, which is called "Careto", operates completely in user mode and is fully compatible with both the 32-bit and 64-bit MW 2000 operating systems and later [42]. Although the main target OS of the malware is MW, Kaspersky has also found evidence of Careto operating on different OSs, including Linux, iOS and Android. Further, both labs describe Careto as built from smaller modules, where each performs a particular function, including components whose capabilities include:

- Stealth rootkit to hide its files and network traffic;
- Sophisticated information-gathering tools to enumerate hardware and software configurations, including intercepting keystrokes, network and Wi-Fi traffic, Skype conversations, screenshots and to monitor file operations;
- User account information stealing;
- Theft of PGP and encryption keys;
- Uploading of user files;
- Downloading of new and updated malware.

In their report, Kaspersky Labs [41] reports that Careto's distribution relied on spear phishing e-mails with links to malicious websites, applying injection attacks and malicious plugins as the attack vectors. We cannot find anything about the malware self-propagating within networks upon infection and, therefore, assume that it does not.

We do not know the origins of Careto; it is according to Kaspersky Labs [41] likely to come from a Spanish-speaking country, due to its name and some pieces of the malware (e.g., a Spanish server name). However, as Kaspersky Labs points out, these language hints may have been put there to confuse investigators, and Spanish is the first language in several countries. The infections per country is more tangible in determining origins, as Morocco is an unusual target for a malware campaign, and the perpetrator is likely one of the handful countries with both political interest in Morocco and a capability to engineer such an advanced piece of malware. Another target of this campaign was located in Gibraltar, which, together with Morocco, lead Bruce Schneier to point to the suspect as Spain [43].

3.13. Icefog

First discovered in 2011, Icefog is one of the recent APTs. Icefog is according to Kaspersky [44] a tool for espionage that has mainly been detected in Japan and South Korea. The targets for the espionage campaign were government organizations, military and privately-owned companies. There are currently not many sources available for review on Icefog. The only source we discovered on this APT is the Kaspersky Labs technical report from 2013 [44].

According to Kaspersky Labs [44], the attacks initiated by Icefog rely on spear phishing mails, where the attackers attempt to trick victims into opening either a malicious attachment or a website. In some instances, the attachments were Microsoft Word documents containing pictures of semi-nude

women and an embedded Trojan. The Word Trojans exploited mainly two vulnerabilities (not zero-days) and were the most common attack method. When victims were tricked into visiting web pages, the attackers exploited java vulnerabilities to infect their computers. The Icefog group also attacked using the proprietary word processing application Hangui Word Processor (HWP files), which is used in the South Korean governmental sector. The malware was found mainly in Taiwan, Japan and South Korea, in governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, mass media, industrial and high-tech companies. The amount of infections identified using sinkhole servers was more than 430 unique victims [44]; however, Kaspersky emphasizes that this is only a fraction of the infected computers.

Kaspersky Labs further describes the malware functions upon infection: the malware establishes the ability to push and run commands on the infected system and performs some basic functions to identify and confirm the nature of the victim. It lists folders (e.g., "My Documents"), adapters and IP configurations and gets information about the victim and their network. After surveying this information and before they continue, the attackers make a decisions regarding if the target is genuine or not, as the attackers work to avoid virtual machines and fake victims. If the target seems real, Icefog is updated with additional maintenance, information stealing and retrieval components. There are several different versions of the malware, but in general, the information stealing components include dumping tools for passwords, hashes, Internet Explorer saved passwords and Outlook e-mail accounts and passwords. Kaspersky Labs documented thefts of Windows address books (.WAB), e-mails, documents (.HWP, .XLS and .DOC) and user account credentials. Further, the malware contain a "RAR"-program that is employed to compress data and split it into volumes (if the file is too big) before transmission to C&C. We did not find anything on self-propagation in the reviewed literature and therefore assume that Icefog does not self-propagate.

A notable aspect of Icefog is what Kaspersky describes as using hit and run tactics. The course of the attack is described: the attack group sets up a C&C using shared hosting (one to two months), creates a malware that uses the server, attacks the victim, infects it and communicates with the victim machine, before the shared hosting expires and the C&C disappears. Kaspersky has found some evidence for the origins of Icefog: such as internal messages/strings in Chinese, Chinese font in the C&C structure and Chinese IP addresses. There were also referrals to Chinese culture discovered in the code, which all points to Chinese hacker groups.

3.14. Dragonfly/Energetic Bear

In mid-summer 2014, a large-scale cyber espionage attack was mounted towards the western energy sector, where the APT named "Dragonfly" or "Energetic Bear" was named as the main culprit (hereby Dragonfly). According to Symantec [45], the attacks managed to compromise strategically important organizations for spying purposes and could have caused major damages if the group had sabotage capabilities open to them. The group had previously also targeted the aviation and defense industries.

Similar to Careto, this attack is so recent that we cannot find peer-reviewed sources on this attack. Symantec has published a technical report on the Dragonfly attacks [45]. Kaspersky Labs have also published a report on Dragonfly, although using the name Energetic Bear [46].

Dragonfly has, according to Kaspersky Labs [46], been active since late 2010 and has in this time span targeted several industries, such as industrial machinery, manufacturing, pharmaceutical, construction, education and IT. The group has, according to Symantec [45], been targeting aviation and defense industries (pre-2013) and more recently the energy sector, such as the energy industry, grid operators, major electricity generation firms, petroleum pipeline operators and industrial control system equipment manufacturers. The recent attacks on the energy sector targeted Europe and the U.S. Similar to other APTs reviewed in this paper, Dragonfly's tactics revolve around use of RAT, and the group possesses several attack vectors to deliver the malicious payload. Symantec reports them to, e.g., have been conducting targeted spear phishing from compromised accounts, watering hole attacks, injection attacks and compromising legitimate software packages to deliver the RAT. Dragonfly favors two malware tools, both targeting MW platforms: one known as "Havex", which is believed to be a custom malware engineered for or by the group, and found in most of the infections; the other, Trojan Karagany, was leaked in the underground market in 2010 and discovered in about 5% of the infections. The spear phishing e-mails were all distributed from a compromised Gmail account, targeted executives and senior employees and had a malicious pdf attachment. A watering hole attack is a method for attacking groups that are resistant to other forms of attack. The watering hole attacks targeted energy-related websites, where the attackers compromised the web pages and redirected the visitors to another compromised site where the visitors were infected by an exploit that dropped the RAT into their computer. Described by Symantec as the most ambitious attack was where the attackers had compromised legitimate packages from ICS/SCADA software producers. Three different providers were targeted, and malware was inserted into the software bundles they had made available for download on their websites [45].

The information-stealing modules maps the computer it infected (system ID, OS, user accounts, country, default browser, processes, proxies, email, list of files and folders, *etc.* [46]). Dragonfly also employs malware to do screen dumps, run shells, load DLLs and update. In addition, Dragonfly employs a password stealer module that has an embedded browser password decrypter and a network scanner that looks for SCADA software.

Kaspersky Labs [46] describes the C&C as maintained through a large network of hacked websites (219 unique domain names) that hosts malware modules, victim information and serve commands to infected systems. Most servers were found in the U.S. and Germany. The malware used in the dragonfly attacks contain lateral movement and second stage tools for propagation.

Kaspersky's analysis of the Dragonfly APT working hours have shown that the bulk of their operations takes place between 8 a.m. to 5 p.m., UTC + 3 time zone, suggesting eastern European origins. Besides this, the complexity and scale of the operations suggests Dragonfly having considerable resources at their disposal. We do not know the motivations behind these attacks, other than the obvious mapping and surveillance of infrastructure, which points in the direction of likely similar incentives as behind Duqu: to gather information on future potential targets.

3.15. Regin

Documentation on Regin was published in November 2014, although the APT had been identified in 2011 and been operative since 2008 [47]. Regin was discovered in a wide range of sectors; however, the

largest amount of infections was found by Symantec in Russia, Saudi Arabia, Ireland and Mexico. Most notable were the targeted attack of a merited French cryptographer and the compromise of the Belgian telecom provider Belgacom. Regin gained publicity due to being highly advanced and elusive.

The white papers published by Symantec [47] and Kaspersky Labs [48] are our sources for this case. The latter specifies that to describe Regin as a malware is not entirely accurate, as they describe it as a cyber-attack platform, meaning that post-infection Regin has a number of modules with different purposes.

Kaspersky [48] reports the infection vector to be unconfirmed, while Symantec reports Regin to have initially compromised targets applying watering hole and spear phishing attacks, although neither reports to have obtained the original dropper. Symantec also reports having found log files documenting infections through "Yahoo! Instant Messenger" using an unconfirmed exploit. Kaspersky reports the malware to propagate by copying itself to administrative shares and executing. Security personnel also discovered it on a USB stick belonging to one of the German Prime Minister Angela Merkel's staff [47].

Regin is a modular cyber-attack platform, with several capabilities. It contains the basic cyber-espionage tools for data collection that we have seen as common for most APTs, such as sniffing traffic, gathering information, stealing passwords, taking screenshots and gathering process and memory information. In addition, Regin also has low-level forensics capabilities, such as the ability to retrieve deleted files. A capability that makes Regin stand out is that it can sniff GSM base station controller (BSC) administration network traffic. This aspect is highlighted by Kaspersky Labs, whereas Regin gives its master a range of commands (see [48]) for information gathering from the infected BSC. This also relates to the Belgacom incident.

The C&C in Regin is complex. According to Kaspersky Labs, Regin relies on several drones within infected networks to communicate. These drones create a "virtual network" where the machines located on the border of the network act as routers by reaching out to the C&C and connecting the victim to attackers. Kaspersky suggests that this architecture is designed to enable deep access into networks and to restrict the traffic to the C&C. The origins of Regin are not known.

4. Taxonomy of Published Major Cyber Espionage Incidents

The main purpose of our taxonomy is to categorize and present different findings in a comprehensive manner. All of the results in this classification are compiled from the reviewed sources in this article. We have divided the taxonomy into two tracks, "impact" and "mechanism", where we categorize the high-level findings in the former and the technical findings in the latter. This way, geopolitical and international relations researchers can focus on the impacts, and malware/security experts can focus on the mechanisms.

In addition, as it is difficult to obtain confirmation of some of the information in the classification, such as APT origins, we only suggest likely origins. Together with "impact: alleged motivations" these two are most vulnerable to the attribution problem. We have decided to keep both of these categories in the taxonomy to make the problem of cyber industrial espionage and APTs visible. The results in the taxonomy shed light on the fact that both attackers and victims come from several parts of the world. While the "impact: alleged motivations" column sheds light on several of the underlying incentives for

conducting espionage and APT actions in cyberspace, underlying motivations for attacks are suggested in the reviewed literature, likely derived from knowledge about which industries and information the APTs targeted.

The amount of infections per malware listed in the mechanism taxonomy in most cases only represents a part of the picture, as the numbers from the reviewed literature often are obtained using sinkholes. It is close to impossible to map all infections for a malware, but the numbers give an indication of how widespread the malware was.

Following is a description of the high-level classifications in the taxonomy:

- Impact (see Table 2): (i)"country" categorizes which countries were attacked; (ii) "target institutions" describes the reported target(s) for the attack; this category will in general be incomplete, as there will always be unrecorded events; (iii) "alleged origins" contains the likely origins of the attackers, based on information gathered on probable origins of the attack; (iv) "alleged motivation" contains gathered information about the possible underlying factors for the espionage campaign, such as financial or political; lastly, (v) "data collection" in which we categorize the type of information that the malware steals.

Table 2. Review of impacts.

APT/Malware name	Year	Impact: Country	Impact: Targeted Institutions	Impact: Alleged Origins	Impact: Alleged Motivation
GhostNet	2009	India, Tibet (Dalai Lama), UN	Government (ministries of foreign affairs), embassies, business, academic computer systems	China	Political
Stuxnet	2010	Iran	Iran's nuclear program	USA, Israel	Delaying Iran Nuclear Program
Duqu	2011	International (Europe and Middle East)	Various international companies (undisclosed)	USA, Israel	Gather information on future targets (?)
BundesTrojaner	2011	Germany	German citizens/suspects	German Government	Law enforcement
Icefog	2011	Japan and South Korea	Government institutions, military contractors, maritime, telecom, industrial/high-tech companies and mass-media.	Chinese Speaking hacker group	Unknown
Political Espionage	2011	Hong-Kong (China)	High-ranking politicians	Likely regional actor	Political and/or financial
Mahdi	2012	Iran, Israel, Afghanistan, and Middle East	Critical infrastructure companies, financial services, government embassies	Iranian	Unknown
Shamoon	2012	Saudi Arabia, Saudi Aramco	Energy industry (oil)	Cutting Sword of Justice/ Arab youth group	Sabotage
Gauss	2012	Lebanon and Middle East	(Lebanese) banking industry	USA, Israel	Unknown
Flame	2012	Middle East, discovered internationally	Governmental Organizations, Educational institutions and private individuals	USA (CIA, NSA), Israel	Gather information on Iran's nuclear program (?)
APT1	2006 2013	International	Major industries	Chinese Military, PLA Unit 61398	Financial, competitive
Red October	2013	International	International embassies and governments (main targets)	Russian hacker group (?)	Political
Careto	2014	International	Government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists.	Spanish-speaking country	Unknown
Dragonfly/Energetic Bear	2014	Europe and North America	Aviation, defense and energy industries	Eastern Europe	Intelligence gathering
Regin	2011, Disc 2014, Rep	Major: Russia, Saudi-Arabia, Minor: Pakistan, Austria, India, Afghanistan, Iran, Belgium, Ireland, Mexico	Telecom operators, government institutions, multinational political bodies, financial institutions, research institutions, hospitality, crypto-researchers	GCHQ?	Intelligence gathering, facilitate other types of attacks

- Mechanism (see Table 3): (i) "dropper" contains a high-level description of the initial attack vector, how the system was initially compromised and the tools involved in establishing control over the system; (ii) "automatic propagation" describes any malware features present for self-propagation; (iii) "target OS/apps" describes which operating systems and applications the APT/malware targeted; (iv) "infection rates" describes the reported infections of each malware; (v) "mechanism: estimated complexity" gives our subjective rating of campaign complexity from our point of view based on the reviewed literature, within the subjective scale high-medium-low.

Table 3. Review of technical mechanisms. RAT, remote access Trojan; PLA, People's Liberation Army.

APT/Malware name	Mechanism: Dropper	Mechanism: Automatic Propagation	Mechanism: Target OS/Apps	Mechanism: Estimated Infection Rates (Known)	Mechanism: Estimated Complexity
GhostNet	Spear phishing, drive by attacks, gh0st RAT	Propagates through Email contact lists	MS Windows/Word	1295 infections	Medium
Stuxnet	USB stick, zero day	USB stick, zero day, self-propagation in LANs	MS Windows, Industrial control systems	Unknown	High
Duqu	Spear phishing e-mails, zero day, RAT, zero day	No	MS Windows/Word	Around 20 unique infections	High
BundesTrojaner	Manually delivered, RAT	No	MS Windows	Few individuals	Low
Icefog	Spear phishing, e-mail attachments and websites, RAT	No	MS Windows/Word, Hangui Word Processor	More than 430 unique infections	High
Political Espionage	Spear phishing, e-mail attachments, RAT	Unknown	MS Windows/ ord	Few	Medium
Mahdi	Spear phishing, e-mail attachments, RAT	No	MS Windows/PowerPoint, jpg, PDF viewer	800 in the Middle-East	Low
Shamoon	Unknown (possibly insider attack)	Through network shares	MS Windows NT	30,000 infections in Saudi Aramco	Medium
Gauss	Unknown, RAT	not found	MS Windows	Over 2000 infections	High
Flame	Unknown, RAT	Several self-propagation methods	MS Windows	About 1000 unique infections	High
APT1, PLA Unit 61398	Spear phishing, e-mail attachments, RAT	No	MS Windows	141 organizations, spanning 20 industries, 900 servers, 849 IP addresses	High
Red October	Spear phishing, e-mail attachments, RAT	Not found	MS Windows/Word and Excel and PDF viewer	Over 300 unique systems.	High
Careto	Spear phishing w/ links to website, RAT	No	MS Windows, Linux, iOS, Android	380 infections/31 countries	High
Dragonfly/Energetic Bear	Spear phishing, email attachments, watering hole, spam campaigns, compromising 3rd party software components	Lateral movement and second stage tools	MS Windows/iExplorer PDF documents 3rd party servers	Unknown	High
Regin	Spear phishing, watering hole, RAT (Unconfirmed)	Unconfirmed	MS Windows platforms and domain controllers, GSM base station controllers	Unknown	High

5. Common Factor Analysis of Cyber Espionage Attacks

In this section, we analyze and discuss common factors that can be derived from case studies and the taxonomy.

5.1. Impact

Upon reviewing this literature, it becomes apparent that cyber espionage and sabotage will continue to evolve in complexity. A classic example of the attack-defense battle, where the two continuously evolve to gain the upper hand, is the development of the "watering hole" attack as an alternative way of compromising organizations with robust security.

Our review also shows that several APT attacks occur in the Middle East. However, we have found documentation of attacks occurring on all continents (except Australia), making APTs a global problem. Although our information on the origins of APTs is not as solid, we see that origins vary and that several groups with different geographical origins have advanced capabilities.

We also see a clear tendency that many APT are well resourced, suggesting government support (such as APT1 [9]). The attackers targeting SCADA and other industry control systems also provides an extra worry and chilling factor in this arms race, as this is where equipment failure bears the biggest risk of human loss. We have also seen how cyber-attacks can be devastating; by wiping 30,000 computers, the Shamoon attack devastated the systems of Saudi Aramco, but luckily did not result in loss of human life. The scale of some of these operations, APT1 likely being the biggest known, also witnesses this being big business. On the underlying motivations for conducting cyber espionage, we see different incentives, ranging from political incentives (GhostNet and Red October), to financial motivations (APT1), to hostility (Stuxnet).

We can also say something about "standard" infection procedures and information stealing capabilities in malware, as several of the reviewed APT1 shared approaches and capabilities. The attacker obtain the initial foothold using social engineering tactics to get a RAT into the victims system. Further, on information stealing capabilities, several functions seem standard: keylogger, screen captures, upload/download files and components, password stealing, directory indexing and mapping files with predetermined parameters (e.g., .pdf or .docx).

5.2. Mechanisms

From our taxonomy, we see that the human factor is ever the target for targeted espionage. Out of the reviewed attacks where we know the attack vector, all relied on social engineering tactics together with technology, tricking users to either visit a website, open an email attachment or to run a USB stick, the most prevalent being spear phishing. Attackers also employ "passive" attacks that rely on patience, Stuxnet being the example; where the malware was distributed widely in the hopes of it actually reaching its target (Iran's uranium centrifuges), showing that the general means of propagation can be applied to conduct targeted attacks. Another example is watering hole, where the attackers make a guesstimate of which websites the target will visit and concentrate their efforts towards these instead. Having infected the websites, the attackers "sit back" and wait for the target to arrive. Upon infection, we found that most attacks installed a remote access Trojan (RAT) with information stealing capabilities. The Dragonfly attacks showed that it is possible to compromise third party software before delivery and to have the malware delivered as a part of the product.

The results also show that self-propagation mechanisms are not common in APT malware. This is likely due to the attackers wanting to keep a tight leash on their malware to keep infection rates under

control, to remain covert and operational as long as possible. Several APTs, e.g., Careto and Duqu, had built-in self-wiping capabilities, which were triggered hours after the announcement of discovery. Thus, traces of the APT disappeared from the Internet, which, together with no one so far claiming responsibility, shows a professionalism and a desire to remain covert from the APTs.

We found that most of the initial APT attacks targeted MW platforms. Only Careto targeted other operating systems, such as Linux, iOS and Android. It is very likely that, once inside the networks, the more sophisticated APTs also took control over other platforms, but MW platforms were the target of the initial attacks. We also saw this from the exploits employed by the different APTs. In addition, Regin had capabilities for spying on GSM base station traffic.

Automatic self-propagation mechanisms seem to be uncommon among APT malware, but this does not hinder the attacker from manually executing a controlled spread of the infection once inside the network. There were also strong similarities in how information on attackers scan for information on compromised systems; upon infection, we see several malwares having modules that scan for file extensions in the local file system. It depends on the malware whether or not these modules are present from the beginning or downloaded as an addition later. From our review, we see that e-mails, general Microsoft documents and pdfs are interesting to collect, but also more specific information on the computer is targeted, such as Windows address books (.WAB), user account credentials, pictures and other valuables. The Mahdi malware was probably the least sophisticated of the reviewed malware, but it had very thorough functionality for scanning and monitoring infected systems, keeping an eye on webmail, social networks and instant messaging accounts, installing a keylogger, taking screen captures and even recording sound. This is not "Mahdi-only" capabilities, as we consider all of this common functionality of most infostealers. There are small deviations from this "norm", such as more sophisticated attacks like Careto going for, e.g., VPN configs and SSH keys, and APTs, like Dragonfly, targeting specific infrastructure. However, the targeted information and the basic methods for obtaining that information remain similar.

One common way of extracting information from the host is to pack and encrypt all stolen data into a .zip or .rar archive stored locally. The attacker downloads it from the infected machine, often through compromised external servers acting as proxies, to hide the attacker's identity. Having several geographically dispersed systems acting as proxies is also beneficial for the attacker, as it hinders investigations. This problem lies in international politics; if the attackers move through several adversarial nations, their track will be hard to follow, as there is often no cooperation or data exchange agreements between these kinds of nations.

From our review, we also see advanced kill and/or wipe mechanisms being present in more sophisticated APT malware, e.g., Duqu was wiped from infected systems hours upon officially being discovered. This functionality makes it harder for malware analysts to obtain samples of the malware and makes the investigation process more difficult.

5.3. General Phases of a Malware Espionage Attack

From the reviewed literature in this article, we have summarized the average malware industrial espionage attack in six phases.We have generalized the phases from the APT1 attack pattern presented

by Mandiant [9] to fit the attacks we have reviewed in this article. We make the claim that these six phases are present in most malware-based APT attacks:

(1) Reconnaissance phase: The attacker does an in-depth recon of the target and gathers information that has the potential of being used in the coming attack. For the social engineering part of the attack, this information includes names of employees and managers, meeting schedules, in general anything that can help the attacker design an attack to trick humans, e.g., spear phishing email, watering hole attack or to trick someone to run an infected USB memory drive. This phase also includes gathering of information about the target's systems and technical vulnerabilities. This phase requires resources within both technical security expertise and industry knowledge, but reconnaissance functions can to partially be automated.

(2) Preparation phase: Making use of the gathered information, the attacker(s) design their attack. This attack usually has an element of social engineering and a technical element, such as an email to a certain individual containing a document with an embedded zero-day exploit. The designed attachment is such that it increases the probability of the recipient opening it. However, the attack can also be a more passive attack, such as watering hole or the "fire and forget" strategy employed by Stuxnet. The watering hole is a way of infecting organizations that have proven resilient towards other types of attack.

For narrowly-targeted attacks, this development phase requires a considerate amount of both time and resources and knowledge of human psychology, and language and culture are crucial when the attack involves aspects of social engineering. Expert knowledge of the industry and its systems is required to be able to gather the targeted information, e.g., if the target is industrial control systems, while considerable engineering and programming skills is required to program the malware.

(3) Attack phase: The attackers launch their attack and attempt to infect the targets. Upon successful infection, the attacker can scan the network for other vulnerable machines and/or services to further increase access to the system and escalate privileges. Additional modules are also deployed for intelligence gathering. It seems seldom for automatic self-propagation mechanisms to be present in APT malware (exceptions to this are, e.g., GhostNet, Stuxnet and Flame), so propagation is likely to be conducted under the control of the attacker to maintain stealth. There has also been reports of APTs compromising non-sensitive servers within the target country to stage the attack. This is part of an attack strategy to avoid detection, as communication between domestic institutions will look like legitimate traffic.

(4) Information collection phase: The attacker scans the infected machine(s) and gathers information. Many malwares come with a predetermined set of file types to look for on the infected system, such as Microsoft Office documents, pdfs and pictures. Several malwares also come with functionalities for wiretapping VoIP conversations, taking screen shots and logging key strokes. This phase requires the attackers to know what information to look for and to maintain stealth. It also requires knowledge of the local language.

(5) Data exfiltration phase: The stolen information is packed into archives and usually encrypted on the infected system. The information is usually transmitted via several proxies to hide the identity of the attacker. In other instances, we see the information being downloaded and stored on compromised Internet servers.

(6) Maintenance and wiping phase: This is the phase where the attacker maintains control over the infected systems and monitors for new valuable information to steal. We also saw from several advanced malwares that they contained a self-wiping function that was remotely controlled by the owners. This function, usually triggered within hours of the initial discovery of the malware, wipes the malware infection from the victim's systems and deletes as many traces as possible of the infection.

6. Discussion

What became apparent when conducting this work was that there is a lack of available peer-reviewed literature on recent cyber espionage involving malware. The main bulk of the literature on APT malware analysis comes from technical reports provided by security companies, and we found that much of the peer-reviewed literature referenced these technical reports. This is not surprising, as security vendors make business out of this and allocate resources accordingly.

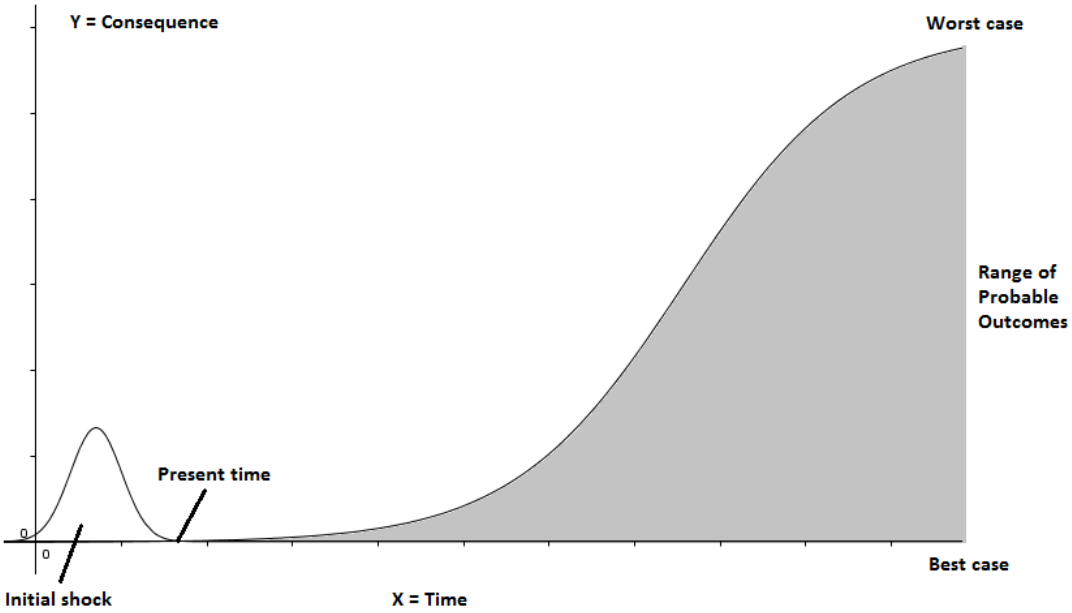

Figure 1. The risk perception of an APT-attack in terms of time and consequence.

There seems to be a lack of interest in cyber espionage in academia and maybe in industry. With the APT1-report in 2013, Mandiant put state-funded cyber espionage on the agenda, but is this a problem that needs to be taken seriously? According to Nassim N. Taleb's Black Swan [49], humans have a hard time depicting future events that deviate from past experiences. The real consequences of successful cyber espionage attack are likely to occur so far into the future, that we may have a hard time to imagine and accept them and, thus, to risk manage them. In comparison, the consequences of a denial of service attack are much more tangible; we get downtime on servers, angry customers and loss of revenue. It is more difficult to imagine events from cyber espionage, as we have likely never experienced them before, and there are many possible outcomes from such an event. We have attempted to capture this aspect in Figure 1, which depicts the consequences and ranges of outcomes from an espionage attack. The initial shock describes detection and handling the incident, while the gray area illustrates the range of probable

outcomes, from benign to severe. The amount of uncertainty related to the consequences of many APT attacks is so large that it is hard to both envision and handle. However, the consequences are real: Stuxnet was the end-result of a carefully-planned and executed espionage campaign. In addition to the serious undertone of cyber espionage attacks directed at critical infrastructure, like the 2014 Dragonfly group attacks, with Stuxnet came a general awareness about the possibilities within cyber-attacks, and Norwegian security analyst Frode Hommedal (Essay *Dance like a Dragonfly, sting like a Bear*, 2014) suggests that it is no longer far-fetched to consider the possibility that APTs are mapping vulnerabilities in critical infrastructure to stockpile digital warheads.

Another possible reason for lack of interest is difficulty in detection. Targeted cyber espionage attacks often use complex and unknown mechanisms that are hard to detect and are, compared to other cyber-attacks, very rare, which makes signature-based detection inefficient. Actively looking for an APT will often be like looking for a needle in a haystack. After obtaining a malware sample from APT, it is likely to require substantial resources to reverse engineer it. As the programmers are often experts and want to hide their identity, so they employ obfuscation and crypto mechanisms to hide the malware.

An approach for raising more awareness regarding the APT issue is performing a detailed study of both monetary and political impacts. This would concretize the consequences of APT issues in societal context, although data collection in this area is hard due to a variety of reasons. Primarily, revealing data on loss incidents can be embarrassing to companies and damaging their reputation.

7. Conclusion

In this article, we have presented a taxonomy of both APT mechanisms and impacts from cyber espionage. The taxonomy sheds light on the different aspects of a growing problem and shows with clarity that cyber espionage knows no boarders. On a technical level, we get a view of APT behaviors, infection rates, target platforms and general attack patterns. On a geographical level, we see the likely targets and origins of attacks, e.g., the historically unstable Middle East is also an attractive target in cyberspace.

The point is that we can obtain a lot of information compiling these types of datasets. With our taxonomy, we have compiled and classified much of the existing information on major cyber espionage attacks, including malware. Knowledge obtained from this taxonomy has the potential to help us defend better against cyber espionage and will assist scholars in both learning and teaching about the subject. However, the dataset compiled in this article requires further expansion and, thus, requires more research. Constructing a comprehensive and open dataset would require collaboration between both the research and professional community, which could further facilitate the geopolitical and/or technical analysis and synthesis of the role of malware in cyber espionage.

Acknowledgments

The author recognizes the contributions made by Yi-Ching Lao, Han-Teng Lao, Andrey Shalaginov, Stephen Wolthusen, Einar Snekkenes and the anonymous reviewers. The author also recognizes the sponsorship made by the COINS Research School for Information Security.

Conflicts of Interest

The author declares no conflict of interest.

References

1. TechTerms.com, Malware Definition. Available online: http://techterms.com/definition/malware (accessed on 12 May 2014).
2. Li, F.; Lai, A.; Ddl, D. Evidence of Advanced Persistent Threat: A case study of malware for political espionage. In Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, PR, USA, 18–19 October 2011; pp. 102–109.
3. Virvilis, N.; Gritzalis, D. The big four-What we did wrong in advanced Persistent Threat detection? In Proceedings of the 2013 Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg, Germany, 2–6 September 2013; pp. 248–254.
4. Bencsáth, B.; Pék, G.; Buttyán, L.; Félegyházi, M. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet* **2012**, *4*, 971–1003.
5. McGraw, G.; Fick, N. Separating Threat from the Hype: What Washington Needs to Know About Cyber Security. *Am. Cyber Future Secur. Prosper. Inf. Age* **2011**, *2*, 43–54.
6. Felt, A.P.; Finifter, M.; Chin, E.; Hanna, S.; Wagner, D. A survey of mobile malware in the wild. In Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Chicago, IL, USA, 17–21 October 2011; pp. 3–14.
7. Deibert, R.; Rohozinski, R. *Tracking GhostNet: Investigating a Cyber Espionage Network*; Technical report; Information Warfare Monitor: Toronto, ON, Canada, 2009.
8. *Beyond the Breach—Mandiant Report*; Mandiant: Alexandria, VA, USA, 2014.
9. *APT1 Exposing One of China's Cyber Espionage Units–Mandiant Report*; Mandiant: Alexandria, VA, USA, 2013.
10. GReAT. *Red October—Diplomatic Cyber Attacks Investigation*; Technical report; Kaspersky Labs: Moscow, Russian, 2013.
11. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51.
12. Falliere, N.; Murchu, L.O.; Chien, E. *W32. Stuxnet Dossier*; Technical report; Symantec Corporation: Cupertino, CA, USA, 2011.
13. Bencsáth, B.; Pék, G.; Buttyán, L.; Félegyházi, M. Duqu: Analysis, detection, and lessons learned. In Proceedings of the ACM European Workshop on System Security (EuroSec), Bern, Switzerland, 10 April 2012.
14. *W32.Duqu—The Precursor to the Next Stuxnet*; Symantec Corporation: Cupertino, CA, USA, 2011.
15. Fidler, D.P. Tinker, Tailor, Soldier, Duqu: Why cyber espionage is more dangerous than you think. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 28–29.
16. Bencsáth, B.; Pék, G.; Buttyán, L.; Félegyházi, M. *Duqu: A Stuxnet-like Malware Found in the Wild*; CrySyS Lab: Budapest, Hungary, 2011.
17. Cherry, S. Sons of Stuxnet. Available online: http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet (accessed on 13 May 2015).

18. Munro, K. Deconstructing Flame: The limitations of traditional defences. *Comput. Fraud Secur.* **2012**, *2012*, 8–11.
19. Bencsáth, B.; Buttyán, L.; Félegyházi, M.; Pék, G. *sKyWIper (aka Flame aka Flamer): A Complex Malware for Targeted Attacks*; CrySyS Lab: Budapest, Hungary, 2012.
20. Gostev, A. The Flame: Questions and Answers. Available online: https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ (accessed on 13 May 2015).
21. Walter, J. *"Flame Attacks": Briefing and Indicators of Compromise*; Technical report; McAfee Labs: Santa Clara, CA, USA, 2012.
22. GReAT. *Resource 207: Kaspersky Lab Research Proves That Stuxnet and Flame Developers are Connected*; Technical report; Kaspersky Labs: Moscow, Russian, 2013.
23. Nakashima, E.; Miller, G.; Tate, J. US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. Available online: http://cyber-peace.org/wp-content/uploads/2013/06/U.S.pdf (accessed on 13 May 2015).
24. Adair, S.; Deibert, R.; Rohozinski, R.; Villeneuve, N.; Walton, G. *Shadows in the Cloud: Investigating Cyber Espionage 2.0.*; A joint report of the Information Warfare Monitor and Shadowserver Foundation, Toronto (2010); Available online: https://www.f-secure.com/weblog/archives/Shadows_In_The_Cloud.pdf (accessed on 13 May 2015).
25. Brulez, N. *The "Madi" infostealers—A detailed analysis*; Technical report; Kaspersky Labs and Seculert: Moscow, Russian; Santa Clara, CA, USA, 2012.
26. GReAT. *The Madi Campaign–Part 1*; Technical report; Kaspersky Labs and Seculert: Moscow, Russian; Santa Clara, CA, USA, 2012.
27. GReAT. *The Madi Campaign—Part 2*; Technical report; Kaspersky Labs and Seculert: Moscow, Russian; Santa Clara, CA, USA, 2012.
28. Brulez, N. *Madi is Back—New Tricks and New Command & Control Server*; Technical report; Kaspersky Labs and Seculert: Moscow, Russian; Santa Clara, CA, USA, 2012.
29. Raff, A. Mahdi—The Cyberwar Savior? Available online: http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html (accessed on 13 May 2015).
30. Zhioua, S. The Middle East under Malware Attack Dissecting Cyber Weapons. In Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops (ICDCSW), Philadelphia, PA, USA, 8–11 July 2013; pp. 11–16.
31. Dehlawi, Z.; Abokhodair, N. Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics (ISI), Seattle, WA, USA, 4–7 June 2013; pp. 73–75.
32. Symantec. *The Shamoon Attacks*; Technical report; Symantec Corporation: Cupertino, CA, USA, 2012, updated 2014.
33. Bumgarner, J. *Decapitating Saudi Aramco with the Sword of Justic*; Available online: http://www.defenceiq.com/cyber-defence/articles/decapitating-saudi-aramco-with-the-sword-of-justic/ (accessed on 13 May 2015).
34. GReAT. *Gauss: Abnormal Distribution*; Technical report; Kaspersky Labs and Seculert: Moscow, Russian; Santa Clara, CA, USA, 2012.

35. GReAT. *Gauss: Nation-state Cyber-surveillance Meets Banking Trojan*; Technical report; Kaspersky Labs: Moscow, Russian, 2012.
36. *Chaos Computer Club Analyzes Government Malware*; Chaos Computer Club: Hamburg, Germany, 2011.
37. Sullivan, S. *More Info on German State Backdoor: Case R2D2*; Available online: https://www.f-secure.com/weblog/archives/00002250.html (accessed on 13 May 2015).
38. Werner, T. Federal Trojan's got a "Big Brother". Available online: https://securelist.com/blog/research/31349/federal-trojans-got-a-big-brother-17/ (accessed on 13 May 2015).
39. Gregory, M.A.; Glance, D. Cyber Crime, Cyber Security and Cyber Warfare. In *Security and the Networked Society*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 51–95.
40. Hypponen, M. Possible Governmental Backdoor Found (case R2D2). Available online: https://www.f-secure.com/weblog/archives/00002249.html (accessed on 13 May 2015).
41. GReAT. *Unveiling "Careto"—The Masked APT*; Technical report; Kaspersky Labs: Moscow, Russian, 2014.
42. *Careto Attack—The Mask*; Technical report; McAfee Labs: Santa Clara, CA, USA, 2014.
43. Schneier, B. "The Mask" Espionage Malware. Available online: https://www.schneier.com/blog/archives/2014/02/the_mask_espion.html (accessed on 13 May 2015).
44. GReAT. *The "Icefog" APT: A Tale of Cloak and Three Daggers*; Technical report; Kaspersky Labs: Moscow, Russian, 2013.
45. Symantec. *Dragonfly: Cyberespionage Attacks Against Energy Suppliers*; Technical report; Symantec Corporation: Cupertino, CA, USA, 2014.
46. GReAT. *Energic Bear—Crouching Yeti*; Technical report; Kaspersky Labs: Moscow, Russian, 2014.
47. Symantec. *Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance*; Technical report; Symantec Corporation: Cupertino, CA, USA, 2014.
48. GReAT. *The Regin Platform: Nation-State Ownage of GSM Networks*; Technical report; Kaspersky Labs: Moscow, Russian, 2014.
49. Taleb, N.N. *The Black Swan: The Impact of the Highly Improbable*, 2nd ed.; Random House: New York, NY, USA, 2010.