IntechOpen Journals

AI, Computer Science and Robotics Technology

RESEARCH PAPER

Feature-based Systematic Analysis of Advanced Persistent Threats

Manuel Miguez and Bahman Sassani (Sarrafpour)*

Department of Computing and Information Technology, UNITEC Institute of Technology, Auckland, New Zealand

*Corresponding author. E-mail: bsarrafpour@unitec.ac.nz

Abstract

Advanced Persistent Threats (APT) and Targeted Attacks (TA) targeting high-value organizations continue to become more common. These slow (sometimes carried on over the years), fragmented, distributed, seemingly unrelated, very sophisticated, highly adaptable, and, above all, stealthy attacks have existed since the large-scale popularization of computing in the 1990s and have intensified during the 2000s. The aim of attackers has expanded from espionage to attaining financial gain, creating disruption, and hacktivism. These activities have a negative impact on the targets, many times costing significant amounts of money and destabilizing organizations and governments.

The resounding goal of this research is to analyze previous academic and industrial research of 72 major APT attacks between 2008 and 2018, using 12 features, and propose a categorization based on the targeted platform, the time elapsed to discovery, targets, type, purpose, propagation methods, and derivative attacks. This categorization provides a view of the effort of the attackers. It aims to help focus the design of intelligent detection systems on increasing the percentage of discovered and stopped attacks.

Keywords: advanced persistent threat, APT, targeted Attack, TA, APT features, AI, APT categorization, cyber espionage, cyberattacks

Citation
Manuel Miguez and Bahman Sassani (Sarrafpour) (2023), Feature-based Systematic Analysis of Advanced Persistent Threats. *AI, Computer Science and Robotics Technology* 2023(2), 1–41.

DOI
https://doi.org/10.5772/acrt.21

Published
22 May 2023

1. Introduction

Various reports and news articles show that cyberattacks are more ambitious than ever. Their landscape complexity has increased with the participation of hacktivists and nations/states with the intent of damage, defacement, and espionage, as well as the traditional cyber criminals looking for financial gain and economic espionage [1–4].

During 2016, over 200 new ransomware strains appeared, encrypting a wide range of files and databases and asking for bitcoin payments for the encryption keys. During 2017, the focus shifted to coinmining, which requires very little code to start using the resources of the targeted computers, and supply chain injections, where malicious software is placed within valid updates and updates sites allowing them to enter almost undetected to well-protected targets. At the same time, the introduction of Ransomware-as-a-Service (RaaS) via several open-source tools in the Dark Web has aided the proliferation of these attacks. Business Email Compromises (BEC) are still present, a reduced number in 2016, they increased in 2017; these are targeting specific high-value users with an e-mail that would introduce backdoors, known as spear-phishing and whaling and then exploiting legitimate networks and scripting tools at hand to produce the actual attack either as malware, ransomware or simple scams. From a historical perspective, cyber threats mainly target the weakest link in cyberspace. From buffer overflow, command injection, and Denial of Service (DoS) targeting Operating Services (OS) during 2001–2005 to Heap Spraying and Code injection and targeting Web applications and services between 2006–2010 to Social Engineering such as Phishing and APT with the popularity of the Internet, targeting the users.

TA and APT represent the third evolutionary wave of attacks targeting humans, related organizational factors, and the cognitive aspects of cybersecurity in general, the weakest link in cybersecurity. A detailed discussion of the techniques used in TA, such as various phishing attacks, is complex and involves cognitive psychology and behavioral foundations, including cultural factors, human capacity, temporal, ethical, and mindset, which is beyond the scope of this paper.

Another area where attacks keep appearing is in Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), where many existing and upcoming platforms and the ever-more present Internet of Things (IoT) have vulnerabilities that could allow remote control due to poor or limited security, the number of these attacks has gone from 6000 in 2016 to 50,000 in 2017. The latest area to see an increase in malicious activity are the mobile platforms which have gone from 17,000 attacks in 2016 to 27,000 in 2017 [1–4].

A group of attackers can mount a sophisticated and systematic malicious attack aimed at a selected organization divided into several stages over long periods of time, applying different methodologies with the intent, and typically succeeding, of being undetected by existing defense mechanisms. These attacks are known as Targeted Attacks (TA), and when backed by nations or states, they are known as Advanced Persistent Threats (APT). Although APT is an intensified variation of TA, the former is the most commonly known name, and it will be used in this work [5–9].

This paper aims to summarize attacks discovered between 2008 and 2018, analyze their features, and categorize them. The analysis of these categories will provide a view of the attackers' focus and aims to deliver samples that would help train detection systems. Rest of this paper is organized as follows: Section 2 introduces

Related Works, Section 3 discusses the Methodology, Section 4 presents the Evolution of APT between 2008 and 2018 and introduces the APT Features Analysis, Section 5 concludes this paper, and Appendix presents a summary of the known campaigns used in this paper.

2. Related work

The first Targeted Attacks, as we define them today, were described in 2005 by the U.K. National Infrastructure Security Co-ordination Centre (UK-NISCC) and the U.S. Computer Emergency Response Team (US-CERT) [10]. In 2006 the U.S. Air Force (USAF) coined the term APT used today to cover attacks on large companies with data and cutting-edge knowledge as well as the traditional military, government, academia, research, and financial targets. However, espionage-motivated attack campaigns are said to have started in the 1990s focusing on military objectives, and in the early 2000s, governmental attacks became more common [11]. After 2010, a significant increase in the complexity of the attacks was seen, using multiple vectors and exploiting the social media phenomenon heavily for propagation and gaining the initial foothold [12, 13].

Ussath *et al.* [14] reviewed 22 attacks focusing on three phases of the well-known Cyber Kill Chain model as proposed by Hutchins *et al.* [10] and the Mandiant Model [15, 16]. The phases selected by the authors are (a) initial compromise, (b) lateral movement, and (c) command and control. The authors' descriptions are based on the attackers' techniques shown in Table 1. It is important to note that the selected attacks were all Windows-based. The authors submit that the (a) initial compromise is commonly made by using spear-phishing where 15 campaigns used attachments and eight used URLs; four attacks used watering-holes; and attacks to web servers and the usage of contaminated storage media were infrequently used. In (b) the lateral movement, nine campaigns used standard Operating System (OS) tools; seven attacks used hash and password dumping tools to collect account credentials; four attacks exploited vulnerabilities, but no zero-day exploits were used in this stage. In (c) command and control, the authors found that 15 attacks used HTTP or HTTPS protocol to communicate with the external command and control servers; five campaigns used custom protocols; nine attacks used a variety of protocols such as FTP or RDP. Also, the authors found that many campaigns use multiple methods during different phases, making them harder to detect.

Lemay *et al.* [17] compiled a comprehensive survey of about 40 APT groups, collating publications from many sources to provide researchers with an easy-to-follow central data source. The authors present a summary table containing 11 content columns that list all the references for each subject; these columns are (1) Spear-phishing samples, (2) Watering hole or web attacks, (3) Exploits used, (4) Description of the implant, (5) Description of post-exploitation tools,

(6) Description of support tools, (7) Command and control protocol, (8) Command and control infrastructure, (9) Tactics, Tools, and Procedures (TTP), (10) Attribution analysis or details of the groups, and (11) Victimization analysis. This same table has four columns indicating the source document type, showing at a glance the quality of the data; these columns are (1) Blog post, (2) Bulletin, (3) Report, and (4) Conference presentation. Also, the authors present a brief description of the findings of each publication group by geographical region. Finally, the authors also put forward that, at the time of their publication, there were a low number of academic publications covering the APT topic.

Alshamrani *et al.* [18] surveyed several APT attackers reviewing techniques and methods employed by attackers and defenses, including monitoring, detection, and mitigation methods. The authors also present clear attack trees for generic APT, for data stealing, for undermining critical components, a to position for future attacks.

Table 1. Techniques and methods of the APT campaigns [14].

APT Campaign/Group	**Initial Compromise**				**Lateral Movement**			**C2**		
	Spear-phishing	**Watering-Hole-Attacks**	**Server Attacks**	**Storage Media**	**Standard OS Tools**	**Hash and Password Dumping**	**Exploit Vulnerabilities**	**HTTP/HTTPS**	**Others**	**Custom Protocols**
Cozy Duke	✓							✓		
Hellsing	✓									
MsnMM (Naikon Group)	✓				✓			✓		
Carbanak	✓	✓			✓	✓		✓	✓	
Duqu 2.0	✓				✓	✓	✓	✓	✓	✓
HearBeat	✓									✓
Darkhotel	✓	✓						✓		
Thamar Reservoir	✓									
Naikon APT	✓				✓			✓		
APT30	✓							✓	✓	
Woolen-Goldfish	✓							✓	✓	
EquationDrug (Equation Group)	✓			✓			✓			
Animal Farm		✓								
Waterbug Group	✓	✓		✓				✓		
Desert Falcons	✓							✓		
Operation Cleaver	✓				✓	✓	✓	✓	✓	
Shell Crew			✓		✓	✓				✓
Icefog	✓					✓		✓		✓
Regin					✓			✓	✓	
APT28	✓							✓	✓	
Anunak	✓				✓	✓	✓	✓	✓	✓
Deep Panda	✓				✓	✓			✓	

3. Methodology

This paper will present the result of the first part of broader research with the following aims:

(1) Feature-based analysis of selected well-known APTs and TAs in order to categorize these attacks, extract related data and gain a better understanding of the relationship of these attacks and techniques used by attackers.
(2) Analysis of current Cyber-Kill Chain models and propose a more fine-tuned model to include the current evolutionary methods used in more recent APT attacks.
(3) And finally, develop a methodology capable of detecting an APT in its early stage by combining an Artificial Immune System (AIS) methodology known as a Dendritic Cell Algorithm (DCA) with a Genetic Algorithm (GA) and Support Vector Machine (SVM) classifiers.

Quantitative research methodology was used for creating and processing the test results with the assistance of statistics and casual theory formulation throughout the study. The methods are discussed in more detail in Section 4.

In terms of the software development process, Secure SDLC was used as described by Microsoft Security Development Lifecycle.

4. APT features analysis

Although it is almost certain that many campaigns still need to be found or made public and new ones are discovered regularly, this section presents a summary of 72 known attack campaigns using 13 features that categorize the characteristics of the attacks. These attacks were discovered between 2008 and 2018, and one discovered in 1998 is presented, in many senses, is a model for modern attacks. A summary of these attacks is shown in Table A.1 of the Appendix section, where the exact date of the first sample is not known uses 1st January, and when only the month and year are known, uses the first day of the month. A description of all the features used to describe each campaign is presented below, including their selection for further analyses: [7, 14, 17–97].

(1) *Attacker*: Not Selected. This feature is the attackers' name and is considered an index not used for categorization.
(2) *First Known Sample*: This feature refers to the first activity recorded for the attack. It is not selected individually but in combination with Discovery Date to

produce the new feature Time Elapsed to Discovery, representing the duration the attacker remained undetected within the target.

(3) *Discovery Date*: Not Selected. This feature indicates when the attack was discovered.

(4) *Number of Targets*: Not Selected. The number of targets is less significant than the seriousness of the attack and the relevance of the targets.

(5) *Current Status*: Not Selected. Regardless of the attackers' active status, the importance of the attacks is still relevant.

(6) *Type*: Selected. This presents the nature of the toolkits utilized in each attack.

(7) *Targeted Platforms*: Selected. Provides the Operating Systems platforms attacked.

(8) *Propagation Method*: Selected. Presents how the attack was distributed and spread within the victim's environment.

(9) *Purpose or Function*: Selected. This represents the goals or reasons that motivated the attack.

(10) *Main Target/Sub-targets*: Selected. Each campaign's intended target or targets are shown in this feature, including their sub-targets.

(11) *Top Targeted Countries*: Not Selected. The geographical distribution of the attacks could be significant, but the nature of these attacks is to be unrestricted just by these boundaries.

(12) *Description*: Not Selected. This presents an informative account of the attack and cannot be used for categorization.

(13) *Based On*: Selected. This feature shows attacks based on, reuse parts, or have relationships to other attacks.

The selected features for statistical analysis are categorized into seven groups using six existing features: targeted platforms, targets, propagation method, type, purpose, and derivative attacks. These categories are expanded and analyzed further in the following subsections:

4.1. Targeted platforms

This category indicates which Operating Systems were attacked and the number of attacks that focused on them.The observations show that Windows is the most targeted platform, representing 65.7% of the total, followed by Linux, Android, and Mac OS X in second place, representing 7.6% each, as seen in Figure 1. Figure 2 and Table 2 show that attacks on Windows platform are always at the top of participation in each of the years analyzed, having been below 50% just once.

(1) *Windows (65.7%)*: There are a total of 52 attacks exclusively focused on this platform, and it is a member of 17 other multi-platform attacks.

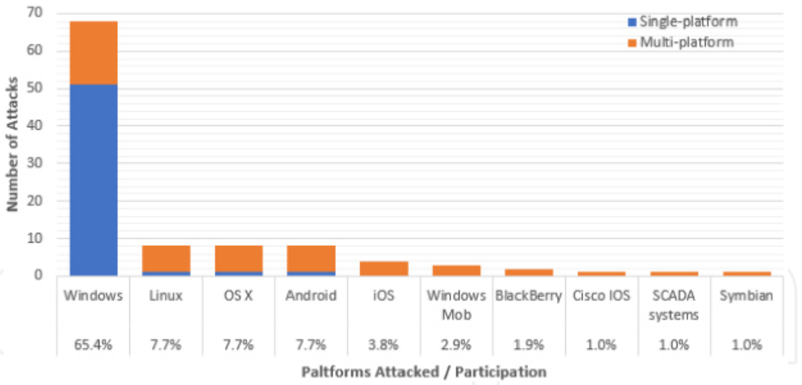


Figure 1. Targeted platforms.

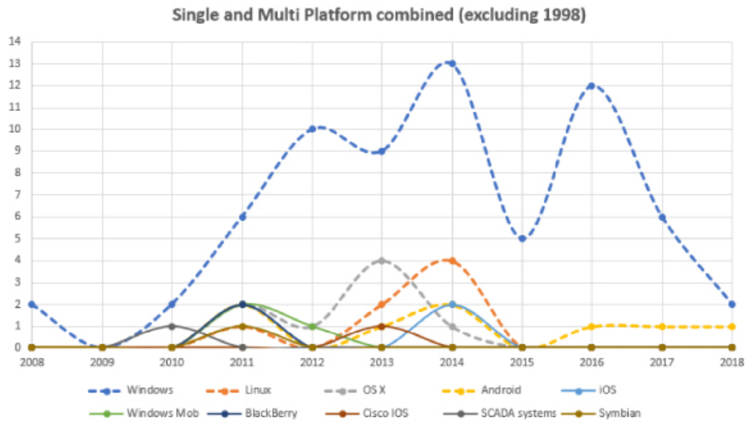


Figure 2. Platform discoveries per year (excluding 1998).

Table 2. Platform discovery distribution.

	1998 (%)	2008 (%)	2010 (%)	2011 (%)	2012 (%)	2013 (%)	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Windows	50	100	67	33	83	53	59	100	92	86	75
Linux	50			6		12	18				
OS X				11	8	24	5				
Android				11		6	9		8	14	25
IOS				11			9				
Windows Mob				11	8						
BlackBerry				11							
Cisco IOS						6					
SCADA systems			33								
Symbian				6							

(2) *Linux (7.6%)*: One attack is solely directed to this OS, two are focused on Windows as well as Linux, and five are multi-platform attacks, including Windows and OS X.

(3) *OS X (7.6%)*: From the eight attacks discovered for Mac OS X, only one exclusively focused on this platform, four where two platforms were attacked, Windows was the second one and three where other platforms were targeted.

(4) *Android (7.6%)*: Although Android is in the shared second place with eight attacks, there is only one dedicated attack on this platform, and all others are stepping stones to gain access to other systems.

(5) *iOS (3.8%)*: All four attacks for this mobile OS are part of multi-platform campaigns using it as an entry point to access other devices, networks, and information.

(6) *Windows Mobile (2.9%)*: No attacks dedicated to this platform were found; however, three attacks used it for surveillance purposes or to gain access to Windows OS.

(7) *Blackberry (1.9%)*: Because of the decline of this platform, we have only found two attacks that used it exclusively for information gathering as part of a multiplatform attack.

(8) *Cisco IOS (1%)*: The Black Energy series of cyberattacks had several variations, and one of those added a plugin capable of exploiting Cisco IOS routers.

(9) *SCADA Systems (1%)*: Only one attack was found directed to Siemens software for PLC (Programmable Logic Controllers), focused explicitly on uranium controllers.

(10) *Symbian (1%)*: The only multi-platform attack using this now-defunct mobile OS used it for surveillance purposes.

4.2. Time elapsed to discovery

One of the indicators of success for an attacker is how long it can remain undetected; this grouping uses the time elapsed between when the attack was first discovered and the first known samples date.As shown in Figure 3, 33.3% of campaigns were found less than 12 months after the attack started and 16.7% between 12 and 24 months; together, they comprise almost 50% of attacks. Although the number of attacks discovered within the first 24 months is a promising indicator, it also means that 50.7% of the attacks remained undetected for over two years, with the longest-running for just over ten years, Figures 4 and 5 present a breakdown of the distribution per month. These attacks have been grouped in years as described here:

(1) *<1 year*: this period consists of 24 attacks representing 33.3% of the total. Figure 4 shows the distribution in months for this category, having an average number of days elapsed to the discovery of 187.83 (6.3 months). In Figure 6 and

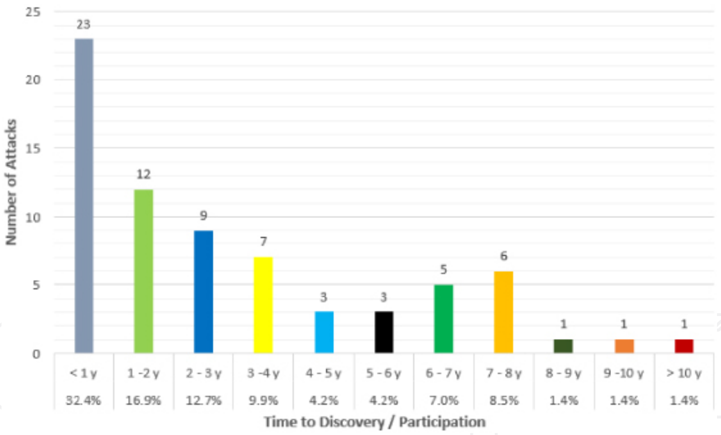


Figure 3. Time elapsed to discovery in years.

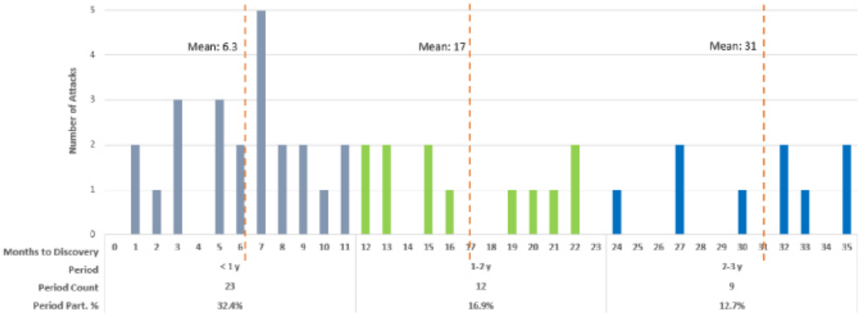


Figure 4. Time elapsed to discovery breakdown <3 years.

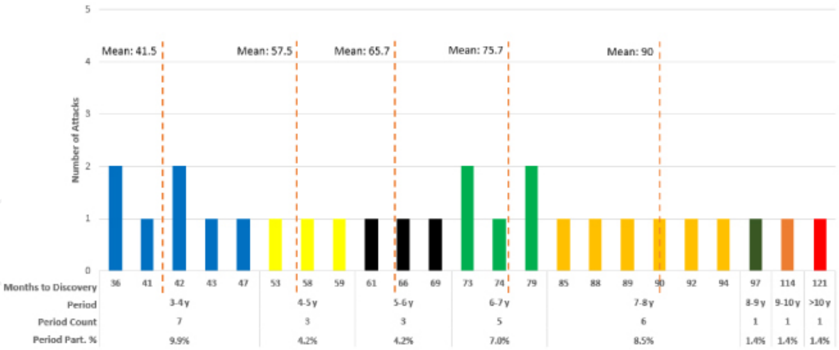


Figure 5. Time elapsed to discovery breakdown >3 years.

Table 3, we can see that the number of attacks discovered in this period has fluctuated over time. However, the overall trend is an increase in the number of discoveries, 2017 had 66.7% of that year's discoveries in this bracket, and 2016 and 2015 had 58.3% and 60%, respectively.

(2) *≥1 year and <2 years*: this period consists of 12 attacks representing 16.7% of the total, with an average number of days passed to the discovery of 509.2 (17 months).

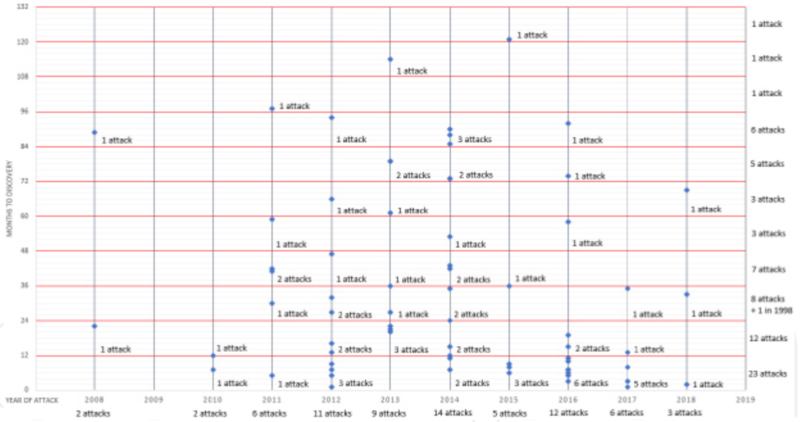


Figure 6. Distribution of attacks discovered per year (excluding 1998).

Table 3. Attacks discovered per year participation.

	1998	2008	2010	2011	2012	2013	2014	2015	2016	2017	2018
	(%)	(%)	(%)	(%)	(%)	(%)	(%)	(%)	(%)	(%)	(%)
<1 y			50.0	16.7	36.4		14.3	60.0	58.3	66.7	25.0
1–2 y		50.0	50.0		18.2	33.3	14.3		16.7	16.7	
2–3 y	100.0			16.7	18.2	11.1	14.3			16.7	25.0
3–4 y				33.3	9.1	11.1	14.3	20.0			
4–5 y				16.7			7.1		8.3		
5–6 y					9.1	11.1					25.0
6–7 y						22.2	14.3		8.3		25.0
7–8 y		50.0			9.1		21.4		8.3		
8–9 y				16.7							
9–10 y						11.1					
>10 y								20.0			

The monthly distribution of the attacks in this period can be seen in Figure 4. In contrast, figure and Table 3 show the participation per year and period; these details indicate that the discoveries in this period have reduced in volume in favor of the first period.

(3) ≥2 *years and* <3 *years*: this grouping holds nine attacks representing 12.5% of the discovered attacks. Figure 4 presents the monthly discoveries for this category, having an average of 929.2 days (31 months) to discovery. Figure 6 and Table 3 show that the participation per year and period has been relatively stable, except for 1998, with only one attack analyzed and a peak of 25% in 2018.

(4) ≥3 *years and* <4 *years*: this category has a total of seven attacks discovered or 9.7% of the total, with an average of 1245.14 days (41.5 months) elapsed to discovery. Figure 5 presents a breakdown of the number of months to discovery,

and Figure 6 and Table 3 show that the participation per year and period peaked at 33.3% in 2011 and has subsided since 2016.

(5) *≥4 years and <5 years*: this grouping has only three attacks discovered or 4.2% of the total, with an average of 1725 days (57.5 months) elapsed to discovery. Figure 5 presents a breakdown of the number of months to discovery, and Figure 6 and Table 3 show that the participation per year and period is very low, having peaked in 2011 at 16.7%.

(6) *≥5 years and <6 years*: this period has only three attacks discovered or 4.2% of the total, with an average of 1969.67 days (65.7 months) elapsed to discovery. Figure 5 presents a breakdown per the number of months to discovery, and Figure 6 and Table 3 show that the participation per year and period is low, except for 2018, which has a participation of 25%.

(7) *≥6 years and <7 years*: this grouping has five attacks discovered or 6.9%, with an average of 2270.8 days (75.7 months) elapsed to discovery. Figure 5 shows a breakdown per number of months to discovery, and Figure 6 and Table 3 show that the participation per year and period has decreased over time, with a peak at 22.2% in 2013.

(8) *≥7 years and <8 years*: this group has six attacks discovered or 8.3% of the total, with an average of 2698.67 days (90 months) elapsed until discovery. Figure 5 shows a breakdown per number of months to discovery, and Figure 6 and Table 3 show that the participation per year and period has fluctuated, having 50% in 2008 and dropping to 9.1% in 2016.

(9) *≥8 years and <9 years*: this period has one attack, or 1.4% of the total, with an average of 2922 days (97.4 months) elapsed to discovery. Figure 6 and Table 3 show that the participation per year and periods of this only attack was 16.7% in 2011.

(10) *≥9 years and <10 years*: this grouping has one attack, or 1.4% of the total, with an average of 3439 days (114.6 months) elapsed until discovery. Figure 6 and Table 3 show that the participation per year and periods of this only attack was 11.1% in 2013.

(11) *≥10 years*: this group has one attack, or 1.4% of the total, with an average of 3652 days (121.7 months) elapsed to discovery. Figure 6 and Table 3 show that the participation per year and periods of this only attack was 20% in 2015.

4.3. Targets of attacks

Each attack is aimed at a primary target or targets for their campaigns. This section groups the attacks into nine main categories composed of 55 subcategories representing the sectors or types of organizations attacked, as shown in Table 4, which could mean many more attacks in the overall total. These two grouping levels exist because attackers often start their campaigns with various targets escalating

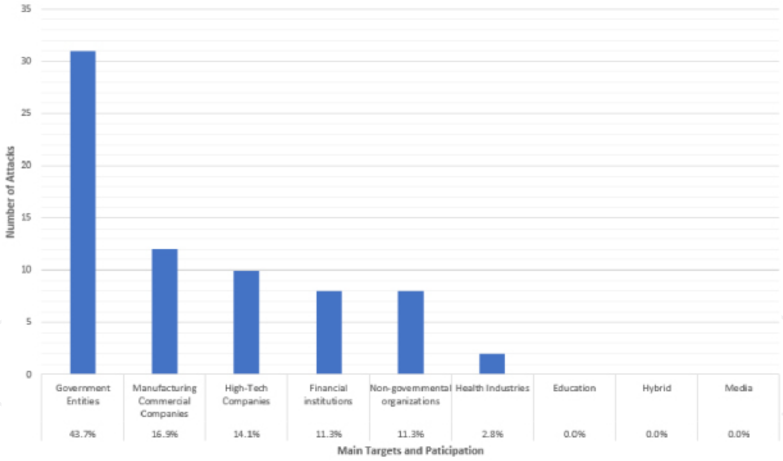


Figure 7. Main targets types.

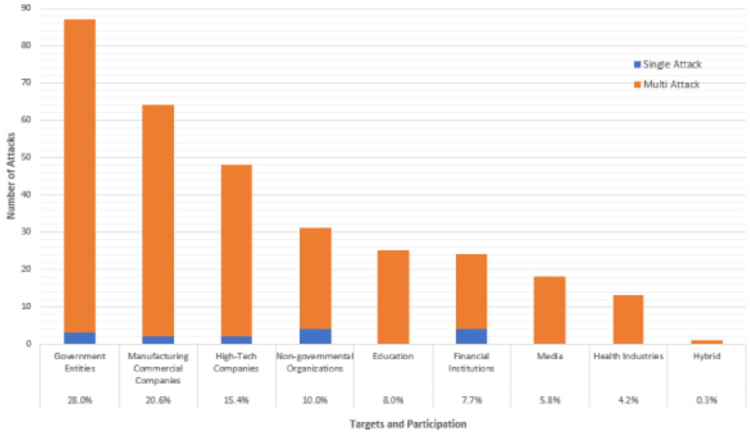


Figure 8. Main targets grouped counting targets sub-categories.

and probing until the main objective is reached. Figure 7 shows the count of main targets per attack. In contrast, Figure 8 displays the main targets grouped by counting targets' sub-categories' participation, including the sub-categories, if shared with another main attack. Figure 9 presents a comparison between the participation shown in the first two diagrams, including a combination of both by averaging them to create united participation. Comparing these charts, Government Entities have the highest participation (44.4%, 28.3%, and 36.3%), followed by Manufacturing and Commercial Companies (16.7%, 20.3%, and 18.5%) and High-Tech Companies (13.91%, 15.6% and 14.7%), these top three categories combined represent over 64% of the attacks in all three measurements over the period analyzed.

The main Targets have been ordered by their combined participation and are described as follows:

Table 4. Main targets and their subcategories.

Main targets	Sub-targets
Education	Academia/Research
	Education
Financial Institutions	Financial institutions
	Investments
Government Entities	Defense industrial base
	Diplomatic organizations/embassies
	Government entities
	Intelligence agencies
	Law enforcement agencies
	Military
	Military contractors
	Multi-national political bodies
	Politicians
	UN Workers
Health Industries	Health insurance services
	Healthcare
	Medical Industry
	Pharmaceuticals
High Tech Companies	Aerospace
	Design
	Electronics manufacturing
	Encryption software users
	High technology companies
	Information technology
	Nanotechnology
	Satellite operators
	Software companies
	Telecoms
Hybrid	No specific targets
	Wide range of targets
Manufacturing and Commercial Companies	Automotive
	Business individuals
	Chemical industry
	Commercial entities
	Construction
	Critical infrastructure engineering firms
	Energy oil and gas companies
	Engineering
	Heavy industry manufacturers
	Industrial/machinery
	Manufacturing
	Maritime and ship-building groups
	Nuclear industry
	Private companies
	Shipping
	Trade and commerce
	Transportation

Table 4. (Continued)

Main targets	Sub-targets
Media	Journalists Mass media and TV Media
Non-Governmental Organizations	Activists Criminal suspects Humanitarian aid organizations Non-governmental organizations Specific individuals

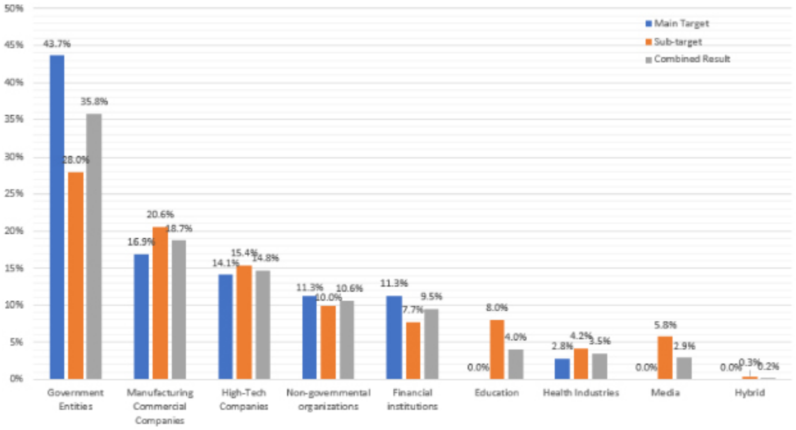


Figure 9. Targets and sub-targets participation compared.

(1) *Government Entities*: this group suffered 32 attacks during the period analyzed, i.e., 36.3% of the combined total, and its subgroups attacks amounted to 89 during the same period. This category includes sub-categories such as Military entities and their contractors, Government Entities, Embassies, Intelligence Agencies, and Multi-national political bodies, which makes them a desirable target for sophisticated attackers. Over time, as shown in Figure 10 and Table 5, this group has usually been over a third of the attackers' focus, and the trend seems steady. However, there was a dip in 2010 and 2017; the latter represents the lowest yearly participation at 17.9% of the attacks.

(2) *Manufacturing and Commercial Companies*: this group has been the focus of 12 attacks, 18.5% of the average total, and its subcategories received 64 attacks during the same period. Within this category, we have Energy Industries, Nuclear Industry, Manufacturing Companies, and Commercial Entities, all of which are the focus of TA and less sophisticated attacks. Figure 10 and Table 5 show that attacking these targets is a steady focus for attackers, except in 2011 when its participation was only 6.3%.

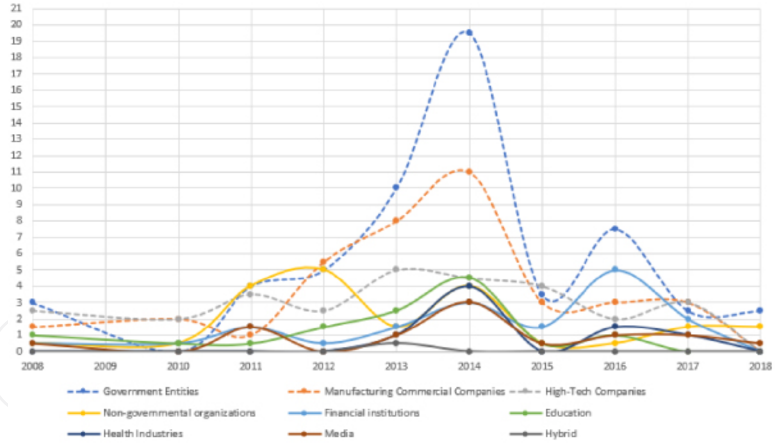


Figure 10. Targets over time (excluding 1998).

Table 5. Targets per year participation.

	1998 (%)	2008 (%)	2010 (%)	2011 (%)	2012 (%)	2013 (%)	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Government Entities	75.0	31.6		25.0	25.0	32.3	36.4	25.9	34.9	17.9	57.1
Manufacturing Commercial Companies		15.8	36.4	6.3	27.5	25.8	20.6	22.2	14.0	21.4	
High-Tech Companies		26.3	36.4	21.9	12.5	16.1	8.4	29.6	9.3	21.4	7.1
Non-governmental organizations		5.3	9.1	25.0	25.0	4.8	7.5	3.7	2.3	10.7	21.4
Financial Institutions		5.3	9.1	9.4	2.5	4.8	5.6	11.1	23.3	14.3	
Education	25.0	10.5	9.1	3.1	7.5	8.1	8.4	3.7	4.7		7.1
Health Industries						3.2	7.5		7.0	7.1	
Media		5.3		9.4		3.2	5.6	3.7	4.7	7.1	7.1
Hybrid						1.6					

(3) *High-Tech Companies*: this group received ten attacks, or 14.7% of the averaged total, l and its subsections counted 48 attacks. Some of the subsections are Software Companies, Aerospace Companies, Encryption Software, and Satellite Operators, few of these are used as gateways or facilitators for further focused attacks or as tools of attacks, but many attacks are the final objective. As seen in Figure 10 and Table 5, over time, there have been peaks and valleys in the attacks directed at these groups. Nonetheless, it has continued participation.

(4) *Non-Governmental Organizations*: this group has been the focus of eight attacks, 10.5% of the average total, and its subcategories received 31 attacks during the same period. Within this category, we have UN workers, activists, and some specific individuals, all prime subjects for data theft and surveillance. After its peak in 2011 and 2012 of 25%, as seen in Figure 10 and Table 5, the participation of this group follows a medium-level firm trend.

(5) *Financial Institutions*: this group had eight attacks during the period analyzed, 9.4% of the combined total and its subgroups attacks amounted to 24 during the same period. This category includes sub-categories such as Banks and Investment Companies, targets for those interested in financial gain. Figure 10 and Table 5 show that attacks on these institutions have been rising steadily since 2015, even though they had been declining until then.

(6) *Education*: although this group did not have direct attacks, it has a combined participation of 4.1% as a part of 26 campaigns focused on other categories that used it as a gateway or part of the attack itself. There have been no reports since 2017 of attacks on this sector, but it has always had a presence in prior years, as shown in Figure 10 and Table 5.

(7) *Health Industries*: this group received two attacks, 3.5% of the average total, and its subsections counted 13 attacks. Some subsections are Pharmaceutical Companies, Healthcare Companies, and Medical Industries, targeted for data theft, data wiping, and entry points to other targets. Figure 10 and Table 5 show a sporadic targeting of this group with no clear trend.

(8) *Media*: although this group did not have direct attacks, it has a combined participation of 2.9% as a part of 18 campaigns focused on other groupings that used it as a doorway or as means to reach the primary goal. The subcategories are Journalists, Mass media, and TV Stations. This group has had low participation over time even though it has appeared in more years than other groups; it has always had low volumes; this can be seen in Figure 10 and Table 5.

(9) *Hybrid*: this sub-section is reserved for attacks with a wide range of targets, almost too wide to be a TA. However, there are a few campaigns initiated as comprehensive that ended up focusing on just a few targets, such as Black Energy. There are no direct attacks in this category and only one under a mixed category, representing only 0.2% of the total.

4.4. Propagation method

This section focuses on how the attackers propagated within the target's network and how the initial distribution of the malware was done.Observing these attacks, 13 propagation methods have been acknowledged and are described in this section. 59.2% of these attacks use multiple propagation methods, here called multi-method, and 40.8% used one method. It is important to note that one of the propagation methods is dedicated to those methods that are unknown to researchers, amounting to 3.6%. Figure 11 shows that over 76% of the attacks used four propagation methods: Social Engineering at 32.9%, Exploits at 22.1%, Watering Holes at 12.9%, and USB Drives at 8.6%. It is essential to point out that the first three methods are the most commonly combined.

The Propagation Methods have been ordered by their popularity and are described as follows:

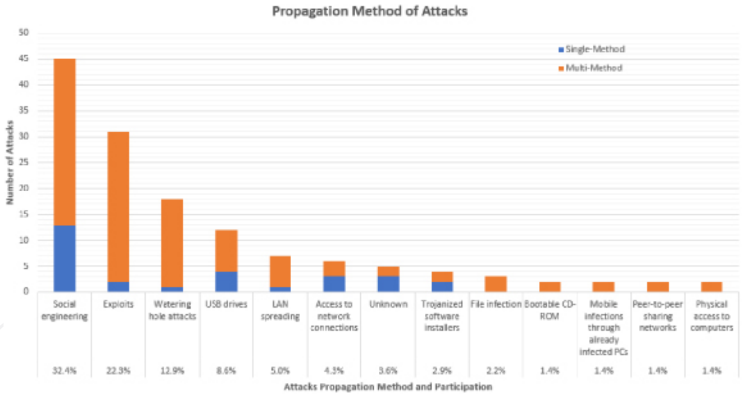


Figure 11. Propagation method.

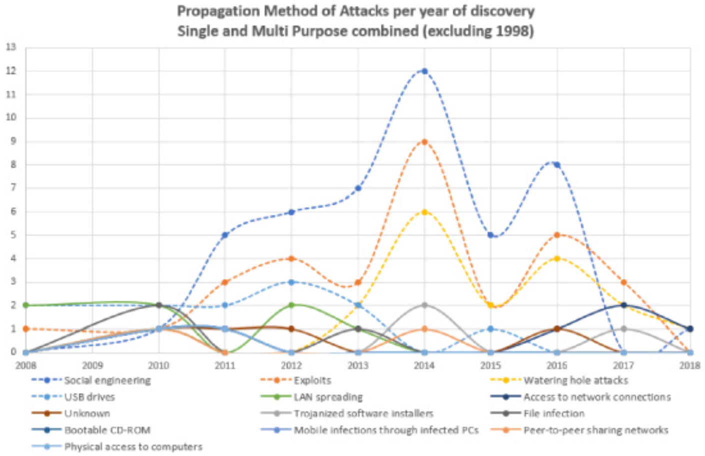


Figure 12. Propagation method over time.

(1) *Social Engineering*: this type refers to those attacks focused on tricking human users into allowing access to sensitive details; several activities fall into this category, such as phishing and tailgating. A combined total of 46 single and multiple occurrences gives this group a 32.9% of the total. Figure 12 and Table 6 show that this technique is a favorite of attackers, even though it has some valleys.

(2) *Exploits*: this category discusses those methods that take advantage of known vulnerabilities in applications, hardware, and Operating Systems. Adding single and multi-type occurrences, this category reported 31 occurrences, 22.1% occurrences of the total. Figure 12 and Table 6 show a slight variation in occurrences with a stable trend.

(3) *Watering Holes*: although this method can be considered a part of Social Engineering, it requires the attacker to compromise sites that the targeted victims visit, which requires an extra step that sets them apart. Furthermore, some Social Engineering attacks, such as phishing, use these as secondary infection points.

Table 6. Propagation method per year participation.

	1998 (%)	2008 (%)	2010 (%)	2011 (%)	2012 (%)	2013 (%)	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Social engineering			6.3	33.3	37.5	43.8	40.0	50.0	42.1	11.1	33.3
Exploits		20.0	6.3	20.0	25.0	18.8	30.0	20.0	26.3	33.3	
Watering hole attacks			6.3			12.5	20.0	20.0	21.1	22.2	33.3
USB drives		40.0	12.5	13.3	18.8	12.5		10.0			
LAN spreading		40.0	12.5		12.5	6.3					
Access to network connections			6.3	6.7					5.3	22.2	33.3
Unknown	100		6.3	6.7	6.3				5.3		
Trojanized software installers			6.3				6.7			11.1	
File Infection			12.5			6.3					
Bootable CD-ROM			6.3	6.7							
Mobile Infections through Infected PCs			6.3	6.7							
Peer-to-peer sharing networks			6.3				3.3				
Physical access to computers			6.3	6.7							

There were 18 appearances observed that represent a 12.9% participation single and multi-type attacks. As observed in Figure 12 and Table 6, this category shows a steadily increasing trend.

(4) *USB Drives*: this type refers to those attacks focused on tricking human users into inserting a malware-infected USB drive; this is another play on human psychology by either mailing or casually leaving a malicious USB drive for a user to open or directly asking for something from the drive, such as print a file. A combined total of 12 single and multiple occurrences gives this group an 8.6% of the total. Figure 12 and Table 6 show that this technique's usage has declined over time to the point of not being detected since its appearance in 2015.

(5) *LAN Spreading*: this type refers to those attacks focused on the traditional worm-like spreading built-in method. A combined total of seven single and multiple occurrences gives this group 5% of the total. Figure 12 and Table 6 show that this technique's usage has declined significantly and has not been used since 2013.

(6) *Access to Network Connections*: this category discusses those methods that take advantage of poorly secured live network ports and Wireless networks, such as LAN connections left live and unattended or Wi-Fi connections with MAC blocking and weak passwords. Adding single and multi-type occurrences, this

category has six occurrences, 4.3% of the total. Figure 12 and Table 6 show a slight variation in participation with a stable trend.

(7) *Unknown*: this type refers to those attacks where the methodologies used were not determined, making them the most successful attacks. A combined total of five between single and multiple occurrences gives this group a 3.6% over the total. Figure 12 and Table 6 show that not finding the methodology used has occurred over time, but it needs a clear trend.

(8) *Trojanised Software Installers*: this category discusses those attacks that successfully embedded themselves in legitimate installers for new applications or updates for existing ones. These are also known as supply chain attacks and are very difficult to implement. Adding single and multi-type occurrences, this category has four occurrences, 2.9% of the total. Figure 12 and Table 6 show that this methodology appears sporadically due to its complexity.

(9) *File Infection*: this category discusses those traditional malware attack methods that are applications written for infecting targets. However, they are relatively easy to identify due to their signature. This category has been used in three multi-method attacks, 2.1% of total. Figure 12 and Table 6 show that it has been sparsely used over time.

(10) *Bootable CD-ROM*: this type refers to those attacks focused on providing a CD-ROM with booting capabilities to take control of the attacked host. Since the demise of this media, these attacks have all but disappeared. This group has been used in two multi-method attacks, 1.4% of total. Figure 12 and Table 6 show that this technique has been used only in 2010 and 2011.

(11) *Mobile Infections Through Infected PCs*: this group refers to those attacks on mobile devices through previously compromised PCs. This group has been used in two multi-method attacks, 1.4% of total. Figure 12 and Table 6 show that this technique has been used only in 2010 and 2011.

(12) *Peer-to-peer Sharing Networks*: this type refers to those attacks focused on ad hoc networks created for sharing resources over internet connections without server intervention. However, there are attacks on public or semi-public networks that can be included in this category. This group has been used in two multi-method attacks, 1.4% of total. Figure 12 and Table 6 show that this technique has been used only in 2010 and 2014.

(13) *Physical Access to Computers*: this group refers to those attacks conducted through direct physical contact with the target's computers; this is the case of lost or stolen laptops or unattended computers. This group has been used in 2 multi-method attacks, 1.4% of total. Figure 12 and Table 6 show that this technique has been used only in 2010 and 2011.

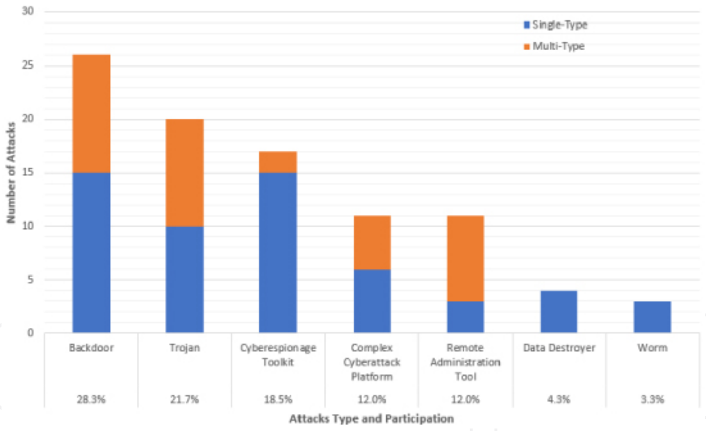


Figure 13. Types of attacks.

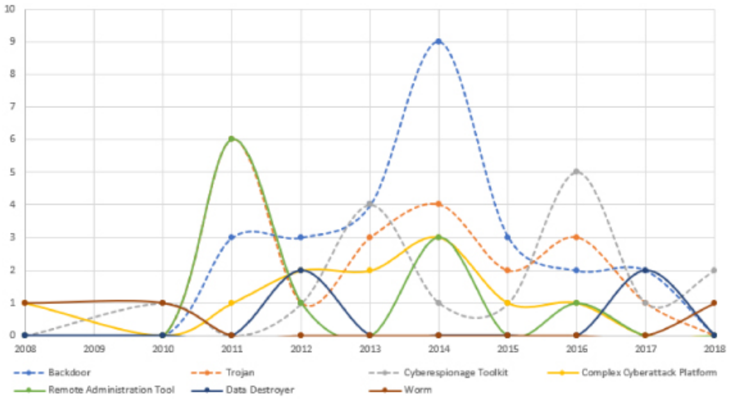


Figure 14. Types of Attacks over time (excluding 1998).

4.5. Type of attack

This section aims to classify the types of attacks based on the tooling utilized; seven of these types have been identified and described here; some are used exclusively and others in combination; here, they are referred to as single-type and multi-type, respectively. As can be seen in Figure 13, the most commonly used type is Backdoor representing 28.3% of the total, being followed by Trojans at 21.7% and Cyberespionage Toolkits at 19.6%; the top three types account for 69.6% of the total observed.

The types of attacks have been ordered by their usage and are described as follows:

(1) *Backdoor*: this type refers to those applications or implementations that allow access to circumvent normal security procedures and processes. A total of 26 occurrences, single and multi-type combined, represented 28.3% of the total. Figure 14 and Table 7 show that although it has ups and downs, growth is the overall trend.

Table 7. Types of attacks per year participation.

	1998 (%)	2008 (%)	2010 (%)	2011 (%)	2012 (%)	2013 (%)	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Backdoor				21.4	27.3	30.8	45.0	42.9	16.7	28.6	
Trojan				42.9	9.1	23.1	20.0	28.6	25.0	14.3	
Cyberespionage Toolkit	100.0		50.0		18.2	30.8	5.0	14.3	41.7	14.3	66.7
Complex Cyberattack Platform		50.0		7.1	18.2	15.4	15.0	14.3	8.3	14.3	
Remote Administration Tool				28.6	9.1		15.0		8.3		
Data Destroyer					18.2					28.6	
Worm		50.0	50.0								33.3

(2) *Trojans and Droppers*: this category discusses those malicious applications or implementations hidden within another, legitimate or not, and those that download and install or "drop" more malicious code. Adding single and multi-type occurrences, this segment reaches 20 and accounts for 21.7% of the total. Figure 14 and Table 7 show that it has a slight variation with a stable trend.

(3) *Cyberespionage Toolkit*: these are a grouping or combination of different tools, pre-existing and specifically designed for the task at hand. Eighteen appearances combining single and multi-type attacks representing 19.6% participation. As observed in Figure 14 and Table 7, this category's participation oscillates with an increasing trend.

(4) *Complex Cyberattack Platform*: this type refers to purposeful design and developed platforms. A total of 12 occurrences, single and multi-type combined, gives this group a 13% participation of the total. Figure 14 and Table 7 show that it has peaks and valleys with a declining overall trend.

(5) *Remote Administration Tool*: this category discusses those applications that provide complete control of the devices to an external party, in this context, with malicious intent. This type also includes Rootkit and Bootkit, which are collections of applications that allow access administration access to a host, including the booting process of the Operating System. Adding single and multi-type occurrences, this category reaches nine, which is 9.8% of the total. Figure 14 and Table 7 show that it has peaks and valleys with a declining overall trend, although its maximum participation reached 28.6% in 2011.

(6) *Data Destroyer/Wiping*: this type is focused on rendering information unusable or erasing it. Four single-type appearances represent a 4.3% participation. As observed in Figure 14 and Table 7, this category's participation was 18.2% in 2012 and 28.6% in 2017, these being the two years that it appeared. Although they have a growing trend, these types of attacks are sporadic.

(7) *Worm*: this category discusses self-propagating malicious applications or implementations. Three single-type appearances represent a 3.3% participation.

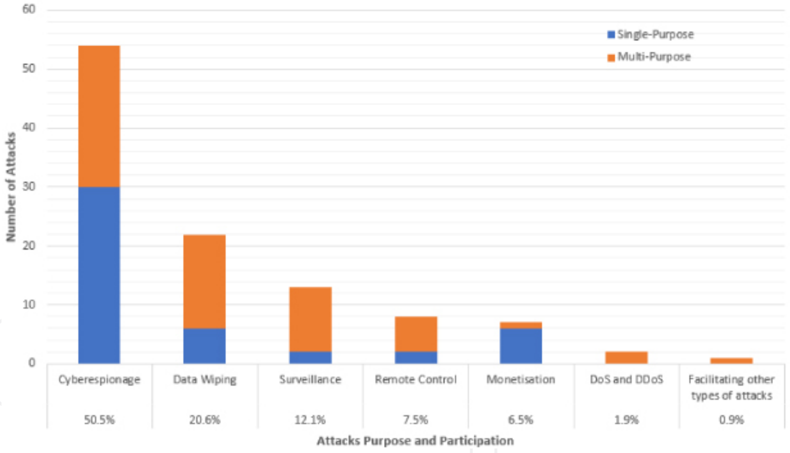


Figure 15. Purpose of Attacks.

Figure 14 and Table 7 show that in the years that appeared, it had high incidence; however, it is occasionally used and shows a declining trend.

4.6. Purpose of attacks

Segmentation based on the purpose of attacks led to the identification of seven different purposes in this research and are described here.Many attacks have more than one purpose, and some have just one and are referred to as multi-purpose and single-purpose, respectively. Figure 15 shows that all the identified purposes have been used in conjunction with others, and few have been used with further attacks. Figure 15 also displays that Cyberespionage is by far the most popular purpose, at 50.9% and well over double of data wiping purpose at 20.4% combined with surveillance at 12%, these top three purposes account for 83.3% of the attacks' goals.

The purpose of attacks has been ordered by their popularity and are described as follows:

(1) *Cyberespionage*: this can be defined as an attack designed to acquire sensitive data or information to obtain an advantage over other governments or targeted companies [97, 98]. Figure 15 shows that this purpose represents 50.9% of the total, and it has been the focus of 30 single-purpose attacks and part of 24 multi-purpose ones for a total of 54 occurrences. Clearly, this is the most common purpose from the samples analyzed. Figure 16 and Table 8 display a very stable occurrence in each year and a near consistent trend.

(2) *Data wiping*: these attacks aim to gain a competitive advantage or inflict damage by destroying the competitors' or adversary's data. This purpose signifies 20.4% of the total. It was the focus of six single-purpose and 16 multi-purpose attacks, adding up to a total of 22, as shown in Figure 15. Figure 16 and Table 8 present a diverse participation over time with a decreasing trend.

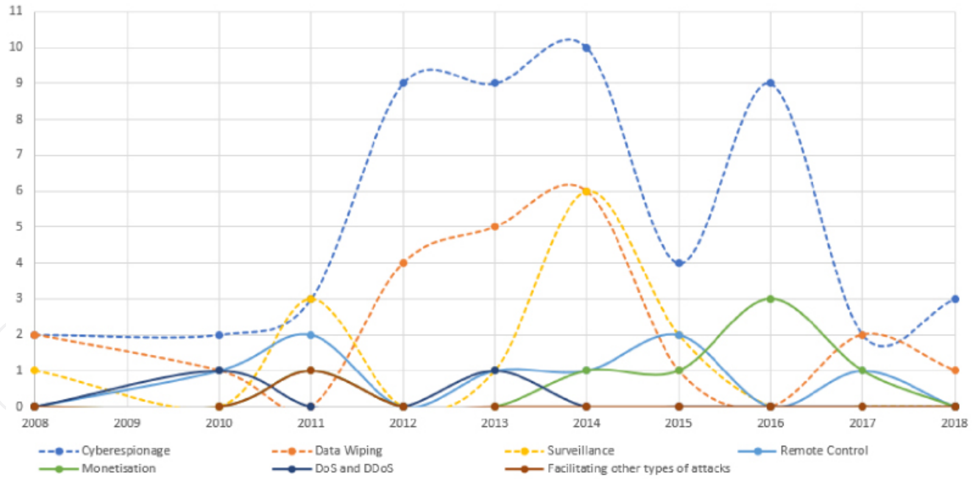


Figure 16. Purpose of Attacks per year of discovery (excluding 1998).

Table 8. Purpose of attacks per year of discovery participation.

	1998 (%)	2008 (%)	2010 (%)	2011 (%)	2012 (%)	2013 (%)	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Cyberespionage	100.0	40.0	40.0	30.0	69.2	52.9	41.7	40.0	75.0	42.9	75.0
Data Wiping		40.0	20.0		30.8	29.4	25.0	10.0		28.6	25.0
Surveillance		20.0		30.0		5.9	25.0	20.0			
Remote Control			20.0	20.0		5.9	4.2	20.0		14.3	
Monetisation				10.0			4.2	10.0	25.0	14.3	
DoS and DDos			20.0			5.9					
Facilitating other types of attacks				10.0							

(3) *Surveillance*: refers to monitoring people or organizations for intelligence or information gathering. Figure 15 displays that this purpose has a 12% participation, with a total of 13 attacks having this purpose; however, only two are single-purpose because those attackers are the makers of surveillance packages. Figure 16 and Table 8 show that in most years, it had a participation of at least 20%; however, it does not occur every year and therefore has a declining trend.

(4) *Remote Control*: this can be defined as the intent to gain complete control of the devices and applications of the attacked party. Figure 15 shows that this purpose represents 7.4% of the total, and it has been the focus of two single-purpose attacks and part of six multi-purpose for a total of eight occurrences. Figure 16 and Table 8 display mostly stable participation each year and an almost slightly decreasing trend.

(5) *Monetization*: this purpose refers to those attacks focused directly on stealing money. This purpose signifies 6.5% of the total. It was the focus of six

single-purpose and one multi-purpose attacks, adding up to a total of seven, as shown in Figure 15. Figure 16 and Table 8 present generally low participation over time with a slowly increasing trend.

(6) *DoS and DDoS*: refer to attacks attempting to overwhelm services with traffic from many sources with the aim of disrupting the service. This purpose has been used as a part of other campaigns exclusively, having the participation of 1.9% and a total of two occurrences. Figure 16 and Table 8 show that this purpose has been sporadic. However, it may have been covertly used too.

(7) *Facilitating other types of attacks*: there is one attack, Regin, that had as a purpose to facilitate further attacks, almost in a malware-as-a-service fashion. This case represents only 0.9% of the total and was used in conjunction with other purposes only once, as shown in Figure 16 and Table 8.

4.7. Secondary and derivative attacks

This category reviews those attacks that are based on, reuse parts, or are related to previous or contemporaneous attacks, as illustrated in Figure 17; this figure illustrates the relationships over time using the year of discovery for grouping. In this category, those attacks that had evolution of themselves are presented as referenced by others as well; these attacks are those that have a very close similarity to the original, resembling a subversion of the attack rather than having significant differences.

From the total sample of campaigns analyzed, only 27 fit this category, or 37.5%, referencing a total of 22 attacks, 11 of these are referred by others and reference others simultaneously; these differences are color-coded in Figure 17, which also shows that Agent.BTZ and Equation through Stuxnet and Flame are the attacks that have influenced the most future campaigns, from their discovery in 2008, they have affected attacks until 2017 with Stonedrill. Other major influencers are Wiper, MiniDuke, and Turla; the latter also refers to the 1998 campaign Moonlight Maze which through Whitebear made its presence felt in 2016.

5. *Conclusion and future work*

In this paper, 72 attack campaigns are summarized using 12 features and then categorized into seven groups using six existing features, namely targeted platforms, targets, propagation method, type, purpose, and derivative attacks, and calculating the time to discovery based on the time elapsed between when the attack was first discovered and the first known sample date. The analysis of these categories provides a view of the efforts and attention of the attackers. It aims to guide the design of detection systems by providing samples that would help train systems to detect attacks and adapt to new ones.

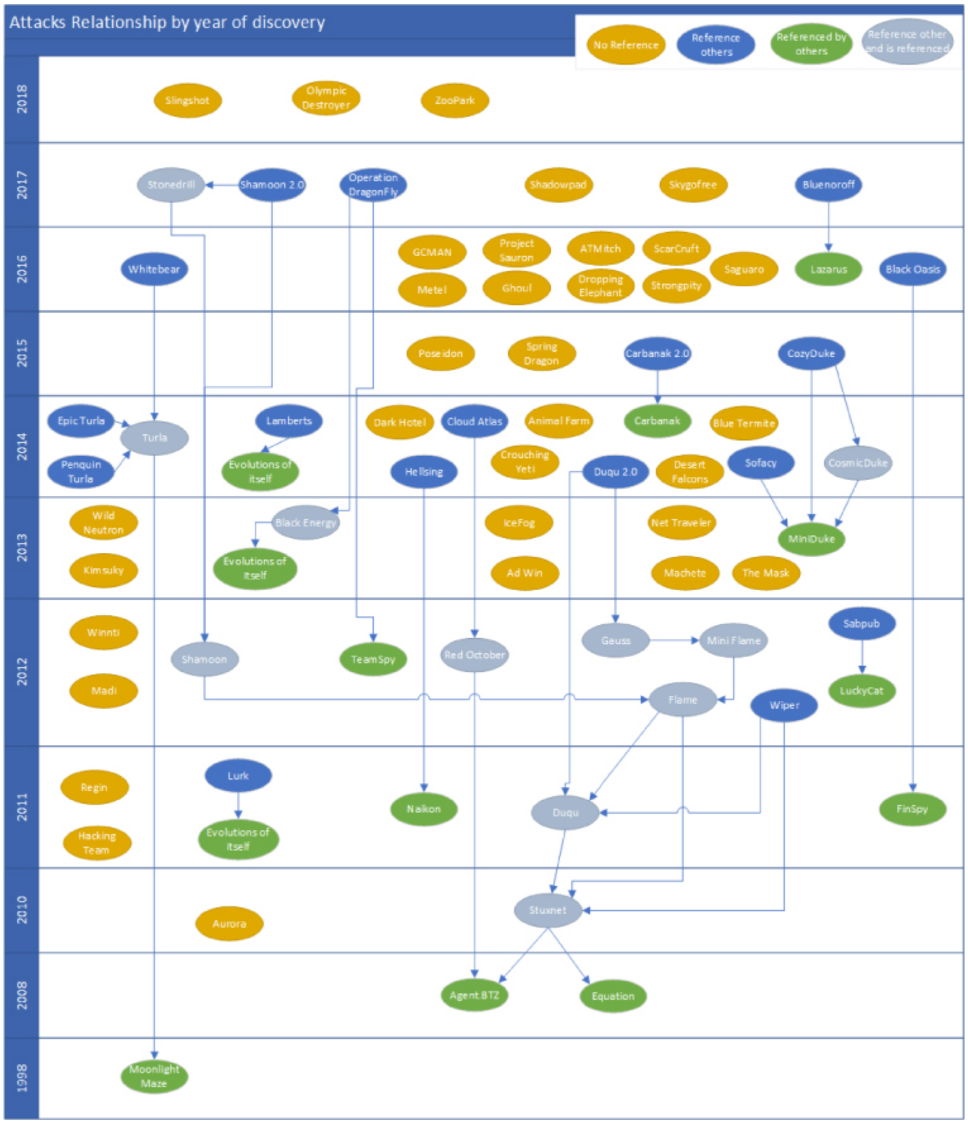


Figure 17. Secondary and derivative attacks.

This research has found a low number of academic publications covering the APT subject; this is mainly due to complexity of APT attacks and victims hesitant to release full data to the public. However, industry-published sources are extensive and have provided much assistance for data gathering, as other authors have also found. Future work would be focused on employing this feature analysis and categorization to create the input for a selection process with modern and representative attack samples to train detection systems.

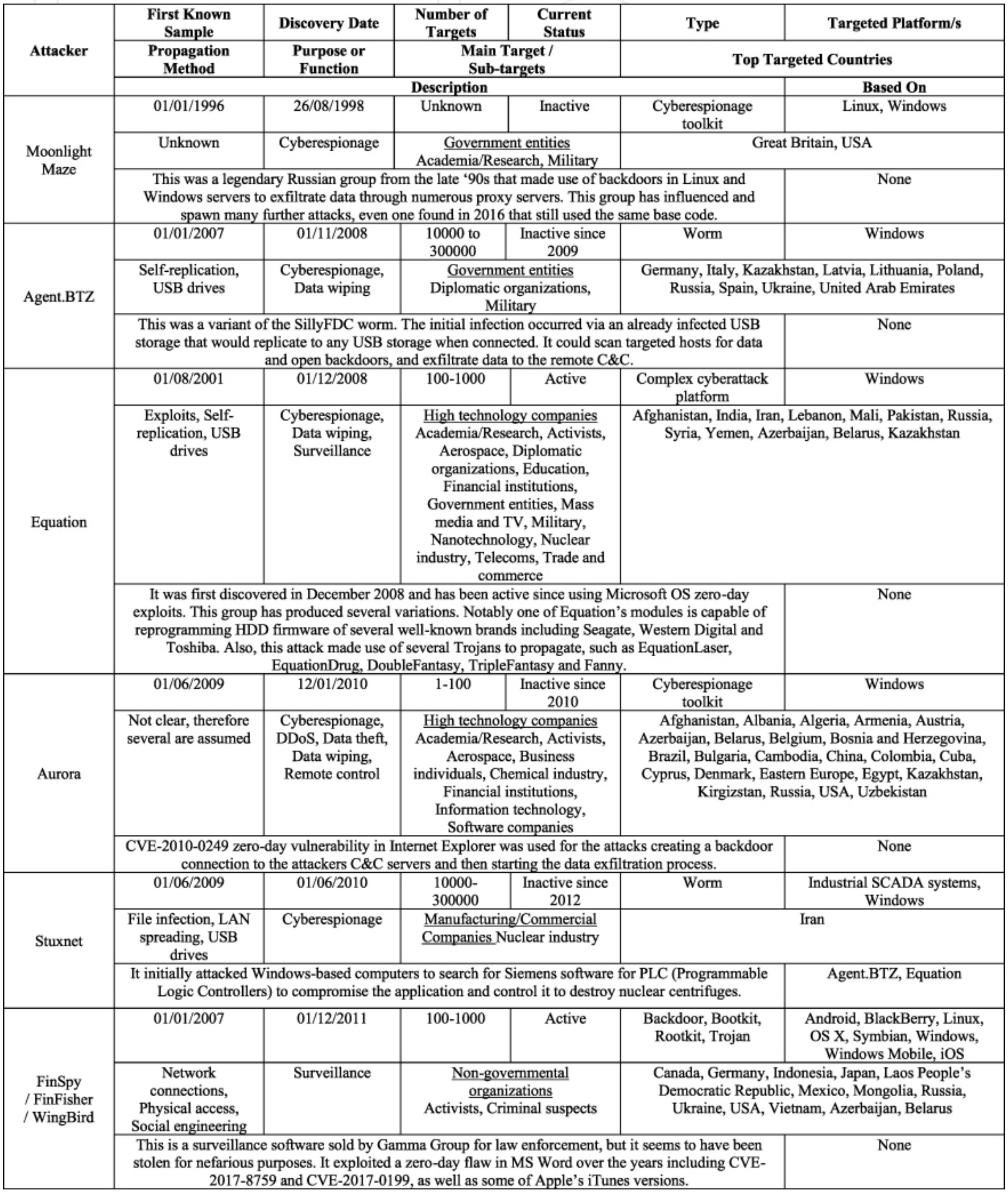
Conflict of interest

The authors declare no conflict of interest.

Appendix

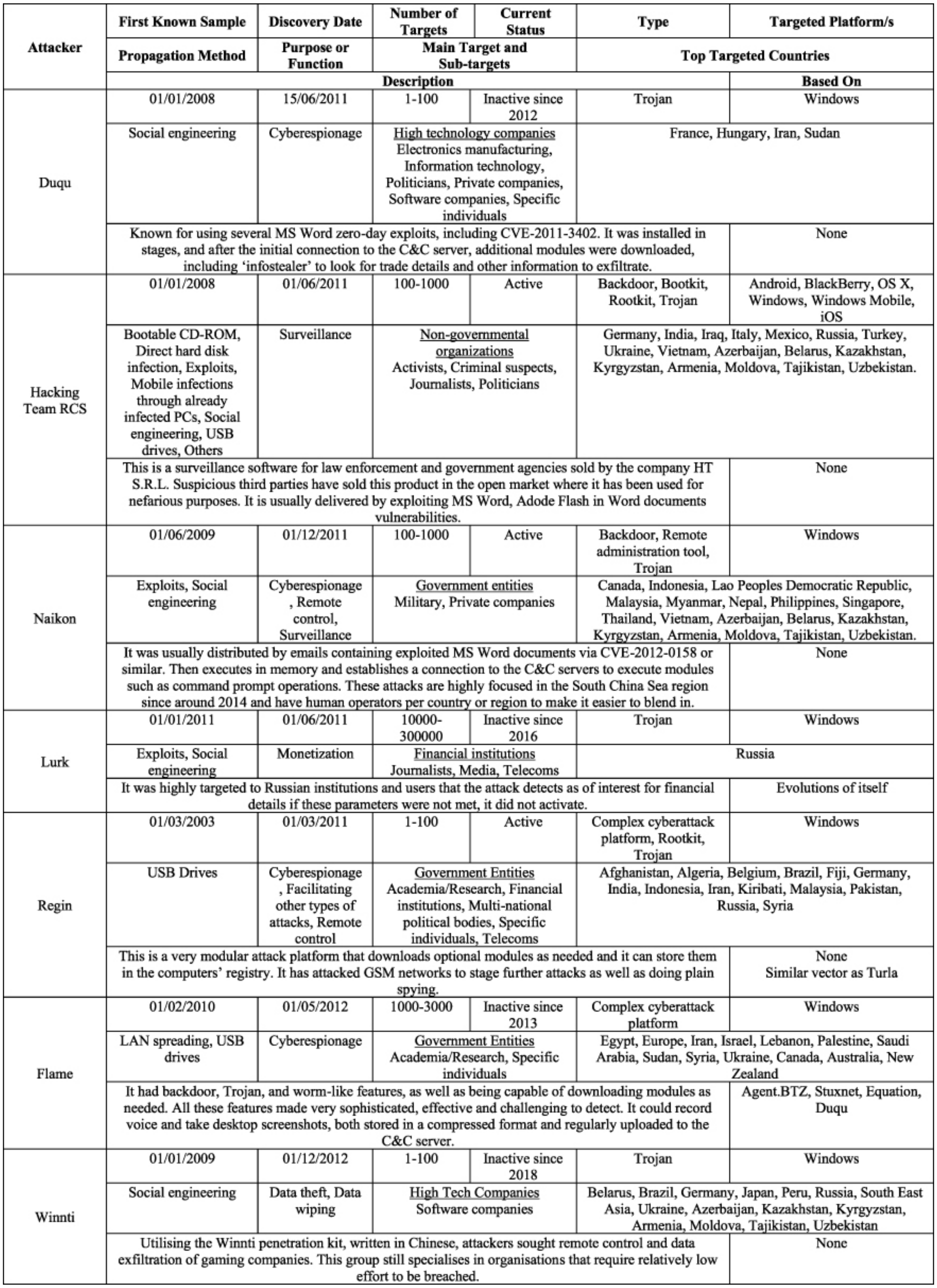
Table A.1 summarizes the attacks used in this work using the 13 categories described in Section 3.

Table A.1. Summary of attacks.



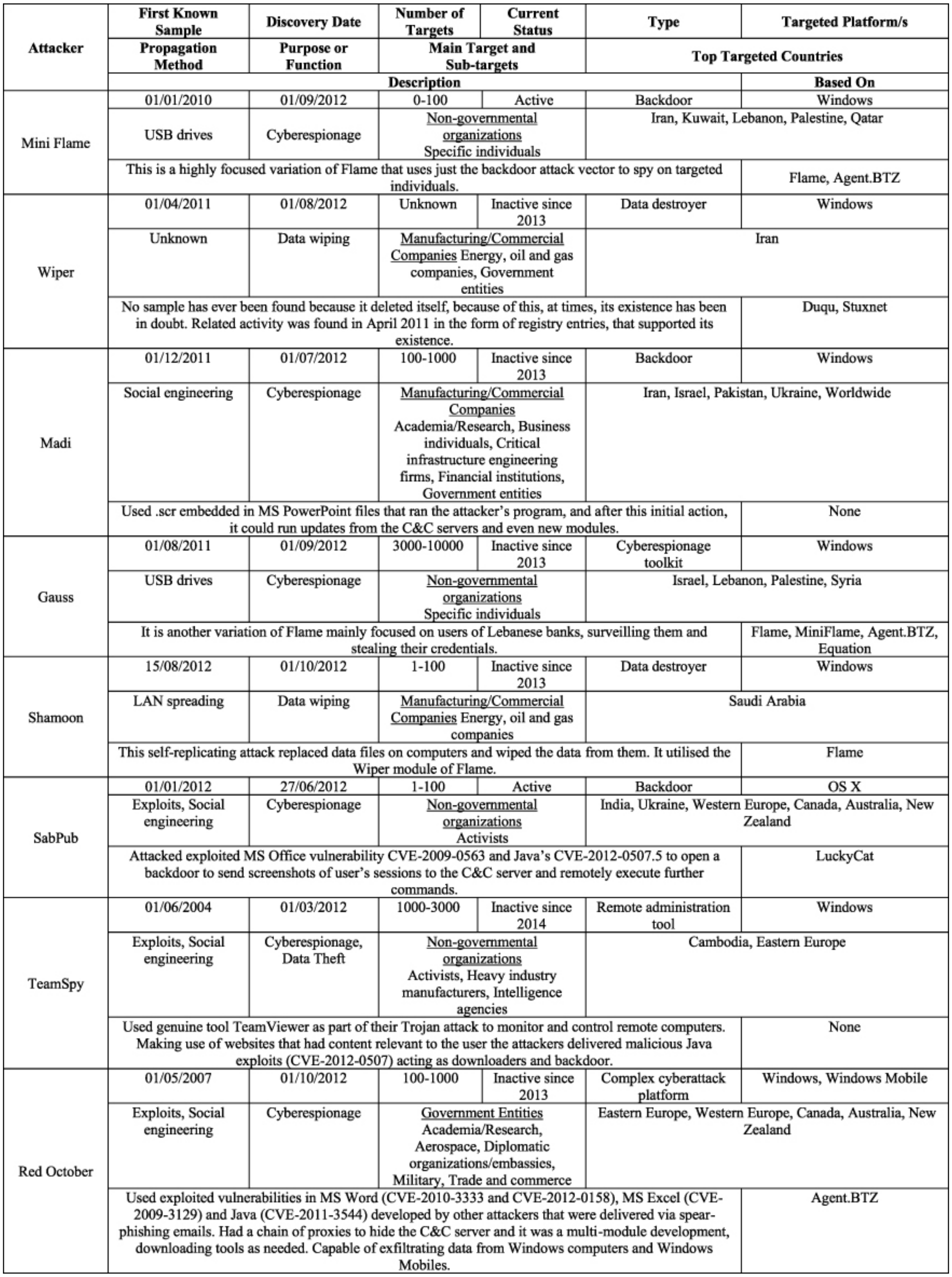
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Moonlight Maze	01/01/1996	26/08/1998	Unknown	Inactive	Cyberespionage toolkit	Linux, Windows
	Unknown	Cyberespionage	Government entities Academia/Research, Military		Great Britain, USA	
	This was a legendary Russian group from the late '90s that made use of backdoors in Linux and Windows servers to exfiltrate data through numerous proxy servers. This group has influenced and spawn many further attacks, even one found in 2016 that still used the same base code.					None
Agent.BTZ	01/01/2007	01/11/2008	10000 to 300000	Inactive since 2009	Worm	Windows
	Self-replication, USB drives	Cyberespionage, Data wiping	Government entities Diplomatic organizations, Military		Germany, Italy, Kazakhstan, Latvia, Lithuania, Poland, Russia, Spain, Ukraine, United Arab Emirates	
	This was a variant of the SillyFDC worm. The initial infection occurred via an already infected USB storage that would replicate to any USB storage when connected. It could scan targeted hosts for data and open backdoors, and exfiltrate data to the remote C&C.					None
Equation	01/08/2001	01/12/2008	100-1000	Active	Complex cyberattack platform	Windows
	Exploits, Self-replication, USB drives	Cyberespionage, Data wiping, Surveillance	High technology companies Academia/Research, Activists, Aerospace, Diplomatic organizations, Education, Financial institutions, Government entities, Mass media and TV, Military, Nanotechnology, Nuclear industry, Telecoms, Trade and commerce		Afghanistan, India, Iran, Lebanon, Mali, Pakistan, Russia, Syria, Yemen, Azerbaijan, Belarus, Kazakhstan	
	It was first discovered in December 2008 and has been active since using Microsoft OS zero-day exploits. This group has produced several variations. Notably one of Equation's modules is capable of reprogramming HDD firmware of several well-known brands including Seagate, Western Digital and Toshiba. Also, this attack made use of several Trojans to propagate, such as EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy and Fanny.					None
Aurora	01/06/2009	12/01/2010	1-100	Inactive since 2010	Cyberespionage toolkit	Windows
	Not clear, therefore several are assumed	Cyberespionage, DDoS, Data theft, Data wiping, Remote control	High technology companies Academia/Research, Activists, Aerospace, Business individuals, Chemical industry, Financial institutions, Information technology, Software companies		Afghanistan, Albania, Algeria, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cambodia, China, Colombia, Cuba, Cyprus, Denmark, Eastern Europe, Egypt, Kazakhstan, Kirgizstan, Russia, USA, Uzbekistan	
	CVE-2010-0249 zero-day vulnerability in Internet Explorer was used for the attacks creating a backdoor connection to the attackers C&C servers and then starting the data exfiltration process.					None
Stuxnet	01/06/2009	01/06/2010	10000-300000	Inactive since 2012	Worm	Industrial SCADA systems, Windows
	File infection, LAN spreading, USB drives	Cyberespionage	Manufacturing/Commercial Companies Nuclear industry		Iran	
	It initially attacked Windows-based computers to search for Siemens software for PLC (Programmable Logic Controllers) to compromise the application and control it to destroy nuclear centrifuges.					Agent.BTZ, Equation
FinSpy / FinFisher / WingBird	01/01/2007	01/12/2011	100-1000	Active	Backdoor, Bootkit, Rootkit, Trojan	Android, BlackBerry, Linux, OS X, Symbian, Windows, Windows Mobile, iOS
	Network connections, Physical access, Social engineering	Surveillance	Non-governmental organizations Activists, Criminal suspects		Canada, Germany, Indonesia, Japan, Laos People's Democratic Republic, Mexico, Mongolia, Russia, Ukraine, USA, Vietnam, Azerbaijan, Belarus	
	This is a surveillance software sold by Gamma Group for law enforcement, but it seems to have been stolen for nefarious purposes. It exploited a zero-day flaw in MS Word over the years including CVE-2017-8759 and CVE-2017-0199, as well as some of Apple's iTunes versions.					None

Table A.1. (Continued)



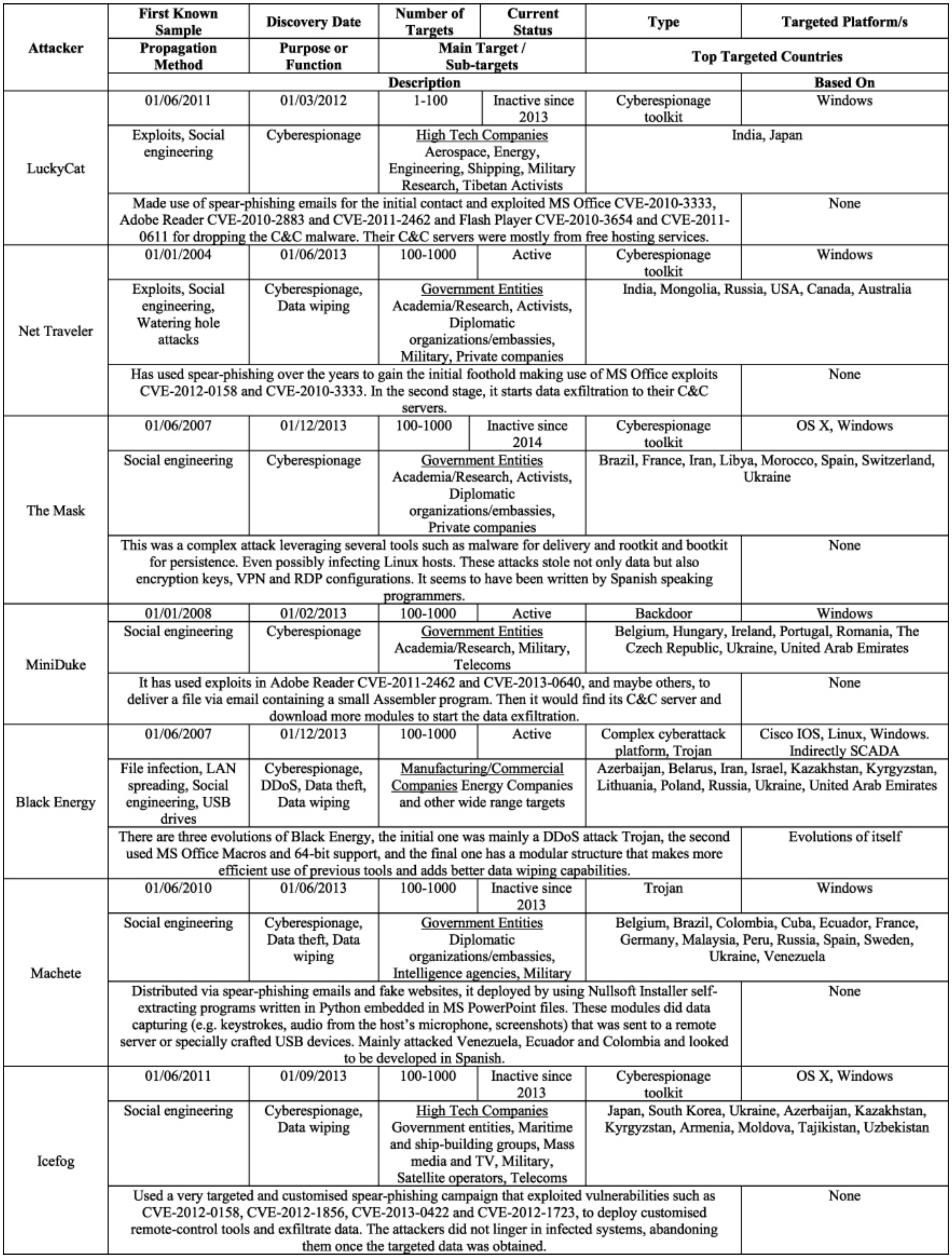
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target and Sub-targets		Top Targeted Countries	
	Description					Based On
Duqu	01/01/2008	15/06/2011	1-100	Inactive since 2012	Trojan	Windows
	Social engineering	Cyberespionage	High technology companies Electronics manufacturing, Information technology, Politicians, Private companies, Software companies, Specific individuals		France, Hungary, Iran, Sudan	
	Known for using several MS Word zero-day exploits, including CVE-2011-3402. It was installed in stages, and after the initial connection to the C&C server, additional modules were downloaded, including 'infostealer' to look for trade details and other information to exfiltrate.					None
Hacking Team RCS	01/01/2008	01/06/2011	100-1000	Active	Backdoor, Bootkit, Rootkit, Trojan	Android, BlackBerry, OS X, Windows, Windows Mobile, iOS
	Bootable CD-ROM, Direct hard disk infection, Exploits, Mobile infections through already infected PCs, Social engineering, USB drives, Others	Surveillance	Non-governmental organizations Activists, Criminal suspects, Journalists, Politicians		Germany, India, Iraq, Italy, Mexico, Russia, Turkey, Ukraine, Vietnam, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Armenia, Moldova, Tajikistan, Uzbekistan.	
	This is a surveillance software for law enforcement and government agencies sold by the company HT S.R.L. Suspicious third parties have sold this product in the open market where it has been used for nefarious purposes. It is usually delivered by exploiting MS Word, Adode Flash in Word documents vulnerabilities.					None
Naikon	01/06/2009	01/12/2011	100-1000	Active	Backdoor, Remote administration tool, Trojan	Windows
	Exploits, Social engineering	Cyberespionage, Remote control, Surveillance	Government entities Military, Private companies		Canada, Indonesia, Lao Peoples Democratic Republic, Malaysia, Myanmar, Nepal, Philippines, Singapore, Thailand, Vietnam, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Armenia, Moldova, Tajikistan, Uzbekistan.	
	It was usually distributed by emails containing exploited MS Word documents via CVE-2012-0158 or similar. Then executes in memory and establishes a connection to the C&C servers to execute modules such as command prompt operations. These attacks are highly focused in the South China Sea region since around 2014 and have human operators per country or region to make it easier to blend in.					None
Lurk	01/01/2011	01/06/2011	10000-300000	Inactive since 2016	Trojan	Windows
	Exploits, Social engineering	Monetization	Financial institutions Journalists, Media, Telecoms		Russia	
	It was highly targeted to Russian institutions and users that the attack detects as of interest for financial details if these parameters were not met, it did not activate.					Evolutions of itself
Regin	01/03/2003	01/03/2011	1-100	Active	Complex cyberattack platform, Rootkit, Trojan	Windows
	USB Drives	Cyberespionage, Facilitating other types of attacks, Remote control	Government Entities Academia/Research, Financial institutions, Multi-national political bodies, Specific individuals, Telecoms		Afghanistan, Algeria, Belgium, Brazil, Fiji, Germany, India, Indonesia, Iran, Kiribati, Malaysia, Pakistan, Russia, Syria	
	This is a very modular attack platform that downloads optional modules as needed and it can store them in the computers' registry. It has attacked GSM networks to stage further attacks as well as doing plain spying.					None Similar vector as Turla
Flame	01/02/2010	01/05/2012	1000-3000	Inactive since 2013	Complex cyberattack platform	Windows
	LAN spreading, USB drives	Cyberespionage	Government Entities Academia/Research, Specific individuals		Egypt, Europe, Iran, Israel, Lebanon, Palestine, Saudi Arabia, Sudan, Syria, Ukraine, Canada, Australia, New Zealand	
	It had backdoor, Trojan, and worm-like features, as well as being capable of downloading modules as needed. All these features made very sophisticated, effective and challenging to detect. It could record voice and take desktop screenshots, both stored in a compressed format and regularly uploaded to the C&C server.					Agent.BTZ, Stuxnet, Equation, Duqu
Winnti	01/01/2009	01/12/2012	1-100	Inactive since 2018	Trojan	Windows
	Social engineering	Data theft, Data wiping	High Tech Companies Software companies		Belarus, Brazil, Germany, Japan, Peru, Russia, South East Asia, Ukraine, Azerbaijan, Kazakhstan, Kyrgyzstan, Armenia, Moldova, Tajikistan, Uzbekistan	
	Utilising the Winnti penetration kit, written in Chinese, attackers sought remote control and data exfiltration of gaming companies. This group still specialises in organisations that require relatively low effort to be breached.					None

Table A.1. (Continued)



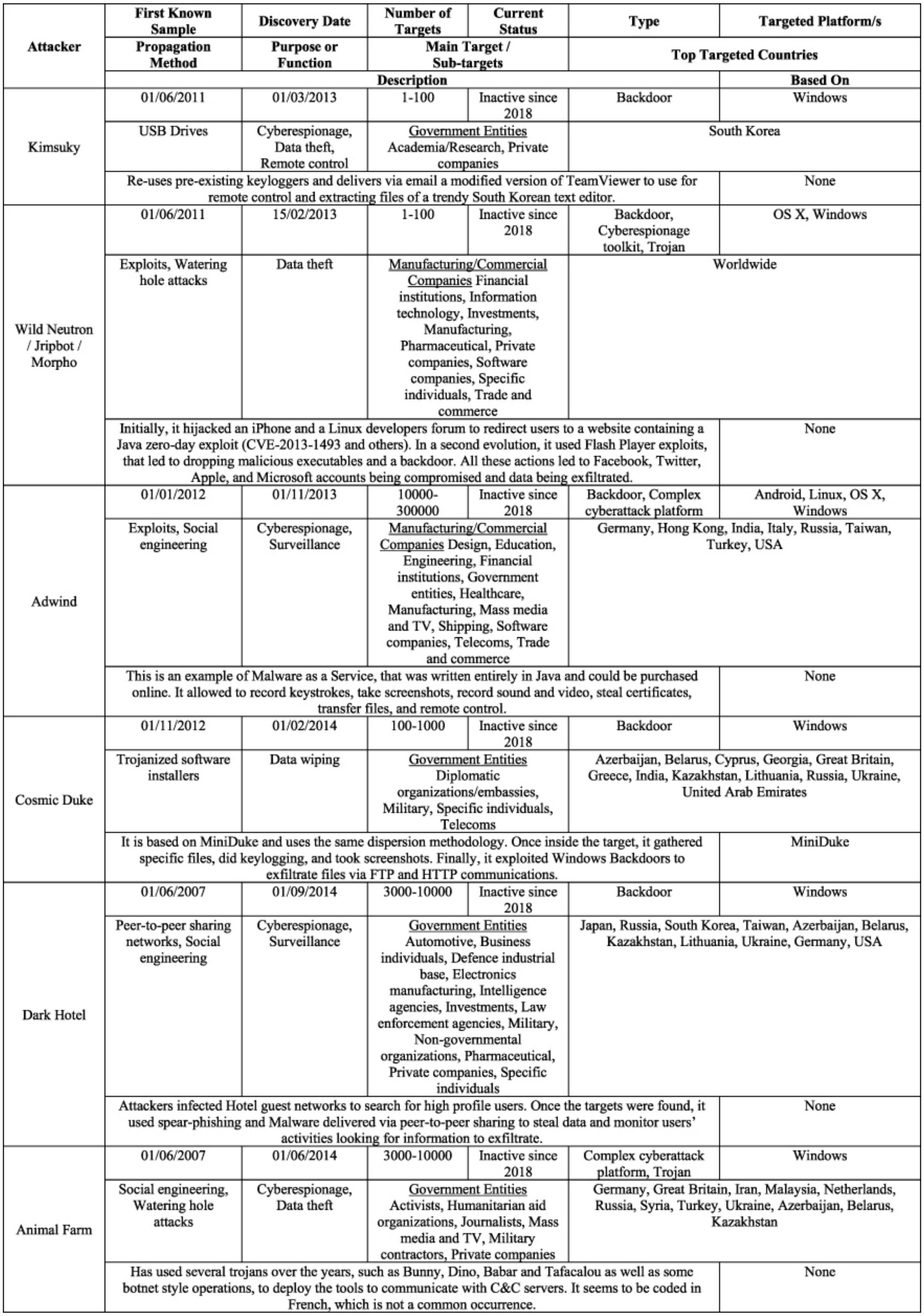
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target and Sub-targets		Top Targeted Countries	
	Description					Based On
Mini Flame	01/01/2010	01/09/2012	0-100	Active	Backdoor	Windows
	USB drives	Cyberespionage	Non-governmental organizations Specific individuals		Iran, Kuwait, Lebanon, Palestine, Qatar	
	This is a highly focused variation of Flame that uses just the backdoor attack vector to spy on targeted individuals.					Flame, Agent.BTZ
Wiper	01/04/2011	01/08/2012	Unknown	Inactive since 2013	Data destroyer	Windows
	Unknown	Data wiping	Manufacturing/Commercial Companies Energy, oil and gas companies, Government entities		Iran	
	No sample has ever been found because it deleted itself, because of this, at times, its existence has been in doubt. Related activity was found in April 2011 in the form of registry entries, that supported its existence.					Duqu, Stuxnet
Madi	01/12/2011	01/07/2012	100-1000	Inactive since 2013	Backdoor	Windows
	Social engineering	Cyberespionage	Manufacturing/Commercial Companies Academia/Research, Business individuals, Critical infrastructure engineering firms, Financial institutions, Government entities		Iran, Israel, Pakistan, Ukraine, Worldwide	
	Used .scr embedded in MS PowerPoint files that ran the attacker's program, and after this initial action, it could run updates from the C&C servers and even new modules.					None
Gauss	01/08/2011	01/09/2012	3000-10000	Inactive since 2013	Cyberespionage toolkit	Windows
	USB drives	Cyberespionage	Non-governmental organizations Specific individuals		Israel, Lebanon, Palestine, Syria	
	It is another variation of Flame mainly focused on users of Lebanese banks, surveilling them and stealing their credentials.					Flame, MiniFlame, Agent.BTZ, Equation
Shamoon	15/08/2012	01/10/2012	1-100	Inactive since 2013	Data destroyer	Windows
	LAN spreading	Data wiping	Manufacturing/Commercial Companies Energy, oil and gas companies		Saudi Arabia	
	This self-replicating attack replaced data files on computers and wiped the data from them. It utilised the Wiper module of Flame.					Flame
SabPub	01/01/2012	27/06/2012	1-100	Active	Backdoor	OS X
	Exploits, Social engineering	Cyberespionage	Non-governmental organizations Activists		India, Ukraine, Western Europe, Canada, Australia, New Zealand	
	Attacked exploited MS Office vulnerability CVE-2009-0563 and Java's CVE-2012-0507.5 to open a backdoor to send screenshots of user's sessions to the C&C server and remotely execute further commands.					LuckyCat
TeamSpy	01/06/2004	01/03/2012	1000-3000	Inactive since 2014	Remote administration tool	Windows
	Exploits, Social engineering	Cyberespionage, Data Theft	Non-governmental organizations Activists, Heavy industry manufacturers, Intelligence agencies		Cambodia, Eastern Europe	
	Used genuine tool TeamViewer as part of their Trojan attack to monitor and control remote computers. Making use of websites that had content relevant to the user the attackers delivered malicious Java exploits (CVE-2012-0507) acting as downloaders and backdoor.					None
Red October	01/05/2007	01/10/2012	100-1000	Inactive since 2013	Complex cyberattack platform	Windows, Windows Mobile
	Exploits, Social engineering	Cyberespionage	Government Entities Academia/Research, Aerospace, Diplomatic organizations/embassies, Military, Trade and commerce		Eastern Europe, Western Europe, Canada, Australia, New Zealand	
	Used exploited vulnerabilities in MS Word (CVE-2010-3333 and CVE-2012-0158), MS Excel (CVE-2009-3129) and Java (CVE-2011-3544) developed by other attackers that were delivered via spear-phishing emails. Had a chain of proxies to hide the C&C server and it was a multi-module development, downloading tools as needed. Capable of exfiltrating data from Windows computers and Windows Mobiles.					Agent.BTZ

Table A.1. (Continued)



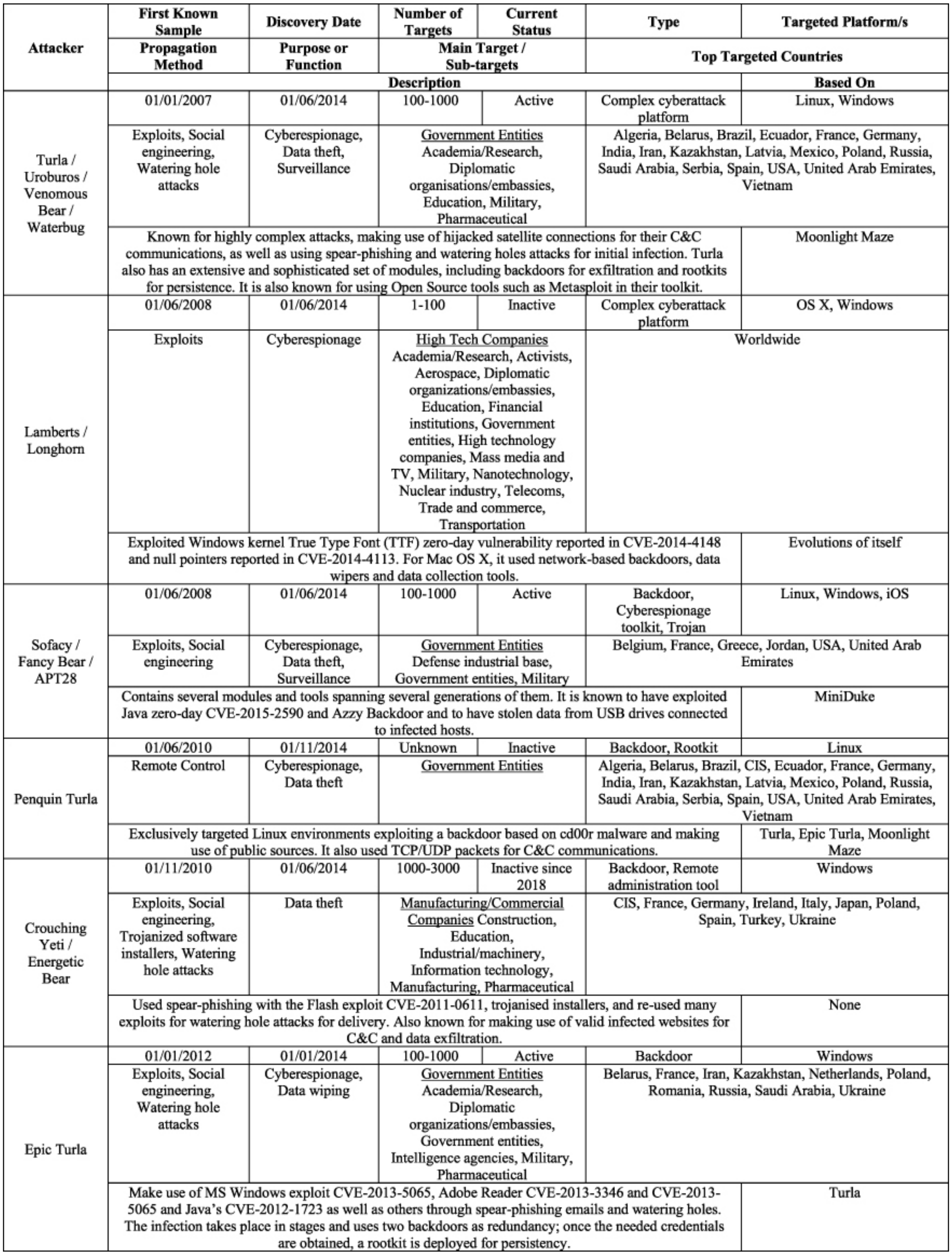
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
LuckyCat	01/06/2011	01/03/2012	1-100	Inactive since 2013	Cyberespionage toolkit	Windows
	Exploits, Social engineering	Cyberespionage	High Tech Companies Aerospace, Energy, Engineering, Shipping, Military Research, Tibetan Activists		India, Japan	
	Made use of spear-phishing emails for the initial contact and exploited MS Office CVE-2010-3333, Adobe Reader CVE-2010-2883 and CVE-2011-2462 and Flash Player CVE-2010-3654 and CVE-2011-0611 for dropping the C&C malware. Their C&C servers were mostly from free hosting services.					None
Net Traveler	01/01/2004	01/06/2013	100-1000	Active	Cyberespionage toolkit	Windows
	Exploits, Social engineering, Watering hole attacks	Cyberespionage, Data wiping	Government Entities Academia/Research, Activists, Diplomatic organizations/embassies, Military, Private companies		India, Mongolia, Russia, USA, Canada, Australia	
	Has used spear-phishing over the years to gain the initial foothold making use of MS Office exploits CVE-2012-0158 and CVE-2010-3333. In the second stage, it starts data exfiltration to their C&C servers.					None
The Mask	01/06/2007	01/12/2013	100-1000	Inactive since 2014	Cyberespionage toolkit	OS X, Windows
	Social engineering	Cyberespionage	Government Entities Academia/Research, Activists, Diplomatic organizations/embassies, Private companies		Brazil, France, Iran, Libya, Morocco, Spain, Switzerland, Ukraine	
	This was a complex attack leveraging several tools such as malware for delivery and rootkit and bootkit for persistence. Even possibly infecting Linux hosts. These attacks stole not only data but also encryption keys, VPN and RDP configurations. It seems to have been written by Spanish speaking programmers.					None
MiniDuke	01/01/2008	01/02/2013	100-1000	Active	Backdoor	Windows
	Social engineering	Cyberespionage	Government Entities Academia/Research, Military, Telecoms		Belgium, Hungary, Ireland, Portugal, Romania, The Czech Republic, Ukraine, United Arab Emirates	
	It has used exploits in Adobe Reader CVE-2011-2462 and CVE-2013-0640, and maybe others, to deliver a file via email containing a small Assembler program. Then it would find its C&C server and download more modules to start the data exfiltration.					None
Black Energy	01/06/2007	01/12/2013	100-1000	Active	Complex cyberattack platform, Trojan	Cisco IOS, Linux, Windows. Indirectly SCADA
	File infection, LAN spreading, Social engineering, USB drives	Cyberespionage, DDoS, Data theft, Data wiping	Manufacturing/Commercial Companies Energy Companies and other wide range targets		Azerbaijan, Belarus, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia, Ukraine, United Arab Emirates	
	There are three evolutions of Black Energy, the initial one was mainly a DDoS attack Trojan, the second used MS Office Macros and 64-bit support, and the final one has a modular structure that makes more efficient use of previous tools and adds better data wiping capabilities.					Evolutions of itself
Machete	01/06/2010	01/06/2013	100-1000	Inactive since 2013	Trojan	Windows
	Social engineering	Cyberespionage, Data theft, Data wiping	Government Entities Diplomatic organizations/embassies, Intelligence agencies, Military		Belgium, Brazil, Colombia, Cuba, Ecuador, France, Germany, Malaysia, Peru, Russia, Spain, Sweden, Ukraine, Venezuela	
	Distributed via spear-phishing emails and fake websites, it deployed by using Nullsoft Installer self-extracting programs written in Python embedded in MS PowerPoint files. These modules did data capturing (e.g. keystrokes, audio from the host's microphone, screenshots) that was sent to a remote server or specially crafted USB devices. Mainly attacked Venezuela, Ecuador and Colombia and looked to be developed in Spanish.					None
Icefog	01/06/2011	01/09/2013	100-1000	Inactive since 2013	Cyberespionage toolkit	OS X, Windows
	Social engineering	Cyberespionage, Data wiping	High Tech Companies Government entities, Maritime and ship-building groups, Mass media and TV, Military, Satellite operators, Telecoms		Japan, South Korea, Ukraine, Azerbaijan, Kazakhstan, Kyrgyzstan, Armenia, Moldova, Tajikistan, Uzbekistan	
	Used a very targeted and customised spear-phishing campaign that exploited vulnerabilities such as CVE-2012-0158, CVE-2012-1856, CVE-2013-0422 and CVE-2012-1723, to deploy customised remote-control tools and exfiltrate data. The attackers did not linger in infected systems, abandoning them once the targeted data was obtained.					None

Table A.1. (Continued)



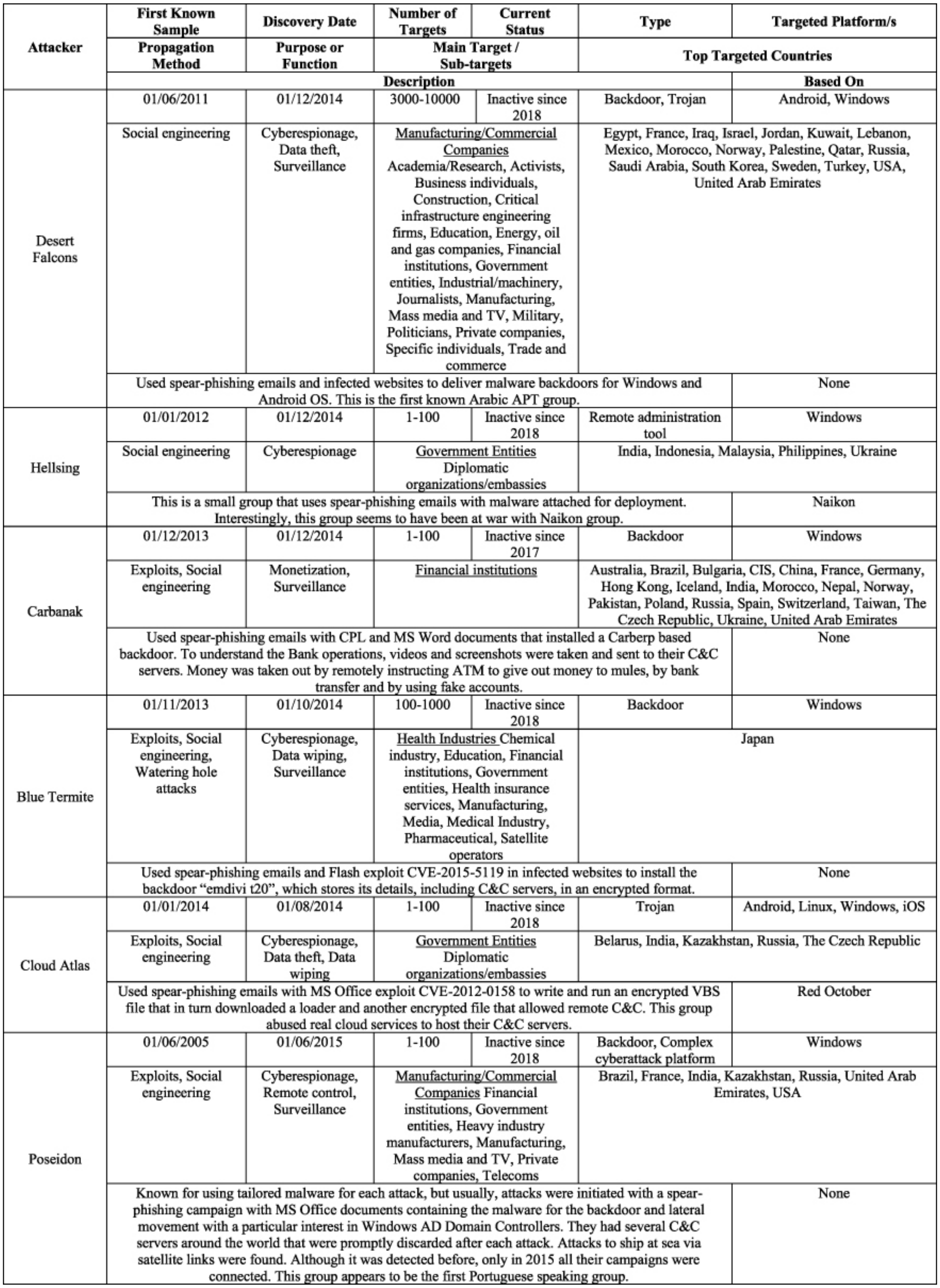
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Kimsuky	01/06/2011	01/03/2013	1-100	Inactive since 2018	Backdoor	Windows
	USB Drives	Cyberespionage, Data theft, Remote control	Government Entities Academia/Research, Private companies		South Korea	
	Re-uses pre-existing keyloggers and delivers via email a modified version of TeamViewer to use for remote control and extracting files of a trendy South Korean text editor.					None
Wild Neutron / Jripbot / Morpho	01/06/2011	15/02/2013	1-100	Inactive since 2018	Backdoor, Cyberespionage toolkit, Trojan	OS X, Windows
	Exploits, Watering hole attacks	Data theft	Manufacturing/Commercial Companies Financial institutions, Information technology, Investments, Manufacturing, Pharmaceutical, Private companies, Software companies, Specific individuals, Trade and commerce		Worldwide	
	Initially, it hijacked an iPhone and a Linux developers forum to redirect users to a website containing a Java zero-day exploit (CVE-2013-1493 and others). In a second evolution, it used Flash Player exploits, that led to dropping malicious executables and a backdoor. All these actions led to Facebook, Twitter, Apple, and Microsoft accounts being compromised and data being exfiltrated.					None
Adwind	01/01/2012	01/11/2013	10000-300000	Inactive since 2018	Backdoor, Complex cyberattack platform	Android, Linux, OS X, Windows
	Exploits, Social engineering	Cyberespionage, Surveillance	Manufacturing/Commercial Companies Design, Education, Engineering, Financial institutions, Government entities, Healthcare, Manufacturing, Mass media and TV, Shipping, Software companies, Telecoms, Trade and commerce		Germany, Hong Kong, India, Italy, Russia, Taiwan, Turkey, USA	
	This is an example of Malware as a Service, that was written entirely in Java and could be purchased online. It allowed to record keystrokes, take screenshots, record sound and video, steal certificates, transfer files, and remote control.					None
Cosmic Duke	01/11/2012	01/02/2014	100-1000	Inactive since 2018	Backdoor	Windows
	Trojanized software installers	Data wiping	Government Entities Diplomatic organizations/embassies, Military, Specific individuals, Telecoms		Azerbaijan, Belarus, Cyprus, Georgia, Great Britain, Greece, India, Kazakhstan, Lithuania, Russia, Ukraine, United Arab Emirates	
	It is based on MiniDuke and uses the same dispersion methodology. Once inside the target, it gathered specific files, did keylogging, and took screenshots. Finally, it exploited Windows Backdoors to exfiltrate files via FTP and HTTP communications.					MiniDuke
Dark Hotel	01/06/2007	01/09/2014	3000-10000	Inactive since 2018	Backdoor	Windows
	Peer-to-peer sharing networks, Social engineering	Cyberespionage, Surveillance	Government Entities Automotive, Business individuals, Defence industrial base, Electronics manufacturing, Intelligence agencies, Investments, Law enforcement agencies, Military, Non-governmental organizations, Pharmaceutical, Private companies, Specific individuals		Japan, Russia, South Korea, Taiwan, Azerbaijan, Belarus, Kazakhstan, Lithuania, Ukraine, Germany, USA	
	Attackers infected Hotel guest networks to search for high profile users. Once the targets were found, it used spear-phishing and Malware delivered via peer-to-peer sharing to steal data and monitor users' activities looking for information to exfiltrate.					None
Animal Farm	01/06/2007	01/06/2014	3000-10000	Inactive since 2018	Complex cyberattack platform, Trojan	Windows
	Social engineering, Watering hole attacks	Cyberespionage, Data theft	Government Entities Activists, Humanitarian aid organizations, Journalists, Mass media and TV, Military contractors, Private companies		Germany, Great Britain, Iran, Malaysia, Netherlands, Russia, Syria, Turkey, Ukraine, Azerbaijan, Belarus, Kazakhstan	
	Has used several trojans over the years, such as Bunny, Dino, Babar and Tafacalou as well as some botnet style operations, to deploy the tools to communicate with C&C servers. It seems to be coded in French, which is not a common occurrence.					None

Table A.1. (Continued)



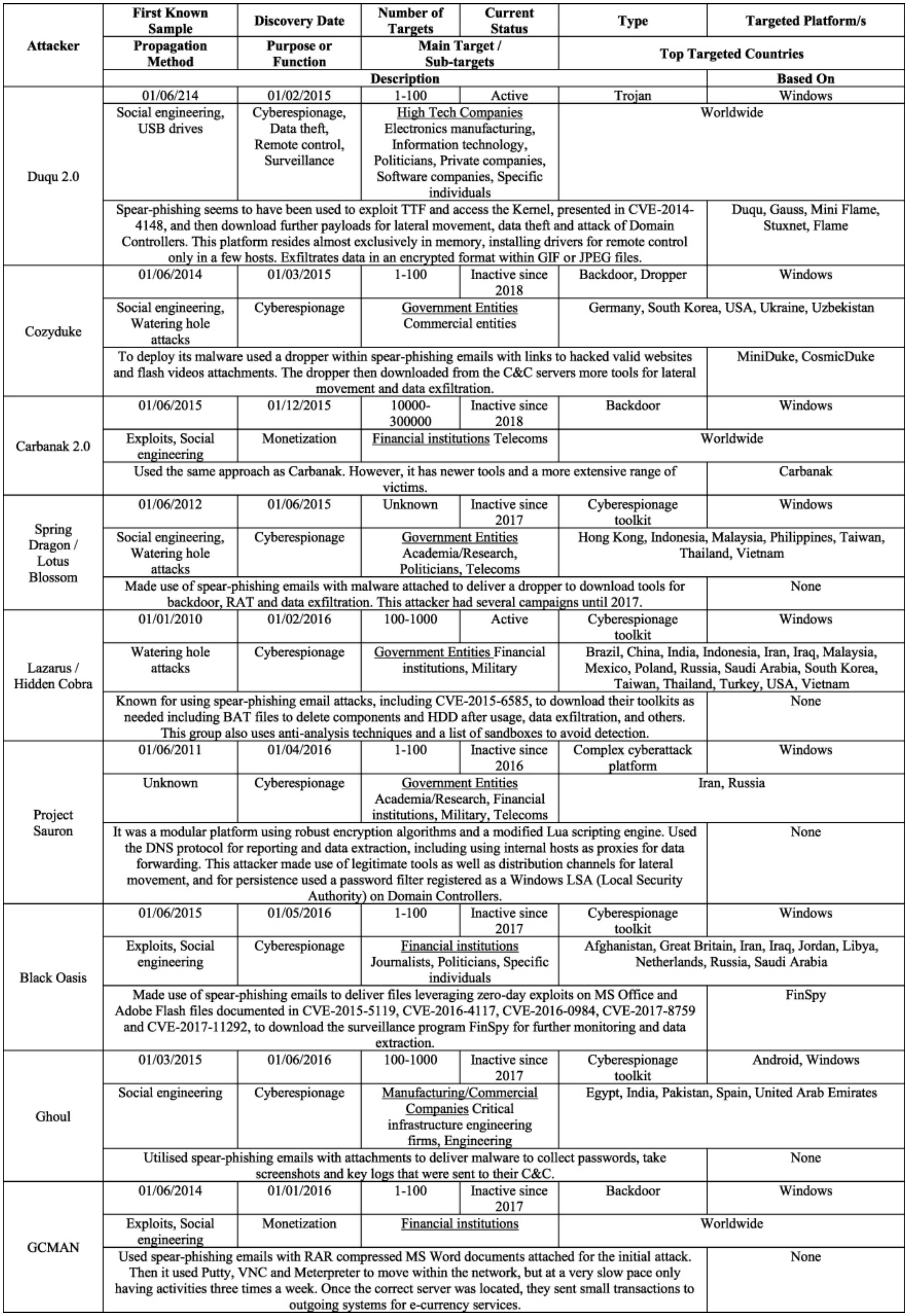
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Turla / Uroburos / Venomous Bear / Waterbug	01/01/2007	01/06/2014	100-1000	Active	Complex cyberattack platform	Linux, Windows
	Exploits, Social engineering, Watering hole attacks	Cyberespionage, Data theft, Surveillance	Government Entities Academia/Research, Diplomatic organisations/embassies, Education, Military, Pharmaceutical		Algeria, Belarus, Brazil, Ecuador, France, Germany, India, Iran, Kazakhstan, Latvia, Mexico, Poland, Russia, Saudi Arabia, Serbia, Spain, USA, United Arab Emirates, Vietnam	
	Known for highly complex attacks, making use of hijacked satellite connections for their C&C communications, as well as using spear-phishing and watering holes attacks for initial infection. Turla also has an extensive and sophisticated set of modules, including backdoors for exfiltration and rootkits for persistence. It is also known for using Open Source tools such as Metasploit in their toolkit.					Moonlight Maze
Lamberts / Longhorn	01/06/2008	01/06/2014	1-100	Inactive	Complex cyberattack platform	OS X, Windows
	Exploits	Cyberespionage	High Tech Companies Academia/Research, Activists, Aerospace, Diplomatic organizations/embassies, Education, Financial institutions, Government entities, High technology companies, Mass media and TV, Military, Nanotechnology, Nuclear industry, Telecoms, Trade and commerce, Transportation		Worldwide	
	Exploited Windows kernel True Type Font (TTF) zero-day vulnerability reported in CVE-2014-4148 and null pointers reported in CVE-2014-4113. For Mac OS X, it used network-based backdoors, data wipers and data collection tools.					Evolutions of itself
Sofacy / Fancy Bear / APT28	01/06/2008	01/06/2014	100-1000	Active	Backdoor, Cyberespionage toolkit, Trojan	Linux, Windows, iOS
	Exploits, Social engineering	Cyberespionage, Data theft, Surveillance	Government Entities Defense industrial base, Government entities, Military		Belgium, France, Greece, Jordan, USA, United Arab Emirates	
	Contains several modules and tools spanning several generations of them. It is known to have exploited Java zero-day CVE-2015-2590 and Azzy Backdoor and to have stolen data from USB drives connected to infected hosts.					MiniDuke
Penquin Turla	01/06/2010	01/11/2014	Unknown	Inactive	Backdoor, Rootkit	Linux
	Remote Control	Cyberespionage, Data theft	Government Entities		Algeria, Belarus, Brazil, CIS, Ecuador, France, Germany, India, Iran, Kazakhstan, Latvia, Mexico, Poland, Russia, Saudi Arabia, Serbia, Spain, USA, United Arab Emirates, Vietnam	
	Exclusively targeted Linux environments exploiting a backdoor based on cd00r malware and making use of public sources. It also used TCP/UDP packets for C&C communications.					Turla, Epic Turla, Moonlight Maze
Crouching Yeti / Energetic Bear	01/11/2010	01/06/2014	1000-3000	Inactive since 2018	Backdoor, Remote administration tool	Windows
	Exploits, Social engineering, Trojanized software installers, Watering hole attacks	Data theft	Manufacturing/Commercial Companies Construction, Education, Industrial/machinery, Information technology, Manufacturing, Pharmaceutical		CIS, France, Germany, Ireland, Italy, Japan, Poland, Spain, Turkey, Ukraine	
	Used spear-phishing with the Flash exploit CVE-2011-0611, trojanised installers, and re-used many exploits for watering hole attacks for delivery. Also known for making use of valid infected websites for C&C and data exfiltration.					None
Epic Turla	01/01/2012	01/01/2014	100-1000	Active	Backdoor	Windows
	Exploits, Social engineering, Watering hole attacks	Cyberespionage, Data wiping	Government Entities Academia/Research, Diplomatic organizations/embassies, Government entities, Intelligence agencies, Military, Pharmaceutical		Belarus, France, Iran, Kazakhstan, Netherlands, Poland, Romania, Russia, Saudi Arabia, Ukraine	
	Make use of MS Windows exploit CVE-2013-5065, Adobe Reader CVE-2013-3346 and CVE-2013-5065 and Java's CVE-2012-1723 as well as others through spear-phishing emails and watering holes. The infection takes place in stages and uses two backdoors as redundancy; once the needed credentials are obtained, a rootkit is deployed for persistence.					Turla

Table A.1. (Continued)



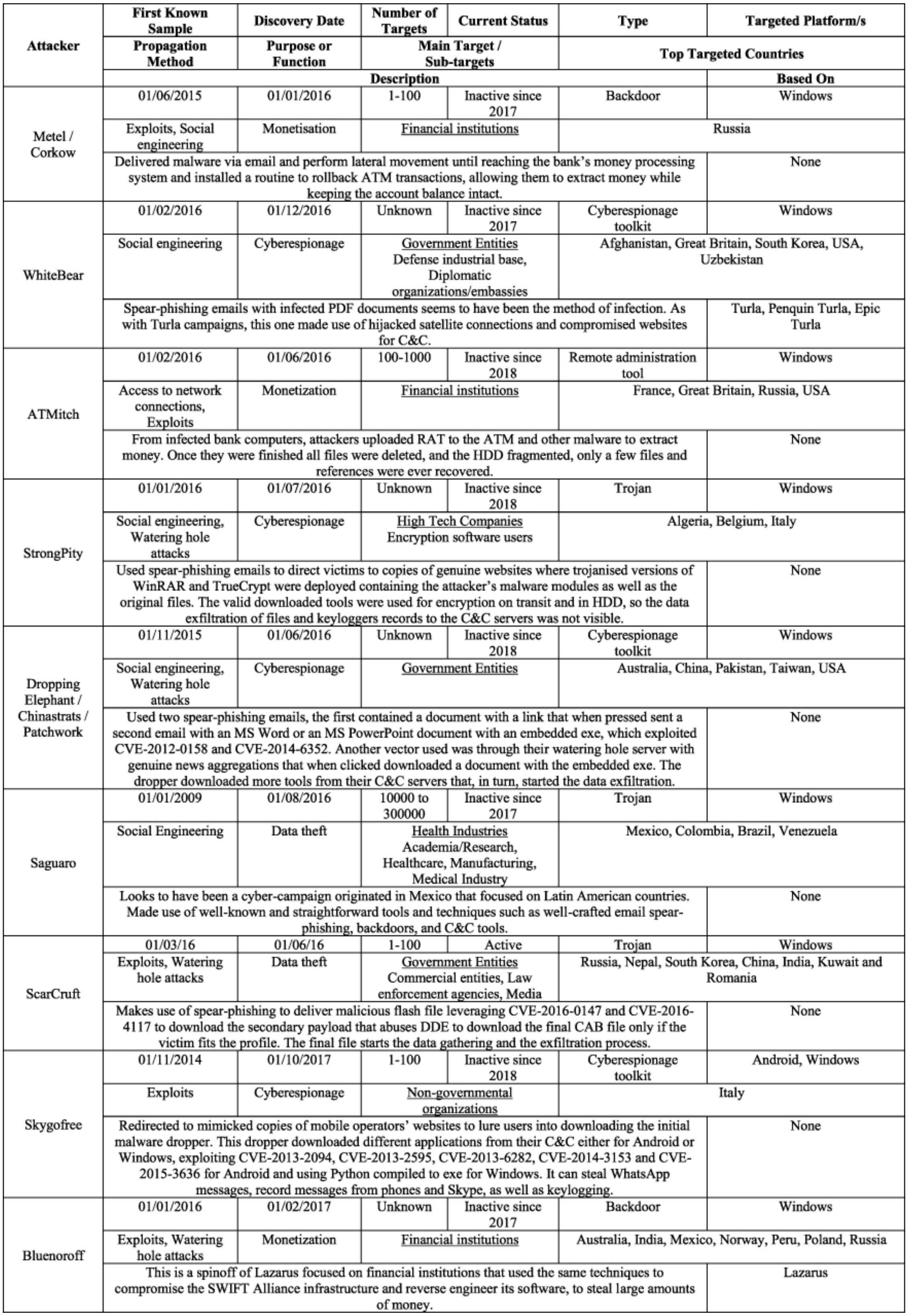
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Desert Falcons	01/06/2011	01/12/2014	3000-10000	Inactive since 2018	Backdoor, Trojan	Android, Windows
	Social engineering	Cyberespionage, Data theft, Surveillance	Manufacturing/Commercial Companies Academia/Research, Activists, Business individuals, Construction, Critical infrastructure engineering firms, Education, Energy, oil and gas companies, Financial institutions, Government entities, Industrial/machinery, Journalists, Manufacturing, Mass media and TV, Military, Politicians, Private companies, Specific individuals, Trade and commerce		Egypt, France, Iraq, Israel, Jordan, Kuwait, Lebanon, Mexico, Morocco, Norway, Palestine, Qatar, Russia, Saudi Arabia, South Korea, Sweden, Turkey, USA, United Arab Emirates	
	Used spear-phishing emails and infected websites to deliver malware backdoors for Windows and Android OS. This is the first known Arabic APT group.					None
Hellsing	01/01/2012	01/12/2014	1-100	Inactive since 2018	Remote administration tool	Windows
	Social engineering	Cyberespionage	Government Entities Diplomatic organizations/embassies		India, Indonesia, Malaysia, Philippines, Ukraine	
	This is a small group that uses spear-phishing emails with malware attached for deployment. Interestingly, this group seems to have been at war with Naikon group.					Naikon
Carbanak	01/12/2013	01/12/2014	1-100	Inactive since 2017	Backdoor	Windows
	Exploits, Social engineering	Monetization, Surveillance	Financial institutions		Australia, Brazil, Bulgaria, CIS, China, France, Germany, Hong Kong, Iceland, India, Morocco, Nepal, Norway, Pakistan, Poland, Russia, Spain, Switzerland, Taiwan, The Czech Republic, Ukraine, United Arab Emirates	
	Used spear-phishing emails with CPL and MS Word documents that installed a Carberp based backdoor. To understand the Bank operations, videos and screenshots were taken and sent to their C&C servers. Money was taken out by remotely instructing ATM to give out money to mules, by bank transfer and by using fake accounts.					None
Blue Termite	01/11/2013	01/10/2014	100-1000	Inactive since 2018	Backdoor	Windows
	Exploits, Social engineering, Watering hole attacks	Cyberespionage, Data wiping, Surveillance	Health Industries Chemical industry, Education, Financial institutions, Government entities, Health insurance services, Manufacturing, Media, Medical Industry, Pharmaceutical, Satellite operators		Japan	
	Used spear-phishing emails and Flash exploit CVE-2015-5119 in infected websites to install the backdoor "emdivi t20", which stores its details, including C&C servers, in an encrypted format.					None
Cloud Atlas	01/01/2014	01/08/2014	1-100	Inactive since 2018	Trojan	Android, Linux, Windows, iOS
	Exploits, Social engineering	Cyberespionage, Data theft, Data wiping	Government Entities Diplomatic organizations/embassies		Belarus, India, Kazakhstan, Russia, The Czech Republic	
	Used spear-phishing emails with MS Office exploit CVE-2012-0158 to write and run an encrypted VBS file that in turn downloaded a loader and another encrypted file that allowed remote C&C. This group abused real cloud services to host their C&C servers.					Red October
Poseidon	01/06/2005	01/06/2015	1-100	Inactive since 2018	Backdoor, Complex cyberattack platform	Windows
	Exploits, Social engineering	Cyberespionage, Remote control, Surveillance	Manufacturing/Commercial Companies Financial institutions, Government entities, Heavy industry manufacturers, Manufacturing, Mass media and TV, Private companies, Telecoms		Brazil, France, India, Kazakhstan, Russia, United Arab Emirates, USA	
	Known for using tailored malware for each attack, but usually, attacks were initiated with a spear-phishing campaign with MS Office documents containing the malware for the backdoor and lateral movement with a particular interest in Windows AD Domain Controllers. They had several C&C servers around the world that were promptly discarded after each attack. Attacks to ship at sea via satellite links were found. Although it was detected before, only in 2015 all their campaigns were connected. This group appears to be the first Portuguese speaking group.					None

Table A.1. (Continued)



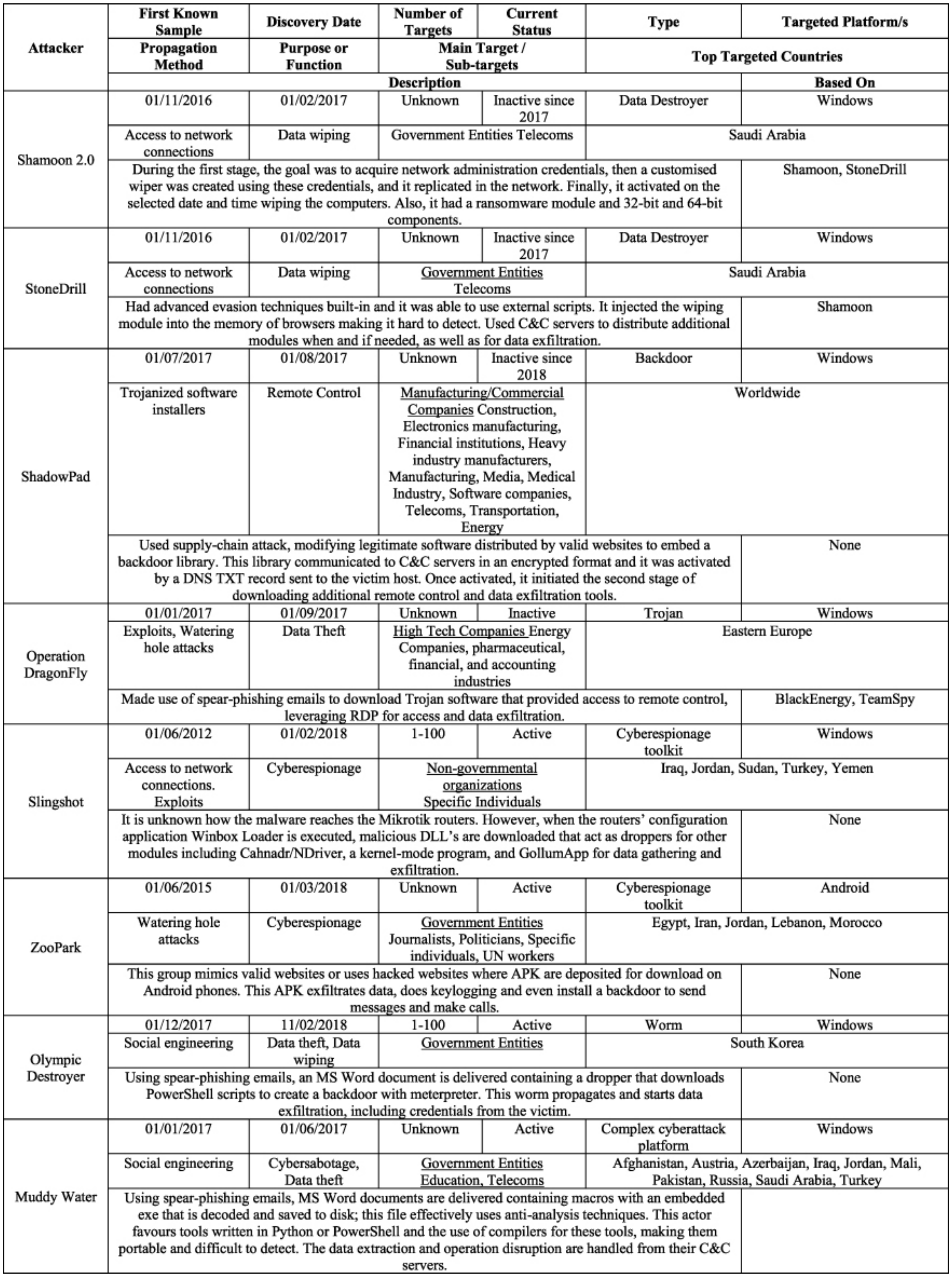
Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Duqu 2.0	01/06/214	01/02/2015	1-100	Active	Trojan	Windows
	Social engineering, USB drives	Cyberespionage, Data theft, Remote control, Surveillance	High Tech Companies Electronics manufacturing, Information technology, Politicians, Private companies, Software companies, Specific individuals		Worldwide	
	Spear-phishing seems to have been used to exploit TTF and access the Kernel, presented in CVE-2014-4148, and then download further payloads for lateral movement, data theft and attack of Domain Controllers. This platform resides almost exclusively in memory, installing drivers for remote control only in a few hosts. Exfiltrates data in an encrypted format within GIF or JPEG files.					Duqu, Gauss, Mini Flame, Stuxnet, Flame
Cozyduke	01/06/2014	01/03/2015	1-100	Inactive since 2018	Backdoor, Dropper	Windows
	Social engineering, Watering hole attacks	Cyberespionage	Government Entities Commercial entities		Germany, South Korea, USA, Ukraine, Uzbekistan	
	To deploy its malware used a dropper within spear-phishing emails with links to hacked valid websites and flash videos attachments. The dropper then downloaded from the C&C servers more tools for lateral movement and data exfiltration.					MiniDuke, CosmicDuke
Carbanak 2.0	01/06/2015	01/12/2015	10000-300000	Inactive since 2018	Backdoor	Windows
	Exploits, Social engineering	Monetization	Financial institutions Telecoms		Worldwide	
	Used the same approach as Carbanak. However, it has newer tools and a more extensive range of victims.					Carbanak
Spring Dragon / Lotus Blossom	01/06/2012	01/06/2015	Unknown	Inactive since 2017	Cyberespionage toolkit	Windows
	Social engineering, Watering hole attacks	Cyberespionage	Government Entities Academia/Research, Politicians, Telecoms		Hong Kong, Indonesia, Malaysia, Philippines, Taiwan, Thailand, Vietnam	
	Made use of spear-phishing emails with malware attached to deliver a dropper to download tools for backdoor, RAT and data exfiltration. This attacker had several campaigns until 2017.					None
Lazarus / Hidden Cobra	01/01/2010	01/02/2016	100-1000	Active	Cyberespionage toolkit	Windows
	Watering hole attacks	Cyberespionage	Government Entities Financial institutions, Military		Brazil, China, India, Indonesia, Iran, Iraq, Malaysia, Mexico, Poland, Russia, Saudi Arabia, South Korea, Taiwan, Thailand, Turkey, USA, Vietnam	
	Known for using spear-phishing email attacks, including CVE-2015-6585, to download their toolkits as needed including BAT files to delete components and HDD after usage, data exfiltration, and others. This group also uses anti-analysis techniques and a list of sandboxes to avoid detection.					None
Project Sauron	01/06/2011	01/04/2016	1-100	Inactive since 2016	Complex cyberattack platform	Windows
	Unknown	Cyberespionage	Government Entities Academia/Research, Financial institutions, Military, Telecoms		Iran, Russia	
	It was a modular platform using robust encryption algorithms and a modified Lua scripting engine. Used the DNS protocol for reporting and data extraction, including using internal hosts as proxies for data forwarding. This attacker made use of legitimate tools as well as distribution channels for lateral movement, and for persistence used a password filter registered as a Windows LSA (Local Security Authority) on Domain Controllers.					None
Black Oasis	01/06/2015	01/05/2016	1-100	Inactive since 2017	Cyberespionage toolkit	Windows
	Exploits, Social engineering	Cyberespionage	Financial institutions Journalists, Politicians, Specific individuals		Afghanistan, Great Britain, Iran, Iraq, Jordan, Libya, Netherlands, Russia, Saudi Arabia	
	Made use of spear-phishing emails to deliver files leveraging zero-day exploits on MS Office and Adobe Flash files documented in CVE-2015-5119, CVE-2016-4117, CVE-2016-0984, CVE-2017-8759 and CVE-2017-11292, to download the surveillance program FinSpy for further monitoring and data extraction.					FinSpy
Ghoul	01/03/2015	01/06/2016	100-1000	Inactive since 2017	Cyberespionage toolkit	Android, Windows
	Social engineering	Cyberespionage	Manufacturing/Commercial Companies Critical infrastructure engineering firms, Engineering		Egypt, India, Pakistan, Spain, United Arab Emirates	
	Utilised spear-phishing emails with attachments to deliver malware to collect passwords, take screenshots and key logs that were sent to their C&C.					None
GCMAN	01/06/2014	01/01/2016	1-100	Inactive since 2017	Backdoor	Windows
	Exploits, Social engineering	Monetization	Financial institutions		Worldwide	
	Used spear-phishing emails with RAR compressed MS Word documents attached for the initial attack. Then it used Putty, VNC and Meterpreter to move within the network, but at a very slow pace only having activities three times a week. Once the correct server was located, they sent small transactions to outgoing systems for e-currency services.					None

Table A.1. (Continued)



Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Metel / Corkow	01/06/2015	01/01/2016	1-100	Inactive since 2017	Backdoor	Windows
	Exploits, Social engineering	Monetisation	Financial institutions		Russia	
	Delivered malware via email and perform lateral movement until reaching the bank's money processing system and installed a routine to rollback ATM transactions, allowing them to extract money while keeping the account balance intact.					None
WhiteBear	01/02/2016	01/12/2016	Unknown	Inactive since 2017	Cyberespionage toolkit	Windows
	Social engineering	Cyberespionage	Government Entities Defense industrial base, Diplomatic organizations/embassies		Afghanistan, Great Britain, South Korea, USA, Uzbekistan	
	Spear-phishing emails with infected PDF documents seems to have been the method of infection. As with Turla campaigns, this one made use of hijacked satellite connections and compromised websites for C&C.					Turla, Penquin Turla, Epic Turla
ATMitch	01/02/2016	01/06/2016	100-1000	Inactive since 2018	Remote administration tool	Windows
	Access to network connections, Exploits	Monetization	Financial institutions		France, Great Britain, Russia, USA	
	From infected bank computers, attackers uploaded RAT to the ATM and other malware to extract money. Once they were finished all files were deleted, and the HDD fragmented, only a few files and references were ever recovered.					None
StrongPity	01/01/2016	01/07/2016	Unknown	Inactive since 2018	Trojan	Windows
	Social engineering, Watering hole attacks	Cyberespionage	High Tech Companies Encryption software users		Algeria, Belgium, Italy	
	Used spear-phishing emails to direct victims to copies of genuine websites where trojanised versions of WinRAR and TrueCrypt were deployed containing the attacker's malware modules as well as the original files. The valid downloaded tools were used for encryption on transit and in HDD, so the data exfiltration of files and keyloggers records to the C&C servers was not visible.					None
Dropping Elephant / Chinastrats / Patchwork	01/11/2015	01/06/2016	Unknown	Inactive since 2018	Cyberespionage toolkit	Windows
	Social engineering, Watering hole attacks	Cyberespionage	Government Entities		Australia, China, Pakistan, Taiwan, USA	
	Used two spear-phishing emails, the first contained a document with a link that when pressed sent a second email with an MS Word or an MS PowerPoint document with an embedded exe, which exploited CVE-2012-0158 and CVE-2014-6352. Another vector used was through their watering hole server with genuine news aggregations that when clicked downloaded a document with the embedded exe. The dropper downloaded more tools from their C&C servers that, in turn, started the data exfiltration.					None
Saguaro	01/01/2009	01/08/2016	10000 to 300000	Inactive since 2017	Trojan	Windows
	Social Engineering	Data theft	Health Industries Academia/Research, Healthcare, Manufacturing, Medical Industry		Mexico, Colombia, Brazil, Venezuela	
	Looks to have been a cyber-campaign originated in Mexico that focused on Latin American countries. Made use of well-known and straightforward tools and techniques such as well-crafted email spear-phishing, backdoors, and C&C tools.					None
ScarCruft	01/03/16	01/06/16	1-100	Active	Trojan	Windows
	Exploits, Watering hole attacks	Data theft	Government Entities Commercial entities, Law enforcement agencies, Media		Russia, Nepal, South Korea, China, India, Kuwait and Romania	
	Makes use of spear-phishing to deliver malicious flash file leveraging CVE-2016-0147 and CVE-2016-4117 to download the secondary payload that abuses DDE to download the final CAB file only if the victim fits the profile. The final file starts the data gathering and the exfiltration process.					None
Skygofree	01/11/2014	01/10/2017	1-100	Inactive since 2018	Cyberespionage toolkit	Android, Windows
	Exploits	Cyberespionage	Non-governmental organizations		Italy	
	Redirected to mimicked copies of mobile operators' websites to lure users into downloading the initial malware dropper. This dropper downloaded different applications from their C&C either for Android or Windows, exploiting CVE-2013-2094, CVE-2013-2595, CVE-2013-6282, CVE-2014-3153 and CVE-2015-3636 for Android and using Python compiled to exe for Windows. It can steal WhatsApp messages, record messages from phones and Skype, as well as keylogging.					None
Bluenoroff	01/01/2016	01/02/2017	Unknown	Inactive since 2017	Backdoor	Windows
	Exploits, Watering hole attacks	Monetization	Financial institutions		Australia, India, Mexico, Norway, Peru, Poland, Russia	
	This is a spinoff of Lazarus focused on financial institutions that used the same techniques to compromise the SWIFT Alliance infrastructure and reverse engineer its software, to steal large amounts of money.					Lazarus

Table A.1. (Continued)



Attacker	First Known Sample	Discovery Date	Number of Targets	Current Status	Type	Targeted Platform/s
	Propagation Method	Purpose or Function	Main Target / Sub-targets		Top Targeted Countries	
	Description					Based On
Shamoon 2.0	01/11/2016	01/02/2017	Unknown	Inactive since 2017	Data Destroyer	Windows
	Access to network connections	Data wiping	Government Entities Telecoms		Saudi Arabia	
	During the first stage, the goal was to acquire network administration credentials, then a customised wiper was created using these credentials, and it replicated in the network. Finally, it activated on the selected date and time wiping the computers. Also, it had a ransomware module and 32-bit and 64-bit components.					Shamoon, StoneDrill
StoneDrill	01/11/2016	01/02/2017	Unknown	Inactive since 2017	Data Destroyer	Windows
	Access to network connections	Data wiping	Government Entities Telecoms		Saudi Arabia	
	Had advanced evasion techniques built-in and it was able to use external scripts. It injected the wiping module into the memory of browsers making it hard to detect. Used C&C servers to distribute additional modules when and if needed, as well as for data exfiltration.					Shamoon
ShadowPad	01/07/2017	01/08/2017	Unknown	Inactive since 2018	Backdoor	Windows
	Trojanized software installers	Remote Control	Manufacturing/Commercial Companies Construction, Electronics manufacturing, Financial institutions, Heavy industry manufacturers, Manufacturing, Media, Medical Industry, Software companies, Telecoms, Transportation, Energy		Worldwide	
	Used supply-chain attack, modifying legitimate software distributed by valid websites to embed a backdoor library. This library communicated to C&C servers in an encrypted format and it was activated by a DNS TXT record sent to the victim host. Once activated, it initiated the second stage of downloading additional remote control and data exfiltration tools.					None
Operation DragonFly	01/01/2017	01/09/2017	Unknown	Inactive	Trojan	Windows
	Exploits, Watering hole attacks	Data Theft	High Tech Companies Energy Companies, pharmaceutical, financial, and accounting industries		Eastern Europe	
	Made use of spear-phishing emails to download Trojan software that provided access to remote control, leveraging RDP for access and data exfiltration.					BlackEnergy, TeamSpy
Slingshot	01/06/2012	01/02/2018	1-100	Active	Cyberespionage toolkit	Windows
	Access to network connections. Exploits	Cyberespionage	Non-governmental organizations Specific Individuals		Iraq, Jordan, Sudan, Turkey, Yemen	
	It is unknown how the malware reaches the Mikrotik routers. However, when the routers' configuration application Winbox Loader is executed, malicious DLL's are downloaded that act as droppers for other modules including Cahnadr/NDriver, a kernel-mode program, and GollumApp for data gathering and exfiltration.					None
ZooPark	01/06/2015	01/03/2018	Unknown	Active	Cyberespionage toolkit	Android
	Watering hole attacks	Cyberespionage	Government Entities Journalists, Politicians, Specific individuals, UN workers		Egypt, Iran, Jordan, Lebanon, Morocco	
	This group mimics valid websites or uses hacked websites where APK are deposited for download on Android phones. This APK exfiltrates data, does keylogging and even install a backdoor to send messages and make calls.					None
Olympic Destroyer	01/12/2017	11/02/2018	1-100	Active	Worm	Windows
	Social engineering	Data theft, Data wiping	Government Entities		South Korea	
	Using spear-phishing emails, an MS Word document is delivered containing a dropper that downloads PowerShell scripts to create a backdoor with meterpreter. This worm propagates and starts data exfiltration, including credentials from the victim.					None
Muddy Water	01/01/2017	01/06/2017	Unknown	Active	Complex cyberattack platform	Windows
	Social engineering	Cybersabotage, Data theft	Government Entities Education, Telecoms		Afghanistan, Austria, Azerbaijan, Iraq, Jordan, Mali, Pakistan, Russia, Saudi Arabia, Turkey	
	Using spear-phishing emails, MS Word documents are delivered containing macros with an embedded exe that is decoded and saved to disk; this file effectively uses anti-analysis techniques. This actor favours tools written in Python or PowerShell and the use of compilers for these tools, making them portable and difficult to detect. The data extraction and operation disruption are handled from their C&C servers.					

References

1 Kaspersky Lab. *Kaspersky press releases [Internet]*. Kaspersky Lab. 2017 Jun 30. Available from: https://www.kaspersky.com/about/press-releases/2017_behind-the-scenes-of-kaspersky-labs-top-apt-discoveries.

2 Trend Micro. *Threat reports [Internet]*. Trend Micro. 2017 Feb 28. Available from: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

3 Symantec Corporation. *ISTR—Internet Security Threat Report*. April 2017. Available from: https://docs.broadcom.com/doc/istr-5-1-en-in.

4 Symantec Corporation. *ISTR—Internet Security Threat Report [Internet]*. March 2018 [cited 2018 March]. Available from: https://www.symantec.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape.

5 Chandra V, Challa N, Pasupuleti S. Advanced persistent threat defense system using self-destructive mechanism for cloud security. In: *2nd IEEE International Conference on Engineering and Technology (ICETECH); 17th & 18th March 2016; Coimbatore, TN, India*. Piscataway, NJ: IEEE; 2016.

6 Messaoud B, Guennoun K, Wahbi M, Sadik M. Advanced persistent threat: new analysis driven by life cycle phases and their challenges. In: *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS); Marrakesh*. Piscataway, NJ: IEEE; 2016.

7 Tankard C. Advanced persistent threats and how to monitor and deter them. *Netw Secur*. 2011;**2011**(8):16–19.

8 Sood AK, Richard EJ. Targeted cyberattacks: a superset of advanced persistent threats. *IEEE Secur Priv*. 2013;**11**(1):54–61.

9 Hu P, Li H, Fu H, Cansever D, Mohapatra P. Dynamic defense strategy against an advanced persistent threat with insiders. In: *2015 IEEE Conference on Computer Communications (INFOCOM); Kowloon*. Piscataway, NJ: IEEE; 2015.

10 Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion Kill Chains. In: *6th Annual International Conference on Information Warfare and Security; Washington, DC*. Reading, MA: Academic; 2011.

11 Bejtlich R. *Understanding the advanced persistent threat [Internet]*. 2010 July. Available from: https://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat.

12 Vukalovic J, Delija D. Advanced persistent threats—detection and defense. In: *2015 38th International Convention on Information and Communication Technology, Electronics, and Microelectronics (MIPRO); Opatija, Croatia*. Piscataway, NJ: IEEE; 2015.

13 Paradise A, Shabtai A, Puzis R, Elyashar A, Elovici Y, Roshandel M, et al. Creation and management of social network honeypots for detecting targeted cyber attacks. *IEEE Trans Comput Soc Syst*. 2017;**4**(3):65–79.

14 Ussath M, Jaeger D, Cheng F, Meinel C. Advanced persistent threats: behind the scenes. In: *Annual Conference on Information Science and Systems (CISS); Princeton*. Piscataway, NJ: IEEE; 2016.

15 McWorther D. *APT1 exposing one of China's cyber espionage units [Internet]*. 2013. Available from: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

16 Bryant BD, Saiedian H. A novel kill-chain framework for remote security log analysis with SIEM software. *ScienceDirect Comput Secur*. 2017;198–210.

17 Lemay A, Calvet J, Menet F, Fernandez J. Survey of publicly available reports on advanced persistent threat actors. *Comput Secur*. 2018;**72**: 26–59.

18 Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. *IEEE Commun Surv Tutor*. 2019;**21**(2):1851–1877.

19 Kaspersky Lab. *Targeted cyberattacks logbook [Internet]*. 2018. Available from: https://apt.securelist.com/#!/threats/.

20 Holloway M. *Stuxnet worm attack on Iranian nuclear facilities [Internet]*. 2015 Jul 16. Available from: http://large.stanford.edu/courses/2015/ph241/holloway1/.

21 Marczk B, Guarnieri C, Marquis-Boire M, Scott-Railton J. *Mapping hacking team's "untraceable" spyware [Internet]*. 2014 Feb 17. Available from: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

22 Tivadar M, Balazs B, Istrate C. *Downloads [Internet]*. Apr 2013. Available from: https://labs.bitdefender.com/wp-content/uploads/downloads/2013/04/MiniDuke_Paper_Final.pdf.

23 F-Secure Labs. *F-secure whitepapers [Internet]*. 2015. Available from: https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf.

24 Zaharia A. *Security alert: TeamSpy malware spammers use TeamViewer as spying tool [Internet]*. 2017 Feb 20. Available from: https://heimdalsecurity.com/blog/security-alert-teamspy-turn-teamviewer-into-spying-tool/.

25 Symantec. *The madi attacks: series of social engineering campaigns [Internet]*. 2012 Jul 17. Available from: https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns.

26 Rascagneres P, Lee M. *Who wasn't responsible for olympic destroyer? [Internet]*. 2018 Feb 26. Available from: https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html.

27 Mercer W, Rascagneres P, Molyett M. *Olympic destroyer takes aim at winter olympics [Internet]*. 2018 Feb 12. Available from: https://blog.talosintelligence.com/2018/02/olympic-destroyer.html.

28 Allievi A. *Snake campaign: a few words about the uroburos rootkit [Internet]*. 2014 Apr 22. Available from: https://blog.talosintelligence.com/search?q=turla.

29 McAfee. *Threat landscape dashboard—campaigns [Internet]*. 2018. Available from: https://www.mcafee.com/enterprise/en-gb/threat-center/threat-landscape-dashboard/campaigns.html.

30 Beek C. *Operation dragonfly [Internet]*. 2017 Dec 17. Available from: https://securingtomorrow.mcafee.com/mcafee-labs/operation-dragonfly-analysis-suggests-links-to-earlier-attacks/.

31 Symantec. *Longhorn: tools used by cyberespionage group linked to vault 7 [Internet]*. 2017 Apr 10. Available from: https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7.

32 Trend Micro Research Team. *Luckycat redux [Internet]*. 2012. Available from: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2012/04/20083243/wp_luckycat_redux.pdf.

33 Bulusu ST, Laborde R, Wazan AS, Barrere F, Benzekri A. Describing advanced persistent threats using a multi-agent system approach. In: *2017 1st Cyber Security in Networking Conference (CSNet); Rio de Janeiro*. Piscataway, NJ: IEEE; 2017.

34 Moubarak J, Chamoun M, Filiol E. Comparative study of recent MEA malware phylogeny. In: *The 2nd International Conference on Computer and Communication Systems; Krakow*. Piscataway, NJ: IEEE; 2017.

35 Virvilis N, Gritzalis D. The big four—what we did wrong in advanced persistent threat detection? In: *Availability reliability and security (ARES) 2013 Eighth International Conference on Regensburg*. Piscataway, NJ: IEEE; 2013.

36 Doman C. *The first cyber espionage attacks: How operation moonlight maze made history [Internet]*. 2016 Jul 7 [cited 2018 March 8]. Available from: https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7.

37 Kaspersky Lab Global Research & Analysis Team (GReAT). *Equation: the death star of malware galaxy [Internet]*. Kaspersky Lab. 2015 Feb 16 [cited 2018 April 8]. Available from: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

38 Shevchenko S. *Agent. btz—a threat that hit Pentagon, Threat Expert Blog [Internet]*. 2008 Nov 30 [cited 2018 April 8]. Available from: http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html.

39 Jiang G, Read B, Bennett J. *FireEye uncove CVE-2017-8759: zero-day used in the wild to distribute FINSPY, FireEye [Internet]*. 2017 Sep 12 [cited 2018 April 8]. Available from: https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html.

40 Kaspersky Lab Global Research & Analysis Team (GReAT). *The TeamSpy crew attacks—abusing TeamViewer for cyberespionage [Internet]*. Kaspersky Lab. 2013 Mar 20 [cited 2018 April 7]. Available from: https://securelist.com/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/35520/.

41 Baumgartner K, Golovkin M. *The Naikon APT [Internet]*. Kaspersky Lab. 2015 Mar 14 [cited 2018 April 7]. Available from: https://securelist.com/the-naikon-apt/69953/.

42 Shulmin A, Prokhorenko M. *Lurk banker Trojan: exclusively for Russia [Internet]*. Kaspersky Lab. 2016 Jun 10 [cited 2018 April 7]. Available from: https://securelist.com/lurk-banker-trojan-exclusively-for-russia/75040/.

43 Kaspersky Lab Global Research & Analysis Team (GReAT). *Regin: nation-state ownage of GSM networks [Internet]*. Kaspersky Lab. 2014 Nov 24 [cited 2018 April 8]. Available from: https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/.

44 Pernet C. *Winnti abuses GitHub for C&C communications, TrendMicro [Internet]*. 2017 Mar 22 [cited 2018 April 7]. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/.

45 Kaspersky Lab Global Research & Analysis Team (GReAT). *What was that Wiper thing? [Internet]*. Kaspersky Lab. 2012 Aug 29 [cited 2018 April 14]. Available from: https://securelist.com/what-was-that-wiper-thing-48/34088/.

46 Symantec Security Response. *The madi attacks: series of social engineering campaigns [Internet]*. Symantec. 2012 Jul 28 [cited 2018 April 14]. Available from: https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns.

47 Kaspersky Lab Global Research & Analysis Team (GReAT). *Gauss: nation-state cyber-surveillance meets banking Trojan [Internet]*. Kaspersky Lab. 2012 Aug 9 [cited 2018 April 14]. Available from: https://securelist.com/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/33854/.

48 Kaspersky Lab Global Research & Analysis Team (GReAT). *Shamoon the Wiper—copycats at work [Internet]*. Kaspersky Lab. 2012 Aug 16 [cited 2018 April 14]. Available from: https://securelist.com/shamoon-the-wiper-copycats-at-work/57854/.

49 Raiu C. *SabPub Mac OS X backdoor: Java exploits, targeted attacks, and possible APT link [Internet]*. Kaspersky Lab. 2012 Apr 14 [cited 2018 April 14]. Available from: https://securelist.com/sabpub-mac-os-x-backdoor-java-exploits-targeted-attacks-and-possible-apt-link-23/33183/.

50 Kaspersky Lab Global Research & Analysis Team (GReAT). *The TeamSpy crew attacks—abusing TeamViewer for cyberespionage [Internet]*. Kaspersky Lab. 2013 Mar 20 [cited 2018 April 14]. Available from: https://securelist.com/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/35520/.

51 Ács-Kurucz G, Molnár G, Vaspöri G, Kamarás R, Buttyán L, Bencsáth B. *Duqu 2.0: a comparison to Duqu [Internet]*. 2015. Available from: https://www.crysys.hu/publications/files/duqu2.pdf.

52 Kaspersky Lab Global Research & Analysis Team (GReAT). *Red october diplomatic cyber attacks investigation [Internet]*. Kaspersky Lab. 2013 Jan 14 [cited 2018 April 15]. Available from: https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/.

53 Kaspersky Lab Global Research & Analysis Team (GReAT). *NetTraveler is running!"—red star APT attacks compromise high-profile victims [Internet]*. Kaspersky Lab. 2013 Jun 4 [cited 2018 April 15]. Available from: https://securelist.com/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/35936/.

54 Kaspersky Lab Global Research & Analysis Team (GReAT). *Kaspersky lab uncovers "the mask" [Internet]*. Kaspersky Lab. 2014 Feb 11 [cited 2018 April 15]. Available from: https://usa.kaspersky.com/about/press-releases/2014_kaspersky-lab-uncovers–the-mask–one-of-the-most-advanced-global-cyber-espionage-operations-to-date-due-to-the-complexity-of-the-toolset-used-by-the-attackers.

55 Kaspersky Lab Global Research & Analysis Team (GReAT). *BlackEnergy APT attacks in Ukraine employ spearphishing with Word documents [Internet]*. Kaspersky Lab. 2016 Jan 28 [cited 2018 April 15]. Available from: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.

56 Kaspersky Lab Global Research & Analysis Team (GReAT). *El Machete [Internet]*. Kaspersky Lab. 2014 Aug 20 [cited 2018 April 15]. Available from: https://securelist.com/el-machete/66108/.

57 Kaspersky Lab Global Research & Analysis Team (GReAT). *The icefog APT: a tale of cloak and three daggers [Internet]*. Kaspersky Lab. 2013 Sep 25 [cited 2018 April 15]. Available from: https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/.

58 Tarakanov D. *Kimsuky APT: operation's possible North Korean links uncovered [Internet]*. Kaspersky Lab. 2013 Sep 11 [cited 2018 April 21]. Available from: https://securelist.com/kimsuky-apt-operations-possible-north-korean-links-uncovered/57335/.

59 Kaspersky Lab Global Research & Analysis Team (GReAT). *Wild neutron—economic espionage threat actor returns with new tricks [Internet]*. Kaspersky Lab. 2015 Jul 8 [cited 2018 April 21]. Available from: https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/.

60 Kaspersky Lab Global Research & Analysis Team (GReAT). *Expert: cross-platform Adwind RAT [Internet]*. Kaspersky Lab. 2016 Feb 11 [cited 2018 April 21]. Available from: https://securelist.com/expert-cross-platform-adwind-rat/73773/.

61 Paganini P. *CosmicDuke malware surprisingly linked to Miniduke campaign, Security Affairs [Internet]*. 2014 July 3 [cited 2018 April 21]. Available from: https://securityaffairs.co/wordpress/26311/cyber-crime/cosmicduke-malware-surprisingly-linked-miniduke-campaign.html.

62 Kaspersky Lab Global Research & Analysis Team (GReAT). *The darkhotel APT [Internet]*. Kaspersky Lab. November 2014 [cited 2018 April 21]. Available from: https://securelist.com/the-darkhotel-apt/66779/.

63 Kaspersky Lab Global Research & Analysis Team (GReAT). *Animals in the APT farm [Internet]*. Kaspersky Lab. 2015 Mar 6 [cited 2018 April 21]. Available from: https://securelist.com/animals-in-the-apt-farm/69114/.

64 Gostev A. *Agent. btz: a source of inspiration? [Internet]*. Kaspersky Lab. 2014 Mar 12 [cited 2018 April 21]. Available from: https://securelist.com/agent-btz-a-source-of-inspiration/58551/.

65 Symantec Security Response. *Longhorn: tools used by cyberespionage group linked to Vault 7 [Internet]*. Symantec. 2017 Apr 10 [cited 2018 April 21]. Available from: https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7.

66 Kaspersky Lab Global Research & Analysis Team (GReAT). *Sofacy APT hits high profile targets with the updated toolset [Internet]*. Kaspersky Lab. 2015 Dec 4 [cited 2018 April 21]. Available from: https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/.

67 Baumgartner K, Raiu C. *The 'Penquin' Turla [Internet]*. Kaspersky Lab. 2014 Dec 8 [cited 2018 April 21]. Available from: https://securelist.com/the-penquin-turla-2/67962/.

68 Kaspersky Lab Global Research & Analysis Team (GReAT). *Energetic bear: more like a Crouching Yeti [Internet]*. Kaspersky Lab. 2014 July 31 [cited 2018 April 21]. Available from: https://securelist.com/energetic-bear-more-like-a-crouching-yeti/65240/.

69 Saad G, Hasbini MA. *The desert falcons targeted attacks [Internet]*. Kaspersky Lab. 2015 Feb 17 [cited 2018 April 21]. Available from: https://securelist.com/the-desert-falcons-targeted-attacks/68817/.

70 Kaspersky Lab Global Research & Analysis Team (GReAT). *The epic Turla operation [Internet]*. Kaspersky Lab. 2014 Aug 7 [cited 2018 April 21]. Available from: https://securelist.com/the-epic-turla-operation/65545/.

71 Raiu C, Golvkin M. *The chronicles of the hellsing APT: the empire strikes back [Internet]*. Kaspersky Lab. 2015 Apr 15 [cited 2018 April 21]. Available from: https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/.

72 Kaspersky Lab Global Research & Analysis Team (GReAT). *The great bank robbery: the Carbanak APT [Internet]*. Kaspersky Lab. 2015 Feb 16 [cited 2018 April 21]. Available from: https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/.

73 Ishimaru S. *New activity of the blue termite APT [Internet]*. Kaspersky Lab. 2015 Aug 20 [cited 2018 April 21]. Available from: https://securelist.com/new-activity-of-the-blue-termite-apt/71876/.

74 Kaspersky Lab Global Research & Analysis Team (GReAT). *Cloud Atlas: October APT is back in style [Internet]*. Kaspersky Lab. 2014 Dec 10 [cited 2018 April 21]. Available from: https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/.

75 Kaspersky Lab Global Research & Analysis Team (GReAT). *Poseidon group: a targeted attack boutique specializing in global cyber-espionage [Internet]*. Kaspersky Lab. 2016 Feb 9 [cited 2018 April 21]. Available from: https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/.

76 Kaspersky Lab Global Research & Analysis Team (GReAT). *The mystery of Duqu 2.0: a sophisticated cyberespionage actor returns [Internet]*. Kaspersky Lab. 2015 June 10 [cited 2018 April 21]. Available from: https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/.

77 Baumgartner K, Raiu C. *The CozyDuke APT [Internet]*. Kaspersky Lab. 2015 Apr 21 [cited 2018 April 21]. Available from: https://securelist.com/the-cozyduke-apt/69731/.

78 Kaspersky Lab Global Research & Analysis Team (GReAT). *APT-style bank robberies increase with Metel, GCMAN, and Carbanak 2.0 attacks [Internet]*. Kaspersky Lab. 2016 Feb 8 [cited 2018 April 21]. Available from: https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/.

79 Shabab N. *Spring dragon—updated activity [Internet]*. Kaspersky Lab. 2017 Jul 24 [cited 2018 April 22]. Available from: https://securelist.com/spring-dragon-updated-activity/79067/.

80 Sherstobitoff R. *Lazarus Resurfaces, Targets Global Banks and Bitcoin Users, McAfee [Internet]*. 2018 Feb 12 [cited 2018 April 22]. Available from: https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/.

81 Kaspersky Lab Global Research & Analysis Team (GReAT). *Lazarus under the hood [Internet]*. Kaspersky Lab. 2017 Apr 3 [cited 2018 April 22]. Available from: https://securelist.com/lazarus-under-the-hood/77908/.

82 Kaspersky Lab Global Research & Analysis Team (GReAT). *ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms [Internet]*. Kaspersky Lab. 2016 Aug 8 [cited 2018 April 22]. Available from: https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/.

83 Kaspersky Lab Global Research & Analysis Team (GReAT). *BlackOasis APT and new targeted attacks leveraging zero-day exploit [Internet]*. Kaspersky Lab. 2017 Oct 16 [cited 2018 April 22]. Available from: https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/.

84 Hasbini MA. *Operation Ghoul: targeted attacks on industrial and engineering organizations [Internet]*. Kaspersky Lab. 2016 Aug 17 [cited 2018 April 22]. Available from: https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/.

85 Kaspersky Lab Global Research & Analysis Team (GReAT). *Introducing WhiteBear [Internet]*. Kaspersky Lab. 2017 Aug 30 [cited 2018 April 22]. Available from: https://securelist.com/introducing-whitebear/81638/.

86 Baumgartner K. *On the StrongPity waterhole attacks targeting Italian and Belgian encryption users [Internet]*. Kaspersky Lab. 2016 Oct 3 [cited 2018 April 22]. Available from: https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/.

87 Kaspersky Lab Global Research & Analysis Team (GReAT). *The dropping elephant—aggressive cyber-espionage in the Asian region [Internet]*. Kaspersky Lab. 2016 July 8 [cited 2018 April 22]. Available from: https://securelist.com/blog/research/75328/the-dropping-elephant-actor/.

88 Buchka N, Firsh A. *Skygofree: following in the footsteps of HackingTeam [Internet]*. Kaspersky Lab. 2018 Jan 16 [cited 2018 April 22]. Available from: https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/.

89 Raiu C, Hasbini MA, Belov S, Mineev S. *From Shamoon to StoneDrill [Internet]*. Kaspersky Lab. 2017 Mar 6 [cited 2018 April 22]. Available from: https://securelist.com/from-shamoon-to-stonedrill/77725/.

90 Kaspersky Lab Global Research & Analysis Team (GReAT). *ShadowPad in corporate networks [Internet]*. Kaspersky Lab. 2017 Aug 15 [cited 2018 April 22]. Available from: https://securelist.com/shadowpad-in-corporate-networks/81432/.

91 Raiu C, Ivanov A. *Operation daybreak [Internet]*. Kaspersky Lab. 2016 June 17 [cited 2018 April 22]. Available from: https://securelist.com/operation-daybreak/75100/.

92 Shulmin A, Yunakovsky S, Berdnikov V, Dolgushev A. *The slingshot APT FAQ [Internet]*. Kaspersky Lab. 2018 Mar 9 [cited 2018 April 22]. Available from: https://securelist.com/apt-slingshot/84312/.

93 First A. *Who's who in the zoo [Internet]*. Kaspersky Lab. 2018 May 3 [cited 2018 May 12]. Available from: https://securelist.com/whos-who-in-the-zoo/85394/.

94 Kaspersky Lab Global Research & Analysis Team (GReAT). *OlympicDestroyer is here to trick the industry [Internet]*. Kaspersky Lab. 2018 Mar 8 [cited 2018 April 22]. Available from: https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/.

95 TrendMicro Forward-Looking Threat Research Team. Kaspersky Lab [Internet]. 2012 [cited 2018 April 22]. Available from: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2012/04/20083243/wp_luckycat_redux.pdf.

96 Lockheed Martin Corporation. *Lockheed Martin [Internet]*. 2015. Available from: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

97 Khosravi M, Ladani BT. Alerts correlation and causal analysis for APT based cyber attack detection. *IEEE Access*. 2020;**8**: 162642–162656. Available from: https://doi.org/10.1109/ACCESS.2020.3021499.

98 Carbon Black. *What is cyber espionage? [Internet]*. 2018. Available from: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.