Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Survey of publicly available reports on advanced persistent threat actors

Antoine Lemay [a,*], *Joan Calvet* [b], *François Menet* [a], *José M. Fernandez* [a]

[a] *Department of Computer & Software Engineering, École Polytechnique de Montréal, Montréal, Quebec, Canada*
[b] *P.N.F. Software, Montréal, Quebec, Canada*

ARTICLE INFO

Article history:
Received 3 April 2017
Received in revised form 19 July 2017
Accepted 8 August 2017
Available online 15 August 2017

Keywords:
Advanced Persistent Threat (APT)
Cyber espionage
Cyber attacks
Targeted attacks
Targeted malware

ABSTRACT

The increase of cyber attacks for the purpose of espionage is a growing threat. Recent examples, such as hacking of the Democratic National Committee and indicting by the FBI of Chinese military personnel for cyber economic espionage, are testaments of the severity of the problem. Unfortunately, research on the topic of Advanced Persistent Threats (APT) is complicated due to the fact that information is fragmented across a large number of Internet resources. This paper aims at providing a comprehensive survey of open source publications related to APT actors and their activities, focusing on the APT activities, rather than research on defensive or detective measures. It is intended to serve as a quick reference on the state of the knowledge of APT actors, where interested researchers can find what primary sources are most relevant to their research. The paper covers publications related to around 40 APT groups from multiple regions across the globe. A short summary of the main findings of each publication is presented.

1. Introduction

Spying is sometimes referred to as the world's second oldest profession. However, that does not mean that spying has not evolved over the years. As information became increasingly digitized, spies turned to electronic means of gathering information. Nowadays, the use of cyber attacks for the purpose of espionage is commonplace. Large-scale breaches by nation-state actors for the purpose of espionage, such as the breach of health insurance companies (Krebs, 2015), entertainment groups (RiskBased Security, 2014), critical infrastructure (Simonite, 2013), and even democratic institutions (Alperovitch, 2016), make the news. The euphemism for state-sponsored espionage groups, advanced persistent threat (APT) actors, is now a marketing line for security products. It is therefore no surprise that the topic of APT research, whether for creating new defenses, or to be better prepared to investigate new cases, has gained increasing interest.

Unfortunately, the documentation necessary to perform such research is difficult to find. While there is no dearth of information, the information is fragmented across a large number of Internet resources, such as industry reports, scarce academic publications, and blog posts from threat researchers or incident responders. This makes the process of getting a global picture of the state of APT activities time consuming.

This paper aims at providing a comprehensive survey of open source publications related to APT actors, and their activities. This survey focuses on summarizing available literature on the attackers, rather than on defensive measures, as defensive research is more easily accessible because it is indexed for the most part in scholarly search engines. For this reason, it is intended to serve as a quick reference on current knowledge of APT actors, where interested researchers

* *Corresponding author.*
E-mail address: antoine.lemay@polymtl.ca (A. Lemay).
https://doi.org/10.1016/j.cose.2017.08.005

can find what primary sources are most relevant to their research.

1.1. A quick note about sources

The majority of sources in this report come from industry, rather than academic publications. This is due to the fact that the industry has a relative monopoly on primary sources of information regarding APTs. In particular, access to incident-response data is crucial to get a full picture of the compromise, and of post-infection actions taken by the threat actor. Additionally, a large database of historic samples is often necessary to conduct research on operations. As the detection rate of APT malware is low, operations are often reverse-engineered from a single, known compromise. For example, a target might detect the attack and forward the malware samples to researchers. The researchers are then able to make a link to other cases, investigate other malware, and start building a global picture of the operation. The operation may go back a number of years, requiring detailed historical data. This capability is often not available to academic research groups, even those dedicated to malware research.

Therefore, there is no alternative to using industry sources. In the academic literature, while multiple researchers have worked on building better defenses to detect or prevent these threats, only Daly (2009) and Li, Lai, and Ddl (Li et al., 2011) discuss the APTs themselves. Daly covers hypothetical scenarios, and Li, Lai, and Ddl a single case affecting Hong Kong. Even research related to how the information is collected, and divulged, is limited. Lee and Lewis publish about techniques to cluster separate attacks, in order to regroup actors and operations (Lee and Lewis, 2011), and Dennesen gives a talk on the impact of divulgations on the attacker's operations (Dennesen, 2016).

While access to primary source data is an asset to the industry, there is a downside to relying on these sources for information. First, there is often a lack of validation of their conclusions. The papers are often not peer-reviewed and, because they rely on confidential information sources, can seldom be independently verified. Furthermore, these publications are primarily marketing tools. While some groups rely on technical credibility and rational analysis as the main drivers of the marketing message, others rely on sensational claims to make headlines. As journalists are eager to publish stories on shadowy espionage groups, stories that sell newspapers and magazines, negative incentives are created. For this reason, it is crucial to maintain a critical eye regarding some of these publications. This is especially true when considering attribution.

1.2. A quick note on attribution

In this survey, we present various publications related to APT actors, organized by country of origin and, if possible, by the specific groups mentioned in the publication. It should be noted that this so-called attribution to specific actors, is based on the judgement of the authors of the original source. This paper does not attempt to present a case for this-or-that actor to be attributed to this-or-that country. Unfortunately, this kind of grouping is, at times, unavoidable in the context of a study of APTs associated with nation states, as multiple sources discuss the issue of attribution, and it is sometimes necessary to comment on it.

In addition, complexities arise when dealing with multiple companies reporting on the same group actor. In a manner similar to naming-convention problems, when dealing with traditional malware, each research group may have a different name for a particular APT group. This problem is made even more difficult by the fact that various research groups have wildly divergent standards for the APT component that should be named. We take an alleged Russian APT group to illustrate this naming confusion. Mandiant, Crowdstrike, iSIGHT partners, and Microsoft have four different names for the group itself (APT28, Fancy Bear, Tsar Team, and Strontium, respectively). Kaspersky and ESET refer to the group by the names that their detection engines use for the malware family used by the group (Sofacy and Sednit, respectively). Finally, TrendMicro refers to the group by the name of one of the espionage campaigns that they have investigated (Operation Pawn Storm). This becomes even more confusing when a group has conducted multiple campaigns, and the group ends up with multiple "operation" names.

Because of the overabundance of names, this paper will, where possible, attempt to merge the information provided on a group. This is done from known associations presented in the literature (for example a research paper may include other known names, or a secondary source, or a journalist could report multiple names), and validated by the authors' judgement. The validation is necessary as, in some cases, sources differ about the attribution of a particular tool to a particular group. In these cases, we give greater credence to sources with direct access to the information, instead of sources reporting on the analysis.

The survey regroups APT actors that the literature associates with China, Russia, "Western" powers (includes groups attributed to the Five Eyes group, France, and Israel), Middle East, and Southeast Asia. A number of groups where no clear attribution is available, are included in the "Actors with uncertain attribution" section.

1.3. Meta-analysis

In order to make this document easier to use, we have categorized, in Table 1, the technical references cited in this paper by threat actor, content, and type. As an example, let us consider reference Jiang et al. (2015), the FireEye blog post titled "The EPS Awakens." As it concerns the APT16 threat actor, it will be listed on the APT16 row in the table. The contents of the post describe the exploits used in an attack, so the reference number will be listed in the "Exploits used" column. Additionally, the reference number will be listed in the "Blog post" column to reference its type.

The threat actor row allows researchers to quickly access all reference material relating to a particular threat actor. Furthermore, it helps researchers identify which threat actors have been extensively covered, and which require further investigation. Actors with a large number of publications are well documented, and may provide more interesting targets for research that requires more sourcing. For readability, the threat actors are listed according to the primary name used as the

Table 1 – References categorized by threat actor, content, and type.

	Spear Phishing samples	Watering hole or web attacks	Exploits used	Description of the Implant	Description of post-exploitation tools	Description of support tools (reconnaissance or VPN)	Command and control protocol	Command and control infrastructure	TTPs	Attribution analysis or details on the groups	Victimization analysis	Blog Post	Bulletin	Report	Conference presentation
China															
Shared tools	(Baumgartner, 2015)	(Bartholomew, 2017; Baumgartner and Golovkin, 2015a)	(Bartholomew, 2017; Baumgartner, 2015)	(Baumgartner, 2015)		(Baumgartner and Golovkin, 2015b)	(Baumgartner, 2015)			(Baumgartner and Golovkin, 2015a, 2015b)	(Bartholomew, 2017; Baumgartner and Golovkin, 2015a)	(Baumgartner, 2015; Baumgartner and Golovkin, 2015a)	(Baumgartner and Golovkin, 2015b)	(Bartholomew, 2017)	
APT16	(Bitdefender, 2015)		(BAE Systems Apllied Intelligence, 2014)	(Bitdefender, 2015)								(BAE Systems Apllied Intelligence, 2014; Bitdefender, 2015)			
Aurora Panda	(Bronk and Tikk-Ringas, 2013)	(Calvet, 2015c)	(Brod, 2014; Calvet, 2015c)	(Blasco, 2016; Bronk and Tikk-Ringas, 2013; Calvet, 2014)	(Calvet, 2014)			(Blasco, 2016; Calvet, 2014)	(Calvet, 2014, 2015a, 2015b)		(Calvet, 2014, 2015c)	(Boutin, 2013; Brod, 2014; Bronk and Tikk-Ringas, 2013)		(Blasco, 2016; Calvet, 2014, 2015a, 2015c)	
Comment Crew	(Calvet et al., 2016; Chen et al., 2014; Cherepanov, 2016)		(Chen et al., 2014)	(Calvet et al., 2016; Chen et al., 2014)	(Calvet et al., 2016)	(Calvet et al., 2016)	(Calvet et al., 2016; Checkpoint Software Technologies, 2015b)	(Calvet et al., 2016)	(Calvet et al., 2016; Checkpoint Software Technologies, 2015a; Cherepanov, 2016)	(Calvet et al., 2016; Chang and Singh, 2016)	(Calvet et al., 2016; Chang et al., 2015)	(Checkpoint Software Technologies, 2015b; Chen et al., 2014; Cherepanov, 2016)	(Chang and Singh, 2016)	(Calvet et al., 2016; Chang et al., 2015; Checkpoint Software Technologies, 2015a)	
Shell_Crew	(Creus et al., 2016)	(Clearsky, 2014)	(Coogan, 2012)	(Clearsky, 2014; Clearsky – Cyber security, 2016; Coogan, 2012)	(Clearsky, 2014, 2015; Clearsky – Cyber security, 2016)	(Creus et al., 2016)		(Cluley, 2016)	(Clearsky, 2014, 2015; Clearsky – Cyber security, 2016)	(Cluley, 2016; Coogan, 2012; Creus et al., 2016)	(Coogan, 2012; Creus et al., 2016)	(Clearsky, 2015; Cluley, 2016)	(Clearsky – Cyber security, 2016)	(Clearsky, 2014; Coogan, 2012; Creus et al., 2016)	
Emissary Panda	(Crowdstrike Global Intelligence Team, 2016)			(Crowdstrike Global Intelligence Team, 2014, 2016)	(Crowdstrike Global Intelligence Team, 2014, 2016)	(Crowdstrike Global Intelligence Team, 2016)	(Crowdstrike Global Intelligence Team, 2016)	(Crowdstrike Global Intelligence Team, 2016)	(Crowdstrike Global Intelligence Team, 2014, 2016)	(Crowdstrike Global Intelligence Team, 2014, 2016)	(Crowdstrike Global Intelligence Team, 2014, 2016)	(Crowdstrike Global Intelligence Team, 2014)		(Crowdstrike Global Intelligence Team, 2016)	
APT3	(Dahl, 2014a, 2014b; Dahms, 2014)		(Cylance, 2014; Dahms, 2014; Daly, 2009)	(Cutler, 2012; Dahl, 2014b)	(Dennesen, 2016)	(Dell SecureWorks Counter Threat Unit™ Threat Intelligence, 2015)		(Dahl, 2014b)		(Dahl, 2014b)	(Dennesen, 2016)	(Cutler, 2012; Cylance, 2014; Dahl, 2014a, 2014b; Dahms, 2014; Daly, 2009; Dell SecureWorks Counter Threat Unit™ Threat Intelligence, 2015; Dennesen, 2016)			
Hurricane Panda			(Dereszowski, 2015)					(Dereszowski, 2014; DiMaggio, 2016)	(Dereszowski, 2014; DiMaggio, 2016; Doherty et al., 2013)			(Dereszowski, 2014, 2015; DiMaggio, 2016; Doherty et al., 2013)			
Icefog	(Doman, 2016)		(Doman, 2016)	(Doman, 2016; Ducklin, 2014)	(Doman, 2016)		(Doman, 2016; Ducklin, 2014)	(Doman, 2016)	(Doman, 2016)	(Doman, 2016)	(Doman, 2016; Ducklin, 2014)	(Ducklin, 2014)		(Doman, 2016)	
Ke3chang	(ESET Research, 2014b)		(Evron and Werner, 2014)	(ESET Research, 2014a, 2014b; Evron and Werner, 2014)	(ESET Research, 2014b)		(ESET Research, 2014a, 2014b; Evron and Werner, 2014)	(ESET Research, 2014a, 2014b)	(ESET Research, 2014b)	(ESET Research, 2014b; Evron and Werner, 2014)	(ESET Research, 2014a, 2014b)	(ESET Research, 2014a; Evron and Werner, 2014)		(ESET Research, 2014b)	
NetTraveler	(F-Secure labs Security Response, 2015; F-Secure Labs Security Response, 2014a)	(F-Secure Labs Security Response, 2014a)	(F-Secure labs Security Response, 2015; F-Secure Labs Security Response, 2014a)	(F-Secure labs Security Response, 2015)	(F-Secure labs Security Response, 2015)		(F-Secure labs Security Response, 2015)	(F-Secure labs Security Response, 2015; F-Secure Labs Security Response, 2014a)		(F-Secure labs Security Response, 2015)	(F-Secure labs Security Response, 2015)	(F-Secure Labs Security Response, 2014a)		(F-Secure labs Security Response, 2015)	

(continued on next page)

Table 1 – (*continued*)

	Spear Phishing samples	Watering hole or web attacks	Exploits used	Description of the Implant	Description of post-exploitation tools	Description of support tools (reconnaissance or VPN)	Command and control protocol	Command and control infrastructure	TTPs	Attribution analysis or details on the groups	Victimization analysis	Blog Post	Bulletin	Report	Conference presentation
Night Dragon		(F-Secure Labs Security Response, 2014b)		(F-Secure Labs Security Response, 2014b)			(F-Secure Labs Security Response, 2014b)	(F-Secure Labs Security Response, 2014b)		(F-Secure Labs Security Response, 2014b)				(F-Secure Labs Security Response, 2014b)	
Ixeshe	(Fagerland, 2012; Falcone et al., 2015)		(F-Secure Labs Threat Intelligence, 2015; Falcone et al., 2015)	(F-Secure Labs Threat Intelligence, 2015; Fagerland, 2012; Falcone et al., 2015)			(F-Secure Labs Threat Intelligence, 2015; Fagerland, 2012; Falcone and Lee, 2016; Falcone et al., 2015)	(F-Secure Labs Threat Intelligence, 2015)	(F-Secure Labs Threat Intelligence, 2015; Fagerland, 2012)	(F-Secure Labs Threat Intelligence, 2015)		(Falcone et al., 2015)		(F-Secure Labs Threat Intelligence, 2015; Fagerland, 2012)	(Falcone and Lee, 2016)
Putter Panda	(Falliere et al., 2011)			(Falliere et al., 2011; Federal Bureau of Investigations, 2015)			(Falliere et al., 2011)	(Falliere et al., 2011; Federal Bureau of Investigations, 2015)		(Falliere et al., 2011; FBI National Press Office, 2014)	(Falliere et al., 2011)	(FBI National Press Office, 2014; Federal Bureau of Investigations, 2015)		(Falliere et al., 2011)	
Hellsing	(Fire Eye Threat Intelligence, 2015)			(Fire Eye Threat Intelligence, 2015)	(Fire Eye Threat Intelligence, 2015)			(Fire Eye Threat Intelligence, 2015)		(Fire Eye Threat Intelligence, 2015)	(Fire Eye Threat Intelligence, 2015)	(Fire Eye Threat Intelligence, 2015)			
Naikon	(FireEye, 2014; FireEye Labs / FireEye Threat Intelligence, 2015b)		(FireEye Labs / FireEye Threat Intelligence, 2015b)	(FireEye, 2014; FireEye Labs / FireEye Threat Intelligence, 2015a, 2015b)	(FireEye, 2014; FireEye Labs / FireEye Threat Intelligence, 2015b)		(FireEye, 2014)	(FireEye Labs / FireEye Threat Intelligence, 2015a, 2015b)	(FireEye, 2014)	(FireEye, 2014)	(FireEye, 2014; FireEye Labs / FireEye Threat Intelligence, 2015a, 2015b)	(FireEye Labs / FireEye Threat Intelligence, 2015a)		(FireEye, 2014; FireEye Labs / FireEye Threat Intelligence, 2015b)	
Russia															
Energetic Bear	(Fisher, 2014)	(Fisher, 2014)	(Fisher, 2014; Gallagher, 2014; GData, 2014)	(Fisher, 2014; Gallagher, 2014; Global Research & Analysis Team, 2012)	(Fisher, 2014; Global Research and Analysis Team, 2011, 2013a)		(Fisher, 2014; Gallagher, 2014)	(Fisher, 2014; Gallagher, 2014)	(Gallagher, 2014)	(Fisher, 2014)	(Fisher, 2014; Gallagher, 2014)	(GData, 2014; Global Research & Analysis Team, 2012; Global Research and Analysis Team, 2011, 2013a)		(Fisher, 2014; Gallagher, 2014)	
Sandworm	(Gostev, 2012a, 2012c, 2012d)		(Global Research and Analysis Team, 2013b; Global Research and Analysis Team Kasperky Labs, 2016; Gostev, 2012a, 2012b, 2012c)	(Goodin, 2015; Gostev, 2012b, 2012c, 2012d; Gostev and Soumenkov, 2011)	(Gostev, 2012c, 2012d; Gostev and Soumenkov, 2011)		(Gostev, 2012d)	(Gostev, 2012c)	(Gostev, 2012d)		(Gostev, 2012c)	(Global Research and Analysis Team, 2013b; Global Research and Analysis Team Kasperky Labs, 2016; Goodin, 2015; Gostev, 2012a, 2012b; Gostev and Soumenkov, 2011)		(Gostev, 2012d)	(Gostev, 2012c)
APT28	(GovCERT.ch, 2016; Gross and C. S. team, 2016; Gross and Walter, 2016; Hentunen and Tikkanen, 2014; Hern, 2016; Karspersky Labs, 2015; Kaspersky Lab, 2014)	(Hentunen and Tikkanen, 2014)	(Gross and C. S. team, 2016; Gross and Walter, 2016; Hentunen and Tikkanen, 2014; Hern, 2016; Huss, 2016; Jiang et al., 2015; Karspersky Labs, 2015; Kaspersky Lab, 2014)	(GovCERT.ch, 2016; Hentunen and Tikkanen, 2014; Hern, 2016; Hjelmvik, 2014; Kaspersky labs, 2014; Kaspersky Lab, 2014)	(GovCERT.ch, 2016; Hentunen and Tikkanen, 2014; Hern, 2016; Hjelmvik, 2014; Kaspersky Lab, 2014)	(Hentunen and Tikkanen, 2014; Hern, 2016; Hjelmvik, 2014; Kaspersky Lab, 2014)	(GovCERT.ch, 2016; Grunzweig, 2015; Hentunen and Tikkanen, 2014; Hjelmvik, 2014; Huss, 2016; Kaspersky labs, 2014; Kaspersky Lab, 2014)	(Huss, 2016)	(GovCERT.ch, 2016; Gross and C. S. team, 2016; Hentunen and Tikkanen, 2014; Hern, 2016; Hjelmvik, 2014; Hoglund, 2011; Kaspersky Lab, 2014)	(GovCERT.ch, 2016; Hentunen and Tikkanen, 2014; Hjelmvik, 2014; Kaspersky Lab, 2014)	(GovCERT.ch, 2016; Hjelmvik, 2014; Karspersky Labs, 2015; Kaspersky labs, 2015; Kaspersky Lab, 2014)	(Gross and Walter, 2016; Grunzweig, 2015; Hoglund, 2011; Huss, 2016; Karspersky Labs, 2015; Kaspersky labs, 2014)		(GovCERT.ch, 2016; Gross and C. S. team, 2016; Hern, 2016; Hjelmvik, 2014; Jiang et al., 2015; Kaspersky labs, 2015)	(Hentunen and Tikkanen, 2014; Kaspersky Lab, 2014)

(*continued on next page*)

Table 1 – (*continued*)

	Spear Phishing samples	Watering hole or web attacks	Exploits used	Description of the Implant	Description of post-exploitation tools	Description of support tools (reconnaissance or VPN)	Command and control protocol	Command and control infrastructure	TTPs	Attribution analysis or details on the groups	Victimization analysis	Blog Post	Bulletin	Report	Conference presentation
The Dukes	(KASPERSKY LAB ZAO, 2013)		(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab's Global Research & Analysis Team, 2014)	(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Labs, 2015; Kaspersky Lab's Global Research & Analysis Team, 2012, 2014, 2015b, 2016; Kasza and Idrizovic, 2016)	(Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Lab's Global Research & Analysis Team, 2012)		(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Lab's Global Research & Analysis Team, 2014, 2015b, 2016; Kasza and Idrizovic, 2016)	(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Labs, 2015)	(Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Labs, 2015; Kaspersky Lab's Global Research & Analysis Team, 2012, 2015a; Kasza and Idrizovic, 2016)	(Kaspersky Lab's Global Research & Analysis Team, 2012)	(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab's Global Research & Analysis Team, 2012; KASPERSKY LAB ZAO, 2013)	(Kaspersky Lab's Global Research & Analysis Team, 2014, 2015a, 2015b, 2016; KASPERSKY LAB ZAO, 2013)		(Kaspersky Lab Global Research and Analysis, 2012; Kaspersky Lab Global Research and Analysis Team, 2014; Kaspersky Labs, 2015; Kaspersky Lab's Global Research & Analysis Team, 2012; Kasza and Idrizovic, 2016)	
Snake	(Krebs, 2016; Lee and Lewis, 2011)	(Krebs, 2016; Lee and Lewis, 2011; Levene et al., 2015)	(Krebs, 2016; Langner, 2013; Lee and Lewis, 2011)	(Kharouni et al., 2014; Krebs, 2015, 2016; Laboratory of Cryptography and System Security (CrySyS Lab), 2012; Langner, 2013; Lee and Lewis, 2011; Li et al., 2011)	(Kharouni et al., 2014; Krebs, 2015, 2016; Levene et al., 2015)	(Krebs, 2015, 2016; Lelli, 2010; Levene et al., 2015)	(Kharouni et al., 2014; Krebs, 2015, 2016; Laboratory of Cryptography and System Security (CrySyS Lab), 2012; Langner, 2013; Levene et al., 2015; Li et al., 2011)	(Krebs, 2015, 2016; Lancaster, 2015; Lee and Lewis, 2011; Levene et al., 2015)	(Lancaster, 2015; Langner, 2013; Lelli, 2010; Levene et al., 2015)	(Kharouni et al., 2014; Krebs, 2015, 2016)	(Kharouni et al., 2014; Krebs, 2016; Lancaster, 2015; Lee and Lewis, 2011; Lelli, 2010; Levene et al., 2015; Li et al., 2011)	(Krebs, 2016; Laboratory of Cryptography and System Security (CrySyS Lab), 2012; Lancaster, 2015; Li et al., 2011)		(Kharouni et al., 2014; Krebs, 2015; Lee and Lewis, 2011; Lelli, 2010; Levene et al., 2015)	(Langner, 2013)
Western Powers															
Animal Farm				(Lipovsky, 2014a, 2014b; Lipovsky and Cherepanov, 2014c; Mandiant, 2013; Marschalek, 2015)			(Mandiant, 2013)	(Lipovsky, 2014b)		(Lipovsky and Cherepanov, 2014c; Marschalek, 2015)	(Mandiant, 2013; Marschalek, 2014)	(Lipovsky, 2014a, 2014b; Lipovsky and Cherepanov, 2014c; Mandiant, 2013; Marschalek, 2014, 2015)			
Regin				(McAfee Foundstone Professional Services and McAfee Labs, 2011; McAfee Labs, 2014)	(McAfee Foundstone Professional Services and McAfee Labs, 2011; McAfee Labs, 2014)		(McAfee Labs, 2014)	(McAfee Foundstone Professional Services and McAfee Labs, 2011)		(Meyers, 2013)	(McAfee Foundstone Professional Services and McAfee Labs, 2011; McAfee Labs, 2014)	(Meyers, 2013)		(McAfee Foundstone Professional Services and McAfee Labs, 2011; McAfee Labs, 2014)	
Equation Group			(Microsoft, 2015; Minerva Labs LTD and ClearSky Cyber Security, 2015)	(Microsoft, 2015)		(Microsoft, 2015)		(Microsoft, 2015)	(Microsoft, 2015)	(Microsoft, 2015; Monnappa, 2016)	(Microsoft, 2015)	(Minerva Labs LTD and ClearSky Cyber Security, 2015; Monnappa, 2016)		(Microsoft, 2015)	

(*continued on next page*)

Table 1 – (*continued*)

	Spear Phishing samples	Watering hole or web attacks	Exploits used	Description of the Implant	Description of post-exploitation tools	Description of support tools (reconnaissance or VPN)	Command and control protocol	Command and control infrastructure	TTPs	Attribution analysis or details on the groups	Victimization analysis	Blog Post	Bulletin	Report	Conference presentation
Olympic Games			(Moran et al., 2014; Myers, 2015; Narang, 2013; NH, 2014; O'Gorman and McDonald, 2012; Pernet and Lu, 2015; Pernet and Sela, 2015)	(Moran et al., 2014; Myers, 2015; Narang, 2013; Novetta, 2014; Parys, 2016; Raiu, 2013; Raiu and Golovkin, 2015)	(Moran et al., 2014; Mushtaq, 2010; Myers, 2015; Narang, 2013; NH, 2014; Parys, 2016; Raiu, 2013; Raiu and Golovkin, 2015)		(Moran et al., 2014; Myers, 2015; Narang, 2013; PwC, 2015; Raiu, 2013; Raiu and Baumgartner, 2014; Raiu and Golovkin, 2015)	(PwC, 2015; Raiu, 2013; Raiu and Baumgartner, 2014; Raiu and Golovkin, 2015)	(Narang, 2013)	(Moran and Oppenheim, 2014; Moran et al., 2014; Nakashima et al., 2012; Narang, 2013; Pernet and Sela, 2015; Raiu, 2013; Raiu and Golovkin, 2015)	(Moran et al., 2014; Mushtaq, 2010; Myers, 2015; Narang, 2013; Novetta, 2014; O'Gorman and McDonald, 2012; PwC, 2015; Raiu, 2013; Raiu and Baumgartner, 2014; Raiu and Golovkin, 2015)	(Moran and Oppenheim, 2014; Moran et al., 2014; Nakashima et al., 2012; Novetta, 2014; O'Gorman and McDonald, 2012; Parys, 2016; Pernet and Lu, 2015; Pernet and Sela, 2015; PwC, 2015; Raiu and Baumgartner, 2014; Raiu and Golovkin, 2015)		(Moran et al., 2014; Mushtaq, 2010; Myers, 2015; Narang, 2013; NH, 2014; Raiu, 2013)	
Project Sauron				(Raiu and Soumenkov, 2015; Raiu et al., 2013)			(Raiu et al., 2013)	(Raiu et al., 2013)		(Raiu et al., 2013)	(Raiu and Soumenkov, 2015; Raiu et al., 2013)	(Raiu and Soumenkov, 2015)		(Raiu et al., 2013)	
Middle East															
Iran	(RSA Incident Response, 2014; Sanger, 2012; Schworer and Liburdi, 2015; Scott and Spaniel, 2016; Scott, 2014; Scott-Railton and Kleemola, 2015)	(Rascagnères, 2015)	(Sancho et al., 2012; Sanger, 2012)	(Sancho et al., 2012; Sanger, 2012; Santos, 2016; Schworer and Liburdi, 2015; Security Response, 2016)	(RSA Incident Response, 2014; Sancho et al., 2012; Sanger, 2012; Schworer and Liburdi, 2015; Scott, 2014; Security Response, 2016)	(Sancho et al., 2012)	(Sancho et al., 2012; Santos, 2016; Schworer and Liburdi, 2015)	(RSA Incident Response, 2014; Sancho et al., 2012; Sanger, 2012; Schworer and Liburdi, 2015; Security Response, 2016)	(Sancho et al., 2012; Scott and Spaniel, 2016; Scott, 2014; Security Response, 2016)	(Rascagnères, 2015; RSA Incident Response, 2014; RSA Research, 2015; Sancho et al., 2012; Sanger, 2012; Schworer and Liburdi, 2015; Scott and Spaniel, 2016; Scott-Railton and Kleemola, 2015; Security Response, 2016)	(Raiu et al., 2014; RSA Incident Response, 2014; Sancho et al., 2012; Schworer and Liburdi, 2015; Scott and Spaniel, 2016; Security Response, 2016)	(Raiu et al., 2014; Rascagnères, 2015; RSA Research, 2015; Santos, 2016; Scott-Railton and Kleemola, 2015)		(RSA Incident Response, 2014; Sancho et al., 2012; Schworer and Liburdi, 2015; Scott and Spaniel, 2016; Scott, 2014; Security Response, 2016)	(Sanger, 2012)
Copy Kittens	(Selvaraj, 2010)			(Selvaraj, 2010)			(Selvaraj, 2010)	(Selvaraj, 2010)						(Selvaraj, 2010)	
Desert Falcons	(Sherstobitoff et al., 2013)			(Sherstobitoff et al., 2013; Simonite, 2013)	(Sherstobitoff et al., 2013; Simonite, 2013)		(Simonite, 2013)	(Sherstobitoff et al., 2013; Simonite, 2013)	(Sherstobitoff et al., 2013)	(Simonite, 2013)	(Sherstobitoff et al., 2013; Simonite, 2013)			(Sherstobitoff et al., 2013; Simonite, 2013)	
Volatile Cedar				(Symantec Security Response, 2011)	(Symantec Security Response, 2011)		(Symantec Security Response, 2011)	(Symantec Security Response, 2011)		(Symantec Security Response, 2011)				(Symantec Security Response, 2011)	
Molerats	(Symantec Security Response, 2016b)			(Symantec Security Response, 2012, 2014a, 2015b, 2016a, 2016b)	(Symantec Security Response, 2016b)		(Symantec Security Response, 2016b)	(Symantec Security Response, 2012, 2014a, 2014b, 2015a, 2015b, 2016a, 2016b)	(Symantec Security Response, 2016b)	(Symantec Security Response, 2015b, 2016b)	(Symantec Security Response, 2012, 2014a, 2014b, 2015b)	(Symantec Security Response, 2014a, 2014b, 2015a, 2015b, 2016a)		(Symantec Security Response, 2012, 2016b)	
Southeast Asia															
Transparent Tribe	(Tanase, 2015; Tarakanov, 2013)		(Tarakanov, 2013)	(Tanase, 2015; Tarakanov, 2013)	(Tanase, 2015)		(Tanase, 2015)	(Tanase, 2015)		(Tanase, 2015)		(Tarakanov, 2013)	(Tanase, 2015)		
Unnamed Group			(ThreatConnect Research Team, 2015)	(ThreatConnect Research Team, 2015)						(ThreatConnect Research Team, 2015)	(ThreatConnect Research Team, 2015)	(ThreatConnect Research Team, 2015)			

(*continued on next page*)

Table 1 – (continued)

	Spear Phishing samples	Watering hole or web attacks	Exploits used	Description of the Implant	Description of post-exploitation tools	Description of support tools (reconnaissance or VPN)	Command and control protocol	Command and control infrastructure	TTPs	Attribution analysis or details on the groups	Victimization analysis	Blog Post	Bulletin	Report	Conference presentation
Lotus Blossom			(TrendMicro, 2015)	(Trend Micro Threat Research Team, 2015)			(Trend Micro Threat Research Team, 2015)	(Trend Micro Threat Research Team, 2015)			(Trend Micro Threat Research Team, 2015)	(TrendMicro, 2015)		(Trend Micro Threat Research Team, 2015)	
Silent Chollima			(Villeneuve et al., 2014; Weedon, 2015)	(U.S. Department of Justice (DoJ), 2014; Varma, 2010)	(U.S. Department of Justice (DoJ), 2014; Varma, 2010)		(U.S. Department of Justice (DoJ), 2014; Villeneuve et al., 2014)	(Varma, 2010)	(Villeneuve et al., 2014; Weedon, 2015)	(U.S. Department of Justice (DoJ), 2014; Varma, 2010; Villeneuve et al., 2013; Weedon, 2015)	(Varma, 2010; Villeneuve et al., 2014; Weedon, 2015)	(Varma, 2010; Villeneuve et al., 2014a,b; Weedon, 2015)	(Villeneuve et al., 2013)	(U.S. Department of Justice (DoJ), 2014)	
Operation Dust Storm			(Wilhoit, 2013)	(Wilhoit, 2013)			(Wilhoit, 2013)	(Wilhoit, 2013)	(Wilhoit, 2013)					(Wilhoit, 2013)	
Platinum	(Wilhoit, 2014)		(Wilhoit, 2014)	(Wilhoit, 2014)	(Wilhoit, 2014)		(Wilhoit, 2014)	(Wilhoit, 2014)	(Wilhoit, 2014)		(Wilhoit, 2014)			(Wilhoit, 2014)	
Uncertain Attribution															
Red October	(Windows Defender Advanced Threat Hunting Team, 2016; Winters, 2015)			(Windows Defender Advanced Threat Hunting Team, 2016; Winters, 2015)	(Winters, 2015)		(Windows Defender Advanced Threat Hunting Team, 2016)	(Windows Defender Advanced Threat Hunting Team, 2016; Winters, 2015)		(Winters, 2015)	(Windows Defender Advanced Threat Hunting Team, 2016)	(Windows Defender Advanced Threat Hunting Team, 2016; Winters, 2015)			
Careto			(Yates et al., 2016)	(Yates et al., 2016; Zetter, 2015)	(Yates et al., 2016; Zetter, 2015)		(Yates et al., 2016)	(Yates et al., 2016)		(Yates et al., 2016)	(Yates et al., 2016)		(Zetter, 2015)	(Yates et al., 2016)	

section header in the paper. Please refer to the paper for alternate group names.

The content columns allow researchers to rapidly see all the references for a given topic, across all threat actors. For example, if a research group wants to investigate victimization by APT actors, it could look at the references listed in the victimization analysis to get the appropriate references. The following content columns are used:

- Spear-Phishing samples: Where the group uses spear phishing, the reference provides information on the content of the email used in the spear phishing. A reference that only provides information on lure documents, or phishing websites is not listed in this category.
- Watering hole or web attacks: The group infiltrates websites to gain a foothold in the victim organization, or to host watering hole attacks. The reference documents the tools or techniques used.
- Exploits used: The reference lists specific software vulnerabilities used by the group.
- Description of the implant: The reference provides an analysis of the main backdoor, Remote Access Tool (RAT), or implant used by the group.
- Description of post-exploitation tools: The reference provides an analysis of additional tools (or modules in the case of advanced implants) loaded onto a victim machine to perform post-exploitation tasks, such as gathering additional information, dumping passwords, or performing lateral movement.
- Description of support tools (reconnaissance or VPN): The reference provides a description of tools used to support operations from the group prior to infection. For example, tools to identify suitable victims, or tools to hide the network presence.
- Command and control protocol: The reference details the protocol(s) used by the attackers for command and control of their infection.
- Command and control infrastructure: The reference details the infrastructure used by the attackers for command and control. This can take the form of a list of command and control domains and IPs, or a full-fledged analysis of the software hosted on a command and control node.
- Tactics, Tools, and Procedures (TTP): The reference includes a description of the attack process followed by the attackers. For example, a description of what tools the attacker uses at particular steps of the kill chain would warrant an inclusion in this category.
- Attribution analysis or details on the groups: The reference includes an attempt at providing artefacts that could be used to attribute the content to a particular threat actor, or provides information on the identity of the threat actor.
- Victimization analysis: The reference contains an analysis of the victims, aimed at presenting a victim profile. Note that references mentioning that a particular sector is targeted, without providing some justification, would not be included in this category. Researchers should also exercise caution when using victimization data from industrial publications, as results and conclusions presented could be the result of selection bias, i.e., showing an inherent bias in the company's customer base rather than a general trend.

The document-type columns allow researchers to quickly get an idea of the quality of information provided in a particular reference. The references are grouped according to the following categories:

- Blog post: The reference is a post on a blog, or a newspaper article available online.
- Bulletin: The reference is a short document on a targeted topic. Threat alerts and FBI announcements are good examples of this type of document.
- Report: The reference is an independent document in the form of a technical report.
- Conference presentation: The reference is a video recording, a slide deck, or a paper from a conference.

Typically, reports are the most exhaustive sources of information, as they typically provide a complete description of a particular threat actor or campaign, while blog posts typically cover a single aspect. The document-type column can therefore be used to estimate the amount of information available on a given threat actor.

From the above, we can quickly identify several topics that are not well covered in the current literature. First, it would appear that the more advanced groups have a tendency to be better covered than the less technically sophisticated groups. This is probably because of the interest of content producers (anti-virus companies, and incident-response companies) to focus on the unusual to attract traffic to their websites. More research on the smaller groups, especially in the emerging Southeast Asian sector, could yield interesting results. Secondly, the topic of reconnaissance, and other support tools, appears to be a significant gap in publicly available literature. As this includes victim selection, addressing this gap could greatly help defenders in assessing their risks. Finally, there is a clear imbalance between the amount of technical information on tools, and the amount of information on how the tools are used by specific groups. This is presumably caused by the important role played by the anti-virus industry in documenting APT actors. The bias for binary analysis present in that industry could limit the availability of contextual information. Research aimed at addressing that limitation could also greatly benefit the community.

2. China

China is home to the largest number of APT groups directly attributed to its state operations. This section summarizes the information available for each group, and on common infrastructure used by multiple Chinese APT actors.

2.1. *Shared tools and services*

A number of researchers have investigated tools, or services, that appear to be used by multiple operations related to Chinese APT groups.

A first example is the sharing of highly valuable 0-day exploits among multiple groups. Symantec reports on the Elderwood project (O'Gorman and McDonald, 2012). In this report, Symantec describes its investigation into a series of targeted trojans that spread via the use of 0-day. They noticed that, when the 0-day vulnerability used by the group became public knowledge, it was quickly replaced by a new 0-day exploit. Due to the rare nature of exploits for which no patch is available, the investigators wondered why the exploit developers appeared to have such a steady supply. After further investigation, they concluded that the exploits were connected. Furthermore, they linked the exploits to other campaigns, such as the Aurora campaign (described in the Aurora Panda section), and other unnamed targeted attacks. The attacks are described as using various methods, some using spear phishing, others using watering hole attacks. However, the report identifies the single source of the exploit as the Elderwood gang. While it is unclear in the report if the gang represents a single APT group, or a common developer providing exploit-development services to multiple APT groups, the report clearly illustrated code reuse across multiple operations.

By contrast, the investigation by Kaspersky into the CVE-2015-2545 vulnerability (Kaspersky Lab's Global Research & Analysis Team, 2016), presents clear evidence of the use of the vulnerability by multiple groups. In their analysis, researchers at Kaspersky detail investigations of multiple incidents involving the vulnerability. For each incident, they analyze the decoy document used in the spear phishing, the shellcode used for the exploit, and the command and control communication. Based on the indicators revealed in this research, they conclude that at least four groups typically associated with China, TwoForOne, APT16, EvilPost, and Danti, used the exploit. A similar investigation was done by Crowdstrike on the targeting of the French Aerospace industry by a threat actor, using the same vulnerability used by Aurora Panda to target the Veterans of Foreign Wars (Dahl, 2014a).

In addition to exploit sharing, other researchers present examples of tool sharing. In their investigation of the ScanBox tool (PwC, 2015), a tool used in attacks against Forbes and Anthem, PwC identifies four distinct clusters using the ScanBox tool, which are mapped to different APT groups. In addition to this investigation, the report details new additions to the ScanBox tool, which includes the ability to list software present on the machine, check drives, check folders, and perform additional settings checks aimed at avoiding analysis.

2.2. *APT 16*

The group APT16 is attributed to China by FireEye. At the time of writing, little is known about APT16, as this group was first mentioned in December 2015. FireEye has published two documents referring to APT16. The first document is a technical analysis of the CVE-2015-2545 vulnerability used in spear phishing for targeted attacks (Jiang et al., 2015). In this analysis, the authors reverse-engineer the exploit-code used. The second document (Winters, 2015) is a more in-depth look at targeted attacks directed at Taiwanese media organizations, including excerpts from the spear-phishing lure, more detail on the malware used, and a brief description of the command and control channel. This document identifies one of the sources of these attacks as the new group APT16.

2.3. *Aurora Panda (a.k.a. APT17 a.k.a. Sneaky Panda a.k.a. Hidden Lynx a.k.a. Tailgater Team a.k.a. The Beijing Group a.k.a. Axiom)*

Aurora Panda is one of the most well known APT groups due to its involvement in one of the first well-documented cases of espionage, the Aurora attacks against Google. Their pseudonym, "the Beijing group," testifies to this notoriety, as it was used to differentiate this group from the other Chinese group, "the Shanghai group" (described in the Comment Crew section).

The first wave of information regarding this group comes from the analysis of the Aurora attacks on Google, which were disclosed in early 2010. Varma from McAfee Labs, provides a brief report (Varma, 2010) on the vulnerability used, and a brief summary of the targeted spear phishing, designed to entice users to visit a malicious website, as well as a list of known malicious URLs. In a series of reports, Symantec provides an analysis of the scope of the attack (Symantec Security Response, 2010), and a detailed reverse-engineering analysis of the exploit in the Hydraq trojan used in the operation (Lelli, 2010), and also surveys the malware and spear-phishing lures used in similar incidents (Selvaraj, 2010).

After this high-profile attack, the group appears to have stayed active. In her RSA 2016 conference (Dennesen, 2016), Dennesen discusses how advanced threat actors retool once their activities are revealed to the public. One of the examples she cites to illustrate her point is Aurora Panda, which she identifies as corresponding to the Axiom group, APT17, and Hidden Lynx. In particular, she discusses how the Axiom report (Novetta, 2014), which discusses the high value HIKIT tool, forced the group to rely more on other tools such as BLACKCOFFEE. In addition to providing insight as to how this group operates, it also enables us to link other publications to this group.

The Axiom report by Novetta (Novetta, 2014), is a detailed description of the group in terms of targeting and TTP. This report, written in the wake of the so-called "Operation SNM," a joint operation by multiple companies to remove the presence of Axiom related malware on client machines, describes the large scale targeting of key targets in the technology sector for industrial espionage, and in NGOs dealing with sensitive issues, such as human rights and democracy. The report further provides indications that the TTP and infrastructure used, matches indicators from other known Chinese sources, such as the Elderwood project (discussed in the Shared Tools and Services section), and Shell_Crew / Deep Panda activities (discussed in the Shell_Crew section). This led some secondary sources to report that Axiom is, in fact, linked to Shell_Crew. Finally, the report describes in detail the five stages used in a typical attack, the tools used in each stage, and the command and control channel used by the Hikit Generation 2 tool. This description paints a picture of a very advanced, operational sophistication, with the development of tailored callback locations, command and control addressing disguised to appear legitimate, and even the use of supply chain attacks.

The loss of the use of the Hikit tool spurred the development of new tools. The report (FireEye Labs / FireEye Threat Intelligence, 2015a) on a new obfuscation technique, using Microsoft TechNet to host encoded command and control addresses for the BLACKCOFFEE / ZoxPNG trojan by FireEye, is an example of this type of retooling. A similar use of the technique was described by RSA (Myers, 2015).

Finally, in their report on Hidden Lynx (Doherty et al., 2013), Symantec presents a group of what they presume are hackers for hire. The report describes two subgroups, based on the trojan used in the later stages of the attacks, Moudoor or Naiad. The report also provides a brief summary of the attacks on the company Bit9, and the VOHO campaign.

2.4. *Comment Crew (a.k.a. APT1 a.k.a. Comment Panda a.k.a. The Shanghai Group)*

The Comment Crew is possibly the most well known APT group, due to the various efforts made to expose it over the years. As with Aurora Panda, their pseudonym of "the Shanghai group" also attests to the longevity of their notoriety.

The APT1 report by Mandiant (Mandiant, 2013) is the primary source for this group's notoriety. This report is the first major exposé regarding state-sponsored hacking that provided both technical details and direct attribution. The report exposes the relation between this hacking group, and unit 61398 of the Chinese People's Liberation Army (PLA), by providing extensive circumstantial evidence. The report also presents a brief overview of cyber incidents involving the group for which Mandiant had performed incident response, to provide an idea of the vast scope of the Comment Crew's operations. The report describes the way the Comment Crew operates, and covers both the general attack lifecycle, and specific details about the tools and infrastructure used. The report concludes by revealing the online identity of suspected members of the Comment Crew. Some of these identities were later confirmed by the FBI in their indictment of members of the Comment Crew for commercial espionage (U.S. Department of Justice (DoJ), 2014).

Other reports have documented the activities of the Comment Crew. The first is the report on Operation ShadyRAT by McAfee (Alperovitch, 2011). This report does not provide much in terms of technical details, but provides a breakdown of incidents related to the ShadyRAT trojan, later revealed to be part of the Comment Crew's activity. This covers the period from 2007–2011, while the Mandiant report concentrates on the 2011–2013 period. The McAfee report provides context to the more detailed Mandiant report.

The second report documenting their activities is on the SCADA (Supervisory Control and Date Acquisition) honeynet, from Trend Micro (Wilhoit, 2013). In this study, Wilhoit investigated the source of the attacks on SCADA systems. While not specifically designed to capture APT activity, during the course of his study he received a spear-phishing email from sources affiliated with the Comment Crew. This provides an interesting insight into the targeting of critical infrastructure from this particular group.

More specialized research was also produced on certain of the tools used by group. Hoglund provides a detailed description of the command and control channel that became the namesake of the group (Hoglund, 2011). The channel, which hid communications in the comment section of a compromised web page, allows the attacker to hide their control traffic in traditional HTTP communications. Narang, from Symantec, provides a brief summary of a Barkiofork backdoor, a tool usually associated with the Comment Crew, in the distribution

campaign targeting the Aerospace industry (Narang, 2013). Finally, another report from Symantec by Coogan, describes the use of WinHelp files to install malware (including the Barkiofork backdoor) (Coogan, 2012), with an example of the lure used in the campaign, and a detection heat map.

2.5. *Shell_Crew (a.k.a. Deep Panda a.k.a. WebMasters a.k.a. KungFu Kittens a.k.a. SportsFan a.k.a. PinkPanther a.k.a. Black Vine)*

The Shell_Crew group is another China-based group that became more widely known around 2014, particularly in the wake of the highly publicized breach at the Anthem insurance company.

The research by RSA is the source of the name, Shell_Crew. In their report on the APT group (RSA incident response, 2014), the researchers expose the propensity of this APT group to install web shells as one of the main techniques for persistence. In addition, the report provides an in-depth technical analysis of multiple tools and techniques, including the registering or alteration of DLLs for persistence, and various tools such as the Derusbi trojan, the Sethc backdoor, and the notepad.exe tool. In addition, the report covers how the Shell_Crew group uses commonly available tools, such as Mimikatz and PwDump, in their operation.

Around the same time, Crowdstrike released a report about an actor they named Deep Panda (Alperovitch, 2014a), targeting think tanks and other targets related to Southeast Asia policy requirements. In their analysis, they present the actor as favoring techniques aimed at avoiding the upload of tools on target machines, preferring the use of native scripting, such as PowerShell and WMI, and the running of malware from memory. They also mention the use of web shells as a method to avoid detection.

In early 2015, the disclosure of a breach at the insurer Anthem, led to more information about the Shell_Crew group. (Krebs (2015) provide a timeline of the events, and a link to other victims. However, he reports that the Shell_Crew group is also known by the name Axiom, which conflicts with other sources. As such, it is difficult to assess the validity of this link. Further reporting on the Anthem breach includes an FBI flash alert (Federal Bureau of Investigations, 2015), detailing the implication of the Shell_Crew, and a list of the tools used as technical indicators. Furthermore, a ThreatConnect report (ThreatConnect Research Team, 2015) traces the breach back to China. This report goes in depth into the infrastructure used in the breaches at Athem, Premeva Blue Cross, VAE, and OPM, to find commonalities. The report also exposes the role of a Chinese security company, and an academic institution in the attack.

Dimaggio from Symantec (DiMaggio, 2016) furthered the research on the group in their report about the Black Vine cyberespionage group. The report provides details about other operations of the group against the energy, aerospace, and healthcare sectors, as well as details of the custom malware used by the group. The report also documents links with other known actors, in particular pointing out that they also appear to have access to 0-day from the Elderwood project.

Finally, the RSA report on the Terracotta VPN (RSA Research, 2015) presents an overview of the network used by the Shell_Crew group to anonymize the source of attacks. In the report, RSA details the inner workings of the tool used by the attackers to reroute their traffic in order to disguise the fact that the traffic originates from China. To do so, they create proxies on servers that are hosted on rented, or compromised servers. The report also provides the method used to infect the remote servers. Finally, the report points out that, while not all activity with the Terracotta VPN is from APT actors, the Shell_Cew definitely made use of this service in the past for attacks.

2.6. *Emissary Panda (a.k.a. Threat Group 3390)*

The group, labelled by Crowdstrike as Emissary Panda, was not covered by a full report. However, some information has surfaced on their activities.

SecureWorks produced a threat report on the group (Dell SecureWorks Counter Threat Unit™ Threat Intelligence, 2015), that provides a high-level summary of the group's capabilities and intent. The report also provides a summary of the main tools used by this actor. This includes both tools used by multiple threat actors, such as PlugX and HttpBrowser, and custom tools, such as the OwaAuth web shell and the ASPXTool web shell. The report concludes by providing a bit more information on the preferences of the group for each step of the kill chain.

In the report on Operation Tiger, Chang et al. (2015) from TrendMicro looked in great detail at a specific campaign launched by Emissary Panda. Their analysis includes example of spear-phishing lures, details of the contents of archives of stolen data, breakdown of targets, and link to a specific online identity. Furthermore, the report provides a detailed description of the tool-set used, including snippets of codes, lines of scripts, reverse-engineered code, and packet captures of command and control traffic. This presents a very thorough view of the inside workings of APT activity.

2.7. *APT3 (a.k.a. UPS a.k.a. Gothic Panda a.k.a. Buckeye)*

The group referred to as APT3, is one of the lesser known Chinese APT groups. However, this does not imply that they are any less proficient than the more documented groups.

The main tool used by the group is the Pirpi backdoor that was documented as early as 2010 by FireEye (Mushtaq, 2010). In this report, Mushtaq from FireEye, discusses the use of a 0-day Internet Explorer exploit by the Hupigon and Pirpi tools. The report presents packet capture of the exploit phase, and the early communication to the command and control. However, today, there is no mention of this APT group.

Another report from researchers at FireEye, from 2014 (Chen et al., 2014), discusses the use of 0-day Internet Explorer exploits. The report presents an in-depth reverse-engineering analysis of the exploit, and the return oriented programming (ROP) used. The report also provides details of the threat, by confirming that this group had first access to a number of web browser 0-days in the past. They also comment that this group is quite proficient at moving laterally, and does not make the common mistake of reusing infrastructure for compromises. A second report on the wave of attacks, dubbed Operation Clandestine Fox by FireEye (Scott, 2014), provides more details on

the spear-phishing techniques used, as well as the attachments included in the emails.

FireEye also documented another wave of attacks, named Operation Double Tap, in a blog post by Moran et al. (2014). In this research, they provide information on the spear-phishing email used, and the downloader that is dropped. They also go into more detail on the types of commands that are available to the attackers, once command and control is established. They conclude by making the case that this attack is linked to the APT3 group, even though this represents a change in the typical modus operandi of the group. They provide a hypothesis for this change in behavior, speculating that requirements for a faster pace of attacks prevent them from relying exclusively on 0-day exploits.

FireEye revisited the investigation on Operation Clandestine Wolf in 2015 in a post by Eng and Caselden (2015). In this research, they detailed a spear-phishing campaign, using an Adobe Flash 0-day that they associated with APT3. The campaign, which was discovered on the compromised web server hosting the exploit, distributed implants associated with the group. The report also provides more details on the specific techniques used, including examples of the spear-phishing email, a short reverse engineering analysis of the ROP chain, and a high-level view of the exploit program flow.

Another wave of attacks in July 2015 spurred publications. First, research by Lee and Falcone from PaloAlto Networks investigate the use of an Adobe Flash vulnerability that was used by the group (Lee and Falcone, 2015). Significantly, they compare the shellcode with the leaked shellcode from the Hacking Team, and notice significant overlaps, concluding that advanced groups, such as APT3, can quickly benefit from public disclosure of vulnerabilities. Second, Lancaster from PwC (Lancaster, 2015), provides more details as to how the group uses a modified version of Scanbox (described in the Shared Tools and Services section) in their attacks. The research shows that the group used the ScanBox framework to make use of the PluginDetect code for server-side identification of plugins in the exploitation phase. The post also provides deobfuscated code for the PluginDetect component used by APT3.

Finally, another wave of attacks targeting Hong Kong, spurred a publication from Symantec on the group (Symantec Security Response, 2016a). The publication presents high-level statistics on the targets of the group, and lists the tools commonly used, including the options available for those tools.

2.8. *Hurricane Panda*

Hurricane Panda is a group primarily associated with a specific campaign that made use of Hurricane Electric DNS resolvers.

The campaign, dubbed Operation Poisoned Hurricane by FireEye, was the subject of a publication by Moran, Homan, and Scott (Moran et al., 2014), who explained how a brand of malware used by APT, was configured to use the DNS resolvers from Hurricane Electric. At the time, it was possible for clients of Hurricane Electric, even clients on free accounts, to declare authoritative entries for any domain, including domains owned by other companies, such as Microsoft or Adobe. The publication also reports on the use of Google Code for command and control, and the use of code signing to make the implants appear legitimate.

Crowdstrike further documents the activities of Hurricane Panda in a series of posts discussing how to respond to incidents involving the group. The reports are mostly concerned about how Crowdstrike products enable defenders to fight the attackers, but all include only snippets of information regarding the methods of how Hurricane Panda operates. The first post (Alperovitch, 2014b), discusses the use of a local-privilege escalation exploit by the team to get administrative level access, required to install kernel level rootkits, or dump passwords. The second post (Schworer and Liburdi, 2015), discusses the use of the Hurricane Electric resolver to hijack well known URLs, such as GitHub and Pinterest, to evade perimeter detection. The third post (Alperovitch, 2015), describes the persistent nature of the group, and the web shell used to maintain persistence in an enterprise network.

2.9. *Icefog (a.k.a. Dagger Panda)*

Icefog is another lesser known Chinese group that has been the target of research by Kaspersky.

The main information on the group comes from a detailed report by Kaspersky (KASPERSKY LAB ZAO, 2013). The report provides extensive details of the various client-side vulnerabilities exploited through spear phishing. The report also contains in-depth information about multiple versions of the Icefog backdoor, its command and control channel, and the spear-phishing lures used to distribute it. The report also details the tools used for lateral movement, and the command and control infrastructure. This includes screenshots of the command and control interface panels. The report concludes by presenting a summary of infection data, and the characteristics used to attribute these attacks to China.

Raiu, Sumenkov, and Kamluk from Kaspersky, performed a follow up investigation (Raiu et al., 2014), where they relate the tale of how investigating a particular command and control domain led them to discover a java-based version of the Icefog backdoor. The publication includes information on how they found the sample, details on how the java version works, and a brief overview of the victims.

2.10. *Ke3chang (a.k.a. Mirage a.k.a. Vixen Panda a.k.a. APT15)*

Because this group was only the feature of reports on some of its operations (operation Ke3chang and operation Mirage), it is difficult to provide clear indications that both operations were, in fact, perpetrated by the same group. However, as Scott and Spaniel (2016) group the two operations together, and link them to the APT group Vixen Panda / APT15, this paper presents them under the same umbrella.

The report on the Mirage campaign by Cutler of SecureWorks (Cutler, 2012), is the first analysis published on this group. This presents a cursory analysis of the espionage campaign distributing the Mirage RAT. It starts by summarizing the method used to distribute the RAT, the artefacts left behind when the RAT is executed, and the communication with the command and control. The research is continued on the variants of the

RAT found in the wild, an overview of the victim and the evidence used for attribution.

The report on Operation Ke3chang by Villeneuve et al. (2014) from FireEye, was published later, but covers a longer period of time. The report analyzes a series of breaches uncovered while investigating attacks against ministries of foreign affairs. The report includes a timeline of the attacks that used this modus operandi, going into details about the implant used in each of these attacks, and the types of lure used. It continues with a detailed exposition of the command and control channel and infrastructure, and concludes by presenting a summary of the indicators pointing to Chinese involvement.

The group has not ceased operations, as evidenced by a post from Yates et al. of PaloAlto Networks (Yates et al., 2016). In this research, they investigate the new TidePool malware, and link it to the malware used in Ke3chang. The post presents a brief overview of the vulnerability used, the TidePool malware itself, and then presents a comparison with the BS2005 malware used in part of operation Ke3chang.

2.11. *NetTraveler*

The NetTraveler group is named after the malware used in one of its operation. While Kaspersky does not directly attribute this actor to China in its open publications (the attribution information is only available in the second part of the report, accessible by contacting the company), they mention that the members of the group are native Chinese speakers.

The main dossier describing the activities of the NetTraveler group is published by the Global Research and Analysis Team (GReAT) from Kaspersky Labs (Global Research and Analysis Team, 2011). This report provides details on attacks investigated by Kaspersky that dropped the NetTraveler malware. They present details on spear-phishing lures used, and the specific files that were dropped when a target was infected. The report also provides an in-depth investigation of the functionality, and command and control, of the malware, including screenshots of configuration tools and exfiltrated data. The report continues by giving more information on the command and control infrastructure used, and analyzing how stolen information is stored on the command and control servers. Finally, the report provides an overview of the infection statistics, and how to remedy the attack. An appendix, providing a very detailed description of the malware's functionality and characteristics, completes the report.

Raiu, from Kaspersky, reports on another attack using NetTraveler (Raiu, 2013). This attack, occurring after the publication of the previous Kaspersky report, shows a change in tactics from the group with the use of a Java exploit, hosted on a watering hole website, instead of sending documents containing exploits by email. The post shows an example of a spear-phishing lure used, cursory information on the .jar file used to deliver the exploit, and more details on the watering hole attack infrastructure.

2.12. *Night Dragon*

The Night Dragon operation is a wave of cyber attacks, targeting the energy sector that was documented by McAfee.

The main source of information on Night Dragon is a report by McAfee Foundstone and McAfee Labs (McAfee Foundstone Professional Services and McAfee Labs, 2011), which explains how the attacker, through web compromises using SQL injection, spear phishing, and abusing VPN access, launched an espionage campaign targeted at the energy industry. The report continues by listing additional tools, many of which are largely available on Chinese hacker websites, and the RATs that were used in the attacks. The report delves a bit deeper into the main tools used, and further analyzes the network communication of the RAT. Appendices providing more information on the ZwShell RAT, and limited attribution information, conclude the report.

2.13. *IXESHE (a.k.a Numbered Panda a.k.a. APT12 a.k.a. DynCalc a.k.a. DNSCALC)*

The IXESHE group is named after the IXESHE operation. However, Dennesen (2016) links the operation to APT12 and Numbered Panda.

The report by Sancho et al. (2012) from Trend Micro, describes the IXESHE campaign that targeted East Asian governments, Taiwanese electronic manufacturers, and a telecommunication company. The report describes the attack vector as spear-phishing emails containing a malicious PDF. Next, it lists the capabilities of the malware used, and the artefacts left behind by the malware's execution. It continues by exposing the format of the command and control channel, and the infrastructure used. It also provides a comparison with the AES malware. Finally, the report presents the clues supporting attribution, and an approximate timeline of the attacks for the duration of the campaign (2009–2011).

The group launched a new campaign in 2014, which led to another round of research on the APT group. Arbor Networks first published a report on the Etumbot backdoor (ASERT Threat Intelligence, 2014), the new malware used by the group. The report starts by providing information on the malware installer, and gives examples of how the malware installer is delivered via zip files attached to a spear-phishing email, and of the right-to-left override trick that is used to disguise the malware. The report then discusses the malware itself, in particular how it achieves persistence, how it communicates with its command and control, and what unique artefacts it leaves behind. The reports conclude by providing an approximate timeline of the attacks for the duration of the campaign (2011–2014).

Follow-up research on Etumbot is performed by Monnappa (2016), and Moran et al. from FireEye (Moran and Oppenheim, 2014). Monnapa provides a presentation on how to reverse engineer the encrypted command and control communication of the malware. The group at FireEye focused on a new version of the Etumbot backdoor called HIGH TIDE, that appears to be the result of retooling after the publication from Arbor Networks. The blog post also includes details on the new communication patterns used by the malware.

2.14. *Putter Panda (a.k.a. APT2)*

Putter Panda is another APT group that has been associated directly with the PLA.

The main documentation for this APT group is an extensive dossier produced by Crowdstrike (Crowdstrike Global Intelligence Team, 2014). The report starts with attribution to the PLA's 12th Bureau Unit 61486, via an investigation of the online identity copy. This investigation also details the targeting interest of the group for aerospace, satellite, and communications companies. The report also provides technical details for a number of Putter Panda tools, such as the 3PARA Remote Access Tool, PNGDOWNER, HTTPCLIENT, and RC4- and XOR-based droppers. The report also provides a list of artefacts left by Putter Panda that could be used for detection purpose. In addition to the information provided in the report, a blog post by the research team revisits the argument and evidence used for attribution (NH, 2014).

In 2016, Gross and Walter (2016) from Cylance present further analysis of activities of Putter Panda, by investigating an attack involving the group. The research provides a detailed analysis of the low-level functionality of the malware that was not detected by anti-virus software at the time of publishing their research results. They were able to leverage their findings to identify other instances of this malware, and present information on similar infections.

2.15. *Hellsing*

The Hellsing group is documented by Raiu and Golovkin from Kaspersky (Raiu and Golovkin, 2015). They report that one of the victims of an attack by the Naikon APT group (described later), responded with an attack of their own. The blog post starts by providing the email exchanges that were used to set up the attack. The last email message contained a custom backdoor. Further investigations from Kaspersky's telemetry database showed other government and diplomatic targets. The report then lists a number of campaigns and their respective command and control servers. This is followed by an analysis of overlap with the infrastructure of other Chinese APT groups, including Ke3chang and Cycldek / Goblin Panda.

2.16. *Naikon (a.k.a. APT 30)*

FireEye wrote a report on the APT 30 group (FireEye Labs / FireEye Threat Intelligence, 2015b), that starts by providing an overview of the group's character. In particular, they note that the group invests in the development of operations, for example registering command and control domains, and in the development of their tool chain. The report notes that the main tools of the group undergo continuous development, and can be tailored to the network of some of the targets, as evidenced by the variants that have been found. The tools also implement version tracking, and update to newer versions if available, testifying to the professional development pipeline. The report then covers the two-stage command and control technique used by the attacker. In this scheme, the victim machines do not directly connect back to the attacker, but connect to an automated command and control server to download instructions. However, if a more direct control is required, it is possible to use a command to connect to the second stage command, and control where the attacker can connect directly to the machine. The report details the remote-control software panel used by the attacker to manage these direct connections. The report also covers the backdoors' data exfiltration capability, that includes the ability to target air-gapped networks, and remarks that the tools are not designed to extract data of financial value, such as credit card numbers. The report also analyzes the targets of the group, and concludes that the targets are consistent only with Chinese national interests. A brief discussion of the use of social engineering by the group, including examples of lure documents, follows. Appendices provide a detailed reverse engineering analysis of the toolset used by the group, and indicators of compromise.

Baumgartner and Golovkin from Kaspersky, follow up on the report by FireEye with a blog post (Baumgartner and Golovkin, 2015a). They begin by mentioning that, while no exact matches with the indicators provided by FireEye were found, the Naikon group, that was discussed in relation to the Hellsing group, aligns with the description of APT 30. The post starts by providing a geographic distribution of victims, and continues with a description of the decoy and social engineering used for spear phishing. Brief details about the main backdoor, in particular related to its configuration, the list of commands available, and its command and control, is provided. The control panel that accepts callbacks from victims is also presented. Finally, an overview of an anonymized operation against a country is presented.

Baumgartner and Golovkin from Kaspersky, document some of the earlier Naikon APT campaigns in a report (Baumgartner and Golovkin, 2015b), that starts with an introduction, summarizing typical attacks from the group. The authors mention the predilection of the attackers to use certain toolsets, customized for the victim's country. Some of the toolsets are reported to come from the Chinese underground. They also mention the effort invested in reconnaissance to customize spear-phishing attempts. Numerous social engineering tricks deployed, such as names with double extensions, or right-to-left override techniques, are also mentioned. The report then lists a number of shared components (exploits, command and control, and malware) that were used to link Naikon attacks. A study of the group's decoy files is presented next. This study is put in perspective with the attention to detail shown by the group to social engineering. The authors propose that that the lures used would provide insight about the victims. The backdoor and lateral movement tools are discussed next, focusing on capabilities and indicators. They note that some components appear to be shared with APT 30, a group associated with China. A custom second-stage backdoor, based on the HDoor tool, is also discussed in more detail, to provide insight into lateral movement capabilities. The report also notes that Naikon attackers use the c:\intel directory as their main staging point, in a manner similar to the Cycldek attack group. The report also mentions that both groups share a preference for tools coming from the Hacker Union code base. The report then covers lure documents and decoys, as well as indicators of compromises, in an appendix.

3. Russia

Russia is another actor that is very active in terms of state-sponsored APT activity. They have also been under intense

scrutiny because of their involvement in high profile intrusions. As such, numerous groups have been identified. This section presents details on individual Russian actors.

For an introduction to Russian state-sponsored cyber activity, the work of Weedon (2015) presents an overview of their cyber-warfare capabilities. Regarding the conflict in the Ukraine, she presents a summary of the capabilities, tools, and procedures of APT 28 / Fancy Bear, and APT 29 / Cozy Bear. She also reviews a number of incidents linked to other Russian groups. The book continues with its analysis of overall Russian objectives in the cyber realm, by arguing that the main focus appears to be information warfare, rather than the creation of kinetic effects. A detailed analysis of the compromise of TV5 Monde is provided to support the argumentation.

3.1. *Energetic Bear (a.k.a. Crouching Yeti a.k.a. Dragonfly a.k.a. Havex)*

This APT group is mostly documented through the lens of a specific campaign targeting the energy sector.

The Energetic Bear–Crouching Yeti report by Kaspersky (Kaspersky Lab Global Research and Analysis Team, 2014) presents a more global view of the group, covering attacks from 2010–2014 across multiple sectors. The report covers the preferred techniques and tools of the group, and starts by discussing the preferred delivery techniques (trojanized legitimate software, spear phishing, and watering holes). The main malware components (Havex and Ddex loaders, and Sysmain, ClientX, and Karagany backdoors) are also described. A brief summary of the command and control techniques used, and the geographical distribution of command and control infrastructure and victims, are also presented. Other statistical information regarding victims is presented. The report concludes by presenting conflicting information on attribution, specifying that it is not possible to attribute the activity of this actor to any specific nation-state based on that information. This is most likely a comment on the categorical attribution to Russia in other sources.

The rest of the publications on Energetic Bear cover the campaign targeting the energy sector. The Symantec report on the Dragonfly campaign (Symantec Security Response, 2014a) includes a timeline of the campaign. The campaign starts by sending spear-phishing emails, but rapidly transitions to other means of distributing the software. In particular, compromising specialized websites for the energy sector to convert them to watering holes, and compromising SCADA software vendors to add trojan horses to their software, were used. The report then presents statistics regarding the distribution of victims, the number of spam emails sent, and so on. The report also contains an appendix that includes technical details on the tools used in the attacks, specifically the LightsOut exploit kit, Oldrea backdoor, and Karagany trojan.

Finally, it was reported that parts of the LightsOut exploit kit campaign distributed the Havex trojan (Fisher, 2014). This spurred more research, as the Havex malware contained a module targeting industrial control systems, a very rare feature found in malware. Hjelmvik from NetResSec published a list of SCADA vendors that were compromised to include the Havex malware (Hjelmvik, 2014). Hentunen and Tikkanen from F-Secure, published a technical analysis of the malware, which includes the characteristic command and control component, and the reverse engineering analysis, demonstrating the presence of a module for OPC (OLE for process control) (Hentunen and Tikkanen, 2014). Finally, Wilhoit from FireEye, presents a more detailed analysis of the OPC component (Wilhoit, 2014).

3.2. *Sandworm (a.k.a. Quedagh)*

The group Sandworm is associated with Russia, and was named after references to the novel Dune were found in its command and control network. The first source document for Sandworm, discussing an espionage campaign attributed to Russia targeting NATO, European Union telecommunications, and energy sectors, is unfortunately only available to iSight subscribers.

Ducklin from Sophos presents an open source overview of the malware (Ducklin, 2014). It describes how the malware relies on a Microsoft (at the time of writing) 0-day exploit. The article then goes on to explain how the malware spreads using remote resources embedded in PowerPoint files. These embedded resources, while disguised as .gif and .inf files, are in fact executables which are downloaded and run by adding them to the registry. Symantec produced a similar publication (Symantec Security Response, 2014b). In addition to discussing the 0-day, this particular publication also discusses the dropped file, which Symantec refers to as Backdoor.Lancafdo.A, but is more commonly known as BlackEnergy.

More technical details are available in a number of publications covering the 2014 campaign. F-Secure has more technical details on the dll injection of the BlackEnergy version without a kernel module (Brod, 2014). ESET has more details on the exploit, including examples of lure documents (Lipovsky, 2014a), and also reports on a lighter version of the malware, that lacks the kernel mode driver of the more complex versions, and provides examples of how that version was distributed (Lipovsky, 2014b). The information from the ESET publications is reproduced in a Virus Bulletin conference presentation (Lipovsky and Cherepanov, 2014c). The information from F-Secure, and more technical details on the BlackEnergy malware, including its history, its dll installation procedure, its components, its plugins, and its command and control traffic, are presented in an F-Secure white paper (F-Secure Labs Security Response, 2014a).

The same BlackEnergy software was used in a much-publicized cyber attack on the Ukrainian power grid that caused black outs in December 2015 (Hern, 2016). Cherenapov, from ESET, has a detailed publication on the malware used in the attacks (Cherepanov, 2016). This includes the KillDisk component and the backdoored SSH server. The information on the KillDisk component includes the name of the specific processes used in the SCADA software that the module intends to kill.

3.3. *APT28 (a.k.a. Fancy Bear a.k.a. Strontium a.k.a. Pawn Storm a.k.a. Sofacy a.k.a. Sednit a.k.a. Tsar Team)*

APT28 is one of the most well-known groups associated with Russia, as they have been the subject of numerous in-depth

dossiers, and have participated in a number of high-profile attacks.

FireEye has published an extensive dossier on APT28 (FireEye, 2014). The report starts with a geopolitical review of a series of campaigns that they use to link the group to Russia. The report then describes, in some detail, the evolution of the main tools of the group, mainly to show that the families are the result of an organized and professional development effort. Additional information on keyboard settings and compile time is provided, to further reinforce the case that this group operates from Russia. Appendices in the report provide more technical depth, in particular for the SOURFACE / CORESHELL (Sofacy / Sednit) malware, the CHOPSTICKS modules, and the OLDBAIT credentials harvester.

The report from TrendMicro on Operation PawnStorm (Kharouni et al., 2014), presents a number of case studies for targeted infections. The first six present operational details, including examples of the spear-phishing lure used, the steps taken after the initial exploit is triggered, and the files dropped in each case. The report also compares each case to highlight the similarities and differences. The report then describes another campaign aimed at harvesting email credentials. The group would send an email containing JavaScript, hoping the user would open it with Outlook Web Access (OWA). The email would contain a link the user is expecting, for example a link to a conference website. If the user clicked on the link, the conference website would be opened in a tab, but the OWA tab would be redirected to a fake page made to look as if the user was disconnected from the OWA session. If the user entered his credentials on the fake page to log back on, he would then be taken to the still-active OWA page, and the credentials would be stolen. The report then compares different cases targeting the U.S. defense sector, that followed this pattern.

ESET has also produced a number of publications related to this wave of attacks. First, ESET research has produced a report on the use of a custom exploit kit (ESET Research, 2014a). This provides technical details on the exploit kit used in some of the attacks described in the Pawn Storm report from TrendMicro. Another publication by Calvet from ESET, covers the use of USBs to jump airgaps (Calvet, 2014). Calvet summarizes the information on the Sednit malware, and how it spreads, at the Northsec conference (Calvet, 2015a). In this presentation, Calvet presents examples of how APT28 performs its initial compromise (attached documents in spear phishing, custom exploit kit, and stealing webmail credentials). The presentation then covers the usual APT28 modus operandi, and provides examples of the first stage implants and decoys, including detailed reverse engineering of the code, and a description of stealth techniques used by the group. A similar study is presented for the stage 2 implants. Finally, the presentation briefly discusses airgap jumping techniques.

The Microsoft Security Intelligence report, covering the first half of 2015 (Microsoft, 2015), contains a section related to APT28, which they name STRONTIUM. They provide a brief profile of the group, and information about how they attack targets, giving examples of targeted spear phishing, and web-based exploit kits. However, they also report on new techniques developed by APT28 since the publication of the previous reports. For example, they divulge how they compress remote payloads in memory, and how they added a Firefox bootstrapped add-on to their compromise techniques. They also reproduce information related to the increase in USBs being used to jump airgaps. They conclude by providing guidance to respond to attacks from this group.

Another report from Bitdefender (2015) presents information on yet another APT28 campaign. The report contains information about custom scanning bots designed to find suitable targets from a list of targets of interest. They then report the typical APT28 attack flow, which starts with a first-stage dropper, followed by a second-stage backdoor, that downloads later-stage modules as needed. The report also provides limited information on the victims of this wave of attacks, but the report contains formatting errors that hide some of the information, and some of the other information has been deliberately redacted. A number of appendices, that cover the tools used by the group, are included in the report. This provides a detailed look at the scanner software used to identify and track vulnerable targets, some of the modules used, and the stage-1 and -2 malware used in the campaign.

A number of other publications have tracked improvements in APT28's toolkit. Kaspersky reports on improvement to the deployment scheme, and on adding DLL side-loading to the AZZY backdoor (Kaspersky Lab's Global Research & Analysis Team, 2015a). Falcone and Lee from PaloAlto, report on a new delivery technique that uses the registry to start the malware each time a Microsoft Office application is opened, and on the Carberp version of Sofacy (Falcone and Lee, 2016). Bailey, from Mandiant, provides a detailed reverse-engineering walkthrough of the exploit payload used in one of APT28's campaigns (Bailey, 2016). Alperovitch, from Crowdstrike, provides more information on the tools used to compromise the Democratic National Convention (DNC) in the lead up to the 2016 USA presidential election (Alperovitch, 2016), and Cluley, from ESET, presents a summary of new APT28 campaigns (Cluley, 2016). This constant retooling is repeated in Dennessen's presentation about the APT28 group's response to public exposure (Dennesen, 2016), that documents how APT28 "keeps on trucking," even in the face of public exposure.

In addition to their constant updating of their techniques to penetrate Windows-based networks, there is evidence that APT28 constantly develops their tool chain to attack other types of systems. Creus, Halfpop, and Falcone, from PaloAlto, present a detailed analysis of the Komplex trojan that targets OS X systems (Creus et al., 2016). This publication, in addition to providing complete details on the workings of the trojan, and its related command and control infrastructure, compares Komplex to other malware used by the group. Similarly, Crowdstrike publishes a report of the use of a trojaned Android application containing tools associated with APT28 (Crowdstrike Global Intelligence Team, 2016). The report contains a description of the malware that is piggy-backed on a Ukrainian application for artillery support, for use on Android smartphones. In addition, the report presents the case that this is part of an operation to gather tactical intelligence on the position of artillery pieces used in the conflict in Ukraine.

In their presentation at the 2016 RECon conference, Calvet, Campos, and Dupuy, from ESET (Calvet et al., 2016), present an end-to-end analysis of APT28 by reverse engineering all the artefacts left in a campaign. They start their research from a misconfiguration, from the attackers, that let the researchers

have access to shortened URLs used in the campaign. They again state that this actor has a significant tool chain at his disposal, and has access to multiple 0-day exploits. They present a lure used for spear phishing to entice the user to access the exploit kit page, which mimics a legitimate website. The presentation then goes into details of both the fingerprinting component, and the exploit factory component of the exploit kit. They also present details on how the vulnerability that was used was customized, and then provide a reverse engineering analysis of the dropper, and the stage 1 payload. This includes an analysis of the content of the command and control communications. A similar analysis is provided for the stage 2 dropper and payloads (i.e., the backdoor). The presentation continues with a similar analysis for various modules that includes an analysis of X-AGENT (CHOPSTICKS) and its command and control protocol, made more detailed due to access to the source code, the password extractor module, the module allowing screen shots, and the X-TUNNEL module. The technical analysis is concluded by a review of the long-term persistence techniques used, which revealed a new bootkit module, which is analyzed in detail. Finally, the conference presents some of the particularities of the code that can be used as hints about the authors of the malware.

3.4. *The Dukes (a.k.a. APT29 a.k.a. Cozy Bear a.k.a. Cozy Dukes)*

The Dukes, another APT group typically attributed to Russia, gets its name from the detection name of their main malware component.

The first report on the Dukes is a report from Kaspersky Labs (Raiu et al., 2013). The report investigates an incident in which an Adobe Reader 0-day was used to drop a, then unknown, piece of malware. The report starts by presenting the PDF lures used in this wave of attacks. A brief analysis of the exploit used in this specific campaign, and the differences with a previous campaign using the same vulnerability identified by FireEye earlier, was presented. The report continues with the reverse-engineering analysis of the backdoor that is dropped, named MiniDuke. A more in-depth analysis of command and control is performed. Notably, the report discusses a peculiar command and control element that uses Twitter (and possibly Google) to update the addresses of its command and control, and the use of steganography to conceal the stage 2 malware. The report also briefly discusses a stage 3 malware element that possesses typical remote access tool functionality, and ends with a brief summary of victims, and a short conclusion highlighting the uniqueness of this attack, hinting at potential nation-state implication. Ultimately, further investigations by other researchers will prove them right.

F-Secure has published the most in-depth research of the Dukes. The first important piece of research is a report on the CosmicDuke malware (F-Secure Labs Security Response, 2014b). The report starts by presenting an overview of a typical infection chain. In this chain, a user receives a PDF file containing an exploit or an executable file, disguised as an innocuous file type. The MiniDuke loader is then dropped, and the Cosmu information stealer is loaded. The report continues to provide technical details of the malware. This includes the right-to-left override trick used to disguise the extension name, examples of decoy files, types of exploits used, full details on the information stealer components including capabilities and forensics traces left, and an analysis of the network communications done by the malware.

The report concludes with an analysis of the history of the malware, and indicators of compromise. The second publication is a report on the CozyDuke malware (F-Secure labs Security Response, 2015). They report on the infection vector, typically a spear-phishing email containing a link to a website hosting a zip file, which drops the malware and a decoy document. They also report on the reuse of the infrastructure with the MiniDuke and OnionDuke malware campaigns. Finally, they present an overview of the inner workings of the malware, including how it persists, the command and control infrastructure used, how it is configured, and the types of tasks it can accomplish. The report ends with the history of the evolution of the Cozyduke malware, and indicators of compromise.

The third report from F-Secure is a report on the APT group itself, summarizing seven years of campaigns (F-Secure Labs Threat Intelligence, 2015). The report starts by commenting on the group's style. In particular, they note that the group employs a "smash-and-grab" tactic at first, which then transitions to a more stealthy approach to establish long-term persistence. The report also comments on the group's obstinacy, citing the group's tendency to continue operations even when their toolset has been publicly exposed, and at the same time reworking their tool set incrementally to avoid detection. They then proceed with a history of the group, starting in 2008 with campaigns in Chechnya, and ending in 2015. The report then continues to cover the main toolset used by the group. For each tool that is associated with the Dukes, the report presents the main capabilities and any particularities found in the tool that could hint at attribution. The report closes with a brief analysis of infection vectors, decoys, and vulnerabilities used, and briefly discusses attribution to the Russian state, and presents indicators of compromise.

ESET reports on new campaigns using Miniduke in 2014 (ESET Research, 2014b). The blog post discusses the new vulnerability being exploited, how the malware is installed, and how the malware is operated. In particular, a large section is dedicated to the Twitter command and control component of the malware. Symantec reports on a new campaign that uses the SeaDuke version of the malware (Symantec Security Response, 2015a). This blog post gives background information on the APT group, and compares the SeaDuke malware to the traditional MiniDuke implant, as they are both stage-2 backdoors dropped by the CozyDuke dropper. In particular, the post notes the difference in the architecture used for command and control.

Grunzweig, from PaloAlto Networks, provides more analysis on the SeaDuke malware (Grunzweig, 2015). The analysis reveals that the malware was written in Python, and, as such, the malware can be decompiled. The post analyzes how the resulting code can be deobfuscated to get the final payload. This provides greater insight into the configuration, capabilities, and command and control protocol used. Levene, Flacone, and Wartell, from PaloAlto, present a similar analysis for the MiniDionis implants (Levene et al., 2015) (a series of implants related to SeaDuke). By reverse engineering the MiniDionis, they are able to provide more information on the protocol used for

command and control, and are also able to provide good visibility into the capabilities of the implant.

Around the same time as the research from PaloAlto, FireEye publishes a report on the stealthy command and control infrastructure, which they call HAMMERTOSS, used by the group (Fire Eye Threat Intelligence, 2015). The technique is to use cloud services, such as Twitter, GitHub, or other storage services, to link malware with images containing command and control instructions hidden with steganography. This allows the group to hide their communications by going to common websites.

Finally, the group is reported to have participated in the high-profile compromise of the DNC, alongside APT28, according to FireEye (Alperovitch, 2016). The post also covers the implant used by the Dukes in the intrusion, which relies on SeaDuke (called SeaDaddy by FireEye). As the malware was written in Python, it can easily be reverse engineered. The results show that the module contains a powershell command to contact the command and control, and download additional powershell modules (for example the Mimikatz powershell module to gather credentials) to run in memory. These attacks appear to have continued after the elections, and Krebs reports on the new campaign (Krebs, 2016).

3.5. *Snake (a.ka. Turla a.k.a. Venomous Bear a.k.a. Waterbug a.k.a. Agent.btz)*

The Snake group, named after the well-publicized Uroburos malware, is another group that is associated in the literature with Russian state interests.

G Data presents a report on the Uroburos rootkit (GData, 2014). The report starts by discussing the fact that this software is probably part of an espionage toolkit due to its sophistication, and due to the fact that it checks for the presence of the Agent.btz malware that hit the Pentagon in 2008 (for more details, see Barnes (2008)), and does not run if it is present. The report then provides technical details of the rootkit. Of note, it describes the inline patching method used to create hooks, the virtual file system created by the rootkit, and the injected libraries. The report also covers the type of tools that were found, stored by the attackers, in the virtual file system. These tools include typical post-exploitation tools to dump passwords, gather system information, and steal and compress documents. The report also mentions a form of peer-to-peer capability to extend command and control to nodes that do not have direct access to the Internet. The report closes by providing more evidence of links to the Agent.btz malware and its suspected Russian roots.

BAE Systems expands the analysis of the Uroburos (that they call Snake) malware (BAE Systems Apllied Intelligence, 2014). They expand the research made by G Data to other strains of the malware. While G Data looked at the kernel mode version of the rootkit, BAE Systems also found user mode versions. The report compares the architecture of both versions of the malware. The report starts by presenting aggregate statistics on the samples found in the database used for their research, and then presents technical details for the user mode version of the rootkit. It presents the types of artefacts left behind, then continues with an analysis of the operations taken when the malware is executed, and a detailed investigation of the command and control communications. A description of communications between local machine processes is also included. The report then covers the kernel mode version of the rootkit, describing the registration and hooking processes required for the rootkit installation. It then describes the virtual file system used by the rootkit. After covering the kernel mode version, the report discusses the particularities of the 64-bit version of the rootkit. A brief description of the reconnaissance module that is downloaded post exploitation is also provided. The report concludes by presenting similar links to the Agent.btz malware that were included in the G Data report. Appendices detailing various indicators of compromise complete the report.

Kaspersky, on the other hand, presented an analysis of a specific campaign involving the Uroburos family (which they call the Turla family) (Kaspersky Lab's Global Research & Analysis Team, 2014). Their investigation starts by investigating the infection vectors, which were not available in the previous literature, and then they discuss the exploits used in spear-phishing attachments, and a significant watering hole operation using injected websites. The blog post then investigates the command and control architecture used to manage the infections. Operation of the backdoor is then discussed. Notably, the investigators were able to obtain command templates that include a detailed description of the type of reconnaissance they perform once they are on a machine, and the methods used to move laterally across the network. They also discuss how more advanced backdoors are uploaded on compromised machines, and conclude by presenting language artefacts, victim statistics, and indicators of compromise.

Raiu and Baumgartner, from Kaspersky, investigate "penquin" Turla (Raiu and Baumgartner, 2014). This malware is a version of the Turla malware that targets Linux computers. The backdoor, based on the openly available cdoor stealth backdoor, is difficult to detect using tools like netstat. The report also discusses the types of "magic packets" that are required to trigger the activation of the backdoor. Another investigation by Tanase from Kaspersky, discusses the use of satellite communication for command and control by the group (Tanase, 2015). The post starts by explaining the usefulness of satellite communications to APT groups to hide the exact location of command and control infrastructure, and then discusses the specific technique used to abuse the satellite communications for command and control, and present a list of Internet ranges that were the target of such abuse by the Snake group.

The conference presentation by Dereszowski at the 2014 FIRST Symposium (Dereszowski, 2014) (which was presented again at the 2015 Rooted conference (Dereszowski, 2015)), presents an overview of Turla Operations. The report starts by presenting a summary of existing versions of Turla, and attempting to clarify the nomenclature used in the open domain literature. The presentation then summarizes the technical information on the various malware elements. Another summary of the communication, including the protocols used in the covert channels follows, and then it covers all the stages of an operation (infection, reconnaissance, lateral movement, and establishment of local command of control). Of note, Dereszowski presents a differing attribution of the malware, hypothesizing that multiple groups are using this particular espionage software.

Symantec published a report on the group, which they call the Waterbug attack group (Security Response, 2016). The report starts by describing the infection vectors (spear phishing, and watering hole attacks). For the watering-hole vector, they provide statistics on the websites that were compromised to hold the infection script, and then briefly describes the two main pieces of malware used: Trojan.Wipbot (called Epic in the Kaspersky research (Kaspersky Lab's Global Research & Analysis Team, 2014)), and the Trojan.Turla malware. The report then compares the two pieces of malware with other components used by the APT group, e.g., the Carbon module described in the BAE report (BAE Systems Apllied Intelligence, 2014).

More research into watering hole techniques led FireEye to publish a report on WITCHCOVEN (FireEye Threat Intelligence, 2015). The report presents the toolset which is used to remotely fingerprint machines, in particular identifying versions of Microsoft Office via ActiveX, and detecting various popular web plugins via Javascript. Although the report does not formally associate WITCHCOVEN with the Snake group, the report presents an analysis of victims, and notes that Snake is one of the APT groups that rely heavily on injecting code on compromised websites, and notice a direct overlap in targeting with other operations from the group.

The Swiss government CERT, published a report on a Turla case (GovCERT.ch, 2016). The report starts by providing a brief timeline of the incident in question, and then provides some background information about the Turla malware. The report describes how the machine is fingerprinted via watering holes, and then continues about the active infection, including describing how each component is dropped, and then delves in the Carbon.dll component, analyzing its capabilities and the network communications. The report continues by describing the tools used for lateral movement, mostly public domain tools such as Mimikatz, and covers the use of pass-the-hash and pass-the-tickets techniques up to the gain of a Kerberos Golden Ticket by the attackers, that was used to infect other systems using command-line commands. The analysis of the incident ends with the methods to exfiltrate the data. The report is concluded with recommendations on how to increase the security posture.

Finally, Bartholomew from Kaspersky, details a new Turla JavaScript payload (Bartholomew, 2017). The publication starts by presenting the technical details, highlighting the differences with the previous version of the tools, and continues by listing the machine profiling commands that are launched by the tool, and the command and control infrastructure. A brief discussion of victims observed from a sinkholed domain is given, but the publication specifies that, as this is a new component, the number of victims is still quite low.

4. "Western" powers

4.1. *Animal Farm*

A single APT group has been publicly attributed to France, about the use of the Animal Farm series of malware.

The first publicly documented analysis of malware from the Animal Farm family, is the study of the EvilBunny malware by Marschalek from Cyphort (Marschalek, 2014). The malware, which can more accurately be described as an execution platform for Lua scripts, is described as very sophisticated, but was not attributed to any particular APT group at that time. The analysis starts with a description of the infection vector and the dropper. Of note, the numerous methods used by the dropper to avoid detection and analysis are presented. The blog post then describes the EvilBunny implant itself, with particular reference to sandbox detection methods, and descriptions of the Lua execution environment.

Marschalek reports on another study on the malware Babar (Marschalek, 2015). The Babar malware, named after a string found in the sample, bears not only a striking similarity to EvilBunny, but also to a description of a Babar implant found in leaked Snowden documents. The report presents the technical details of the Babar implant. The malware is essentially a user space rootkit that can provide spying functionalities, such as logging keystrokes, taking screenshots, capturing voice data from softphone applications, and so on. The blog post also describes in more detail, the hooking process, and the command and control architecture used.

Rascagnères from G Data, continues the analysis of the Babar implant (Rascagnères, 2015). The analysis starts by taking the slides from the Communications Security Establishment Canada (CSEC) in the Snowden leak, describing the Babar malware (labelled SNOWBALL in the documents), and comparing it to the Babar samples described by Marschalek. Globally, the samples studied by Rascagnères match the description from the slides, which attributes the implant to French developers. The investigation is continued by comparing the EvilBunny and Babar implants to find commonalities. Both use the same WMI technique to list installed software on the machine, and share some components for API obfuscation. The report then discusses some differences observed in API obfuscation, and goes into more depth in the analysis of Babar's configuration and espionage features.

Calvet from ESET, studies another malware from the same source, named Casper (Calvet, 2015b). The blog post starts by presenting context on how the malware was discovered after investigating the injection of 0-day exploits on a Syrian government website, and then describes the dropper in more details. The use of a file to adapt its strategy to different situations, changing the way it deletes itself after infection, or how it contacts the command and control, is particularly noted. The investigation then covers how the Casper implant itself is installed, and how it contacts the command and control server. The post is concluded by a brief comparison to EvilBunny and Babar, and comments about the likely victims.

Kaspersky expands on the malware family in a study of the Animal Farm APT (Kaspersky Lab's Global Research & Analysis Team, 2015b). The post adds to the toolset of the APT group the Dino, Tafacalou, and NBot malwares, and provides a summary of the role of each piece of malware. The report provides a brief timeline of the group's use of each component, and closes by providing statistics obtained from the sinkholing of command and control domains by Kaspersky.

Finally, Calvet, from ESET, studies the Dino malware (Calvet, 2015c). Contrary to Casper, Dino is a more fully fledged espionage platform, with more capability to snoop on the victim. The publication starts by listing the modules included in the

Dino malware, and the data structure and configuration files, and continues by listing the commands available to Dino's operators, and describing a custom file structure used by the malware. The analysis is concluded by showing the evidence linking Dino to the rest of the Animal Farm family, and linking the creation to native French-speaking developers.

4.2. *Regin*

The Regin platform is an advanced malware platform for the purpose of espionage, typically attributed to the Five Eyes community.

Kasperky presents the first analysis of the Regin platform (Kaspersky Lab, 2014). The report focuses on the platform itself, as the researchers did not find traces of the initial compromise. However, they mention traces of lateral movement by using Windows shares and remote execution. The platform itself has multiple stages. First, a loader module is installed, then depending if the system is 32- or 64-bits, different later stages are loaded to create a virtual system where the payload modules are finally loaded, to perform whatever tasks the operators have in mind. The report then goes into more detail to describe each stage, focusing on details showcasing the high level of sophistication of the malware and the operation. For example, in the first stage, they note the use of NTFS extended attributes to store the malware, the use of code signing certificates, and on the ability of the malware to run in kernel mode or user mode, depending if the system is 32- or 64-bits. The report also describes in detail the main components of the platform, the virtual file system and the dispatcher module. These components allow the operators to load additional functionalities onto the platform to perform whatever task they require. A few examples of modules and known data blocks are provided. The report then provides elements of information about interesting strings found in the code, details on the compromise of a GSM network using the platform, the command and control architecture, some victim statistics, and comments on attribution. Of note, they do not attribute the Regin platform to any specific country in this report, but comment on the fact that this is the most sophisticated espionage platform at the time of publication.

Symantec follows suit with another analysis of the Regin platform (Symantec Security Response, 2015b). The report starts by providing brief statistics on victims, showing the bulk of the victims to be ISPs, or telecom providers. They also provide one documented vector of infection, which appeared to be a Yahoo! Instant Messenger exploit, and then summarize the technical information on the malware, essentially covering the same ground as the Kaspersky report. However, they provide more information about the protocols used for command and control.

Finally, Raiu and Soumenkov, from Kasperky, dissect the 50251 Regin module (Raiu and Soumenkov, 2015). In particular, they analyze the Regin module to compare it to a Qwerty keylogger that is included in the files leaked by Snowden. Through reverse engineering, they conclude that the Qwerty malware is in fact the Regin module. While attribution is not specifically addressed, the link with the Snowden files leaves it implied.

4.3. *Equation group*

While Regin was the most advanced cyber espionage platform at the time of the writing of the Kaspersky Regin report, the crown was taken by another group, dubbed the Equation group by Kaspersky.

Kaspersky published a report documenting the group (Kaspersky labs, 2015). The report is organized in the form of a Q&A, and primarily focuses on the toolset used by group. It discusses the DOUBLEFANTASY validator (a backdoor that validates that the target is worthy of upgrading to a more sophisticated backdoor), the EQUATIONDRUG and GRAYFISH espionage platforms, and the FANNY worm. Because of the highly sophisticated nature of GRAYFISH, which contains bootkit functionalities, the report provides more details on the working of that particular component. Similarly, Fanny, a worm that spreads through the same vulnerabilities as Stuxnet, is discussed. The report then discusses methods of infection and vulnerabilities that were used by the group, and provides more details about the most advanced capability observed in the toolset, the ability of GRAYFISH and EQUATION to infect harddrive firmware for persistence. The report then answers questions about victimizations, providing high level statistics obtained from command and control sinkholing, and how the group appears to perform careful fingerprinting and selection of victims, and then briefly discusses the use of encryption by the group, and provides some indicators of compromise.

In late 2016, a group of hackers calling themselves the Shadow Brokers, leaked tools that allegedly belonged to the Equation group. Santos, from Cisco, provides a technical analysis of the tools related to Cisco products (Santos, 2016). The analysis covers the EXTRABACON exploit code, a 0-day exploit for certain types of Cisco firewalls, the EPICBANANA exploit, another 0-day exploit for Cisco ASA, and JETPLOW, a persistent implant of EPICBANANA.

Finally, Goodin from Ars Technica reports on the Kaspersky divulgation (Goodin, 2015). In addition to providing a non-technical summary of the main findings of the Kaspersky report, the article delves into attribution. In particular, it compares the names of some of the modules identified by Kaspersky to interdiction techniques used by NSA, and contents of the leaked Snowden documents.

4.4. *Olympic Games*

The Olympic Games cyber attacks were a series of attacks aimed at disrupting Iran's nuclear weapon program. Numerous elements of the press have attributed the program, which led to the development of Stuxnet and Flame, to a joint effort by the USA and Israel (Sanger, 2012) (Nakashima et al., 2012).

While some APT research was already under way, at the time of publication, the Stuxnet dossier by Falliere, O Murchu, and Chien (Falliere et al., 2011), is one of the first reports documenting an advanced cyber weapon. The report starts by presenting a timeline of Stuxnet's discovery, followed by statistics of the victims that were observed by Symantec. The report then launches into its reverse engineering analysis of the malware. It starts by providing an overview of the complex modular organization of the malware, organized around a

central DLL injected in a trusted process, and then reports how Stuxnet is installed, including a brief analysis of the 0-day privilege escalation exploit used. The command and control protocol is covered next, followed by the Windows rootkit functionality. The methods by which Stuxnet expands its access inside a compromised network, that also contains a remotely exploitable 0-day vulnerability, and a 0-day used for USB propagation, are then discussed. The listing of Stuxnet capabilities is continued by covering the capabilities to attack industrial control systems (ICS), in particular the ability to infect Siemens Step 7 files, modify programmable logic controllers (PLCs), and hide its presence on an ICS network. The report is concluded with a summary of the DLL exports, and a survey of the Stuxnet variants found by Symantec.

Another Stuxnet report by Langner (2013) analyzes, in more depth, the behavior of Stuxnet in relation to ICS. In his report, he presents evidence based on the PLC component of the malware and open source information on the Iranian nuclear weapon program, and concludes that Stuxnet targeted centrifuges were used in the Iranian nuclear program.

Symantec published a report on Duqu (Symantec Security Response, 2011), which they claim shares source code with elements of Stuxnet. However, unlike Stuxnet, Duqu has no capability to attack ICS, but instead is an espionage tool to extract information for future attacks. The report starts by providing more context of how, and where, the malware was found, and then describes the general architecture, that uses a driver, a main DLL used to load resources, and an encrypted configuration file. The report continues with a detailed technical analysis of the method of installation, the capabilities of the main DLL, and the various exports of the payload loader resource, and then covers both the command and control protocols and architecture (remote, and peer-to-peer). This is followed by examples of further modules that are downloaded, the techniques used to propagate inside a network, and a comparison of the variants that have been encountered. The report also includes, as an appendix, the technical report from the CrySyS labs at the Budapest University of Technology and Economics, the original discoverer of the malware.

Gostev and Soumenkov, from Kaspersky, researched the evolution of the drivers used with the Stuxnet malware, and their eventual evolution to the form used with the Duqu malware (Gostev and Soumenkov, 2011). This creates a timeline of the use of various components of the validator component that was used to distribute both Stuxnet and Duqu.

A new version of Duqu was discovered by Kaspersky in 2015, while investigating a compromise in their own office, and they published a report on the version they call Duqu 2.0 (Karspersky Labs, 2015). They start by discussing how they are unclear about the infection vector, but suspect a spear-phishing attack that triggered a 0-day vulnerability. They then discuss lateral movement, how attackers escalated their privilege on one machine, using a privilege escalation 0-day, and leveraged the elevated permission to deploy the malware on other machines, for example by creating a MSI installer. The report then discusses how the MSI packages are layered and unpackaged. In particular, the methods to bypass security mechanisms are described in detail. The report then describes the payload containers that can be loaded in the basic backdoor of the module, and present a similar analysis for the advanced version, that contains a more fully-fledged espionage suite to be deployed on more "interesting" targets. It continues by providing summaries of persistence, and command and control mechanisms, and then provides an analysis of the similarities between the original version of Duqu and this new version, providing an overview of victims, in order to comment on attribution. They comment that the attacks observed were consistent with a GMT +2, or +3, time zone work day, with Fridays and Saturdays off. In addition, they mentioned that some victims appeared to be infected with this version of Duqu and Equation group software, suggesting a lack of cooperation between the groups. This would suggest that this version should not be attributed to the USA side of the Olympic Games project.

The CrySyS lab found yet another iteration of this family, named Flame or Flamer, and produced a technical report on it (Laboratory of Cryptography and System Security (CrySyS Lab), 2012). The report is aimed at providing a first insight into the malware, and starts by presenting contextual information as to how the malware was found, and how it relates to Duqu and Stuxnet. The report then continues with a list of the main modules. However, the functionalities are not described, as they were unknown at the time of writing. The report then discusses the investigation into how the malware is installed, and how modules are loaded when it is run. Similar analyses are presented for various storage components (registry, encrypted files, etc.). A brief investigation of what could be the command and control module is then presented. Similarly, fragmented information is provided on database structure, Lua scripts found in the code, and so on. Unfortunately, the preliminary nature of the report makes claims, often unsupported or dubious.

After the CrySyS publication, Symantec posted a follow-on analysis (Symantec Security Response, 2012). They present an overview of victims that can be gathered, based on the information in the CrySyS report, and finally, they present an overview of the components which include a Lua interpreter, SSH code, and database functionality. The post also mentions additional modules that are loaded, including a wiper virus, a tool to capture screenshots, and a tool to steal documents.

Gostev from Kaspersky, then published a series of analyses of the Flamer malware. First, he publishes a Q&A style publication that covers the general information (Gostev, 2012a). In his answers, he mentions the general characteristics of the Flame malware (most notably the Lua scripting engine), and comments on the differences in code to Duqu and Stuxnet, theorizing that Flame does not share the same "Tilded" platform used by the other two. He also mentions that Flame is much less selective in terms of targets. However, he mentions that they share some vulnerabilities and techniques, including the unique method Stuxnet spread via USBs, and the print spooler vulnerability used in Stuxnet, and speculated that they were developed in parallel by the same group. In his second report (Gostev, 2012b), he discusses the various modules that provide Flame with its capabilities. His third report covers the method used to spread across the network (Gostev, 2012c). Through a more detailed analysis of the Munch gadget, Gostev discovered the ability of Flame to act as a man-in-the-middle for Windows Update, in order to spread itself across the network. His fourth post describes the reverse engineering of

Stuxnet's "Resource 207." (Gostev, 2012d). The analysis demonstrates a common ancestry between Flame and Duqu / Stuxnet, even if Gostev concludes that they use two distinct platforms. Another report analyzes the command and control infrastructure (Gostev, 2012e). Starting by comparing Flame and Duqu command and control infrastructure, the posts also include numerous examples of fake registry addresses. Furthermore, by sinkholing a number of command and control domains, the authors could gather a great deal of information regarding victims, and summarize them in the publication.

Further analysis of the Flame malware led Kaspersky to the discovery of Gauss (Kaspersky Lab Global Research and Analysis, 2012). The report starts by providing infection statistics, and continues by exposing the modular architecture of the malware. As with the discovery of Duqu, they have no information on the initial-infection vector. The report then discusses the similarities with Flame. The main body of the report comprises a technical analysis of each of the known modules. The main installation, command and control module (ShellHW), numerous system fingerprinting modules and a series of modules to infect USB drives, are discussed. The USB infection payload is unique in the fact that it is not used for propagation, but to steal information from systems in which an infected USB is plugged in. The report then presents an analysis of the command and control infrastructure used by Gauss. Finally, a timeline of known dates of creation for Flame and Gauss modules, and a complete list of files dropped by Gauss, are summarized.

Having received a hard drive image of servers used as Flame command and control nodes, Kaspersky was able to fully investigate the contents of a command and control server (Kaspersky Lab's Global Research & Analysis Team, 2012). Due to their full access to the machine, the researchers were able to inspect the directory structure, and access the command panel used by the operators. This enabled the researchers to discover the exact protocol used for uploading commands. However, they also found that the server acted as command and control, not only for Flame, but for three other unknown malware strands. It was also possible to directly access scripts loaded on the machine, including the developers' comments included in the scripts. The publication delves deeper into a script designed to erase logging, and stop all future logging activity on the server, and also presents a slew of other scripts designed to hide the traces of its activity.

Kaspersky later found one of the unknown malware strands connecting to the investigated server, and published their analysis of the "miniFlame" malware (Global Research & Analysis Team, 2012). According to their analysis, the miniFlame malware is a small version of Flame that can work, either as a standalone component, or as a Flame- (or Gauss-) module. This version appears to have been used in more targeted attacks, as the number of documented victims is low. The report starts by providing context about how the sample was discovered, and a timeline of the samples of the malware, and comparisons between the different versions are presented. Infection statistics coming from both internal Kaspersky telemetry, and command and control sinkholing are provided. The report goes on to cover the technical details of the modules. The command and control protocol is then discussed, as well as some of the commands available for information stealing. A USB infector module is also covered in detail.

4.5. *Project Sauron (a.k.a. Strider)*

While project Sauron is not directly associated with Western powers, circumstantial evidence in the literature strongly pointed toward its inclusion in this section.

In August 2016, Symantec reports on a new threat actor, targeting espionage targets in Russia, China, Sweden, and Belgium (Symantec Security Response, 2016b). The main tool used by this threat actor, called Remsec, is an advanced espionage backdoor, with the capacity to load additional functionalities through Lua modules. The report notes the similarities with Flamer, as well as the fact that one of the targets was previously targeted by Regin. The report also mentions that the group is very selective in its compromises, with only 36 victims present in the Symantec database, and then presents an overview of the backdoor capabilities, and of the capabilities of some of the Lua modules.

Two days later, Kaspersky published an extensive report on the same topic, entitled Project Sauron (Global Research and Analysis Team Kasperky Labs, 2016). The report starts by providing a technical summary that paints the picture of a very advanced threat actor, installing itself on domain admin servers, creating complex peer-to-peer commands, and control on internal networks, loading Lua modules, and executing modules exclusively from memory. The report proper starts by providing information on malware deployment, noting that the malware is deployed by modifying legitimate deployment scripts used by network administrators. The report then covers an apparent capability to use USB devices to jump airgaps, and a capability to capture information for an unusual communication protocol that was used by the victims. Various methods available for data exfiltration are then presented. The Lua module capability, and the virtual file system are described next. A brief overview of the command and control infrastructure that could be found is presented, as well as a brief discussion of possible attribution. This discussion primarily presents language artefacts, but is mostly inconclusive. However, the conclusion implies that this is a new espionage platform, based on lessons learned from Flame, Duqu, Equation, and Regin.

5. Middle East

A number of actors are active in the Middle East, where, however, accurate attribution information is more difficult to obtain. Furthermore, some of these actors blur the line of being considered APT groups, as they often engage more in internal surveillance, than foreign espionage.

5.1. *Iran*

Of the actors in the Middle East, Iran possesses the most well-defined capacity, with a number of incidents and groups attributed to the country.

Bronk and Tikk-Ringas write on the Shamoon attacks (Bronk and Tikk-Ringas, 2013). In these attacks, a worm containing a

wiper element was introduced in the network of Saudi oil-giant Saudi Aramco, and later propagated to other oil and gas networks. This attack echoes the use of the wiper component in Flame that targeted the Iranian oil industry. Zetter reports on NSA documents leaked by Snowden, that appears to confirm this hypothesis (Zetter, 2015). Bronk and Tikk-Ringas' publication provides ample geopolitical context for the attack, and summarizes the key elements of the Shamoon worm. The paper also comments on attribution, as the group, that is the self-proclaimed author of the worm, the "Cutting Sword of Justice," appears to have ambiguous motivations, and Iran has a tradition of providing state backing to loosely affiliated organization, such as Hezbollah. Bronk and Tikk-Ringas' thesis is that the "Cutting Sword of Justice" is a similar front for Iranian state interests.

Meyers from Crowdstrike, reports on an actor called Clever Kitten (Meyers, 2013), that is characterized by its use of the Acunetix web scanner for reconnaissance. The actor audits public websites to find vulnerabilities, and then installs a common PHP web shell. The post discusses briefly why the actor is attributed to Iran, without going into specifics. The use of vulnerabilities on public websites to pivot in the network by Iranian hackers is also reported by Gallagher (2014). As this concerns the network of the U.S. Navy, and occurred at around the same time as the FireEye report, it is possible that this concerns the same actor.

Villeneuve et al. from FireEye, report on Operation Saffron Rose (Villeneuve et al., 2014). The report covers the Ajax security team, and their introduction to cyber espionage following years of patriotic hacking. The report provides some context for this transition, and goes into technical characteristics of the group. It starts by covering the infection vectors used (spear phishing, credential phishing for VPN and OWA login pages, and trojanized software). The report then provides more technical details on the main tool used by the group, the Stealer malware. Even though it is not an advanced espionage platform, it still possesses all the capabilities to fingerprint a system, and exfiltrate information. The report then describes the builder tool used to compile the various samples of the Stealer malware, and discusses the command and control infrastructures for attacks targeting the aerospace industry, and for attacks targeting dissidents. A brief study of the victims from a sinkholed domain, used to target dissidents, shows that most of the victims appear to be Persian. The report concludes by discussing attribution, putting an emphasis on the progressing transition of the group from cybercrime, to political espionage.

Dahl from Crowdstrike follows on the FireEye report (Dahl, 2014b), by publishing information of the group that Crowdstrike calls Flying Kittens, that was involved in Operation Saffron Rose. The publication goes into more detail on the use of spoofed websites to harvest credentials, and continues with a discussion of attribution, linking the attacks to the Ajax team, via the name used to register the fake websites.

Cylance publishes a report on OpCleaver (Cylance, 2014), an Iranian group targeting infrastructure. The report starts by putting the operation in context, linking the group to the attacks on the U.S. Navy associated with Clever Kitten. The report provides attribution to Iran, lists affected victims, and reports on how the skills of the attackers have significantly improved since the first reported incidents. The report continues by providing more analysis of the victim set, and more links to Iran, gives an overview of the custom tools used by the group, and identifies the handles of a number of group members that could be gleaned from artefacts left in the tools. The report lists the techniques and procedures used by the attackers, including how they perform the initial compromise (SQL injection, and numerous spear-phishing examples), how they expand their presence (various Mimikatz and psExec tools, remote exploits, and ARP cache poisoning), how data is exfiltrated, and how persistence is achieved (TinyZbot, backdoors, and the PVZ tool chain). The report expands on the analysis of TinyZBot, including details of its command and control protocols, a version history, and various components of the PVZ tool chain are also detailed. The report concludes with some speculation about the intent of the group.

Evron and Werner gave a talk at a conference about off-the-shelf tools used by an Iranian APT group (Evron and Werner, 2014). The group, which they called Rocket Kitten in their presentation title, uses macro-enabled Office documents as the main method of compromise. The documents are reverse engineered to look at the metadata to gain more information about the timing of the operation. The name of the author of "Wool3n.h4t" is also revealed. The file installed by the dropper is analyzed, and revealed to be the Core Impact agent, the infection module of the Core Impact penetration testing tool. The module is reverse engineered, and an analysis of the command and control infrastructure is presented. As some of the infections used the SSL version of the module, it was possible to track the campaign via the server certificates, and this was used to identify more victims of the campaign. Examples of lure documents are also presented. Finally, the custom credential-stealer module that the group uses in addition to commercial tools is discussed. The talk is closed by stipulating that they are not certain of their attribution, but that they are confident that the attack comes from Iran.

Clearsky researched a malware called Gholee, and published a blog post on their research (Clearsky, 2014). The malware was delivered via a macro-enabled Excel file. The analysis concludes that the dropped file is a Core Impact agent, with an entry point named Gholee, the same name as a popular Iranian singer.

Pernet and Lu, from Trend Micro, published a report on operation Woolen-Goldfish (Pernet and Lu, 2015), an operation launched by the group Rocket Kitten. The operation bears a striking resemblance to the attacks described in the Evron and Werner talk. The report starts by discussing the Gholee malware, a modified Core Impact product, distributed via macro-enabled Excel spreadsheets. A brief overview of the victims is then presented, and a list of command and control servers, and an analysis of the domain registrants, is offered. The report mentions an improvement in the tactics used by the attackers, using spear phishing with documents hosted on cloud services, instead of attached directly to the email, and also presents artefacts left in the code and metadata, that points to the Wool3n.h4t identity. Additionally, it expands on the custom keylogger associated with Wool3n.h4t.

Clearsky writes a report on the Thamar Reservoir campaign (Clearsky, 2015). The report describes one attack in great detail to demonstrate the attacker's obstinacy. The attackers started with a spear-phishing email containing a weaponized

Excel document, followed by three emails with links to phishing web-sites, for two-factor authentication, two direct phone calls from the attackers to build a story for a phishing email, numerous attempts to gain control of the account via account recovery, and numerous direct messages via Facebook or email. The report continues by providing statistics for other targets. An analysis of attribution is also presented, mentioning a high degree of similarities with attacks associated with Rocket Kittens, and a medium similarity with techniques used by the Ajax team. A brief overview of the tools used in the attacks, which correspond to Rocket Kitten tools, concludes the report.

Pernet from Trend Micro, and Sela from Clearsky, published another report on Rocket Kitten, covering a new wave of attacks (Pernet and Sela, 2015). The report starts by providing context for the attacks, explaining that the group appears to be targeting specific individuals, rather than companies. The report describes the group's modus operandi, which was similar to the previous attacks. They do note the group's overall sloppiness, that can be observed by multiple mistakes in social engineering attempts, or phishing pages. The report then goes into more details about the use of fake identities to target individuals repeatedly, until they slip, and present a case example. The case showcases a new version of the custom keylogger, and finally provides two fully detailed examples that include the spear phishing, and an analysis of the binaries included. An appendix providing safety tips to guard against the group is also included.

Scott-Railton and Kleemola (2015) from CitizenLab, report on attempts to fish two-factor credentials for Gmail from various victims. In this attack, the attackers attempt to get the victim to divulge their one-time passwords token, to be able to get access while the token is still valid. The publication presents four case studies giving examples of the techniques used, with screen shots of the various lures. The report discusses attribution, by describing the command and control architecture, email headers, and various registrants' entries. They link the attack with Rocket Kitten, based on the use of misspellings in WHOIS records.

Checkpoint also publishes a report on the activities of Rocket Kitten (Checkpoint Software Technologies, 2015a). The report starts with a literature review of the activities of Rocket Kitten to create a timeline of the documented attacks. The report then goes on to cover the tools used by the group, citing in addition to Gholee and CWoolger, numerous publicly available hacking tools such as Acunetix, Metasploit, and SQLmap, and new custom tools such as a .NET version of the custom keylogger, and a custom RAT named MPK. The report covers the command and control infrastructure used. A lucky break occurred when the authors found a misconfigured command and control server that allowed root access, with no authentication, and provides the source for an in-depth look at the attacker's operations, including lists of stolen files, and a series of messages from an experimental messaging app. The phishing templates on the server provide another link to Wool3n.h4t, and an operation database provides the contacts of all the victims, along with the template values for the phishing page, a timestamp, and an operator I.D. This gave the researchers a full view of the campaign. Logs, recording access to phishing web pages by victims, were also found on the server. In addition, through reverse engineering, the authors managed to find a hard-coded password used by the group, and were able to access the interface used to launch operations. A similar technique was used to access the FTP servers designed to hold the data gathered by the keylogger. Of particular note, the data found on the server included the information from the developer's own workstation from the testing phase of the tool. This included the developer (Wool3n.h4t) logging into his own email account, that enabled the researchers to find his real identity, and provide evidence supporting their conclusion, including the individual recording, a video tutorial (which was recorded prior to Rocket Kitten divulgations), in which the working directory includes the name Wool3n.h4t. The report then continues by analyzing the data found on the server to provide statistics on the victim's distribution, the attacker's success rate, the types of victims targeted by each operator, and so on. The report also includes an appendix listing indicators of compromise.

5.2. *Copy Kittens*

Minerva Labs and Clearsky publish a report on the Copy Kittens group (Minerva Labs LTD and ClearSky Cyber Security, 2015). The group starts by spear phishing documents with macro-enabled Office documents, or use right-to-left override tricks. The group's main malware is then dropped. This malware has three stages (dropper, loader, and RAT). The malware sets them apart from other groups in the regions that tend to use a collection of various tools, rather than a single integrated tool chain. However, a number of the tools are built off open-source projects. For example, components in the loader used to detect virtualization artefacts, appear to be based on the Pafish project, and the reflexive DLL injection was also based on an open-source project. Once the DLL is injected into memory, it launches the RAT component, and, as the RAT is launched from memory, it evades anti-virus detection. The report continues with an analysis of the DNS-based command and control, and of the RAT main capabilities, that also appear to have been copied from a number of open-source projects. Appendices end the paper, and include examples of spear-phishing lures, and indicators of compromise.

5.3. *Desert Falcons (a.k.a. Arid Vipers and Advtravel)*

Kaspersky published a report on the Desert Falcons, a group of Arabic origin (Kaspersky Labs, 2015). The report first presents a summary of the victims, and notes that the victims are selected for political or military intelligence. However, a traditional criminal aspect also appears to be a factor. The report then discusses the operations of the group, looking at Infection vectors first. The group appears to favor spear phishing, or social engineering via social media, as a method to deliver malware. The report notes the high quality of the crafted emails and messages that could include technical tricks, such as the right-to-left override trick. An overview of the main tools of the group, their main dropper, and the DHS series of malware, are presented next. Of particular note, the group's toolkit also includes mobile malware. The last component of operations

covered is the command and control architecture, that includes the directory structure of the command and control servers, as one server was found to be misconfigured, to allow access. Finally, the report closes on attribution notes, associating the group with individuals from Egypt, Palestine, and Turkey, and present artefacts from the code to support the conclusions, as well as discussing how access to the command and control server allowed the researchers to learn the identities of some of the attackers. Indicators of compromise are listed in an appendix.

Trend Micro wrote a report on Operation Arid Viper (Trend Micro Threat Research Team, 2015). The publication commences by providing a summary of the victims targeted in the operation, and then goes on to give details on the attacks. First, the victims are sent a spear-phishing email containing a malicious compressed file. This extracts to a .SCR file that installs the main malware component, and launches pornographic video content. Various artefacts left by the malware, and a description of the command and control protocol and infrastructure, are provided next. The report then goes on to cover Operation Advtravel that was found while investigating Arid Viper. They hypothesize that both operations are operated by the same group, even if the malware used was different, as they share command and control infrastructure, and appear to have a Gaza Strip nexus. The Advtravel command and control was also mentioned in the Kaspersky report on Desert Falcons. A poorly secured server allowed the researchers to access the command and control infrastructure, and this allowed them access to the attackers' files. They use the information to provide a timeline of the operation, and an analysis of a large percentage of the files present on the server. The files include a large portion of the attacker's toolset, and details on the files stolen from the victims. Of note, while there appeared to be files stolen from victims' cell phones, the malware used to infect the phones was not found in the toolset. The report then goes on to expose the personal identities of a number of group members, that includes numerous photos and posts from their social media profiles. An appendix describes the indicators of compromise.

Trend Micro also published a blog post summarizing the main findings related to advtravel (TrendMicro, 2015). In the post, they mention that, since the publication of the report, the various individuals exposed had modified, or deleted, their social media profiles.

5.4. *Volatile Cedar*

Checkpoint Software investigated the Volatile Cedar campaign (Checkpoint Software Technologies, 2015b). Their report starts with an overview of the group's modus operandi. The group appears to favor performing vulnerability scans of public facing servers, and, once vulnerabilities are found, a web shell is pushed onto the server and the Explosive malware, the main tool used by the group, is installed on the server. An attack timeline is presented next, followed by the main tactics used by the group, in terms of stealth, but also in terms of command and control, and how they expand their access in the network. The report then presents some of the hints used for attribution, hypothesizing that the group operates from Lebanon. A complete analysis of the Explosive tool, that includes an analysis of the configuration files, the command and control protocols, and the updater methods, was conducted. Appendices covering other versions of the Explosive malware, the USB-infection module, and indicators of compromise, round out the report.

5.5. *Molerats (a.k.a. Gaza gang a.k.a. Gaza Hackers Team a.k.a. DustySky)*

Fagerland first exposed cyber attacks against Israeli and Palestinian targets in a 2012 report (Fagerland, 2012). The report describes a group sending off-the-shelf RATs (in particular Xtreme RAT) in self-extracting archives, via spear phishing. The report includes examples of lures, and the fake code-signing certificate used to sign the malware. The report analyzes the command and control infrastructure used by the attackers, and how the researcher was able to track more infection cases connected to these servers. The report then notes that Palestinians have been targeted, and show a number of lures aimed at Palestinian targets.

In 2013, Villeneuve, Haq, and Moran, investigate another series of attack from the same group (Villeneuve et al., 2013). The attacks, described as self-extracting archives delivered via spear phishing, contained the Poison Ivy off-the-shelf RAT. The blog post presents lure examples, as well as an analysis of the command and control infrastructure. Dhams reports on another wave of attacks in 2014 (Dahms, 2014). This time, the attackers returned to the Xtreme RAT payload, but use essentially the same tactics for delivery. More examples of lures and fake code-signing certificates are shown. A new wave of attacks is reported in late 2016 by Pwc (Parys, 2016), Vectra (Doman, 2016) and Palo Alto Networks (Kasza and Idrizovic, 2016). PwC provides indicators for the campaign, and Vectra studies the victimization, and provides examples of lure documents. Finally, Palo Alto Networks provides a detailed reverse engineering analysis of the malware and its builder.

Clearsky published a report on operation DustySky (Clearsky – Cyber security, 2016), an operation performed by the group in early 2016. The report starts by describing the same modus operandi for infection, i.e., spear phishing using lures extracted from headlines. However, they also mention that, if the victim is not using a Windows machine, the victims are then redirected with a fake login page designed to harvest credentials. The attackers also resorted to creating fake websites for software companies, and distributed their malware bundled with the original software. The researchers then report on some of the actions that were performed by the attackers, post exploitation, focusing on the type of information stolen. The report goes on to describe the DustySky malware, that comprises the dropper, the core element, and the keylogger. The dropper first validates that the machine is not a virtual machine, and then loads the core component, and ensures persistence, if it is not the case. The core component handles the communications and orchestration of received commands. Afterwards, the command and control protocol, and infrastructure, are analyzed in more detail. The report ends by providing evidence to attribute this particular series of campaign to the Molerats group. Examples of lures and indicators of compromise are provided in an appendix.

6. Southeast Asia

This section covers a number of groups operating in the Southeast Asia region.

6.1. *Transparent tribe*

Huss, from Proofpoint, writes a report on targeted attacks against Indian diplomatic and military sources (Huss, 2016). The attacks come as spear-phishing emails that include a crafted RTF document, exploiting a known vulnerability. The exploit downloads a first stage dropper that then downloads a full-featured RAT. The report continues by providing examples of lure news stories, hosted on a website controlled by the attackers, and of lure documents. The report provides a cluster analysis to link the attack with similar attacks, presumably from the same group, providing even more examples of lures and decoys for four clusters. However, the authors conclude that, while the information is not sufficient to make a claim, the four clusters are probably related, as they share numerous operational characteristics. An in-depth analysis of some of the main tools used by the group is provided, and an appendix containing indicators finishes the report.

Chang and Singh, from FireEye, published a blog post covering the same group (Chang and Singh, 2016). The post starts by providing context for the attacks by the group, attributing them more clearly to an APT group from Pakistan. In contrast to the Proofpoint report, the blog post focuses primarily on a technical analysis of the exploit used in the campaign. However, the publication still provides background information of the malware delivery method.

6.2. *Unnamed group operating in Southeast Asia*

Boutin from ESET reports on a group targeting mainly Pakistani targets (Boutin, 2013). The blog post starts with a timeline of the malware samples used by this group that can be established authoritatively because of the use of a code signing certificate. The attack uses two main vectors: a vulnerability in Microsoft Office, or executable files disguised as PDF or Office documents. The post also presents examples of decoy documents, and lists the various additional payloads that are loaded by the attackers on victims' machines. They also note the peculiarity of not using encryption to exfiltrate data, allowing the data to be seen as clear text in the network traffic. The relative simplicity of the technique used for persistence, registering in the start menu with a fake name, is also noted. A brief note on the command and control infrastructure, gleaned from strings present in the malware samples, is also included. Finally, notes on the possible Indian origin, and statistics on the victims are presented.

6.3. *Lotus Blossom (a.k.a. Spring Dragon)*

Falcone et al. from Palo Alto Networks, present a report on operation Lotus Blossom (Falcone et al., 2015), built around the Elise backdoor, that focused on government and military victims in Southeast Asia, in particular Vietnam and the Philippines. The report starts by providing an overview of each attack wave, describing what types of lures were used for spear phishing, the command and control infrastructure used, and the campaign codes for the attack. The report continues with an analysis of the Elise backdoor, that provides standard RAT capabilities, enabling custom configuration via an encrypted file, manages command and control communication, performs basic reconnaissance, and executes command and read/write files. Three variants of the backdoor are covered. The slight differences between each variant (for example a different machine fingerprinting script, or a different data structure) are described. The report is concluded by referencing other publications involving this group. Indicators of compromise are also provided in an appendix.

Baumgartner, from Kaspersky, expands on the Palo Alto publication (Baumgartner, 2015). The publication focuses on exposing other intrusion techniques that are part of the group's arsenal. It points to an example where a website from Myanmar was compromised to distribute a malware installer, instead of the font required to view the content. Use of a wider variety of exploits than the one mentioned in other publications, is also noted. Finally, an attack where a fake Adobe Flash installation web page was loaded, with an installer bundled with the Elise backdoor, is documented. The post is concluded by pointing out that the Lotus Blossom attackers, that Kaspersky calls Spring Dragon, are more creative than what other publications would lead one to believe.

6.4. *Silent Chollima (a.k.a. Lazarus group)*

This is an attack group associated with North Korea that participated in a number of high-profile compromises.

Sherstobitoff, Liba, and James from McAfee Labs, published a report on operation Troy, more commonly known as DarkSeoul (Sherstobitoff et al., 2013). While DarkSeoul made the news, mainly due to the use of wiper software that caused disruption in South Korea, the report concludes that this was only the tail-end of a long-term espionage operation. The report starts by providing a timeline for the event, and by reporting the claims from a group called the New Romanic Cyber army, who declared themselves be responsible for the attack. The publication continues with an analysis of the malware used in the attack. The dropper and the master boot record wiper components are thoroughly analyzed, and more emphasis is put on the RAT involved in the attack. The report links the MBR wiper campaign to other malware campaigns focused on espionage in South Korea, based on reverse-engineered artefacts. The report concludes that the different malwares were, in fact, part of a single encrypted network used to exfiltrate secret and confidential information. An extensive study of this network, and on the types of documents the spying software was looking for, is provided next. Links between the different malware campaigns are restated to conclude the paper. While this particular report did not specifically consider attribution to North Korea, this wave of attacks is attributed to North Korean state actors by the operation Blockbuster joint investigation.

Tarakanov from Kaspersky covers the Kimsuky operation (Tarakanov, 2013). The operation targets a number of South Korean defense and unification groups. The malware is delivered via spear phishing, and comprises a DLL acting as a loader for further malware. The report lists the spying modules

available, and other capabilities. Notably, the author comments on the ability of the malware to stop firewall services. However, this capability only targets a brand of firewall used almost exclusively in South Korea. The lack of capability to stop firewalls with a larger market share is taken as a sign of a limited scope of operations. The communications and data exfiltration capabilities are covered next, and other spying modules, including a keylogger, a directory listing tool, a tool to steal documents from a Korean language processor, and a set of tools to enable direct remote access, are described. A brief analysis of attribution information from the domain registry and source IP address conclude the report, and provide some attribution, with very limited confidence, to North Korea. Indicators of compromise are also listed in an appendix.

The attack on the Sony Pictures is the most publicized campaign of the group. An ultimatum was sent by a group called "The Guardians of Peace" (GOP) to the Sony Pictures company, stating that a group was in the possession of confidential documents. The documents would be released unless the release of a satirical movie about a group sent to assassinate the North Korean leader, was cancelled. Sony Pictures did not comply with the ultimatum and a series of confidential documents were leaked, including unreleased movies, internal emails, credentials to internal and external services, and confidential employee information. This demonstrated the complete compromise of the company's networks. The daily leaks and back and forth communication with the GOP continued, until the GOP promised to bomb theaters showing the movie. This led multiple cinemas to cancel scheduled screenings that, in turn, led to the cancellation of the release by Sony Pictures. RBS provides a timeline of the events in their breakdown and analysis of the attack (RiskBased Security, 2014). The breakdown includes the communications between the attackers, the company, and the authorities, as well as involvement from third parties that muddied the waters further. The attack was later categorically linked to North Korea by the FBI (FBI National Press Office, 2014). However, their report cites secret sources to provide this attribution. It does note, however, that malware and command and control infrastructure used by North Korean hackers, in particular in operation Dark Seoul, was used in the Sony Picture attack.

In February 2016, Novetta led a coalition of multiple security industry companies to divulge information about the group. Blasco from AlienVault (Blasco, 2016), Kochetkova from Kaspersky (Kochetkova, 2016), and Raiu and Guerrerro-Saade from Kaspersky (Raiu et al., 2016), published posts in relation to the mass divulgation. Kochetkova presents a summary of the information that was previously published about the group, linking the group to Operation Troy, the Sony Picture hacks, and numerous other known brands of malware, such as Hangman and Wild Positron. She also provides statistics about the malware related to the group, to show the increase in terms of activity. Raiu and Guerrerro-Saade report on the technical indicators that led to the clustering of the activities of the group. They cover a number of technical details demonstrating a shared ancestry, including network functionality, self-deleting scripts, anti-analysis techniques, and sandbox detection. They provide malware and victims statistics that could be used for attribution, which is left to the reader. Blasco shares other indicators used to link the group. He focuses on shared encryption keys, batch scripts, obfuscation functions, network communication, Hangul word Processor exploits, and backdoored software.

6.5. *Operation Dust Storm*

Gross, from Cylance, publishes a report on operation DustStorm (Gross and C. S. team, 2016). The report starts by providing a history of previous attacks, including the types of exploits used, and the command and control infrastructure for each attack. It notes adaptability on the part of the attackers that started with spear-phishing attacks, but moved to watering holes as the group got access to 0-day exploits. The report then notes that the targeting focus changed in 2013, to Japanese critical infrastructure. In fact, the report notes that the attackers may check for the keyboard settings of the victim, to ensure that it is set to Japanese keyboards, and then produces a series of analyses and indicators for the tools used by the group, which are mostly backdoors and RAT, available on the underground.

6.6. *Platinum*

The Windows Defender threat-hunting team produced a report on a series of attacks in Southeast Asia, from a group called Platinum (Windows Defender Advanced Threat Hunting Team, 2016). The report starts with a threat profile for the group that indicates a high level of sophistication with the use of numerous 0-days, a full custom tool set, and good operational security. Next, the report goes into more detail of the group's method of attacks, mainly spear phishing, including documents exploiting vulnerabilities, often 0-day. Care is taken to ensure that only the intended victim gets the final payload. The report shows the attackers invest significantly in reconnaissance, often targeting victims at their personal address, and carefully crafting topical lures for spear phishing. The report goes on to cover a number of examples of how the group compromises networks, listing the specific vulnerabilities used in each case, and then discusses the tool set of the group, providing an overview of the capabilities of each tool. Among the custom backdoors and keyloggers, the group also uses an unusual tool to perform hot patching, and a port knocking back door. The report provides a bit more technical detail of how the particular tool functions as this is a rare capability. The report goes into more detail of one of the recent (at the time of writing) vulnerabilities of the group, and then discusses information that could be used for attribution, but is mostly inconclusive. Finally, the report provides defensive guidance, and indicators of compromise.

7. Actors with uncertain attribution

A number of other actors are involved in espionage, but have not been confidently attributed to a specific nation state.

7.1. *Red October*

The Red October actor is engaged in espionage of targets which would be consistent with Russian interests, however, as the

authors of the publication do not specifically comment on attribution, we have included this group in this section.

Kaspersky published a series of report on the group they call Red October. The first report (Global Research and Analysis Team, 2013a) covers the investigation on diplomatic cyber attacks against victims in Eastern Europe, former USSR members, and Central Asia. The report provides an overview of the attacks that start with an Office document containing exploits, that the authors hypothesize arrived via spear-phishing emails. The authors note that some of the vulnerabilities used, were copied from a previous targeted attack with Chinese origins. The boobytrapped Office document contains a dropper that installs the main backdoor payload. The authors note that the dropper also includes a line to activate the ability to address files, and directories, containing Cyrillic characters. The publication then discusses the technique used for command and control. The backdoor can function in two modes: offline where files are dropped on the machine, or online where no files are dropped, and everything runs from memory. The publication discusses another method used by the attackers for persistence, using an innocuous document that includes executable code, and special tags. The document can be delivered to a victim where command and control was lost. As the document does not contain active code, it would not be flagged as malicious. However, if the document is opened on a system that has been infected, the backdoor would be able to interpret the special tags, and run the code to re-establish command and control. The publication provides a timeline of the attacks, and statistics of the victims, both from Kaspersky telemetry, and sinkholed domains. An analysis of the command and control infrastructure that functions as a chain of proxies, is also provided.

The second part of the publication (Global Research and Analysis Team, 2013b) covers the technical analysis of the malware modules used in the attack. The report is in the form of Q&A. It starts with a summary of the findings of the previous publication, and, by expanding a bit on the types of victims that are targeted, also mentions that targets in North America and Western Europe were also affected. They comment on attribution, mentioning that the malware modules are of Russian origin, and the exploits appear to have Chinese origins. They also mention that no evidence of nation-state backing is evident, although some of the information stolen appears to be of primarily geopolitical interest. The publication then discusses the main capabilities of the malware, both for tasks that are continually performed by the main component, and for tasks that can be performed on command by uploading extra modules. The continually performed tasks focus on information stealing, providing keylogging, screen captures, and information extraction from email. It also includes capabilities to steal documents from attached USB storage media, and various makes of phones. The malware can also propagate on Windows phones. The on-demand tasks offer the capabilities to fingerprint the machine, extract additional information, such as saved passwords, and expand access on the network. The publication compares the attack with various high-profile targeted attacks, noting that there does not appear to be any connections with these attacks. Finally, the report presents a summary of the information on the command and control infrastructure that was presented in the first report.

7.2. *Careto (a.k.a. the Mask)*

The Careto group was the object of a detailed report from Kaspersky (Kaspersky labs, 2014). The group was named after strings found in the main component of the malware that is an advanced espionage platform, more advanced than Duqu according to the authors. The report starts with a description of the attack that starts with spear-phishing emails sent to exploit websites. The exploited website then redirects the victim to a sub domain, which simulates news sites. The malware is digitally signed to avoid detection. The report goes on to analyze the backdoor components, and mentions that the Careto malware leverages three separate backdoors. The report also mentions a rootkit, bootkit, 32-bit Windows, 64-bit Windows, and Mac OS X version for which the authors have samples, and MacOS and iPad versions for which they did not find samples. The report goes on to list all the types of information that can be stolen by the malware, and discusses the SGH backdoor, that is the advanced kernel-mode backdoor. The report continues by presenting numerous artefacts left by the Careto backdoor, and the numerous add-on modules, and reports on the list of commands implemented. The commands show the capability of the malware to load additional capabilities from remotely downloaded modules. A similar analysis is presented for the more advanced SGH backdoor, and the SBD and OSX SBD backdoors. The analysis is continued by looking at the command and control communications and infrastructure. This analysis benefits from direct access to a command and control server that was obtained from incident response. Of note, the report provides a list of IP addresses that belonged to security researchers that were blacklisted. The report then discusses the exploits that were found on the server, and presents an analysis of the victims, and speculations on possible attribution. While the report notes a large number of Spanish language artefacts in the malware, they do not attribute it to a specific actor. An appendix providing indicators of compromise, and detailed technical analysis of some of the components, is also included in the report.

McAfee also reports on the malware cluster associated with the group (McAfee Labs, 2014). This publication presents a more in-depth technical analysis of the malware in the Careto cluster found in the McAfee database. As such, the report is intended more for an audience interested in reverse engineering, than for general consumption.

8. Conclusion

While the number of academic publications covering the topic of APT actors is fairly low, the industry has provided a host of information regarding these attacks. The sheer volume of publications shows, not only the interest in the topic, but also the magnitude of the problem. Furthermore, there is evidence of a proliferation of capabilities as new actors, such as India and Pakistan, join the ranks of the Western powers, China, and Russia, in the field of computer-based espionage. This implies that the threat is likely to expand, and that more attention should be focused on this problem in the research space.

Even the more established actors show signs of adaptability and improvement. We have seen numerous examples of

actors retooling after a divulgation, or just improving their tool chain as time passes. As such, unless significant improvements to defensive technologies are found, the challenges of fighting off APT attacks is likely to become harder and harder. Future research in defensive solutions to combat APT threats would be well advised to study current capabilities and study the history of capability development to ensure the long-term value of the solution.

Furthermore, significant gaps still exist in our knowledge of APT threats. As evidenced by the literature, for most advanced actors, the initial vector of compromise is often unknown. Similarly, a number of groups are proficient at hiding their traces, making the investigation of past cases, and the generation of future knowledge about their activities difficult. In that sense, investigating methods to cover these knowledge gaps appear to be worthwhile research paths.

Acknowledgments

This research was funded by the Canadian Center for Security Science (CSS) as part of the Canadian Safety and Security Program (CSSP).

REFERENCES

Alperovitch D. Revealed: operation shady RAT; 2011. [Online]. Available from: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf. [Accessed 11 January 2017].

Alperovitch D. Deep in thought: Chinese targeting of National Security Think Tanks. Crowdstrike, 7 July 2014a. [Online]. Available from: https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/. [Accessed 11 January 2017].

Alperovitch D. CrowdStrike discovers use of 64-bit zero-day privilege escalation exploit (CVE-2014-4113) by Hurricane Panda. Crowdstrike, 14 October 2014b. [Online]. Available from: https://www.crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/. [Accessed 11 January 2017].

Alperovitch D. Cyber deterrence in action? A story of one long HURRICANE PANDA campaign. Crowdstrike, 13 April 2015. [Online]. Available from: https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/. [Accessed 11 January 2017].

Alperovitch D. Bears in the midst: Intrusion into the Democratic National Committee. Crowdstrike, 15 June 2016. [Online]. Available from: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. [Accessed 12 January 2017].

ASERT Threat Intelligence. Arbor threat intelligence brief 2014-07 - illuminating the etumbot APT backdoor. June 2014. [Online]. Available from: https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf. [Accessed 11 January 2017].

Bailey M. MATRYOSHKA MINING lessons from operation RussianDoll. January 2016. [Online]. Available from: http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.03.09.Operation_RussianDoll/wp-mandiant-matryoshka-mining.pdf. [Accessed 12 January 2017].

Barnes JE. Pentagon computer networks attacked. Los Angeles Times, 28 November 2008. [Online]. Available from: http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28. [Accessed 31 January 2017].

Bartholomew B. KopiLuwak: a new JavaScript payload from Turla. Kaspersky, 2 February 2017. [Online]. Available from: https://securelist.com/blog/research/77429/kopiluwak-a-new-javascript-payload-from-turla/. [Accessed 2 February 2017].

Baumgartner K. The Spring Dragon APT. Kaspersky Labs, 17 June 2015. [Online]. Available from: https://securelist.com/blog/research/70726/the-spring-dragon-apt/. [Accessed 11 January 2017].

Baumgartner K, Golovkin M. The Naikon APT. Kaspersky, 14 May 2015a. [Online]. Available from: https://securelist.com/analysis/publications/69953/the-naikon-apt/. [Accessed 4 February 2017].

Baumgartner K, Golovkin M. The MsnMM campaigns – the earliest Naikon APT campaigns. May 2015b. [Online]. Available from: https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf. [Accessed 11 January 2017].

BAE Systems Apllied Intelligence. SNAKE CAMPAIGN. CYBER ESPIONAGE TOOLKIT; 2014. [Online]. Available from: http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/snake_whitepaper.pdf. [Accessed 12 January 2017].

Bitdefender. APT28 under the scope a journey into exfiltrating intelligence and government information. December 2015. [Online]. Available from: https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf. [Accessed 12 January 2017].

Blasco J. Operation BlockBuster unveils the actors behind the Sony attacks. Alien Vault, 24 February 2016. [Online]. Available from: https://www.alienvault.com/blogs/labs-research/operation-blockbuster-unveils-the-actors-behind-the-sony-attacks. [Accessed 11 January 2017].

Boutin J-I. Targeted information stealing attacks in South Asia use email, signed binaries. ESET, 16 May 2013. [Online]. Available from: http://www.welivesecurity.com/2013/05/16/targeted-threat-pakistan-india/. [Accessed 11 January 2017].

Brod. Beware BlackEnergy if involved in Europe/Ukraine diplomacy. F-Secure, 30 June 2014. [Online]. Available from: https://www.f-secure.com/weblog/archives/00002721.html. [Accessed 27 January 2017].

Bronk C, Tikk-Ringas E. Hack or attack? Shamoon and the evolution of cyber conflict. Survival, Global Politics and Strategy, March 2013.

Calvet J. Sednit Espionage Group attacking air-gapped networks. ESET, 11 November 2014. [Online]. Available from: http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/. [Accessed 12 January 2017].

Calvet J. The Sednit Group: "Cyber" espionage in Eastern Europe. In NorthSec, Montreal; 2015a.

Calvet J. Casper malware: after Babar and Bunny, another espionage cartoon. ESET, 5 March 2015b. [Online]. Available from: http://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/. [Accessed 11 January 2017].

Calvet J. Dino – the latest spying malware from an allegedly French espionage group analyzed. ESET, 30 June 2015c. [Online]. Available from: http://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/. [Accessed 11 January 2017].

Calvet J, Campos J, Dupuy T. Visiting the bear den a journey in the land of (Cyber-)espionage. In RECon, Montreal; 2016.

Chang YH, Singh S. APT group sends spear phishing emails to Indian Government Officials. FireEye, 3 June 2016. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html. [Accessed 11 January 2017].

Chang Z, Lu K, Luo A, Pernet C, Yaneza J. Operation iron tiger: exploring Chinese cyber-espionage attacks on United States defense contractors; 2015. [Online]. Available from: https://www.erai.com/CustomUploads/ca/wp/2015_12_wp_operation_iron_tiger.pdf. [Accessed 11 January 2017].

Checkpoint Software Technologies. Rocket Kitten: a campaign with 9 lives; 2015a. [Online]. Available from: http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf. [Accessed 11 January 2017].

Checkpoint Software Technologies. Volatile cedar. 30 March 2015b. [Online]. Available from: https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf. [Accessed 11 January 2017].

Chen X, Scott M, Caselden D. New zero-day exploit targeting internet explorer versions 9 through 11 identified in targeted attacks. FireEye, 26 April 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html. [Accessed 11 January 2017].

Cherepanov A. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. ESET, 3 January 2016. [Online]. Available from: http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/. [Accessed 12 January 2017].

Clearsky. Gholee – a "protective edge" themed spear phishing campaign. Clearsky, 4 September 2014. [Online]. Available from: http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/. [Accessed 1 February 2017].

Clearsky. Thamar Reservoir An Iranian cyber-attack campaign against targets in the Middle east. June 2015. [Online]. Available from: http://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf. [Accessed 2 February 2017].

Clearsky – Cyber security. Operation DustySky. January 2016. [Online]. Available from: http://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf. [Accessed 11 January 2017].

Cluley G. New ESET research paper puts Sednit under the microscope. ESET, October 2016. [Online]. Available from: http://www.welivesecurity.com/2016/10/20/new-eset-research-paper-puts-sednit-under-the-microscope/. [Accessed 12 January 2017].

Coogan P. Targeted attacks make WinHelp files not so helpful. Symantec, 15 October 2012. [Online]. Available from: https://www.symantec.com/connect/blogs/targeted-attacks-make-winhelp-files-not-so-helpful. [Accessed 11 January 2017].

Creus D, Halfpop T, Falcone R. Sofacy's 'Komplex' OS X Trojan. PaloAlto Networks, 26 September 2016. [Online]. Available from: http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/. [Accessed 12 January 2017].

Crowdstrike Global Intelligence Team. CrowdStrike intelligence report – Putter Panda; 2014. [Online]. Available from: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf. [Accessed 11 January 2017].

Crowdstrike Global Intelligence Team. Use of Fancy BearAndroid malware in tracking of Ukrainian field artillery unit. 22 December 2016. [Online]. Available from: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf. [Accessed 27 January 2017].

Cutler S. Threat analysis – The Mirage Campaign. Dell SecureWorks, 18 September 2012. [Online]. Available from: https://www.secureworks.com/research/the-mirage-campaign. [Accessed 11 January 2017].

Cylance. #OPCLEAVER; 2014. [Online]. Available from: https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf. [Accessed 11 January 2017].

Dahl M. The French connection: French aerospace-focused CVE-2014-0322 attack shares similarities with 2012 capstone turbine activity. Crowdstrike, 25 February 2014a. [Online]. Available from: https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/. [Accessed 11 January 2017].

Dahl M. Cat scratch fever: CrowdStrike tracks newly reported Iranian actor as FLYING KITTEN. Crowdstrike, 13 May 2014b. [Online]. Available from: https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/. [Accessed 11 January 2017].

Dahms T. Molerats, Here for Spring! FireEye, 2 June 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html. [Accessed 11 January 2017].

Daly MK. The advanced persistent threat (or informationized force operations). In 23rd Large Installation System Administration Conference (LISA), Baltimore; 2009.

Dell SecureWorks Counter Threat Unit™ Threat Intelligence. Threat analysis – threat group 3390 cyberespionage. Dell SecureWorks, 5 August 2015. [Online]. Available from: https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage?_ga=1.132970126.1294297346.1479934134. [Accessed 11 January 2017].

Dennesen K. Hide and Seek: How Threat Actors Respond in the Face of Public Exposure. In RSA Conference, San Francisco; 2016.

Dereszowski A. Turla – development & operations. In FIRST, Tbilisi; 2014.

Dereszowski A. Andrzej Dereszowski – Turla: Development & Operations [Rooted CON 2015 - ENG]. Spain, 2015.

DiMaggio J. The Black Vine cyberespionage group. 6 August 2016. [Online]. Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf. [Accessed 11 January 2017].

Doherty S, Gegeny J, Spasojevic B, Baltazar J. Hidden lynx – professional hackers for hire. 17 September 2013. [Online]. Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf. [Accessed 11 January 2017].

Doman C. Moonlight – targeted attacks in the Middle East. Vectra, 26 October 2016. [Online]. Available from: https://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks. [Accessed 3 February 2017].

Ducklin P. The "Sandworm" malware – what you need to know. Sophos, 15 October 2014. [Online]. Available from: https://nakedsecurity.sophos.com/2014/10/15/the-sandworm-malware-what-you-need-to-know/. [Accessed 12 January 2017].

Eng E, Caselden D. Operation Clandestine wolf – adobe flash zero-day in APT3 phishing campaign. FireEye, 23 June 2015. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html. [Accessed 11 January 2017].

ESET Research. Sednit espionage group now using custom exploit kit. ESET, 8 October 2014a. [Online]. Available from: http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/. [Accessed 27 January 2017].

ESET Research. Miniduke still duking it out. ESET, 20 May 2014b. [Online]. Available from: http://www.welivesecurity.com/2014/05/20/miniduke-still-duking/. [Accessed 30 January 2017].

Evron G, Werner T. Rocket Kitten: advanced off-the-shelf targeted attacks against nation states. In 31c3 Chaos Communication Congress, Hamburg, 2014.
F-Secure labs Security Response. COZYDUKE; 2015. [Online]. Available from: https://www.f-secure.com/documents/996508/1030745/CozyDuke. [Accessed 11 January 2017].
F-Secure Labs Security Response. BLACKENERGY & QUEDAGH; 2014a. [Online]. Available from: https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf. [Accessed 27 January 2017].
F-Secure Labs Security Response. COSMICDUKE – Cosmu with a twist of MiniDuke; 2014b. [Online]. Available from: https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf. [Accessed 11 January 2017].
F-Secure Labs Threat Intelligence. THE DUKES - 7 years of Russian cyberespionage. September 2015. [Online]. Available from: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf. [Accessed 12 January 2017].
Fagerland S. Systematic cyber attacks against Israeli and Palestinian targets going on for a year. November 2012. [Online]. Available from: http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf. [Accessed 11 January 2017].
Falcone R, Lee B. New sofacy attacks against US government agency. PaloAlto Networks, 14 June 2016. [Online]. Available from: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/unit42-operation-lotus-blossom. [Accessed 12 January 2017].
Falcone R, Grunzweig J, Miller-Osborn J, Olson R. Operation lotus blossom; 2015. [Online]. Available from: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/unit42-operation-lotus-blossomath%3D%2Fcontent%2Fpan%2Fen_US%2Fresource. [Accessed 11 January 2017].
Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier version 1.4. Symantec Security Response; 2011.
FBI National Press Office. Update on Sony investigation. United States Government, 19 December 2014. [Online]. Available from: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. [Accessed 11 January 2017].
Federal Bureau of Investigations. FBI liaison alert system #A-000049-MW. February 2015. [Online]. Available from: http://krebsonsecurity.com/wp-content/uploads/2015/02/FBI-Flash-Warning-Deep-Panda.pdf. [Accessed 11 January 2017].
Fire Eye Threat Intelligence. HAMMERTOSS: stealthy tactics define a Russian cyber threat group. July 2015. [Online]. Available from: https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf. [Accessed 12 January 2017].
FireEye. APT28: a window Inot Russia's Cyber espionage operations? FireEye, October 2014. [Online]. Available from: http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf. [Accessed 12 January 2017].
FireEye Labs / FireEye Threat Intelligence. Hiding in plain sight: FireEye and Microsoft expose obfuscation tactic. FireEye, Milpitas, CA; 2015a.
FireEye Labs / FireEye Threat Intelligence. APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION – how a cyber threat group exploited governments and commercial entities across Southeast Asia and India for over a decade. FireEye; 2015b.
FireEye Threat Intelligence. PINPOINTING TARGETS: exploiting web analytics to Ensnare victims. November 2015. [Online]. Available from: https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf. [Accessed 12 January 2017].
Fisher D. Energy watering hole attack used lightsout exploit kit. Threatpost, 13 March 2014. [Online]. Available from: https://threatpost.com/energy-watering-hole-attack-used-lightsout-exploit-kit/104772/. [Accessed 11 January 2017].
Gallagher S. Iranians hacked Navy network for four months? Not a surprise. Ars Technica, 19 February 2014. [Online]. Available from: https://arstechnica.com/information-technology/2014/02/iranians-hacked-navy-network-for-4-months-not-a-surprise/. [Accessed 2 February 2017].
GData. Uroburos highly complex espionage software with Russian roots. February 2014. [Online]. Available from: https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf. [Accessed 12 January 2017].
Global Research & Analysis Team. miniFlame aka SPE: "Elvis and his friends". Kaspersky, 15 October 2012. [Online]. Available from: https://securelist.com/analysis/publications/68560/miniflame-aka-spe-elvis-and-his-friends/. [Accessed 1 February 2017].
Global Research and Analysis Team. The NetTraveler (aka 'Travnet'). April 2011. [Online]. Available from: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf. [Accessed 11 January 2017].
Global Research and Analysis Team. "Red October" diplomatic cyber attacks investigation. Kaspersky, 14 January 2013a. [Online]. Available from: https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/. [Accessed 4 February 2017].
Global Research and Analysis Team. The "Red October" campaign – an advanced cyber espionage network targeting diplomatic and government agencies. Kaspersky, 14 January 2013b. [Online]. Available from: https://securelist.com/blog/incidents/57647/the-red-october-campaign/. [Accessed 4 February 2017].
Global Research and Analysis Team Kasperky Labs. The PROJECTSAURON APT. 9 August 2016. [Online]. Available from: https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf. [Accessed 11 January 2017].
Goodin D. How "omnipotent" hackers tied to NSA hid for 14 years – and were found at last. Ars Technica, 16 February 2015. [Online]. Available from: https://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/. [Accessed 1 February 2017].
Gostev A. The Flame: questions and answers. Kaspersky, 28 May 2012a. [Online]. Available from: https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/. [Accessed 1 February 2017].
Gostev A. Flame: bunny, frog, munch and beetlejuice. Kaspersky, 30 May 2012b. [Online]. Available from: https://securelist.com/blog/incidents/32855/flame-bunny-frog-munch-and-beetlejuice-2/. [Accessed 1 February 2017].
Gostev A. 'Gadget' in the middle: Flame malware spreading vector identified. Kaspersky, 4 June 2012c. [Online]. Available from: https://securelist.com/blog/incidents/33081/gadget-in-the-middle-flame-malware-spreading-vector-identified-22/. [Accessed 1 February 2017].
Gostev A. Back to Stuxnet: the missing link. Kaspersky, 11 June 2012d. [Online]. Available from: https://securelist.com/blog/incidents/33174/back-to-stuxnet-the-missing-link-64/. [Accessed 1 February 2017].
Gostev A. The roof is on fire: tackling flame's C&C servers. Kaspersky, 4 June 2012e. [Online]. Available from: https://securelist.com/blog/incidents/33033/the-roof-is-on-fire-tackling-flames-cc-servers-6/. [Accessed 1 February 2017].
Gostev A, Soumenkov I. Stuxnet/Duqu: the evolution of drivers. Kaspersky, 28 December 2011. [Online]. Available from:

https://securelist.com/analysis/publications/36462/stuxnetduqu-the-evolution-of-drivers/. [Accessed 1 February 2017].
GovCERT.ch. APT case RUAG technical report. 23 May 2016. [Online]. Available from: https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf. [Accessed 12 January 2017].
Gross J, C. S. team. Operation dust storm. February 2016. [Online]. Available from: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.02.23.Operation_Dust_Storm/Op_Dust_Storm_Report.pdf. [Accessed 11 January 2017].
Gross J, Walter J. Puttering into the Future… Cylance, 12 January 2016. [Online]. Available from: https://blog.cylance.com/puttering-into-the-future. [Accessed 24 January 2017].
Grunzweig J. Unit 42 technical analysis: Seaduke. PaloAlto Networks, 14 July 2015. [Online]. Available from: http://researchcenter.paloaltonetworks.com/2015/07/unit-42-technical-analysis-seaduke/. [Accessed 12 January 2017].
Hentunen D, Tikkanen A. Havex hunts for ICS/SCADA systems. F-Secure Labs, 23 June 2014. [Online]. Available from: https://www.f-secure.com/weblog/archives/00002718.html. [Accessed 11 January 2017].
Hern A. Ukrainian blackout caused by hackers that attacked media company, researchers say. The Guardian, 7 January 2016. [Online]. Available from: http://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company. [Accessed 21 January 2016].
Hjelmvik E. Full disclosure of Havex Trojans. NetResSec, 27 October 2014. [Online]. Available from: http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans. [Accessed 11 January 2017].
Hoglund G. Inside an APT covert communications channel. Fast Horizon, 16 August 2011. [Online]. Available from: http://fasthorizon.blogspot.ca/2011/08/inside-apt-comment-crew-covert.html. [Accessed 11 January 2017].
Huss D. Operation transparent tribe. March 2016. [Online]. Available from: https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf. [Accessed 11 January 2017].
Jiang G, Caselden D, Winters R. The EPS awakens. FireEye Threat Research, 16 December 2015. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html. [Accessed 11 January 2017].
Karspersky Labs. The Duqu 2.0 technical details. 11 June 2015. [Online]. Available from: https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf. [Accessed 11 January 2017].
Kaspersky labs. Unveiling “Careto” - the masked APT. February 2014. [Online]. Available from: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf. [Accessed 11 January 2017].
Kaspersky labs. Equation group: questions and answers. February 2015. [Online]. Available from: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf. [Accessed 11 January 2017].
Kaspersky Lab. The regin platform – Nation-State Ownage of GSM Networks. 24 November 2014. [Online]. Available from: https://cdn.securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf. [Accessed 11 January 2017].
Kaspersky Lab Global Research and Analysis. Gauss: abnormal distribution. June 2012. [Online]. Available from: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf. [Accessed 1 January 2017].
Kaspersky Lab Global Research and Analysis Team. Energetic bear – crouching yeti. July 2014. [Online]. Available from: https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf. [Accessed 12 January 2017].
Kaspersky Labs. The desert falcons targeted attacks. February 2015. [Online]. Available from: https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf. [Accessed 11 January 2017].
Kaspersky Lab’s Global Research & Analysis Team. Full analysis of flame’s command & control servers. Kaspersky, 17 September 2012. [Online]. Available from: https://securelist.com/blog/incidents/34216/full-analysis-of-flames-command-control-servers-27/. [Accessed 1 February 2017].
Kaspersky Lab’s Global Research & Analysis Team. The epic turla operation. Kaspersky, 7 August 2014. [Online]. Available from: https://securelist.com/analysis/publications/65545/the-epic-turla-operation/. [Accessed 12 January 2017].
Kaspersky Lab’s Global Research & Analysis Team. Sofacy APT hits high profile targets with updated toolset. Kaspersky, 4 December 2015a. [Online]. Available from: https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/. [Accessed 12 January 2017].
Kaspersky Lab’s Global Research & Analysis Team. Animals in the APT farm. Kaspersky Labs, 6 March 2015b. [Online]. Available from: https://securelist.com/blog/research/69114/animals-in-the-apt-farm/. [Accessed 11 January 2017].
Kaspersky Lab’s Global Research & Analysis Team. CVE-2015-2545: overview of current threats. Kaspersky Labs, 25 May 2016. [Online]. Available from: https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/. [Accessed 11 January 2017].
Kasza A, Idrizovic E. Houdini’s magic reappearance. Palo Alto Networks, 25 October 2016. [Online]. Available from: http://researchcenter.paloaltonetworks.com/2016/10/unit42-houdinis-magic-reappearance/. [Accessed 3 February 2017].
KASPERSKY LAB ZAO. The ‘Icefog’ APT: a tale of cloak and three daggers. September 2013. [Online]. Available from: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/icefog.pdf. [Accessed 11 January 2017].
Kharouni L, Hacquebord F, Huq N, Gogolinski J, Mercês F, Remorin A, et al., Operation pawn storm using decoys to evade detection. October 2014. [Online]. Available from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf. [Accessed 12 January 2017].
Kochetkova K. What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes. Kaspersky Lab, 24 February 2016. [Online]. Available from: https://blog.kaspersky.com/operation-blockbuster/11407/. [Accessed 11 January 2017].
Krebs B. Anthem breach may have started in April 2014. Krebs on Security, 15 February 2015. [Online]. Available from: https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/. [Accessed 11 January 2017].
Krebs B. Russian ‘Dukes’ of hackers pounce on trump win. Krebs On Security, 16 November 2016. [Online]. Available from: https://krebsonsecurity.com/2016/11/russian-dukes-of-hackers-pounce-on-trump-win/. [Accessed 12 January 2017].
Laboratory of Cryptography and System Security (CrySyS Lab). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks v1.05. 31 May 2012. [Online]. Available from: https://www.crysys.hu/skywiper/skywiper.pdf. [Accessed 11 January 2017].
Lancaster T. A tale of pirpi, scanbox & CVE-2015-3113. PwC, 23 July 2015. [Online]. Available from: http://pwc.blogs.com/cyber_security_updates/2015/07/pirpi-scanbox.html. [Accessed 11 January 2017].

Langner R. To kill a centrifuge a technical analysis of what stuxnet's creators tried to achieve. November 2013. [Online]. Available from: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf. [Accessed 11 January 2017].
Lee B, Falcone R. APT group UPS targets US government with hacking team flash exploit. PaloAlto, 10 July 2015. [Online]. Available from: http://researchcenter.paloaltonetworks.com/2015/07/apt-group-ups-targets-us-government-with-hacking-team-flash-exploit/. [Accessed 11 January 2017].
Lee M, Lewis D. Clustering disparate attacks: mapping the activities of the advanced persistent threat. In Virus Bulletin Conference, Barcelona; 2011.
Lelli A. The Trojan. Hydraq incident: analysis of the Aurora 0-day exploit. Symantec, 21 January 2010. [Online]. Available from: https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit. [Accessed 11 January 2017].
Levene B, Falcone R, Wartell R. Tracking MiniDionis: CozyCar's new ride is related to Seaduke. PaloAlto Networks, 14 July 2015. [Online]. Available from: researchcenter.paloaltonetworks.com/2015/07/tracking-minidionis-cozycars-new-ride-is-related-to-seaduke/. [Accessed 12 January 2017].
Li F, Lai A, Ddl D. Evidence of advanced persistent threat:a case study of malware for political espionage. In 2011 6th International Conference on Malicious and Unwanted Software, Farjado, Porto Rico; 2011.
Lipovsky R. CVE-2014-4114: details on August BlackEnergy PowerPoint campaigns. ESET, 14 October 2014a. [Online]. Available from: http://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/. [Accessed 27 january 2017].
Lipovsky R. Back in BlackEnergy *: 2014 targeted attacks in Ukraine and Poland. ESET, 22 September 2014b. [Online]. Available from: http://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/. [Accessed 27 January 2017].
Lipovsky R, Cherepanov A. Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland. In Virus Bulletin, Seattle; 2014c.
Mandiant. APT1 - exposing one of China's cyber espionage units. February 2013. [Online]. Available from: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. [Accessed 8 August 2013].
Marschalek M. EvilBunny: malware instrumented By Lua. Cyphort, 16 December 2014. [Online]. Available from: https://www.cyphort.com/evilbunny-malware-instrumented-lua/. [Accessed 11 January 2017].
Marschalek M. Babar: suspected nation state spyware in the spotlight. Cyphort, 18 February 2015. [Online]. Available from: https://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/. [Accessed 11 January 2017].
McAfee Foundstone Professional Services, McAfee Labs. Global energy cyberattacks: "Night Dragon". 10 February 2011. [Online]. Available from: http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf. [Accessed 11 January 2017].
McAfee Labs. Careto attack – the mask. 12 February 2014. [Online]. Available from: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25037/en_US/McAfee_Labs_Threat_Advisory_Careto_Attack_The%20Mask_3.pdf. [Accessed 11 January 2017].
Meyers A. Whois Clever Kitten. Crowdstrike, 4 April 2013. [Online]. Available from: https://www.crowdstrike.com/blog/whois-clever-kitten/. [Accessed 11 January 2017].
Microsoft. Microsoft security intelligence report volume 19 | January through June, 2015; 2015. [Online]. Available from: http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_A_Profile_Of_A_Persistent_Adversary_English.pdf. [Accessed 12 January 2017].
Minerva Labs LTD and ClearSky Cyber Security. CopyKittens attack group. 23 November 2015. [Online]. Available from: https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf. [Accessed 11 January 2017].
Monnappa. 2nd meetup – reversing and decrypting the communications of APT malware. CYSINFO, 7 July 2016. [Online]. Available from: https://cysinfo.com/sx-2nd-meetup-reversing-and-decrypting-the-communications-of-apt-malware/. [Accessed 11 January 2017].
Moran N, Oppenheim M. Darwin's favorite APT group. FireEye, 3 September 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html. [Accessed 11 January 2017].
Moran N, Homan J, Scott M. Operation poisoned hurricane. FireEye, 6 August 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html. [Accessed 11 January 2017].
Moran N, Scott M, Oppenheim M, Homan J. Operation double tap. FireEye, 21 November 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html. [Accessed 11 January 2017].
Mushtaq A. More on the IE 0-day – Hupigon joins the party. FireEye, 4 November 2010. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html. [Accessed 11 January 2017].
Myers J. Wolves among us: abusing trusted providers for malware operations. RSA, 18 May 2015. [Online]. Available from: https://blogs.rsa.com/wolves-among-us-abusing-trusted-providers-malware-operations/. [Accessed 11 January 2017].
Nakashima E, Miller G, Tate J. U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. Washington Post, 19 june 2012. [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.3a60888d2377. [Accessed 1 February 2017].
Narang S. Backdoor. Barkiofork targets aerospace and defense industry. Symantec, 30 January 2013. [Online]. Available from: https://www.symantec.com/connect/blogs/backdoorbarkiofork-targets-aerospace-and-defense-industry. [Accessed 11 January 2017].
NH. Hat-tribution to PLA unit 61486. Crowdstrike, 9 June 2014. [Online]. Available from: https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/. [Accessed 11 January 2017].
Novetta. Operation SMN: axiom threat actor group report 公理队. October 2014. [Online]. Available from: http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf. [Accessed 11 January 2017].
O'Gorman G, McDonald G. The Elderwood Project; 2012. [Online]. Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf. [Accessed 11 January 2017].
Parys B. MoleRats: there's more to the naked eye. PwC, 21 November 2016. [Online]. Available from: http://pwc.blogs.com/cyber_security_updates/2016/11/molerats-theres-more-to-the-naked-eye.html. [Accessed 11 January 2017].
Pernet C, Lu K. Operation WOOLEN-GOLDFISH. 18 March 2015. [Online]. Available from: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf. [Accessed 11 January 2017].
Pernet C, Sela E. The spy kittens are back: Rocket Kitten 2. September 2015. [Online]. Available from:

https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf. [Accessed 11 January 2017].
PwC. Cyber threat operations tactical intelligence bulletin ScanBox II. 24 February 2015. [Online]. Available from: http://pwc.blogs.com/files/cto-tib-20150223-01a.pdf. [Accessed 11 January 2017].
Raiu C. NetTraveler is back: the 'Red Star' APT returns with new tricks. Kaspersky Labs, 3 September 2013. [Online]. Available from: https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/. [Accessed 11 January 2017].
Raiu C, Baumgartner K. The 'Penquin' turla a turla/snake/uroburos malware for Linux. Kaspersky, 8 December 2014. [Online]. Available from: https://securelist.com/blog/research/67962/the-penquin-turla-2/. [Accessed 12 January 2017].
Raiu C, Golovkin M. The chronicles of the Hellsing APT: the empire strikes back. Kaspersky, 15 April 2015. [Online]. Available from: https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/. [Accessed 11 January 2017].
Raiu C, Soumenkov I. Comparing the Regin module 50251 and the "Qwerty" keylogger. Kaspersky, 27 January 2015. [Online]. Available from: https://securelist.com/blog/research/68525/comparing-the-regin-module-50251-and-the-qwerty-keylogger/. [Accessed 1 February 2017].
Raiu C, Soumenkov I, Baumgartner K, Kamluk V, G. R. a. A. Team. The MiniDuke mystery: PDF 0-day government spy assembler 0x29A micro backdoor. February 2013. [Online]. Available from: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf. [Accessed 12 January 2017].
Raiu C, Soumenkov I, Kamluk V. The Icefog APT hits US targets with Java backdoor. Kaspersky Labs, 14 January 2014. [Online]. Available from: https://securelist.com/blog/incidents/58209/the-icefog-apt-hits-us-targets-with-java-backdoor/. [Accessed 11 January 2017].
Raiu C, K. L. G. R. &. A. Team, Guerrero-Saade JA. Operation Blockbuster revealed. Kaspersky, 24 February 2016. [Online]. Available from: https://securelist.com/blog/incidents/73914/operation-blockbuster-revealed/. [Accessed 11 January 2017].
Rascagnères P. Babar: espionage software finally found and put under the microscope. G Data, 18 February 2015. [Online]. Available from: https://blog.gdatasoftware.com/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope. [Accessed 11 January 2017].
RiskBased Security. A breakdown and analysis of the December, 2014 Sony Hack. RiskBased Security, 5 December 2014. [Online]. Available from: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/. [Accessed 11 January 2017].
RSA Incident Response. RSA incident response: emerging threat profile shell_crew. January 2014. [Online]. Available from: https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf. [Accessed 11 January 2017].
RSA Research. TERRACOTTA VPN – enabler of advanced threat anonymity. 4 August 2015. [Online]. Available from: https://blogs.rsa.com/wp-content/uploads/2015/08/Terracotta-VPN-Report-Final-8-3.pdf. [Accessed 11 January 2017].
Sancho D, dela Torre J, Bakuei M, Villeneuve N, McArdle R. IXESHE – an APT campaign; 2012. [Online]. Available from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf. [Accessed 11 January 2017].
Sanger DE. Obama order sped up wave of cyberattacks against Iran. New York Times, 1 June 2012. [Online]. Available from: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all. [Accessed 8 August 2013].
Santos O. The shadow brokers EPICBANANA and EXTRABACON exploits. Cisco, 21 September 2016. [Online]. Available from: https://blogs.cisco.com/security/shadow-brokers. [Accessed 11 January 2017].
Schworer A, Liburdi J. Storm chasing: hunting Hurricane Panda. Crowdstrike, 26 January 2015. [Online]. Available from: https://www.crowdstrike.com/blog/storm-chasing/. [Accessed 11 January 2017].
Scott J, Spaniel D. ICIT briefing: China's espionage dynasty. Institute for Critical Infrastructure Technology, Washington, D.C.; 2016.
Scott M. Clandestine fox, Part deux. FireEye, 10 June 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html. [Accessed 19 January 2017].
Scott-Railton J, Kleemola K. London calling: two-factor authentication phishing from Iran. Citizenlab, 27 August 2015. [Online]. Available from: https://citizenlab.org/2015/08/iran_two_factor_phishing/. [Accessed 11 January 2017].
Security Response. The Waterbug attack group. 14 January 2016. [Online]. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf. [Accessed 12 January 2017].
Selvaraj K. Hydraq (Aurora) attackers back? Symantec, 13 September 2010. [Online]. Available from: https://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back. [Accessed 11 January 2017].
Sherstobitoff R, Liba I, Walter J. Dissecting Operation Troy: cyberespionage in South Korea," July 2013. [Online]. Available from: http://www.mcafee.com/ca/resources/white-papers/wp-dissecting-operation-troy.pdf. [Accessed 11 January 2017].
Simonite T. Chinese hacking team caught taking over decoy water plant. 2 August 2013. [Online]. Available from: http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/. [Accessed 10 October 2013].
Symantec Security Response. Hydraq – an attack of mythical proportions. Symantec, 15 January 2010. [Online]. Available from: https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions. [Accessed 11 January 2017].
Symantec Security Response. W32.Duqu the precursor to the next Stuxnet. 23 November 2011. [Online]. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf. [Accessed 11 January 2017].
Symantec Security Response. Flamer: highly sophisticated and discreet threat targets the Middle East. Symantec, 28 May 2012. [Online]. Available from: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east. [Accessed 1 February 2017].
Symantec Security Response. Dragonfly: cyberespionage attacks against energy suppliers. 7 July 2014a. [Online]. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf. [Accessed 12 January 2017].
Symantec Security Response. Sandworm Windows zero-day vulnerability being actively exploited in targeted attacks. Symantec, 14 October 2014b. [Online]. Available from: https://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks. [Accessed 12 January 2017].
Symantec Security Response. "Forkmeiamfamous": Seaduke, latest weapon in the Duke armory. Symantec, 13 July 2015a.

[Online]. Available from: https://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory. [Accessed 12 January 2017].
Symantec Security Response. Regin: Top-tier espionage tool enables stealthy surveillance. 27 August 2015b. [Online]. Available from: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/regin-top-tier-espionage-tool-15-en.pdf. [Accessed 11 January 2017].
Symantec Security Response. Buckeye cyberespionage group shifts gaze from US to Hong Kong. Symantec, 6 September 2016a. [Online]. Available from: https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong. [Accessed 11 January 2017].
Symantec Security Response. Strider: Cyberespionage group turns eye of Sauron on targets. Symantec, 7 August 2016b. [Online]. Available from: https://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets. [Accessed 11 January 2017].
Tanase S. Satellite turla: APT command and control in the sky. Kaspersky, 9 September 2015. [Online]. Available from: https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/. [Accessed 12 January 2017].
Tarakanov D. The "Kimsuky" Operation: a North Korean APT? 11 September 2013. [Online]. Available from: https://securelist.com/analysis/publications/57915/the-kimsuky-operation-a-north-korean-apt/. [Accessed 11 January 2017].
ThreatConnect Research Team. The anthem hack: all roads lead to China. ThreatConnect, 27 February 2015. [Online]. Available from: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/. [Accessed 11 January 2017].
Trend Micro Threat Research Team. Operation arid viper. 16 February 2015. [Online]. Available from: http://www.trendmicro.es/media/wp/operation-arid-viper-whitepaper-en.pdf. [Accessed 11 January 2017].
TrendMicro. When big fish bite: operation arid viper and advtravel discovered by trend micro. TrendMicro, 15 March 2015. [Online].
U.S. Department of Justice (DoJ). U.S. charges five Chinese military hackers with cyber espionage against U.S. corporations and a labor organization for commercial advantage. Federal Bureau of Investigation, 19 May 2014. [Online]. Available from: https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage. [Accessed 18 January 2017].
Varma R. McAfee Labs: combating Aurora; 2010. [Online]. Available from: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Combating%20Threats%20-%20Operation%20Aurora.pdf. [Accessed 11 January 2017].
Villeneuve N, Haq T, Moran N. Operation Molerats: Middle East cyber attacks using poison ivy. FireEye, 23 August 2013. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html. [Accessed 11 January 2017].
Villeneuve N, Moran N, Haq T, Scott M. Operation Saffron rose. May 2014. [Online]. Available from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf. [Accessed 11 January 2017].
Villeneuve N, Bennett JT, Moran N, Haq T, Scott M, Geers K. Operation "KE3CHANG": targeted attacks against ministries of foreign affairs; 2014. [Online]. Available from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf. [Accessed 11 January 2017].
Weedon J. Beyond 'Cyber War': Russia's use of strategic cyber espionage and information operations in Ukraine. In: Cyber war in perspective: Russian aggression against Ukraine. Talinn: NATO CCD COE Publications; 2015. p. 67–77.
Wilhoit K. The SCADA that didn't cry wolf – who's really attacking your ICS equipment? (part 2); 2013. [Online]. Available from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf. [Accessed 11 January 2017].
Wilhoit K. Havex, it's down with OPC. FireEye, 17 July 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html. [Accessed 11 January 2017].
Windows Defender Advanced Threat Hunting Team. PLATINUM Targeted attacks in South and Southeast Asia; 2016. [Online]. Available from: https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf. [Accessed 11 January 2017].
Winters R. The EPS awakens – part 2. FireEye Threat Intelligence, 15 December 2015. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html. [Accessed 11 January 2017].
Yates M, Scott M, Levene B, Miller-Osborn J, Keigher T. Operation Ke3chang resurfaces with new TidePool malware. PaloAlto, 22 May 2016. [Online]. Available from: http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool-malware/. [Accessed 11 January 2017].
Zetter K. The NSA acknowledges what we all feared: Iran learns from US cyberattacks. Wired, 10 February 2015. [Online]. Available from: https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/. [Accessed 1 February 2017].

Antoine Lemay is a researcher at École Polytechnique de Montréal in the Department of Computer and Software Engineering, specializing in securing ICS and SCADA networks against threats from nation states. He also has work experience as a security analyst and holds a number of professional certifications, including CISSP, GSEC and GCIH.

Joan Calvet is a security researcher developing reverse-engineering tools for a small company called PNF Software. He previously worked as a malware researcher, focusing on in-depth malware investigations. He defended his Ph.D. thesis in 2013, and has spoken at security conferences such as REcon, Virus Bulletin and hack.lu.

François Menet is a former cyber-security consultant, now working for Polytechnique Montreal's high-security Lab (SecSI Lab) researching as a master's student. He focuses on innovative ways to detect malicious network intrusion, and studies malware obfuscation, to identify nefarious behaviour within a network at any step of a cyber-attack.

José M Fernandez is an associate professor in the Department of Computer & Software Engineering at the École Polytechnique de Montréal. He heads the Laboratory for Information Security Research (SecSI) and his main area of research is computer security. His current research interests include malware and botnet analysis, security product testing methodologies, critical infrastructure security and security and integration of logical and physical access control systems. He has several years of professional experience as a practitioner of Information Security in both industry and government.