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).

http://dx.doi.org/10.1016/j.cose.2017.08.005
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

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