International Journal of Systems and Society
Volume 4 • Issue 2 • July-December 2017

A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness

Nikolaos Serketzis, Aristotle University of Thessaloniki, Thessaloniki, Greece
Vasilios Katos, Bournemouth University, Poole, UK
Christos Ilioudis, Alexander Technological Educational Institute of Thessaloniki, Thessaloniki, Greece
Dimitrios Baltatzis, International Hellenic University, Thessaloniki, Greece
George J Pangalos, Aristotle University of Thessaloniki, Thessaloniki, Greece

ABSTRACT

In this article, a DFR framework is proposed focusing on the prioritization, triaging and selection of Indicators of Compromise (IoC) to be used when investigating of security incidents. A core component of the framework is the contextualization of the IoCs to the underlying organization, which can be achieved with the use of clustering and classification algorithms and a local IoC database.

KEYWORDS

Advanced Persistent Threats, Digital Forensic Readiness, Indicators of Compromise, Intelligent Evidence Storage System, IOC, STIX, TAXII, Threat Intelligence

1. INTRODUCTION

Digital forensics dates over four decades. Unlike other forensic science disciplines, digital forensics faces the challenge to operate in a problem domain where the subject of study evolves in an intermittent, nonlinear fashion. For instance, a routine, nightly update of the software or introduction of new hardware may substantially change the behavior of the underlying system, requiring a significant revision of the digital forensics acquisition and analysis processes. Consider for example the case of evolution of traditional hard disks to solid state disk (SSD) technology. The way the latter operate invalidate many key assumptions under which forensic acquisition and investigation of disks is performed (Bednar & Katos, 2011).

Moreover, the proliferation of heterogeneous networked devices and the amount of data they are capable of producing – as captured under the terms IoT and Big Data respectively – has exacerbated the problems and challenges of digital forensics. As such, digital forensic readiness (DFR) has become a critical function of the organization's security processes and achieving efficient DFR has become a high priority. Research in digital forensics has primarily evolved through a responsive, practitioner-based attitude. The relevant literature on digital forensics is dominated by techniques and practical approaches for obtaining and analyzing data in specific contexts and system configurations. When it comes to considering DFR approaches, the level of abstraction is high causing a void and eventually a disjoint between DFR and digital forensic investigations. Most DFR research publications are limited to describing high-level and generic steps, whereas contextualization is mostly absent. This work aims

DOI: 10.4018/IJSS.2017070105

to bridge the gap by proposing a framework for a closer coupling between DFR, forensics and incident response for addressing Advanced Persistent Threats. We argue that inevitably, the prioritisation and contextualisation of the Indicators of Compromise is a sociotechnical challenge, since ultimately the forensic analyst needs to leverage automated tools to support their cyber situational awareness posture. That is, following a detection of a security breach, the threat related information needs to be quickly accessed, correlated and highlighted to allow the forensic analyst to triage, prioritise and guide their investigation in an effective manner.

The rest of the paper is structured as follows. Section 2 presents the relevant literature. In Section 3 our approach is developed. Section 4 outlines a typical APT scenario to be used as a vehicle to showcase our approach, and section 5 summarises the conclusions.

2. RELATED WORKS

In a seminal paper, Hutchins et al. (Hutchins, Cloppert, & Amin, 2011) proposed an approach for studying and improving incident response against APTs. They introduced a cyber kill chain which identifies a path comprised of 7 discrete and sequential phases an attacker follows to meet their adversarial goals. From a digital forensics perspective, the kill chain is particularly helpful in highlighting the following:

- Every successful (to the attacker) phase is a direct consequence of the respective security control failures.
- Detecting the security breach early in the chain infers low impact and potential damage.
- Late detection of the security breach implies that there are more security failures. Hence the scope of the digital forensic artifact collection is wider.

For the remainder of this section, the relevant subtopics that will enable the key chain to leverage the proposed DFR framework are presented.

2.1. Threat Intelligence

It can easily become apparent from the current literature that there is limited consensus on a definition of threat intelligence. Threat intelligence has been defined for example as a product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (Sanders & Smith, 2014). It can be therefore considered that threat intelligence is the elaborate information about threats targeting one or more organizations.

Threat intelligence can be produced both from internal (e.g., Firewall, IDS) and external sources, such as public or commercial threat and vulnerability repositories. Externally obtained intelligence is sought as being particularly beneficial to the organization as this promotes cyber situational awareness, revealing thus the socio-technical aspects of the forensic investigation problem; an analyst will need the right technical tools to access the threat information in a timely manner, but will also need to coordinate with external to the organisation parties and peers in order to understand the subtle aspects of an APT.

Research on threat intelligence has highlighted the need for automated information exchange. To this extent, various standards and formats (openIoC, CybOX, STIX,) have been developed (MITRE, 2017a) (MITRE, 2017b) (Mandiant Corporation, 2013), with the most promising and publicly acceptable being CybOX, STIX and TAXII (Sauerwein, Sillaber, Mussmann, & Breu, 2017), (Fransen, Smulders, & Kerkdijk, 2015).

Cyber Observable eXpression (CybOX) is a standardized approach which leverages eXtensible Markup Language (XML) to encode and share information about observables in the operational cyber