Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A survey on technical threat intelligence in the age of sophisticated cyber attacks

Wiem Tounsi *, *Helmi Rais*

Managed Security Services Division, AlliaCERT Team, Alliacom, France

ARTICLE INFO

Article history:
Received 24 April 2017
Received in revised form 24 July 2017
Accepted 5 September 2017
Available online 25 September 2017

Keywords:
Technical threat intelligence
Indicators of compromise (IOC)
Malware
Trust
Reputation
Ontologies
Cyber crime
Preventative strategies
Risk analysis
Threat sharing

ABSTRACT

Today's cyber attacks require a new line of security defenses. The static approach of traditional security based on heuristic and signature does not match the dynamic nature of new generation of threats that are known to be evasive, resilient and complex. Organizations need to gather and share real-time cyber threat information and to transform it to threat intelligence in order to prevent attacks or at least execute timely disaster recovery. Threat Intelligence (TI) means evidence-based knowledge representing threats that can inform decisions. There is a general awareness for the need of threat intelligence while vendors today are rushing to provide a diverse array of threat intelligence products, specifically focusing on Technical Threat Intelligence (TTI). Although threat intelligence is being increasingly adopted, there is little consensus on what it actually is, or how to use it. Without any real understanding of this need, organizations risk investing large amounts of time and money without solving existing security problems. Our paper aims to classify and make distinction among existing threat intelligence types. We focus particularly on the TTI issues, emerging researches, trends and standards. Our paper also explains why there is a reluctance among organizations to share threat intelligence. We provide sharing strategies based on trust and anonymity, so participating organizations can do away with the risks of business leak. We also show in this paper why having a standardized representation of threat information can improve the quality of TTI, thus providing better automated analytics solutions on large volumes of TTI which are often non-uniform and redundant. Finally, we evaluate most popular open source/free threat intelligence tools, and compare their features with those of a new AlliaCERT TI tool.

1. Introduction

Today, the constant progress of IT infrastructure connectivity and the unending innovations in digital technologies, make systems more and more complex. As a system gets more complex, it gets less secure (Schneier, 2000). This complication in digital systems has led to a change in the cyber attacks forms, functions, and sophistications from just a few years ago targeting individual end users, businesses and government agencies. No longer are these cyber attacks originated from digital hacktivists or online thugs. Held by well-funded and well-organized threat actors, cyber attacks have been transformed from hacking for kicks to advanced attacks for profit which may range from financial gains to political aims. Consequently, attacks designed for mischief have been replaced with dynamic, stealthy and persistent attacks, and terms like advanced malwares and Advanced Persistent Threats (APTs) appeared. Despite spending over 20 billion dollars annually on traditional security defenses (Piper, 2013), organizations find

* *Corresponding author.*
E-mail address: wiem.tounsi@alliacom.com (W. Tounsi).

https://doi.org/10.1016/j.cose.2017.09.001

themselves faced to this new generation of cyber attacks, which easily bypass traditional defenses such as traditional firewalls, intrusion prevention systems, anti-virus, and security gateways. Those defenses, built for a previous generation of attacks, rely heavily on static malware signature-based or list-based pattern matching technology. This approach leaves those defenses extremely vulnerable to ever evolving threats that exploit unknown and zero-day vulnerabilities. What is therefore needed is a real-time system for information and intelligence sharing, in order to identify threat agents and targeted assets rather than to perpetuate the endless cycle of signature scanning.

Starting from observing that cyber attackers often target similar types of organizations (Klump and Kwiatkowski, 2010) (i.e., an incident at one location can be succeeded by an attack at another similar location), a knowledge about a threat can be distributed across individual defenders. This leads to what is commonly named Threat Intelligence (TI). We deal with TI as an actionable defense to reduce the gap between advanced attacks and organization defenses means. We focus specifically on Technical Threat Intelligence (TTI), which is rapidly becoming an ever-higher business priority (Chismon and Ruks, 2015), since it is immediately actionable and is easier to quantify than other TI sub-categories. TTI is also the most shared intelligence, because of its easy standardization (Yamakawa, 2014). With TTI, we can feed firewalls, gateways, Security Information and Event Management (SIEM) or other appliances of various types with indicators of compromise (IOC) (Verizon, 2015), e.g., malicious payloads and IP addresses. We can also ingest IOC into a searchable index or just use IOC for visualization and dashboards.

Despite its prevalence, many problems exist with technical threat intelligence. This is mainly related to the quality of IOC (i.e., IP addresses lifetime, malware signatures) and the massive repositories of threat data given by provider's databases which overwhelms their consumers (e.g., threat analysts) with not always useful data, that should be essential for generating intelligence. In many cases, threat feeds can simply amount to faster signatures that still fail to reach the attackers. Specific malicious payloads, URLs and IP addresses are so ephemeral that they may only be used once in the case of a true targeted attack.

To date, few analyzes are made on different types of TI and specifically on technical threat intelligence. There is also little research surveys on how new techniques and trends try to overcome TTI problems. Most existing literature reveals technical reports exposing periodic statistics regarding the use of threat intelligence (Ponemon, 2015; Shackleford, 2015, 2016), and interesting empirical investigations for specific threat analyzes techniques (Ahrend et al., 2016; Sillaber et al., 2016). In order to develop effective defense strategies, organizations can save time and bypass confusions if they start defining what threat intelligence actually is, and how to use it and mitigate its problems given its different sub-categories. Our paper aims to give a clear idea about threat intelligence and how literature subdivides it given its multiple sources, the gathering methods, the information lifespan and who consumes the resulted intelligence. It helps to classify and make distinction among existing threat intelligence types to better exploit them. For example, given the short lifetime of TTI indicators, it is important to search for how much time these indicators could be useful. We focus particularly on the TTI issues, emerging researches, trends and standards to mitigate these issues. Finally, we evaluate most popular open source/free threat intelligence tools, and compare their features with those of a new AlliaCERT TI tool. Through our analysis, we find that (1) differently from what is known, fast sharing of TI is not sufficient to avoid targeted attacks, (2) trust is a key for an effective sharing of threat information between organizations, (3) a common standardized format for sharing TI minimizes the risk of losing the quality of threat data, which provides better automated analytics solutions on large volumes of TTI and (4) choosing the best threat intelligence tool depends on the organization objectives, since some organizations privilege standardization and automatic analytics needs, while others focus on high speed requirements.

Paper organization. Section 2 introduces new generation of cyber attacks and the cyber threat intelligence sub-categories. Section 3 surveys related work. Section 4 presents most known initiatives supporting cooperation between threat defenders. Section 5 presents problems with threat intelligence sharing experience. Section 6 presents TTI issues. Section 7 gives a discussion. Section 8 evaluates most known open source tools offering TTI and compares them to the AlliaCERT TI tool. Finally, Section 9 concludes the paper.

2. Background

Cyber security is a trade-off, a non-static balancing act between attacker and defender (Schneier, 2012). Defenders are in "the position of the interior" as per the military strategist Carl von Clausewitz (Schneier, 1998) in a context of war. They have to defend against every possible attack, even against unrealized attacks yet, while attackers have only to find one weakness to penetrate a system. Today, while the implementation of new security technologies implies agreement, coordination and possibly a lengthy bureaucratic process, an attacker can just use this new technology to reach his goal. In addition, the complexity of new technologies makes it easier for the attacker to find a weakness and harder for the defender to secure systems (Schneier, 2000). As a result, attackers have a first mover advantage, by trying new attacks first, while defenders have the disadvantage to be in a constant position of responding, e.g., better anti-virus software to combat new malwares, better intrusion detection system to detect malicious activities, etc.

2.1. *New generation threats*

New generation threats are multi-vectored and often multi-staged: multi-vectored, because attacks can use multiple means of propagation (e.g., web, email, applications) and multi-staged, as attacks can infiltrate networks, spread, and ultimately exfiltrate the valuable data (FireEye Inc., 2012). This new generation threats resulting in new attack scenarios, can be understood from the defensive perspective of a "kill chain" (Hutchins et al., 2011). "Kill chain" is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it (Barraco, 2014). More information about "Kill chain" is provided in Appendix. On the other hand, to realize new generation attacks, attackers are armed with the latest zero-day vulnerabilities and social engineering techniques. They utilize advanced tactics such as polymorphic threats and composite threats, which are personalized to appear unknown to signature based tools and yet authentic enough to bypass spam filters. Composite and multi-stage attacks evade easily traditional security defenses, which are typically set up to inspect each attack vector as a separate path and each stage as an independent event. Thus, they do not view and analyze the attack as an orchestrated series of cyber incidents. A comprehensive taxonomy of threat landscape is done by ENISA in early 2017 (ENISA: European Union Agency for Network and Information, 2017). In the following, we cite examples of this new generation threats.

2.1.1. *Advanced persistent threats (APT)*

APT are examples of multi-vectored and multi-staged threats. They are defined as sophisticated network attacks (FireEye Inc., 2014; Piper, 2013) in which an attacker keeps trying until he gains access to a network and stays undetected for a long period of time. The intention of an APT is to steal data rather than to cause damage to the network. APT target organizations in sectors with high-value information, such as, government agencies and financial industries.

2.1.2. *Polymorphic threats*

Polymorphic threats are cyber attacks, such as viruses, worms or Trojans that constantly change ("morph") (Piper, 2013). Evolution of polymorphic threats can occur in different ways (e.g., filename changes and file compression). Despite the changing appearance of the code in a polymorphic threat after each mutation, the essential function usually remains the same. For example, a malware intended to act as a key logger will continue to perform that function even though its signature has changed. The evolution of polymorphic threats has made it nearly impossible to detect using signature-based defenses. Vendors that manufacture signature-based security products are constantly creating and distributing new threat signatures (a very expensive and time-consuming proposition (Piper, 2013)), while clients are constantly deploying the signatures provided by their security vendors. It is a vicious cycle which goes to the advantage of the attacker.

2.1.3. *Zero-day threats*

Zero-day threats are cyber threats on a publicly unknown vulnerability of an operating system or application. It is so named because the attack was launched on "day zero" or before a public awareness of the vulnerability and, in many cases, before the vendor was aware (Piper, 2013). In some cases, the vendor is already aware of the vulnerability, but has not disclosed it publicly because the vulnerability has not yet been patched. Zero-day attacks are extremely effective because they can be undetected for long periods (i.e., for months, if not years), and when they are finally identified, patching the vulnerability still takes days or even weeks.

2.1.4. *Composite threats*

Cyber attacks can either be classified as syntactic or semantic attacks. A combination of these two approaches is known to as composite attacks or blended attacks (Choo et al., 2007). Syntactic attacks exploit technical vulnerabilities in software and/or hardware, e.g., a malware installation to steal data; whereas semantic attacks exploit social vulnerabilities to gain personal information, e.g., scam solicitations. In recent years, progress has been made using the two approaches to realize composite attacks. This means, using a technical tool to facilitate social engineering in order to gain privileged information, or using a social engineering means to realize a technical attack in order to cause harm to network hosts. Composite attacks include phishing attacks (named also online scam) which frequently use emails to send to carefully selected victims a plausible-looking message including a malicious attachment targeting a zero-day vulnerability. Phishing is positioned in the first three steps of the kill chain. Phishing attacks forge messages from legitimate organizations, particularly banking and finance services, to deceive victims into disclosing their financial and/or personal identity information or to download a malicious files, in order to facilitate other attacks (e.g., identity theft, credit card fraud, ransomeware (Dutch National Police, 2016)). When the attack focuses on a limited number of recipient to whom a highly personalized message is sent, the technique is named spear phishing. Phishing abuses mostly information found in social media (Fadilpasic, 2016).

Obviously, the attack morphology is different depending on the aimed scenario, e.g., cyber crime might use stealthy APT to steal intellectual property, while cyber war uses botnets to run Distributed Denial of Service (DDoS) attacks (Skopik et al., 2016).

2.2. *Threat intelligence*

Threat intelligence (TI), also known as cyber threat intelligence, is any evidence-based knowledge about threats that can inform decisions (McMillan, 2013), with the aim of preventing an attack or shortening the window between compromise and detection. TI can also be information that, instead of aiding specific decisions, helps to illuminate the risk landscape (Chismon and Ruks, 2015). Other definitions exist such as in Dalziel (2014); Steele (2014). A more rigorous one (Dalziel, 2014) states that TI is an information that should be relevant (i.e., potentially related to the organization and/or objectives), actionable (i.e., specific enough to prompt some response, action, or decision) and valuable (i.e. the information has to contribute to any useful business outcome). TI can be information collected from a variety of technical sources (e.g., local sensor traffic) or human sources (e.g., discussions observed in underground forums, communication with a peer). Thus, threat intelligence includes technical indicators, context, mechanisms, implications and actionable advice about an existing or emerging threat.

2.2.1. *Threat intelligence sub-domains*

With the different sources of TI, it is useful to have subdivisions to better manage the information and focus effort. TI can be categorized in sub-domains. Ahrend et al. (2016) divide TI in formal and informal practices to uncover and utilize tacit knowledge between collaborators. Informal intelligence means that collaborators share knowledge, tools and advices to prevent

Table 1 – Threat intelligence subdivision.

TI sub-domains	Depends on	References
Formal, Informal	the gathering method	(Ahrend et al., 2016)
Strategic, Operational	the analysis form used to produce intelligence	(Gundert, 2014; Hugh, 2016)
Strategic, Tactical	the gathering method, its cost and who consumes the intelligence	(Chuvakin and Barros, 2016)
Strategic, Operational, Tactical, Technical	the intelligence aim and who consumes it	(Chismon and Ruks, 2015; Korstanje, 2016)

new attacks whereas formal intelligence leads to the sharing of technical indicators of compromise. Authors Gundert (2014); Hugh, (2016) categorize TI as strategic and operational. Strategic intelligence requires highly skilled human analysts to develop external relationships and proprietary information sources whereas operational intelligence is produced entirely by computers, from data identification and collection to enrichment and analysis. Another reference (Chuvakin and Barros, 2016) classifies TI into strategic intelligence versus tactical intelligence. The first is high-level and geared towards strategic planners, executives and threat analysts, whereas the second is low-level and is easier to quantify than strategic intelligence. In Chismon and Ruks (2015); Korstanje (2016), a more refined model divides threat intelligence into four distinct domains: Strategic threat intelligence, Operational threat intelligence, Tactical threat intelligence and Technical threat intelligence. This subdivision is also known to as the four levels of intelligence analysis (Steele, 2007a). It is originally used in the military context as the model of expeditionary factors analysis which distinguishes between these four levels (Steele, 2007b). Table 1 summarizes these different subdivisions. We show that all of them converge in separating technical intelligence from strategic one. We find that the more the TI is subdivided, the more we can investigate and discuss their limitations. In the sequel, our study follows the last subdivision.

- **Strategic threat intelligence** is high-level information consumed by decision-makers. The purpose is to help strategists understand current risks and identify further risks of which they are yet unaware. It could cover financial impact of cyber activity or attack trends, historical data or predictions regarding the threats activity. As a result, a board has to consider possible attacks targeting it, to help it weighing risks and to allocate effort and budget to mitigate these possible attacks. Strategic TI is generally in the form of reports, briefings or conversations.
- **Operational threat intelligence** is information about specific impending attacks against the organization and is initially consumed by higher-level security staff, e.g., security managers or heads of incident response team (Chismon and Ruks, 2015). Such intelligence is very rare. For example, it is not possible for a private entity to legally access to attack groups and their infrastructure (i.e. relevant communication channels) necessary to obtain good operational TI. Generally, only a government have this privilege. However, when an organization is targeted by more public actors (i.e., attacks by groups communicating openly), including hacktivists, it will be able to access the information. It focuses on details of these attacks found in open source intelligence or providers with access to closed chat forums.
- **Tactical threat intelligence** is often referred to as Tactics, Techniques, and Procedures and is information about how threat actors are conducting attacks (Chismon and Ruks, 2015). Tactical TI is consumed by incident responders to ensure that their defenses and investigation are prepared for current tactics. For example, understanding the attacker tooling and methodology is tactical intelligence that could prompt defenders to change policies. Tactical TI is often gained by reading technical press, white papers, communicating with peers in other organizations to know what they are seeing attackers do, or by purchasing from a provider of such intelligence.
- **Technical threat intelligence (TTI)** is information that is normally consumed through technical resources (Chismon and Ruks, 2015). Technical TI typically feeds the investigative or monitoring functions of an organization e.g., firewalls and mail filtering devices, by blocking attempted connections to suspect servers. TTI serves also for analytic tools, or just for visualization and dashboards. For example, after including an IOC in organizations defensive infrastructure such as firewalls and mail filtering devices, historical attacks can be detected, by searching logs of previously observed connections or binaries (Chismon and Ruks, 2015).

From their definitions, strategic and tactical threat intelligence are gainful for a long-term use whereas operational and technical threat intelligence are profitable for a short-time/immediate use. In case technical IOC are for short time use, a key question we try to respond to is: How long can we expect those indicators to remain useful? In the sequel, we deal with TTI in more details.

2.2.2. *Technical threat intelligence (TTI)*

Not only do defenders need to be aware of threat actors and attacks nature they are facing, they should also be aware of the data fundamentals associated with these cyber attacks known to as indicators of compromise (IOC). IOC are closely linked to TTI, but are often confused with intelligence. IOC are an aspect which enables the production of intelligence. The feeds by themselves are just data. By conducting the analysis with the internal data intelligence which is relevant to the organization, an actionable decision is able to recover from any incident (Dalziel, 2014). IOC are commonly partitioned into three distinct categories (Ray, 2015): Network, Host-based indicators and Email indicators, as depicted in Fig. 1.

- **Network indicators** are found in URLs and Domain names used for Command & Control (C&C) and link-based malware delivery. They could be IP addresses used in detecting attacks from known compromised servers, botnets and systems

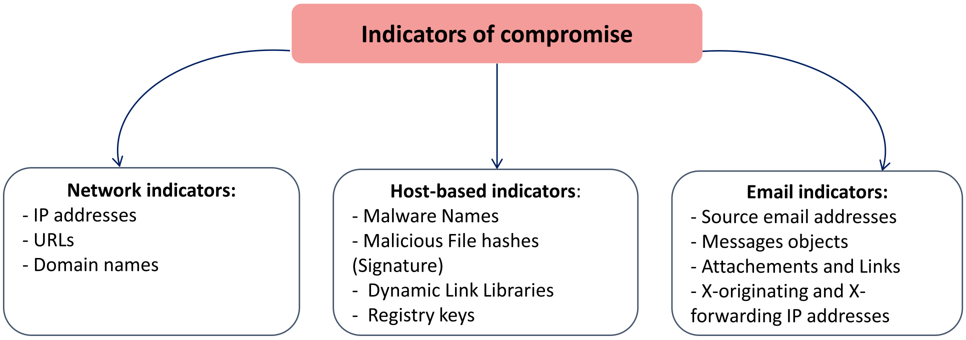


Fig. 1 – Most Common Indicators of Compromise.

conducting DDoS attacks. However, this type of IOC has a short lifetime as threat actors move from one compromised server to another, and with the development of Cloud-based hosting services, it is no longer just compromised servers that are used, but also legitimate IP addresses belonging to large corporations.

- **Host-Based indicators** can be found through analysis of an infected computer. They can be malware names and decoy documents or file hashes of the malware being investigated. The most commonly offered malware indicators are MD5 or SHA-1 hashes of binaries (Chismon and Ruks, 2015). Dynamic Link Libraries (DLLs) are also often targeted, as attackers replace Windows system files to ensure that their payload executes each time Windows starts. Registry keys could be added by a malicious code and to allow for persistence, specific keys are modified in a computer registry settings. This is a common technique that malware authors use when creating Trojans (Ray, 2015).
- **Email indicators** are created typically when attackers use free email services to send socially engineered emails to targeted organizations and individuals. Source email address and email subject are created from addresses that appear to belong to recognizable individuals or highlight current events to create intriguing email subject lines, often with attachments and links. X-originating and X-forwarding IP addresses are email headers identifying the originating IP address of (1) a client connecting to a mail server, (2) a client connecting to a web server through a HTTP proxy or load balancer, respectively. Monitoring these IP addresses when available provide additional insight into attackers.

Spam is the main mean to transport malicious URLs and malwares. These latter are wrapped in the form of spam and phishing messages (cf. Section 2.1.4 for more details on phishing attacks). Spam is mainly distributed by large spam-botnets (i.e., devices that are taken over and form large network of zombies adhering to C&C servers (ENISA: European Union Agency for Network and Information, 2017)). Obfuscation methods (Symantec, 2016) have been observed in 2015 and continues in 2016 to evade detection of this type of attack. These methods could be the expedition of a massive amounts of spam to a wide IP range to reduce the efficiency of spam filters or the usage of alphanumeric symbols UTF-8 characters to encode malicious URLs.

IOC come from a variety of sources (Holland et al., 2013) including commonly internal sources (i.e., crowdsourcing, log and network data, honeynets, i.e., a group of interactive computer systems that are configured to trap attackers), government-sponsored sources (i.e., law enforcement, national security organizations), industry sources (i.e., business partners), Open Source INTelligence OSINT (i.e., public threat feeds such as Dshield (Dshield, 2001), ZeuS Tracker (Tracker, 2009), in-house intelligence collection such as attacker forums, social media) and commercial sources (i.e., threat feeds, Software-as-a-Service (SaaS) threat alerting, security intelligence providers).

3. Related work

Cyber threats and attacks are currently one of the most discussed about phenomenons in the IT industry and the general media (e.g., news) (iSightPartners, 2014). Fig. 2 (a) shows Google results for cyber "threat intelligence" in general and in terms of research publications in particular, while Fig. 2 (b) shows Google results for "indicators of compromise" in general and in terms of research publications in particular, in the last ten years. These numbers are taken year per year. Even if an exponential interest to threat intelligence and IOC fields is seen, we observe a gap between the evolution of cyber threat intelligence activities and related research works. Actually, a large number of threat intelligence vendors and advisory papers are found describing very different products and activities under the banner of threat intelligence. The same conclusion is observed with technical threat intelligence category via the indicators of compromise. However, few researches have been done to examine and identify characteristics of TI and its related issues. It is also noteworthy that only during these recent years that significant research progress is done regarding this field. Regarding surveys related to our work, most of them are exposing yearly new trends and statistics which are relevant to strategic intelligence (Ponemon, 2015; Shackleford, 2015, 2016). In the research side, a significant body of work has been dedicated to threat intelligence sharing issues. Many guidelines, best practices and summaries on existing sharing standards and techniques have been published. In contrast, less research has been devoted to areas like TTI problems and how to mitigate them.

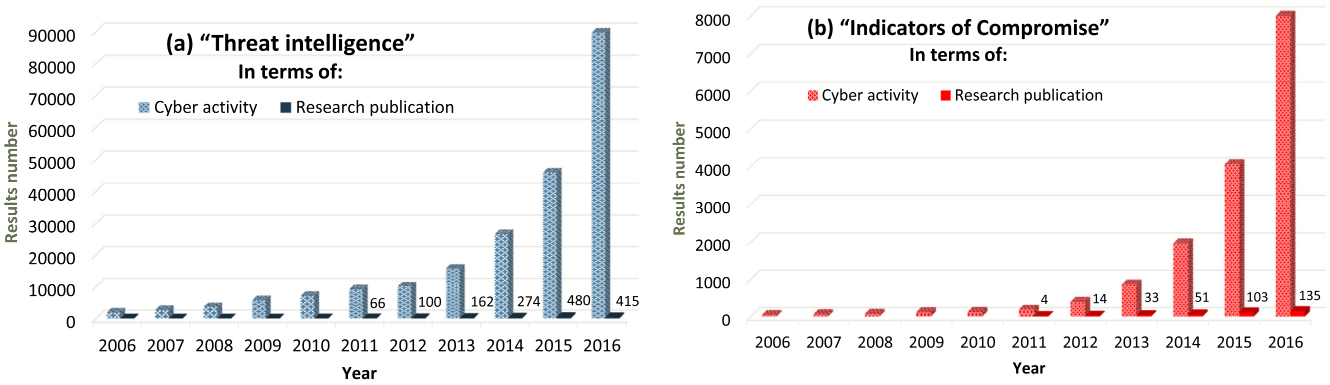


Fig. 2 – Trend of “Threat intelligence” and “Indicators of compromise” in cyber activity from the ten last years.

Moriarty (2011) is one of the first papers surveying incident information sharing techniques, including indicators of compromise. The author indicates the importance of a common format for organizations to ingest incident information. He presents the limited methods in 2011 to coordinate incident handling between organizations and their service providers and even law enforcement. The unique standard formats to represent incident information for the purpose of exchange between Computer Security Incident Response Teams (CSIRTs) were the Object Description Exchange Format (Danyliw et al., 2007) (IODEF) succeeded by the Real-Time Inter-Network Defense (Moriarty, 2012) (RID) to share incidents (i.e., both are Internet Engineering Task Force (IETF) standard formats). As security and privacy are of high concern when exchanging potentially sensitive information, the RID message contains technical options to address security, policy, and privacy issues related to the exchange of potentially sensitive information. More recent formats have been appeared, such as STIX and TAXII (Barnum, 2014) for representation and sharing of IOC, respectively. Both are copyrighted by MITRE to ensure change control. These standards will be presented and discussed in Section 7.4. In Skopik et al. (2016) a survey on the implementation and organization of information sharing platforms is realized to discuss the overall dimension of information sharing. Authors discuss relevant regulations, standards, concepts, supporting tools, and protocols used for setting up effective information sharing procedures. For example, the authors realize a comparison between the main open-source correlation tools (used to remove false positives and duplication of data), and expose current technical sharing standards and ontologies. The authors conclude that the effectiveness of the sharing platforms could be increased by having a strongly active sector-oriented community, within which incidents could be shared rapidly. Finally, some barriers that limit the possibilities to cooperate between incident handling teams across the world have been exposed. In Choo (2011), the author contributes to a better understanding of the ever-evolving cyber threat landscape by providing a snapshot of several risk areas mainly focusing on financially-motivated cyber criminal activities. He also provides cyber crime prevention strategies. In Burger et al. (2014), the authors propose a layered taxonomy to classify existing threat-sharing standards using an abstracted framework. The aim is to decompose these standards and analyze dependency and interoperability within the current cyber threat sharing communities. In Ring (2014), the author explains the importance of sharing threat intelligence and exposes the problems behind not sharing. These problems could be related to the changing nature of cyber attacks, to the natural instinct for organizations to not sharing, to a budgeting problem, or to the quality of shared information that could impact the time to react to an incident. In Johnson et al. (2016), guidelines for information sharing in addition to their benefits and challenges are discussed. Finally, an interesting investigation of data quality challenges in sharing threat intelligence is reported (Sillaber et al., 2016) through a series of focus group discussions (i.e., ten threat intelligence stakeholders working at security operation centers of different operating organizations). The authors reveal that despite the large number of threat intelligence sharing tools in the market, several data quality issues exist related particularly to scalability and data source integration. The authors stress that the main factors affecting shared threat intelligence data are integrating and consolidating shared threat intelligence from different sources while ensuring the data usefulness. The authors found that the data quality dimensions of timeliness and relevance are important to the security decision makers. In addition, they mention that existing threat intelligence sharing tools lack customization, filters, and new stream aggregation and search capabilities required for analysts daily work. Authors describe the advantages of using a common standard (e.g. STIX, TAXII) to share threat intelligence but in addition to standards, results from interviews show the importance of using and enforcing a common vocabulary for data entry to prevent data quality issues. Finally, authors reveal that manual data export and import from threat intelligence tools makes it hard to find quality errors which are frequently semantic.

Our survey complements the aforementioned related research work by separating TI categories. It analyzes specifically technical threat intelligence problems per type (i.e., problems of information quantity over quality and specific limitations related to each type of IOC). Then, it shows how to mitigate them. We also survey the reasons behind not sharing threat information with peers and present solutions to share this information by avoiding either attack and business risks for organizations. We show how a common standardized representation of TTI improves the quality of threat information and how this quality improves automated analytics solutions on large volumes of TTI suffering from non-uniformity and redundancy. Finally, we evaluate TI tools, which aim to share threat intelligence between organizations. In the following section, we cite most known initiatives supporting cooperation and threat information sharing between threat defenders.

4. Initiatives to encourage threat information sharing

Many national and international organizations encourage the threat information/intelligence sharing by supporting cooperation and coordination aspects between threat defenders. Some organizations focus on vulnerabilities and incident response. Others focus on identifying intrusions and potential threats. Taken together, these services provide members a current and coherent picture of the security of the IT infrastructure. We briefly review the role of most known organizations. In Skopik et al. (2016), authors give more details on these organizations.

4.1. *Incident response teams and international cooperation*

CERTs: Computer Emergency Response Teams are a vital part of every cyber security ecosystem, in a regional point of view. They collect information on new threats, issue early warnings and, could provide help on request. CERT cooperation has proved to be the most effective within regions (i.e., similarity of the participating-teams cultural backgrounds make social networking easier). However, the global nature of cyber threats also calls for international collaborations (Herzog, 2011). Therefore, CERTs are also internationally well connected with each other.

FIRST: The Forum for Incident Response and Security Teams has an effective role in building the international community of CERTs. FIRST is an organization formed in 1990 with the goal of establishing better communication and coordination between incident response teams. Today, the FIRST membership consists of about 300 teams across more than 60 countries. Organizations include educational, commercial, vendor, government and military sectors.

TF-CSIRT: The Euro-CERT group forms in May 2000 a task force of TERENA called TF-CSIRT (TF-Computer Security Incident Response Teams). Sharing statistical data about incidents in order to observe common trends, developing an European accreditation scheme, establishing education and training and assisting new teams are some of the main common objectives of this cooperation.

EGC: The European Government CSIRTs group is an informal group of governmental CERTs. Many EGC teams are members of FIRST and TF-CSIRT. The aim is to cooperate with other international CERT initiatives dealing with vulnerabilities and incident management on a global scale.

4.2. *ISACs: Information Sharing and Analysis Centers*

Information Sharing and Analysis Center is the first formal mechanism to facilitate threat information sharing. It was proposed by the U.S. government and described in Presidential Decision Directive-63 (PDD-63), published in 1998 (i.e., The U. S. CERT (USCERT) also cooperates with ISACs, by hosting meetings limited to organizations dealing with the protection of critical national infrastructure). ISACs collect, analyze and disseminate private-sector threat information to industry and government and provide members with tools to mitigate risks and enhance resiliency (National Council of ISACs, 2003). ISACs can also disseminate government information to the private sector (MITRE Corporation, 2012). It serves as a framework that enables stakeholders to develop their defense strategies across different kill chain steps. A number of ISACs have been created covering different sectors and industries (Financial, Oil&Gas, Aviation, Information Technologies, etc.) (ENISA: European Union Agency for Network and Information, 2015). Finally, several threat intelligence platforms were realized by ISAC teams. More details on these platforms could be found in Section 8.

4.3. *Other coordination initiatives*

ENISA: The European Network and Information Security Agency is the main European body aiming to improve the convergence of efforts from the different European institutions and Member States by encouraging the exchange of network and information security threats, methods and results and avoiding duplication of work.

NIST: The National Institute of Standards and Technology supports the coordination of existing CSIRTs, when responding to computer security incidents, by identifying standards, methodologies, procedures, and processes related to Computer Security Incident Coordination (CSIC). NIST provides guidance and best practices on how to cooperate while handling computer security incidents.

No More Ransom: A cooperation project between law enforcement and private sector in Europe to inform the public about ransomwares (Dutch National Police).

These initiatives are not without limitations. Legal requirements, sensitivity and criticality of data are examples of most known issues that are behind reluctance to expand cooperations. Legal requirements especially concern international cooperation. As for sensitivity of threat data, participating companies still have a reluctant position in revealing potential threats to their peers and the government (MITRE Corporation, 2012). Another important issue that affects ISAC operations concerns the overall approaches that are used to exchange information (MITRE Corporation, 2012). All these limitations have reduced the benefits of information sharing and thus limited the cooperation between participants.

5. TI sharing problems

The benefits of collective sharing and learning from extended and shared threat information are undeniable. Yet, various barriers limit the possibilities to cooperate. In the sequel, we detail some of these benefits and expose the reasons behind not to share threat information.

Table 2 – Reasons for not to share.

1	Fearing negative publicity	(Chismon and Ruks, 2015; Choo, 2011; Peretti, 2014; Richards, 2009)
2	Legal rules, Privacy issues	(ENISA: European Union Agency for Network and Information Security, 2013; Murdoch and Leaver, 2015; Peretti, 2014; Skopik et al., 2016)
3	Quality issues	(ENISA: European Union Agency for Network and Information Security, 2013; Ponemon, 2015; Ring, 2014; Sillaber et al., 2016)
4	Untrusted participants	(ENISA: European Union Agency for Network and Information Security, 2013; Murdoch and Leaver, 2015; Ponemon, 2015)
5	Believing that the incident is not worth to share	(Chismon and Ruks, 2015; Choo, 2011; Ring, 2014)
6	Budgeting issues	(Ring, 2014; Skopik et al., 2016)
7	Natural instinct to not to share	(Ring, 2014)
8	Changing nature of cyber attacks	(Ring, 2014)
9	Unawareness of the victimized organization about a cyber incident	(Choo, 2011)
10	Believing that there is a little chance of successful prosecution	(Choo, 2011)

5.1. *Benefits of TI sharing for collective learning*

Many organizations and participants today agree on the importance of threat information sharing for many reasons. First, the exchange of critical threat data has been shown to prevent potential cyber-attacks and mitigate ongoing attacks and future hazards. According to Bipartisan Policy Center (2012), leading cyber crime analysts recognize that public-private cyber information sharing can speed identification and detection of threats. Thus, if organizations are able to find an intruder in his active phases, they have a greater chance of stopping the attacker before data is stolen (Zurkus, 2015). In addition, threat sharing is a cost-effective tool in combating cyber crime if properly developed (Peretti, 2014; Ponemon, 2014). In Gilligan et al. (2014), a study on the economics of cyber security identified a number of "investment principles" for organizations to use in developing data security programs with high economic benefit. One of these principles is the participation in multiple cyber security information sharing exchanges. Advantages of sharing include also a better situational awareness of the threat landscape, a deeper understanding of threat actors and their TTPs, and a greater agility to defend against evolving threats (Zheng and Lewis, 2015). This is approved in a recent survey (Ponemon, 2015), where 692 IT and IT security practitioners are surveyed across various industries. Results reveal that there is more recognition that the threat intelligence exchange can improve an organization security posture and situational awareness. More broadly, sharing threats improve coordination for a collective learning and response to new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors (Zheng and Lewis, 2015). Many attacks do not target a single organization in isolation, but target a number of organizations, often in the same sector (Chismon and Ruks, 2015). For example, a company can be damaged when a competing business's computers are attacked, since the information stolen can often be used against other organizations in the same sector.

5.2. *Reasons for not sharing*

Despite the obvious benefits of sharing threat intelligence, a reluctant position in reporting breaches is observed. The issue was seriously highlighted at a pan-European level when ENISA, the EU's main cyber-security agency, published a report (ENISA: European Union Agency for Network and Information Security, 2013) in 2013, capitalizing intentionally the word "SHARE". The report warned around 200 major CERTs across the Europe that "the ever-increasing complexity of cyber-attacks requires more effective information sharing" and that organizations were not really involved in doing so. In its last report on threat landscape published in early 2017 (ENISA: European Union Agency for Network and Information, 2017), ENISA continues to recommend sharing information as a mitigation vector for malwares. Authors recommend the development of methods for the identification and sharing of Modus Operandi without disclosing competitive information.

Many concerns are deterrent to participation in such sharing initiative. We identify in Table 2 ten major reasons for not sharing threat information by order of importance.

Fearing negative publicity is one of the main reasons for not sharing threat information which could result in a competitive disadvantage (Chismon and Ruks, 2015; Choo, 2011; Peretti, 2014; Richards, 2009), e.g., competitors might use the information against victimized organization. In some sectors, even a rumor of compromise can influence purchasing decisions or market valuations (Bipartisan Policy Center, 2012).

Legal rules and privacy issues are also cited among the most important reasons for not to share (ENISA: European Union Agency for Network and Information Security, 2013; Murdoch and Leaver, 2015; Peretti, 2014; Skopik et al., 2016). Organizations may be reluctant to report an incident because they are often unsure about what sort of information can be exchanged to avoid legal questions regarding data and privacy protection. In the same country legal rules may not be the same for the collaborating parties. Affiliation to a specific sector for example might force adherence to specific regulations (ENISA: European Union Agency for Network and Information Security, 2006). Regarding international cooperations, confidence between cooperating teams while handling sensitive information is most of the time prevented by international regulations that limit the exchange and usage of such information. Teams working in different countries have to comply to different legal environments. This issue influences the ways the teams provide their services, the way they treat particular kinds of attacks and therefore limits the possibilities to cooperate, if not making cooperation impossible (Skopik et al., 2016).

Quality issues are one of the most common barrier to effective information exchange, according to different surveys realized on CERTs and other similar organizations (ENISA: European Union Agency for Network and Information Security, 2013; Ponemon, 2015; Ring, 2014; Sillaber et al., 2016). Data quality includes relevance, timeliness, accuracy, comparability, coherence and clarity. For example, many interviewees report that a lot of what is shared is usually a little bit old and becomes not actionable. It is also not specific enough to aid decision-making process.

Untrusted participants is also cited in recent surveys (ENISA: European Union Agency for Network and Information Security, 2013; Murdoch and Leaver, 2015; Ponemon, 2015) among the crucial obstacles to effective communication between organizations. Some interviewees in ENISA: European Union Agency for Network and Information Security (2013) have pointed that trust is undermined when only few parties are active in a sharing program, without getting much in return from the other parties. In Murdoch and Leaver (2015), authors explain that the conflict between the need for sharers to keep anonymity while ensuring that recipients still trust the information (i.e. even when the source is unknown), is a barrier to participate in a threat intelligence sharing platform. Believing that the incident is not worth to share is also commonly stated (Chismon and Ruks, 2015; Choo, 2011; Ring, 2014). The victimized organizations simply deal internally with the incident believing that it is not serious enough to warrant reporting it to an external party including law enforcement and other competent agencies.

Budgeting issues are reasons to limit building a valuable level of cooperation (Ring, 2014; Skopik et al., 2016). Some interviewees have stated that qualified real time threat intelligence is typically expensive to receive/share. They think that they are mainly dedicated to big organizations. Yet third party providers generally offer a discount to their TI platform subscribers for their willingness to share threat information in addition to consume it (Piper, 2013).

The natural instinct for organizations to not share is another problem of sharing (Ring, 2014). In some organizations, there is still the perception of a blame culture (i.e., if something happens then obviously it is somebody's fault and he needs to pay the price). Thus, people are naturally reticent about advertising it too widely.

The changing nature of cyber attacks which are becoming increasingly personalized is highlighted (Ring, 2014). Even if organizations succeed in sharing data on an attack, especially when these organizations fall in the targeting scope of a given adversary (cf. the Waking Shark II exercise (Keeling, 2013)), the issue of personalized attacks do not help them to defend themselves. This moves to a different kind of intelligence requirement.

The unawareness of the victimized organization about a cyber incident is another reason for not sharing threat information (Choo, 2011). When asked, analysts indicate that they had not experienced any such incidents. Yet the organization has been attacked one or more times.

Believing that there is a little chance of a successful prosecution (Choo, 2011) discourages organizations to report an incident to law enforcement and other competent agencies.

It is worth noting that some of these aforementioned concerns have been alleviated by recent government measures (Peretti, 2014) (e.g., Legal rules). However, in all cases, organizations should understand any potential risks associated with exchanging TI and take steps to mitigate such risks. The good news is that organizations are making strides in sharing threat data. The question that should be asked now is: how useful are these shared threats and how long they remain worthy of alerting/blocking?

6. Technical threat intelligence limitations

While a decade ago, no one was talking about threat intelligence except government agencies, as depicted in Fig. 2, organizations attempting to have technical threat intelligence are now overwhelmed with a massive amount of threat data (Chismon and Ruks, 2015; Zurkus, 2015), leaving them challenged with identifying what is relevant. A problem of quantity over quality is then appeared.

6.1. *Quantity over quality*

Most security teams cannot make valuable use of their threat data because there is just too much of them. The daily dump of indicators seen as suspicious in Internet, provides information approximating 250 to millions of indicators per day (Trost, 2014), which allows consumers to pivot around and glean their own intelligence. The brain power needed to analyze at the speed at which the threat data is produced is, thus, humanly impossible (Zurkus, 2015).

Timeliness of information is also very important when protecting against aggressive attackers and zero-day exploits. According to (Ponemon, 2013), 57% of surveyed IT professionals say the intelligence currently available to their enterprises is often out of date to enable them to understand the motivations, strategies and tactics of attackers and to locate them. In a more recent survey of IT professionals (Ponemon, 2014), the authors report that most of the threat information the IT professionals received was not timely or specific enough (i.e., actionable) to meet their perceived need. Finally, according to a recent survey (Ponemon, 2015), threat intelligence needs to be timely and easy to prioritize. In this latter survey, 66% of respondents who are only somewhat or not satisfied with current approaches explain that the information is not timely. On the other hand, 46% complain that the threat information is not categorized according to threat types. This is approved in (Ring, 2014), where the author explains that qualified real-time threat intelligence is typically expensive, otherwise, most available commercial and open source threat intelligence products are not effective enough, or provide information that is out-of-date.

6.2. *IOC specific limitations*

Let us now deal in more details with the limitations of each type of indicator of compromise as categorized in Fig. 1.

6.2.1. *Network indicators*

A number of network indicators can be collected as TTI (as shown in Section 2.2.2). Attackers use in some cases different

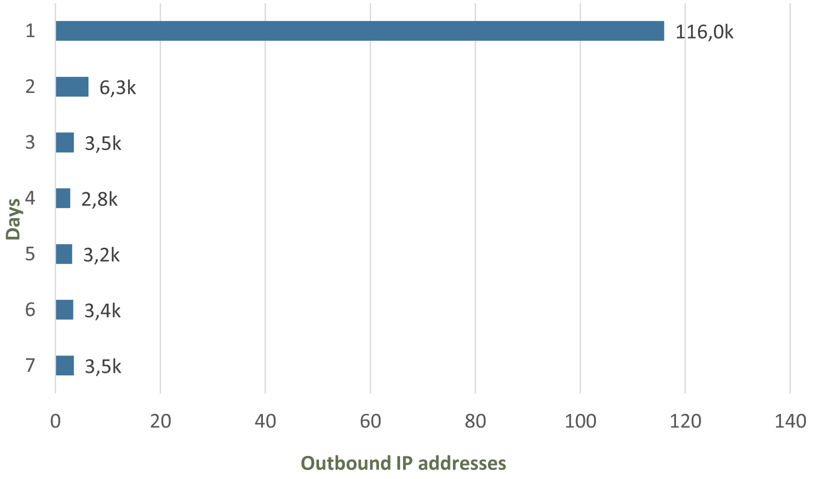


Fig. 3 – Count of indicators by days as observed in (Verizon, 2015) in at least one feed.

nodes from which to conduct attacks to a targeted victim. In other cases, they use the same node for multiple victims. Thus, an IP address that has been observed by others, functioning as a C&C (Command and Control) node can be a useful indicator (cf. Appendix, for more details). However, attackers often use different IP addresses, changing C&C nodes as they are discovered or as victimized computers become unavailable. Regarding domain names, a malware will attempt to connect to a domain name, which can then be pointed to the IP address the attacker is currently using. It is also considered as a useful indicator when a malware uses a hard-coded domain. However, it is quite common for malwares to use a domain generation algorithm to avoid the need to connect to the same domain twice. In such case, a domain name has little value as an IOC (Chismon and Ruks, 2015). A stark detail in Verizon (2015) illustrates such indicators value. The most important experiments conducted in this field are to determine (1) the IP addresses cumulative uniqueness (i.e., the overlap between the IP address feeds), (2) the time needed for an attack to spread from one victim to another and (3) the time validity of the IP address.

Cumulative uniqueness observations: During six months, Niddel (Pinto and Sieira, 2015) combined daily updates from 54 different sources of IP addresses and domain names tagged as malicious by their feed aggregator TIQ-Test (Niddel Corp.). The company then performed a cumulative aggregation (i.e., if ever two different feeds mention the same indicator throughout the six-month experimental period, they would be considered to be in overlap on this specific indicator). To add some context to the indicator feeds being gathered, Niddel separated them in groups of inbound feeds (i.e., information on sources of scanning activity and spam/phishing e-mail) and outbound feeds (i.e., information on destinations that either serve exploit kits, malware binaries, or even locations of C&C servers). The results show significant overlap only on the inbound feeds, which is in some way expected as everyone gets probed and scanned all the time. However, despite everyone is generally subjected to the same threats, the overlap in outbound feeds is surprisingly small, even with a long exposure of six months' time. This result suggests that either attackers are using huge numbers of IP addresses (i.e., Organizations would need access to all threat intelligence indicators in order for the information to be helpful, which is a very hard task) or only a minority of IP addresses contained within the feeds are of intelligence value. It is likely that the truth is a mixture of both explanations (cf. experience in Time validity observations).

Time spread observations: Experiments on attacks observed by RiskAnalytics (Verizon, 2015) display some pretty interesting and challenging results: 75% of attacks spread from Victim 0 to Victim 1 within 24 hours and over 40% hit the second organization in less than an hour. These findings put quite a bit of pressure on the security community to collect, vet, and distribute IOC very quickly in order to maximize the collective preparedness. Let us assume that indicators are shared quickly enough to help subsequent potential victims. The next question that needs to be answered is: how long we can expect those indicators to remain valid (i.e., malicious, active, and worthy of alerting/blocking).

Time validity observations: RiskAnalytics has already studied the question of IP addresses validity. Fig. 3 shows how long most IP addresses were on the block/alert list. The graphic is restricted to seven days of outbound IP address feeds.

While some IP addresses remain valid for some time, most do not last even a day. These findings track well with Niddel's cumulative uniqueness observations where the overlap in outbound feeds is very small. According to Verizon (2015), these results reflect an urgent need to share quickly: "the faster you share, the more you theoretically will stop". Recall that these are results from one data source which is geared toward threats of a more opportunistic, high-volume, and volatile nature (e.g., brute forcing, web application exploits, etc.), rather than more slow targeted attacks. With targeted attacks, sharing IOC faster is not always useful (cf. Discussion in Section 7.1).

6.2.2. *Malware indicators*

A growing sophistication in the evolution of malware has been noticed (Choo, 2011). Knowing that modified malware do not require great skills or resources, attackers reuse malware to keep ahead of the anti-malware industry and security professionals. They adapt their "products" over time employing many different obfuscation techniques. The simplest way is to change a single bit in the binary, then a different hash will be obtained. Attackers can use open source tools and make more complex modifications to change the hashes. The Zeus bot malware creator kit is an example of easy-to-use toolkits. It can be bought or found for free on some underground forums (Falliere and Chien, 2009) with detailed instructions on how to use such kits. Any individual including one with limited programming or hacking skills could use such kits to create sophisticated malwares or customize them to his own needs and launch advanced attacks. A study realized by Symantec (Fossi et al., 2010) has shown nearly 90,000 unique variants of the basic Zeus toolkit in 2009, which was the second most common new malicious code family observed in the Asia Pacific/Japan region in that year. The widespread availability of such toolkit facilitates the commitment of cyber crime. Consequently, there is a marked increase in the number of amateur cyber attackers who make their pocket money from distributing spam or selling stolen credentials and information (Choo, 2011). Indicators such as created registry keys or file artifacts can be more useful for threat intelligence as they are less commonly changed by attackers, even if it is still possible to give dropped files a random or pseudorandom component in their names.

6.2.3. *Email indicators*

A large number of attacks start with a phishing or spear phishing attack, containing either a document exploit or simply a malware disguised as something benign. Thus, email indicators can provide useful threat intelligence. Attackers often ensure that emails are either targeted or generic (Choo, 2011). Sharing generalist feeds of spam email subjects will be less useful than details of phishing emails sent to similar organizations.

7. Discussion

7.1. *Sharing faster is not sufficient*

As seen before, a variety of security vendors and open source providers offer now a wide assortment of threat feeds of the latest indicators of compromise (Williamson, 2016). The idea behind these threat feeds is generally the same. As attackers are getting faster, security providers find a way to quickly aggregate and share the latest threats that have been seen. Timeliness of threat information is very important when protecting against aggressive attackers and zero-day exploits, but in many cases, threat feeds of TTI can simply amount to faster signatures that still fail to track the attackers. Actually, a key failing of TTI is that it is relatively simple for an attacker to target a specific organization in a way that ensures no pre-existing indicators will have been available. For example, specific network indicators may only be used once in the case of a true targeted attack. In addition, a large percentage of malwares used in breaches were reported unique to the organization that was infected (Shackleford, 2015; Verizon, 2015). Clearly, if a threat is only used once, as for targeted attacks, faster sharing of IOC alone is not going to solve the problem. Actually, targeted attacks need targeted defense as well (Chismon and Ruks, 2015).

To defend against this new trend of personalized attacks, organizations need to focus not only on gathering and sharing threat data across their industry sector, but also on their individual threat analysis and incident response (Ring, 2014). Obviously, they cannot protect themselves if they do not know what they are protecting against and who are their adversaries (Pepper, 2015; Zurkus, 2015). To realize such need, internal audit should be done regularly to understand organizations internal and external vulnerabilities. The objective is to make assumptions about what the attacker can do and to get an initial response, a one step forward by focusing on specific devices and attacks investigations.

7.2. *Reducing the quantity of threat feeds*

The other important concern is about the large amounts of data sold as technical threat intelligence which lack contextual information. Certainly, anything that leads to the discovery of an incident is worthwhile, but in most cases, context is key. Adding the context in which previously detected attacks have taken place, enables a wider audience to make a broader defensive capability. Additional context includes indicator role, kill chain stage, originating MD5, malware family and/or adversary group (Trost, 2014). It could also be attack methodology (tactic information) and attack targeted sector (operational information). The heart of the issue is that the vast majority of information included in threat feeds are made to answer a question to a particular test. If the question on the test is changed, then the data become usefulness (Williamson, 2016). In such case, an atomic indicator has its own life which has no value to be shared with others.

Facing this challenge, the following solutions could be worth considering. Security teams need to contextualize the threat data they collect with the specific vulnerabilities and weaknesses they have internally (Bellis, 2015). For this purpose, they should select the data they collect, or build/purchase large analytics platforms to cope with the quantity of data. There are massive dedicated teams, cleaning the Internet, looking at the targeted attacks, analyzing staff and trying to find associations (i.e., indicators associated to targeted attacks). Following the same idea, it is suggested in (Ring, 2014), to use managed security services, as more and more organizations start to outsource this area. In this case, the question of trust is raised.

Regarding the huge flow of malware variants which is gaining access to networks and computer systems or reaching organizations honeypots, it is impossible to handle them individually. Identifying the mutations of malware variants is essential in order to recognize those belonging to the same family. Data science and machine-learning models are looking to deliver entirely new ways of searching malwares. Instead of taking a 1-for-1 approach where each threat is mapped to a signature or/and IOC, data science models are analyzing a huge amount of threats, to learn what they all have in common. Methods of malware analysis, detection, classification, and clustering should be either automated or designed in such a way that makes future automation possible (Ghanaei et al., 2016). As for new research work, in (Ghanaei et al., 2016), the authors propose a supervised learning method based on statistics to classify new malware variants into their related malware families. In the same vein, VirusBattle (Miles et al., 2014) is a prototype system that employs state of the art malware analyzes to automatically discover interrelationships among instances of malware. This solution analyzes malware interrelations over many types of malware artifacts, including binaries, codes, dynamic behaviors and malware metadata. The result is a malware interrelation graph.

Cuckoo (Guarnieri et al., 2016) and Malheur (Rieck, 2013) are well-known open source platforms that automate the task of analyzing malicious files in a sandbox environment. Cuckoo uses static analysis (i.e., code or binary analysis) and dynamic analysis (i.e., behavior analysis) (Oktavianto and Muhardianto, 2013) whereas Malheur uses dynamic analysis. To identify a malware family using Cuckoo, one can create some customized signatures that can be run against the analysis results in order to identify a predefined pattern that might represent a particular malicious behavior. On the other hand, Malheur uses machine learning to collect behavioral analysis data inside sandbox reports and categorizes malwares into similar groups called "clusters" (Rieck et al., 2011). Malheur builds on the concept of dynamic analysis, which means that malware binaries are collected in the wild and executed. The execution of each malware binary results in a report of recorded behavior. Malheur analyzes these reports for discovery and discrimination of malware classes using machine learning.

Now, well known public sandboxes such as Cuckoo and Malheur become highly detectable by malwares (Ferrand, 2015; Issa, 2012). Once such systems are made publicly available, malware authors try to protect themselves and to evade detection by checking whether they are in an emulated environment or in a real one (e.g., by checking the execution time). To face this issue, new researches are made. For example, in Ferrand (2015), the author shows that with few modifications and tricks on Cuckoo and the virtual machine, it is possible to prevent malwares to detect that they are under analyze, or at least make this detection harder.

7.3. *Trust to share threat data & to save reputation concerns*

Effective sharing requires trust. Since shared threat data might be sensitive (e.g., they reveal that an organization has been attacked), organizations will be reluctant to share when they are not in a trusted environment.

Trust is important for many reasons. First, sensitive information can be used for negative publicity. This is approved in some studies on the economic cost of sharing security data which have demonstrated that sharing can result in a loss of market due to negative publicity (Campbell et al., 2003; Cavusoglu et al., 2004). To avoid such consequences, techniques for fine-grained and context-based access control are critical to protect confidentiality and privacy of data (Tounsi et al., 2013). Second, if not shared in a trusted environment, threat data could also be contaminated by malicious activity and contain erroneous information. In such case, establishing trust requires at least authentication of transmissions and encryption of content. To avoid the consequences of identity revelation, anonymous sharing is another solution that provides participants a channel in which they can communicate anonymously. In a recent work (Dunning and Kresman, 2013), the authors have developed an algorithm to anonymously share private data between participants.

Trust is also important on another level. It is generally unwise to allow threat actors to learn what you know about them, lest they change their methods. Thus, closed and trusted groups can enable deeper sharing than would otherwise be possible (e.g., groups of organizations via community Cloud platforms). Generally, the more a group can trust its members and the security of information within the group, the more effective the sharing tends to be (Chismon and Ruks, 2015). However, a certain level of trust in the group should be guaranteed. If a participant believes there is more consumption of the threat information than sharing in the network, the motivation to share information will rapidly decline. To address this issue, some research work have been initiated. In Cascella (2008), the game theory with the prisoner's dilemma approach is employed to model the interactions of rational and selfish nodes in distributed systems. The study shows that by incepting a reputation system, it is possible to distinguish good players (threat sharers) and bad players (threat consumers). In Seredynski et al. (2007), a sanction mechanism that makes a decision to discard/forward packets is proposed based on an evolving genetic algorithm. The aim is to enhance trust between several nodes transmitting data packets. However, in a voluntary threat sharing mechanisms, the use of sanction and punishment would not be very interesting. Other researches have shown that instead of punishing, encouraging good behaviors increases the likelihood of participants to be more involved in a sharing program in the long run. For example, participants that receive social approval can have a significant positive impact on cooperative behavior (Cook et al., 2013). It is also shown that having organizations involved in the quality assurance process improves the cooperation among participants and increases the level of trust (Gerspacher and Lemieux, 2010). Finally, it is concluded in Furnell et al. (2007) that competitive advantage of threat intelligence can be gained for whoever side employs social factors better, involving human, social and organizational matters that are mostly uncharted on the computer security research agenda. For example, assuming that face-to-face interactions usually occur in a trusted environment (MITRE Corporation, 2012), the one-to-one human contacts can be one of the simplest, yet most effective and trusted sources of actionable information (Chismon and Ruks, 2015).

7.4. *Standards for TI representation and sharing*

Sharing security knowledge between experts across organizations is an essential countermeasure to recent sophisticated attacks and organizations can benefit from other organizations' experiences to build a collective knowledge (Williamson, 2016).

Organizations have traditionally shared threat information using ad-hoc solutions such as phone calls, encrypted emails, or ticketing systems. More recently, they used portals and blogs, a trend to building interconnected communities with associated platforms to exchange semi automatically threat information (Sillaber et al., 2016). LSA (Latent Semantic analysis) (Landauer et al., 1998) was used to find semantically related topics in web blog corpus. Important keywords of each topic are assigned quantitative measure through PLSA (Probabilistic LSA) (Hofmann, 1999). The results prove the efficiency of this approach to broadly search security related news in massive web blogs. However, this approach was limited because of the limitation of web blogs in representing threat scenarios in a real-time and structured manner. In Li et al. (2007), authors focus on the problem of true threat identification where network security data are managed at distributed locations. The authors provide several means of finding correlations between alerts arriving from distributed components. The major limitation of this work is once more the lack of standardization as alert data need to be converted to a uniform representation given the multiple TTI sources of information. A concept that has emerged is the use of a threat intelligence libraries, named also threat intelligence platforms (Poputa-Clean and Stingley, 2015). These libraries were designed to solve the collection and storing problems of TTI and to facilitate sharing threat information with other organizations. However, efficient automation and collection from diverse set of products and systems require structured and standardized threat information representation (Barnum, 2014; Wagner et al., 2016), which is expected to be expressive, flexible, extensible, machine-parsable and human-readable (Barnum, 2014; Heckman et al., 2015).

Several efforts have been made to facilitate threat information sharing in a standardized manner. IODEF (Danyliw et al., 2017), RID (Moriarty, 2012), STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information) (Barnum, 2014), OpenIOC (Open Incident of Compromise) (Mandiant, 2010), CyBox (Cyber Observable Experssion) (MITRE, 2011), VERIS (Vocabulary for Event Recording and Incident Sharing) (Verizon), CAPEC (Common Attack Pattern Enumeration and Classification) (MITRE, 2007), MAEC (Malware Attribution and Enumeration Characterization) (MITRE, 2013) and ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) (MITRE, 2015) are popular examples of such standardized efforts. Despite these initiatives of standardization, an interesting survey from SANS (Shackleford, 2015) indicates that in 2015, only 38% of organizations are using TI data in standard formats and well-known open source toolkits. In order to select the right standard for a particular use case, authors in Burger et al. (2014) provide an agonistic framework in which standards can be evaluated and assessed. In the sequel, we briefly examine the aforementioned standards.

STIX and TAXII have appeared as an improvement initiatives to IODEF and RID, where, RID and TAXII are the transport protocols for IODEF and STIX respectively. Formerly developed by the MITRE corporation, STIX and TAXII are sponsored by the Department of Homeland Security (DHS) office of cyber security and communications. They have been introduced to combine human and machine data to share information.

Today, STIX is the most commonly used standard (Shackleford, 2015) even though, it is very complex to implement (Kampanakis, 2014). STIX is modular and can incorporate other standards efficiently (Burger et al., 2014). The STIX architecture is composed of eight core cyber threat concepts: Campaigns, Indicators, Observables, TTP (Tactics, Techniques and Procedures), Incidents, ThreatActors, ExploitTargets and Courses of Action.

STIX can embed CybOX, IODEF and some OpenIOC extensions, in addition to XML namespaces, extensions for YARA rules (Google Inc. et al., 2014), Snort rules (Snort IDS team, 2002), and non-XML bindings (i.e., using JSON). STIX uses CybOX to represent Observables. CybOX is a schema for the specification, capture and characterization of observable operational events. STIX can also include IODEF in place of the IncidentType extension and OpenIOC extensions in place of CybOX, to express non-standard Indicator patterns.

XML namespaces that STIX can embed are the MITRE CAPEC, MAEC and ATT&CK, to cite a few. CAPEC schema attributes characterize how cyber threats are executed and provide ways to defend against these threats. MAEC schema provides a standardized language about malwares based on artifacts, behaviors and attack patterns. ATT&CK was released as a framework of adversary post-compromise techniques (Strom, 2016). It describes patterns to characterize adversarial behavior on the network and end-points to achieve its objectives in a standard way. Since CAPEC enumerates a range of attack patterns across the entire cyber attack life-cycle (i.e., not just techniques used during post-compromise), the CAPEC ID references are added to the attack pattern descriptions in ATT&CK. For malware researchers using YARA for regular expression matching/analysis and for communities whose interest is intrusion detection using Snort, there are extensions for YARA and Snort rules supported by STIX (Kampanakis, 2014). YARA is an engine and language for scanning files and memory blocks. When a rule matches a pattern, YARA presumes to classify the subject according to the rule's behavior. Snort is an open source packet analyzer with intelligence to match rule sets and trigger actions when there are expression matches (Burger et al., 2014). Finally, VERIS system is a characterization of cyber incidents after they have occurred, which is intended for strategic trend analysis and risk management and metrics framework.

These multiple efforts to obtain different data ontologies for threat information sharing are not without disadvantages. These ontologies often overlap and do not offer a solution to the entire community (Burger et al., 2014). There could be duplications and gaps in the threat information ontologies in different communities, which lead to a duplication of effort for effective collaboration. Thus, there is a need for participants to have a common language and toolset to facilitate sharing and threat analytics.

7.5. *Big data analytics for threat intelligence*

The proliferation of sophisticated cyber attacks and consequently the huge size of available indicators of compromise (i.e., GB of threat data are handled per day) make it paramount to automate both information gathering and analysis, considering the diverse sources of threat data and their complexity. The analysis of these data requires the development of big data engines and architectures, which should take into account both real time information and history records in order to provide an effective threat intelligence. Threat intelligence libraries or platforms were designed to solve the collection and storing problems of TTI and to facilitate sharing threat information with other organizations in the threat intelligence space (Poputa-Clean and Stingley, 2015). They are large repositories that often use big data technologies (e.g., for data warehousing and graph analysis) to draw links between the different types of TTI, with the aim of analyzing and generating quicker response to the detected threats, as well as an historical record of the received IOC. Structured and/or standardized representation of TTI could be used with different data ontologies. More information on threat intelligence platforms can be found in Section 8.

However, because of the limited available mechanisms to automatically validate TTI reports before sharing them (Qamar et al., 2017), standardized reports are usually generated by a threat intelligence analyst. The aim is to maintain the quality of the threat information before sharing it, by assessing the fidelity of the sources and methods used to collect and generate this information. Despite this hard manual work, threat data often include incomplete, incorrect or redundant information, since threat data are shared between different participants, aggregated from different sources and linked to other data already present in the data sets. This non-uniformity, as well as redundancy of data, makes it more challenging to analyze a sample TTI report and to identify its relevance for a particular community.

An automated analytics derived from data is one solution. In Qamar et al. (2017), the authors propose a framework named STIX-Analyzer to perform analytics on data obtained from existing repositories of intelligence standards (i.e., STIX/TAXII). The objective is to identify threat relevance in a given community. The solution relies on a data-driven approach, which is tightly dependent, again, on the quality of imported information.

To prevent data quality issues in order to obtain better automated analytics, authors Sillaber et al. (2016) emphasize the need to use a common vocabulary to enter data in threat intelligence platforms. Examples of common vocabulary are: a common language for full-text data fields, a common understanding of flags, tags and meta-data. For example, In STIX, an IOC can appear in four different places (Trost, 2015), as follows, making harder the automatic analysis of TTI:

STIX- > Indicator
CybOX- > Observable
STIX- > Description
STIX- > TTP

Thus, the quality of threat information remains an important issue. Using a common standard to share threat information and intelligence as discussed in Section 7.4 is a first step to improve the quality of imported and shared data. However, it is also important to use and enforce a common vocabulary when entering data in threat intelligence sharing tools (Sillaber et al., 2016) to provide better automated analytics solutions on large volumes of threat data.

8. Threat intelligence tools evaluation

Now that organizations have found ways to collect a huge amounts of information from a wide variety of sources using threat libraries, they are in need of tools to manage the flow of information and convert it into knowledge and actions. Although the existing TI tools need to mature more (Shackleford, 2016), they have been able to achieve a level of maturity that enables organizations to start filtering and sharing information effectively (Brown et al., 2015). There are several open source projects and commercial enterprises offering products to access to threat intelligence. These solutions aim mainly at content aggregation and collaborative research such as IBM X-Force Exchange (IBM, 2015), Alienvault OTX Pulse (AlienVault, 2015), Checkpoint IntelliStore (Checkpoint, 2014), and Crowdstrike intelligence exchange (CrowdStrike Inc., 2014). Other solutions are focused on TI advanced management options and some of them provide the possibility to have private instances. These include, Threatstream (Anomali, 2015), ThreatQuotient (ThreatQuotient, 2015), ThreatConnect (Threatconnect, 2011), MISP (Andre et al., 2011), CRITs (MITRE, 2013), Soltra Edge (Soltra, 2014), CIF v3 (named also bearded-avenger) (CSIRT Gadgets, 2016) and Threatelligence (Phillips, 2014). We are interested in free and/or open source tools that are offering advanced management options, which we compare to AlliaCERT TI tool (AlliaCERT, 2016).

8.1. *Presentation of selected tools*

Some of the aforementioned tools have begun to gain popularity as they promise a more organized storage of the IOC. We name MISP, CRITs, Soltra edge and CIF v3. Other tools are no more usable in their open source version because of using old librairies e.g., Siemens Django Mantis Intelligence framework, or they are simply no more supported. In the following, we focus on the first ones with an introduction of the AlliaCERT TI tool (AlliaCERT, 2016). This is followed by an evaluation of the selected tools according to different functional dimensions (cf. Section 8.2). Technical information related to these tools is taken from various sources: official tools sites, white papers, research articles, live interactions with some of the tools authors as well as AlliaCERT software testers.

MISP (Andre et al., 2011) (Malware Information Sharing Platform) is an open source software solution mainly developed by the Belgian Defense CERT and the NATO Computer Incident Response Capability (NCIRC). It aims at collecting technical and non-technical information about malware and attacks, storing data in a standardized format, and distributing and sharing cyber security indicators and malware analysis with trusted parties. MISP is a community based solution where multiple instances of the platform hosted by different members can be interconnected. Then, MISP synchronizes the information between them (The NATO Communications and Information Agency, 2014). MISP provides functionalities to support the exchange and the consumption of information by Network Detection Intrusion System (NIDS), LIDS, log analysis tools and SIEMs (Belgian Ministry of Defence (CERT), 2012). To improve IOC description, MISP has integrated the ENISA threat taxonomy to the vocabulary used in the tool (ENISA: European Union Agency for Network and Information Security, 2017).

CRITs (MITRE, 2013) (Collaborative Research into Threats) is an initiative from MITRE Corporation which open sourced the project in 2013. CRITs is a platform that provides analysts with the means to conduct collaborative research into malware and threats. It plugs into a centralized intelligence data repository, but can be also used as a private instance.

Soltra Edge (Soltra, 2014) Initiated by the Financial Services Information Sharing and Analysis Center (FS-ISAC), the basic free version of Soltra Edge is named Avalanche. Though it started as a free model, it is now developed into a quasi-commercial product supported by Soltra. It supports a community defense model that is highly inter-operable and extensible. It is built with industry standards including STIX and TAXII.

CIF v3 (CSIRT Gadgets, 2016) (Collective Intelligence Framework) was developed by REN-ISAC, the Research and Education Networking Information Sharing and Analysis. The last version is named *bearded-avenger*. CIF v3 helps to aggregate, normalize, store, post process, query, share and produce data sets of threat intelligence. It pulls in various data-observations from multiple sources and creates a series of observations "over time" (eg: reputation). When there is a query for data, a series of observations are output chronologically (Iovino, 2016). Regarding the exchange of data with peers, CIF requires to give an API token to a peer and use the "smrt plugins" to pull data with REST/JSON calls. In CIF v3, a new ZeroMQ technology is in progress named ZYRE[1]. This technology enables users to connect their CIF-routers together over a P2P (Peer-to-Peer) style framework.

Threatelligence (Phillips, 2014) is a cyber threat intelligence feed collector, using ElasticSearch, Kibana and Python. It was created in 2014 by a professional and a very implicated developer in cyber security. It fetches TI data from various custom or public sources into ElasticSearch while slightly enriching them (i.e., looking for geographic locations). It automatically updates feeds and tries to further enhance data for dashboards. The dashboards which are built using Kibana, are used to display data and make easy searching through them. Threatelligence was designed to be as generic as possible to be able to easily add custom sources of TI with all types of data or to produce intelligence.

AlliaCERT TI tool (AlliaCERT, 2016; Tounsi et al., 2017) is a cyber threat intelligence collector and correlator which was designed by the AlliaCERT Team in 2016. The main goal of the AlliaCERT TI project is to collect security-related information from multiple sources and to provide mechanisms to query, correlate, and share it. The first priority of AlliaCERT team was to ensure speed response and search of IOC. AlliaCERT TI tool proposes a reputation analysis module which searches for history of indicators of compromise as well as real time information from referenced sources including forums and social networks (e.g., Twitter). It also searches in real time whether a legitimate domain is used in a phishing campaign or in other targeted attacks. This module includes an anti-cybersquatting option, allowing to know if a brand is targeted by an attacker to degrade its reputation. Users have also the possibility to create triggers to receive afterwards alerts every time a new suspected phishing URL is detected and to export results into different formats such as XML and PDF.

The AlliaCERT team has focused its efforts to improve the context of an attack before sharing it. First, the AlliaCERT TI tool refines the results by correlating them using more than 150 sources of information (e.g., OSINT, honeynet, client incidents). This serves for example to search with precision whether a requested URL is a phishing, has hacking potential or has a reputation score that deems it untrustworthy. The tool adds a relevance parameter for each identified IOC depending on the source of information. It also proposes an additional feature that allows users after identifying an IOC to check malicious files and to analyze their behaviors with a sandbox service using dynamic and static approaches.

Sources of Alliacom AlliaCERT TI tool are frequently checked and results in the dashboard are updated (i.e., once an hour) to enrich the obtained information about threats. One of the private privileged sources of AlliaCERT TI tool is the Lebahnet honeynet (Malaysia CERT, 2005), a passive honeypot based distributed system used to emulate vulnerabilities of most used operating systems and to trap attackers via attractive websites. AlliaCERT team has contributed with five instances of the honeynet by installing its sensors in four different European countries (i.e., two in France, one in Netherland, one in Poland and one in Germany). As output, users obtain detailed results about the attempted attacks, e.g., steps of a given attack, attacker profile, cf. Fig. 4.

8.2. *Comparative discussion*

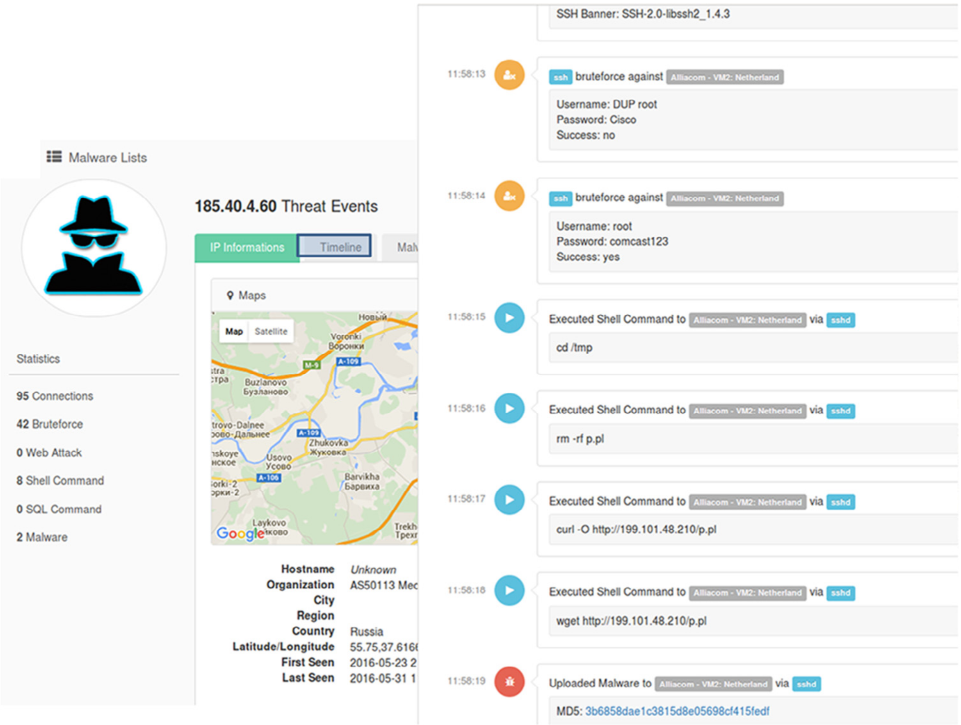
The market maturation is encouraging all of the TI vendors and open-source initiatives to adopt a common set of features. Among these core features the following gain importance (Poputa-Clean and Stingley, 2015): (1) Integration with security tools (i.e., SIEM and SIEM-like systems, other detective and preventive control tools), (2) Data enrichment (i.e., the possibility of integrating other intelligence platforms, seamlessly ingesting OSINT and commercial feeds, having a sandbox service) and (3) sharing TI features.

Taking into account the aforementioned criteria, we focus our evaluation on the intelligence sharing functionalities, the standardized representation, the integration possibilities with standard security tools, the analysis and graphs generation capabilities. Table 3 summarizes this evaluation.

From this evaluation, we conclude that MISP, CRITs and Soltra Edge are the most flexible tools offering multiple collaboration possibilities with standardized formats of distribution. Even if standardized formats are not natively supported in some of these tools, they can be added as extra modules. Several of these tools could be used together in the same organization, as they are complementary. For example, it is possible to combine outputs from CRITs and to use MISP for sharing the results among various communities.

While Soltra Edge has been designed to support the STIX/TAXII standards to input/dump data, CIF v3 supports using STIX standard only in a very basic format with extra modules. Actually, standardization depends on what each tool aims to realize. Soltra Edge approach is to support standards such as STIX/TAXII for the long-term usage, as these standards seem to get a considerable amount of traction. However, this limits short-term accomplishments due to the lack of STIX/TAXII threat intelligence feeds and STIX/TAXII-compliant security tools (Magar and Bernier, 2015). On the other hand, CIF has an extremely high speed requirement and is heavily based on ZeroMQ (iMatix Corporation, 2014) for that reason. CIF v3 supports partially STIX format and do not support any TAXII stuff

[1] https://github.com/zeromq/zyre).



185.40.4.60 Threat Events

Statistics

95 Connections
42 Bruteforce
0 Web Attack
8 Shell Command
0 SQL Command
2 Malware

Hostname	*Unknown*
Organization	AS50113 Mec
City	
Region	
Country	Russia
Latitude/Longitude	55.75,37.616
First Seen	2016-05-23 2
Last Seen	2016-05-31 1

```
SSH Banner: SSH-2.0-libssh2_1.4.3

11:58:13  ssh bruteforce against Alliacom - VM2: Netherland
          Username: DUP root
          Password: Cisco
          Success: no

11:58:14  ssh bruteforce against Alliacom - VM2: Netherland
          Username: root
          Password: comcast123
          Success: yes

11:58:15  Executed Shell Command to Alliacom - VM2: Netherland via sshd
          cd /tmp

11:58:16  Executed Shell Command to Alliacom - VM2: Netherland via sshd
          rm -rf p.pl

11:58:17  Executed Shell Command to Alliacom - VM2: Netherland via sshd
          curl -O http://199.101.48.210/p.pl

11:58:18  Executed Shell Command to Alliacom - VM2: Netherland via sshd
          wget http://199.101.48.210/p.pl

11:58:19  Uploaded Malware to Alliacom - VM2: Netherland via sshd
          MD5: 3b6858dae1c3815d8e05698cf415fedf
```

Fig. 4 – Lebahnet Honeynet: Attaker profile and attack steps.

at the moment. The reason is that TAXII is based on legacy technology that pull data with REST/JSON calls which is too slow for what CIF is intented to do. Thus, if STIX/TAXII are too heavy regarding the organization objectives, then CIF is probably not the best tool to use.

Threatelligence was designed to collect data from the same or similar sources used for CIF v1 tool. The developer made the data collector as generic as possible to let users easily add their own custom sources of cyber intelligence data to the environment. Users are able to add all kinds of data, whatever they determine as intelligence to the schema-less database ElasticSearch. It further enriches the data collected by looking up country, geographic location, etc.

The same as for CIF and Threatelligence, AlliaCERT team first motivation was to search for a speed response and to offer to users a flow of last seen IOC, in order to feed other security tools. This justifies the use of schema-less databases, which are able to store large data quickly and efficiently. At the same time, AlliaCERT has focused its efforts to improve the context of an attack before sharing it. The tool uses multiple sources including the Lebahnet honeynet, which provides more detailed information on IOC including tactic information such as attack methodology and steps. The tool also relies on additional functionalities, such as, sandbox and anti-cybersquatting services for reputation analysis. Using a standardized representation of IOC to improve reputation search as well as sharing TI with communities are works in progress.

9. Conclusion and future work

As the IT landscape continues to evolving (e.g., movement to the Cloud, usage of mobile devices), newer points of attack insertion appear, making indicators of compromise (IOC) also changing. Discovering covert cyber attacks and new malwares, issuing early warnings, and selectively distributing threat data are just some of the advantages of technical threat intelligence (TTI). The aim of TTI is to help preventing attacks or at least shorten the window between compromise and detection. We have given a clear definition of threat intelligence and how literature subdivides it. We have focused on TTI and the major problems related to it. We have found that on one hand, timeliness of information is very important when protecting against zero-day exploits and aggressive attacks. On the other hand, fast sharing of IOC is not sufficient when dealing with targeted attacks, since specific network and host-based indicators may only be used once by the attacker in a true targeted attack. In this case, targeted defenses are also needed where security teams within organizations have to collect and filter threat data with a focus on their internal vulnerabilities and weaknesses. We surveyed new researches, trends and standards to mitigate TTI problems and delivered most used sharing strategies based on trust and anonymity so participating organizations can do away with the risks of business leak. Clearly, the more a group can trust its organization members, the more effective the sharing tends to be. However, before building a community based organizations, it is worth considering some common factors that are related to business process, stability, and cooperation policy. From our evaluation of most known open source/free tools offering TTI, we have found that different approaches seem to emerge. Some are focusing at scale and speed in order to face zero-day exploits, using fast ways to exchange threat information (e.g., JSON files, non-relational systems such as MongoDB and Hadoop). Other tools are focusing on the meaning of this information by applying big data analytics. This approach implies defining ontologies, taxonomies

Table 3 – Threat Intelligence tools evaluation.

Tool / Criteria	Import format[a]	Integration with/ export to standard security tools[b]	Support of collaboration	Data exchange standards	Analysis	Graph generation	License
MISP	bulk-import, batch-import, OpenIOC import, GFI sandbox, ThreatConnect CSV, JSON, OCR, VMRAY	(1) generating OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with network IDS, host IDS. (2) generating network IDS data to export to Suricata, Snort and Bro or RPZ zone. (3) integration with SIEM using a restful API	Private instance or multiple instances interconnected with a selected community (many sharing options)	STIX, CybOX, TAXII[c]	(1) Analysis of the history records and displaying a trend (2) Correlation of analysis finding relationships between attributes and indicators (3) May include any other result from additional analysis of malware like tools output.	misp-graph to analyze a MISP XML, export and generate graphs from correlation between events and IOC. The export formats: Graphviz and gexf files	Open source (GNU General Public License)
CRITs	bulk-import via CSV file, blob, and spreadsheet, STIX CybOx, TAXII	(1) STIX CybOx, TAXII, CSV to export to network IDS and host IDS (2) a RESTful API for import/export/updates (3) Other services readily available that integrate with external sources and services[d]	Private instance or shared with a trusted community	STIX, TAXII, OpenIOC; Send/receive information through Facebook's ThreatExchange[d]	(1) Analysis of uploaded files with the possibility to link a Cuckoo sandbox (2) Upload threat data and automatically uncover critical information (3) Analysis of Samples, PCAPs, etc.	mcrits to visualize CRITs DB via local Maltego transforms.	Open source (GNU General Public License)
Soltra Edge	CSV, STIX, TAXII, CISCP[g]	Export to ArcSight, CRITs, XML Snort, Support of python scripts to add more entities	Private instance or shared with a trusted community	STIX, CybOx, TAXII, TLP[g]	Possibility of using a sandbox via stream redirections	-	Closed source with a free version.
CIF v3	XML, JSON, Zip archives,[e]	Output into multiple formats (CSV, JSON, html, table) to integrate with various tools including Snort, Bro, Bind, TippingPoint, Elsa, PassiveDNS, FireEye	Private instance, or shared with a trusted community among different CIF instances via a centralized service.	STIX, CybOX[f], Feeds from a CIF instance can be added as a data source to another CIF instance	(1) Finding related threats e.g. different domains/URLs that point to IP addresses in the same autonomous system (2) Whitelist observations from entering a feed during the feed generation process (3) Setup filters for what kind of data to pull from the instance	Kibana to generate statistics, trends and maps	Open source (GNU General Public License)

(continued on next page)

Table 3 – (*continued*)

Tool / Criteria	Import format[a]	Integration with/ export to standard security tools[b]	Support of collaboration	Data exchange standards	Analysis	Graph generation	License
Threatelligence	XML, JSON	-	Private instance with a web access	-	(1) Add a limit to the amount of days to keep data (2) Possibility of using a sandbox via stream redirections	Kibana to generate statistics, trends and maps	Open source (GNU General Public License)
AlliaCERT TI tool	XML, JSON (including STIX, CyBOx formats)	CSV, XML for RSS outputs	Private instance with a web access	A work in progress	(1) Analysis of uploaded files using a Cuckoo sandbox (2) an anti-cybersquatting analysis tool (3) A honeynet source with data correlation and steps of the attack (4) A real time search from multiple sources	Home made graphic tool to generate statistics	Closed source with a trial version

[a] Various input formats (e.g., .pdf, .doc, .docx, .xls, .xlsx, .txt) are supported by the majority of tools but are not added in this table.
[b] Security tools: log systems, SIEM and SIEM-like systems, detection and prevention systems.
[c] With an extra module: https://github.com/MISP/MISP-Taxii-Server.
[d] With extra services: https://github.com/crits/crits_services.
[e] STIX is partially parsed (basic format), with an extra module: https://github.com/csirtgadgets/csirtg-smrt-py/tree/master/csirtg_smrt/parser.
[f] STIX is partially dumped (basic format), with an extra module: https://github.com/csirtgadgets/cif-sdk-stix-py.
[g] CISCP: Cyber Information Sharing and Collaboration Program; TLP: Traffic Lightweight Protocol.

and standardized representations of IOC. Future work could be to implement in TI tools, quality evaluation methods such as scoring from the crowd and to incorporate techniques based on sound methodology. In addition, interaction between threat intelligence and vulnerability assessment of products could be more investigated in security teams. For example, if the threat intelligence team identifies that a particular vulnerability is being actively exploited, especially when this exploitation is occurring within the organization's industry sector, it should trigger a vulnerability assessment. This ensures that such attacks on the organization are likely to fail, by coordinating with different monitoring teams. The ultimate goal is to guarantee intelligent threat intelligence.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. The authors also gratefully acknowledge AlliaCERT team for their help on testing the Threat Intelligence tools. Finally, words are not enough to thank L&E for their existence and their support.

Appendix. The defensive perspective of a "Kill Chain"

"Kill chain" is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. As shown in Fig. A1 considered in the context of network intrusions, the adversary's attack unfolds in a series of steps using different vectors, ending with the attacker having established foothold in the victim network. This is the modus operandi of today's sophisticated Advanced Persistent Threats (cf. Section 2.1.1 for more details).

- *Reconnaissance and weaponization*: The reconnaissance consists of research, identification and selection of targets, often by browsing websites (e.g., conference proceedings, mailing lists, social relationships), pulling down PDFs or learning the internal structure of the target organization. The weaponization is realized by developing plan of attack based on opportunities for exploit.
- *Delivery*: It consists of the transmission of the weapon to the targeted environment. It is often a blended attack delivered across the web or email threat vectors, with the email containing malicious URLs (i.e., phishing attack). Whether it is an email with a malicious attachment or a hyperlink to a compromised website or an HTTP request containing SQL injection code, this is the critical phase where the payload is delivered to its target.
- *Exploitation*: Most often, exploitation targets an application or operating system vulnerability, but it could exploit the users themselves or leverage an operating system feature that auto-executes code.
- *Installation and persistence*: a single exploit translates into multiple infections on the same system. More malware executables payloads such as key loggers (i.e., unauthorized malware that records keystrokes), password crackers and Trojan backdoors could be then downloaded and installed. Attackers have built in this stage long-term control mechanisms to maintain persistence into the system.
- *Command & Control (C&C)*: As soon as the malware installs, a control point from organizational defenses is established. Once its permissions are elevated, the malware establishes communication with one of its C&C servers for further instructions. The malware can also replicate and disguise itself to avoid scans (i.e., polymorphic threats), turn off anti-virus scanners, or can lie dormant for days or weeks, using slow-and-low strategy to evade detection. By using callbacks from the trusted network, malware communications are allowed through the firewall and could penetrate all the different layers of the network.
- *Data exfiltration*: Data acquired from infected servers are exfiltrated via encrypted files over a commonly allowed protocol, e.g., FTP or HTTP, to an external compromised server controlled by the attacker. Violations of data integrity or availability are potential objectives as well.
- *Spread laterally*: The attacker works to move beyond the single system and establishes long-term control in the targeted network. The advanced malware looks for mapped drives on infected systems, and can then spread laterally into network file shares.

REFERENCES

Ahrend JM, Jirotka M, Jones K. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge, in: Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), 2016 International Conference On, IEEE, pp. 1–10; 2016.

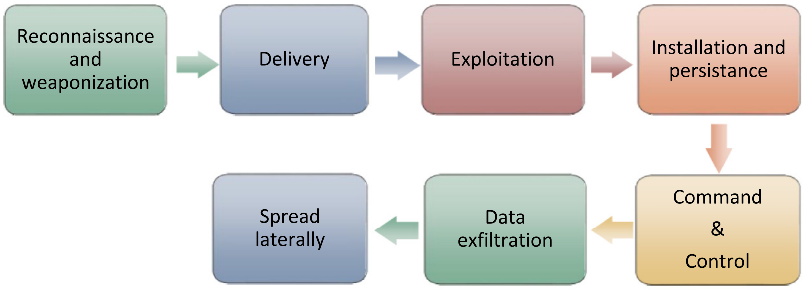


Fig. A1 – Typical Steps of Multi-vector and Multi-stage Attacks.

AlienVault, AlienVault Open Threat Exchange; 2015. Available from: https://www.alienvault.com/open-threat-exchange. [Accessed January 2017].

AlliaCERT, AlliaCERT TI tool; 2016. Available from: https://alliacert.com/login. [Accessed July 2017].

Andre D, Dereszowski A, Dulaunoy A, Iklody A, Vandeplas C, Vinot R. MISP: Malware Information Sharing Platform; 2011. Available from: http://www.misp-project.org/. [Accessed January 2017].

Anomali, Threatstream; 2015. Available from: https://www.anomali.com/product/threatstream. [Accessed January 2017].

Barnum S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). MITRE Corp 2014;11:1–22.

Barraco L. Defend like an attacker: Applying the cyber kill chain; 2014. Available from: www.alienvault.com/blogs/security-essentials/defend-like-an-attacker-applying-the-cyber-kill-chain. [Accessed December 2016].

Belgian Ministry of Defence (CERT), CIRCL Computer Incident Response Center Luxembourg, Iklody IT Solutions, NATO NCIRC, Cthulhu Solutions, CERT-EU, MISP contributos, User guide of MISP Malware Information Sharing Platform, a Threat Sharing Platform, GitBook; 2012.

Bellis E. The Problem with Your Threat Intelligence, White paper, Kenna Security; 2015.

Bipartisan Policy Center, Cyber security Task Force: Public-Private Information Sharing – National Security Program; 2012.

Brown S, Gommers J, Serrano O. From Cyber Security Information Sharing to Threat Management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, pp. 43–49; 2015.

Burger EW, Goodman MD, Kampanakis P, Zhu KA. Taxonomy model for cyber threat intelligence information exchange technologies, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, ACM, pp. 51–60; 2014.

Campbell K, Gordon LA, Loeb MP, Zhou L. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 2003;11(3):431–48.

Cascella RG. The "Value" of reputation in Peer-to-Peer networks, in: Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE, IEEE, pp. 516–520; 2008.

Cavusoglu H, Cavusoglu H, Raghunathan S. How should we disclose software vulnerabilities, in: Proceedings of Workshop on Information Technology and Systems, pp. 243–248, 2004.

Checkpoint, ThreatCloud IntelliStore; 2014. Available from: https://www.checkpoint.com/products/threatcloud-intellistore/. [Accessed January 2017].

Chismon D, Ruks M. Threat intelligence: Collecting, analysing, evaluating, MWR Infosecurity, UK Cert, United Kingdom; 2015.

Choo K-KR. The cyber threat landscape: challenges and future research directions. Comput Secur 2011;30(8):719–31.

Choo K-KR, Smith RG, McCusker R, Australian Institute of Criminology. Future directions in technology-enabled crime: 2007-09. Australia: Australian Institute of Criminology Canberra; 2007.

Chuvakin A, Barros A. How to Collect, Refine, Utilize and Create Threat Intelligence, Tech. rep., Gartner; 2016.

Cook KS, Cheshire C, Rice ER, Nakagawa S. Social exchange theory, 61–88; 2013.

CrowdStrike Inc., CSIX:CrowdStrike Intelligence Exchange; 2014. Available from: https://www.crowdstrike.com/products/falcon-intelligence/. [Accessed November 2016].

CSIRT Gadgets, bearded-avenger (CIF v3); 2016. Available from: http://csirtgadgets.org/bearded-avenger/. [Accessed February 2017].

Dalziel H. How to define and build an effective cyber threat intelligence capability. Syngress Publishing of Elsevier; 2014.

Danyliw R, Meijer J, Demchenko Y. The Incident Object Description Exchange Format (IODEF), Internet Engineering Task Force (IETF), RFC-5070, 2007.

Dshield. SANS Internet Storm Center, Dshield; 2001. Available from: https://www.dshield.org/ [Accessed January 2017].

Dunning LA, Kresman R. Privacy preserving data sharing with anonymous ID assignment. IEEE Trans Inform Forens Secur 2013;8(2):402–13.

Dutch National Police, Europol's European Cybercrime Centre, Kaspersky Lab, Intel Security, No More Ransom Project; 2016. Available from: https://www.nomoreransom.org/index.html. [Accessed July 2017].

ENISA: European Union Agency for Network and Information, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches; 2015. Available from: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/at_download/fullReport. [Accessed January 2017].

ENISA: European Union Agency for Network and Information, ENISA Threat Landscape Report 2016 - 15 Top Cyber Threats and Trends; 2017.

ENISA: European Union Agency for Network and Information Security, CERT cooperation and its further facilitation by relevant stakeholders; 2006.

ENISA: European Union Agency for Network and Information Security, Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs; 2013.

Fadilpasic S. Social media still an important tool for phishing; 2016.

Falliere N, Chien E. Zeus: King of the bots, Symantec Security Response, 2009.

Ferrand O. How to detect the cuckoo sandbox and to strengthen it? J Comput Virol Hack Techniq 2015;11(1):51–8.

FireEye Inc., Advanced Targeted Attacks – How to Protect Against the Next Generation of Cyber Attacks, Tech. rep., FireEye; 2012.

FireEye Inc., Taking a Lean-Forward Approach to Combat Today's Cyber Attacks, Tech. rep., FireEye; 2014.

Fossi M, Turner D, Johnson E, Mack T, Adams T, Blackbird J, et al., Symantec Global Internet Security Threat Report trends for 2009, White Paper, Symantec Enterprise Security 15, 97; 2010.

Furnell S, Clarke N, Beznosov K, Beznosova O. On the imbalance of the security problem space and its expected consequences. Inform Manage Comput Secur 2007;15(5):420–31.

Gerspacher N, Lemieux F. A market-oriented explanation of the expansion of the role of Europol: filling the demand for criminal intelligence through entrepreneurial initiatives, International Police Cooperation: Emerging Issues, Theory and Practice. Culompton, UK: Willan Publishing; 2010. p. 62–78.

Ghanaei V, Iliopoulos CS, Overill RE. Statistical approach towards malware classification and detection, in: SAI Computing Conference (SAI), 2016, IEEE, pp. 1093–1099; 2016.

Gilligan J, Heitkamp K, Heitkamp K, Dix R, Palmer C, Sorenson J, et al., The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework, Tech. rep., Armed Forces Communications and Electronics Association Cyber Committee; 2014.

Google Inc., Bengen H, Metz J, Buehlmann S, Alvarez VM. YARA; 2014. Available from: http://virustotal.github.io/yara. [Accessed July 2017].

Guarnieri C, Tanasi A, Bremer J, Schloesser M. Cuckoo sandbox; 2016. Available from: https://www.cuckoosandbox.org. [Accessed July 2017].

Gundert L. Producing a World-Class Threat Intelligence Capability, Tech. rep., Recorded Future White Paper; 2014.

Heckman KE, Stech FJ, Thomas RK, Schmoker B, Tsow AW. Cyber denial, deception and counter deception. Springer; 2015.

Herzog S. Revisiting the Estonian cyber attacks: Digital threats and multinational responses; 2011.

Hofmann T. Probabilistic latent semantic indexing, in: Proceedings of the 22nd annual international ACM SIGIR conference on Research and development in information retrieval, ACM, pp. 50–57; 1999.

Holland R, Balaouras S, Mak K. Five Steps To Build An Effective Threat Intelligence Capability, Forrester research, inc.; 2013.

Hugh P. What Is Threat Intelligence? Definition and Examples; 2016. Available from: https://www.recordedfuture.com/threat-intelligence-definition. [Accessed December 2016].

Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead Issues Inform Warfare Secur Res 2011;1:80.

iMatix Corporation, ZeroMQ; 2014. Available from: http://zeromq.org/intro:read-the-manual. [Accessed February 2017].

iSightPartners, What is Cyber Threat Intelligence and why do I need it?, iSIGHT Partners Inc; 2014.

IBM, X-Force Exchange; 2015. Available from: https://exchange.xforce.ibmcloud.com/. [Accessed January 2017].

Iovino G. The CIF book. GitHub; 2016.

Issa A. Anti-virtual machines and emulations. J Comput Virol 2012;8(4):141–9.

Johnson CS, Badger ML, Waltermire DA, Snyder J, Skorupka C. Guide to Cyber Threat Information Sharing, Tech. rep., NIST Special Publication; 2016.

Kampanakis P. Security automation and threat information-sharing options. IEEE Secur Priv 2014;12(5):42–51.

Keeling C. Waking Shark II – Desktop Cyber Exercise – Report to participants, Tech. rep.; 2013.

Klump R, Kwiatkowski M. Distributed ip watchlist generation for intrusion detection in the electrical smart grid, in: International Conference on Critical Infrastructure Protection, Springer, pp. 113–126; 2010.

Korstanje ME. Threat mitigation and detection of cyber warfare and terrorism activities. IGI Global; 2016.

Landauer TK, Foltz PW, Laham D. An introduction to latent semantic analysis. Discourse Process 1998;25(2–3):259–84.

Li Z, Lei J, Wang L, Li D, Ma Y. Towards identifying true threat from network security data, in: Pacific-Asia Workshop on Intelligence and Security Informatics, Springer, pp. 160–171; 2007.

Magar A, Bernier M. Soltra edge open cyber intelligence platform report, Bell Canada and Sphyrna Security; 2015.

Malaysia CERT, LebahNET; 2005. Available from: https://dashboard.honeynet.org.my. [Accessed February 2017].

Mandiant, OpenIOC; 2010. Available from: http://www.openioc.org/. [Accessed July 2017].

McMillan R. Definition: threat intelligence. Gartner; 2013.

Miles C, Lakhotia A, LeDoux C, Newsom A, Notani V. VirusBattle: State-of-the-art malware analysis for better cyber threat intelligence, in: Resilient Control Systems (ISRCS), 2014 7th International Symposium on, IEEE, pp. 1–6, 2014.

MITRE, CAPEC: Common Attack Pattern Enumeration and Classification; 2007. Available from: https://capec.mitre.org. [Accessed July 2017].

MITRE, MAEC: Malware Attribute Enumeration and Characterization; 2013. Available from: https://maec.mitre.org/. [Accessed July 2017].

MITRE, ATT&CK: Adversarial Tactics, Techniques & Common Knowledge; 2015. Available from: https://attack.mitre.org/wiki/Main_Page. [Accessed July 2017].

MITRE, Cyber Observable eXpression; 2011. Available from: https://cybox.mitre.org/about/. [Accessed July 2017].

MITRE, CRITs: Collaborative Research Into Threats; 2013. Available from: https://crits.github.io/. [Accessed January 2017].

MITRE Corporation, Cyber Information-Sharing Models: An overview, Case Number 11–4486; 2012.

Moriarty KM. Real-time Inter-network Defense (RID), Internet Engineering Task Force (IETF), RFC-6545, 2012.

Moriarty KM. Incident coordination. IEEE Secur Priv 2011;9(6):71–5.

Murdoch S, Leaver N. Anonymity vs. trust in cyber-security collaboration, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, pp. 27–29; 2015.

National Council of ISACs, About ISACs; 2003. Available from: https://www.nationalisacs.org/about-isacs. [Accessed July 2017].

Niddel Corp., TIQ-Test – Threat Intelligence Quotient Test; 2007. Available from: https://github.com/mlsecproject/tiq-test. [Accessed November 2016].

Oktavianto D, Muhardianto I. Cuckoo malware analysis. Packt Publishing Ltd; 2013.

Pepper C. Applied Threat Intelligence, Tech. rep., Securosis; 2015.

Peretti K. Cyber Threat Intelligence: To Share or Not to Share – What Are the Real Concerns?, Tech. rep., Bureau of National Affairs – Privacy and security report; 2014.

Phillips G. Threatelligence v0.1; 2014. Available from: https://github.com/syphon1c/Threatelligence. [Accessed October 2017].

Pinto A, Sieira A. Data-Driven Threat Intelligence: Useful Methods and Measurements for Handling Indicators, in: 27th Annual FIRST Conference; 2015.

Piper S. Definitive guide to next generation threat protection, CyberEdge Group, LLC, 2013.

Ponemon, Live Threat Intelligence Impact Report 2013, Tech. rep., Ponemon Institute research report; 2013.

Ponemon, Exchanging Cyber Threat Intelligence: There Has to Be a Better Way, Tech. rep., Ponemon Institute research report; 2014.

Ponemon, Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way, Tech. rep., Ponemon Institute research report; 2015.

Poputa-Clean P, Stingley M. Automated Defense – Using Threat Intelligence to Augment Security, in: SANS Institute InfoSec Reading Room; 2015. Available from: https://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligence-augment-35692. [Accessed January 2017].

Qamar S, Anwar Z, Rahman MA, Al-Shaer E, Chu B-T. Data-driven analytics for cyber-threat intelligence and information sharing. Comput Secur 2017;67:35–58.

Ray J. Understanding the Threat Landscape: Indicators of Compromise (IOCs), Verisign; 2015.

Richards K. The Australian Business Assessment of Computer User Security (ABACUS): A national survey, Australian Institute of Criminology; 2009.

Rieck K. Malheur; 2013. Available from: http://www.mlsec.org/malheur. [Accessed July 2017].

Rieck K, Trinius P, Willems C, Holz T. Automatic analysis of malware behavior using machine learning. J Comput Secur 2011;19(4):639–68.

Ring T. Threat intelligence: why people don't share. Comput Fraud Secur 2014;2014(3):5–9.

Schneier B. Software complexity and security, Crypto-Gram, 2000.

Schneier B. Security pitfalls in cryptography, in: EDI FORUM-OAK PARK-, Vol. 11, THE EDI GROUP, LTD., pp. 65–69; 1998.

Schneier B. How changing technology affects security. IEEE Secur Priv 2012;2(10):104.

Seredynski M, Bouvry P, Klopotek MA. Modelling the evolution of cooperative behavior in ad hoc networks using a game based model, in: Computational Intelligence and Games, 2007. CIG 2007. IEEE Symposium on, IEEE, pp. 96–103; 2007.

Shackleford D. Who's Using Cyberthreat Intelligence and How? - A SANS Survey, Tech. rep., SANS Insitute; 2015.

Shackleford D. The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing, Tech. rep., SANS Institute; 2016.

Sillaber C, Sauerwein C, Mussmann A, Breu R. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, pp. 65–70; 2016.

Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput Secur 2016;60:154–76.

Snort IDS team, Snort; 2002. Available from: https://www.snort.org. [Accessed July 2017].

Soltra, Soltra Edge; 2014. Available from: http://www.soltra.com/en/. [Accessed January 2017].

Steele R. Applied collective intelligence: human-centric holistic analytics, true cost economics, and open source everything. Spanda J 2014;2:127–37.

Steele RD. Open source intelligence, Chapter 6. In: Johnson LK, editor. Strategic intelligence, vol. 2. Praeger; 2007a [Chapter 6].

Steele RD. Open source intelligence, Chapter 10. In: Johnson LK, editor. Handbook of intelligence studies. Routledge; 2007b [Chapter 10].

Strom B. ATT&CK Gaining Ground; 2016. Available from: https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck%E2%84%A2-gaining-ground. [Accessed July 2017].

Symantec, Internet Security Threat Report, Tech. rep.; 2016.

The NATO Communications and Information Agency, Malware Information Sharing Platform, Tech. rep., NCIRC TC; 2014.

Threatconnect, Threatconnect platform; 2011. Available from: https://www.threatconnect.com/platform/. [Accessed January 2017].

ThreatQuotient, THREATQ; 2015. Available from: https://www.threatq.com/threatq/. [Accessed January 2017].

Tounsi W, Cuppens-Boulahia N, Cuppens F, Garcia-Alfaro J. Fine-grained privacy control for the RFID middleware of EPCGlobal networks, in: Proceedings of the Fifth International Conference on Management of Emergent Digital EcoSystems, ACM, pp. 60–67; 2013.

Tounsi W, Xu J, Rais H, Langar R. AlliaCERT Threat Intelligence Tool; 2017. Available from: http://perso.u-pem.fr/~langar/papers/alliasp2.pdf. [Accessed July 2017].

Tracker Z. Abuse, Zeus tracker; 2009. Available from: https://zeustracker.abuse.ch [Accessed January 2017].

Trost R. Threat Intelligence Library: A new revolutionary Technology to Enhance the SOC Battle Rhythm!, Blackhat-Webcast; 2014.

Trost R. Crowdsourcing Intelligence: Friend or Foe?!, 2015 Cybersecurity Innovation Forum; 2015.

Verizon, Vocabulary for Event Recording and Incident Sharing. Available from: http://veriscommunity.net/. [Accessed July 2017].

Verizon, 2015 Data Breach Investigations Report, Tech. rep., Verizon entreprise solutions; 2015.

Wagner C, Dulaunoy A, Wagener G, Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, pp. 49–56, 2016.

Williamson W. Distinguishing Threat Intelligence From Threat Data, Security Week Network; 2016. Available from: http://www.securityweek.com/distinguishing-threat-intelligence-threat-data. [Accessed February 2017].

Yamakawa N. Threat intelligence climbs the ladder of enterprise proliferation, Tech. rep., 451 Research; 2014.

Zheng DE, Lewis JA. Cyber Threat Information Sharing – Recommendations for Congress and the Administration, A Report of the Center for Strategic and International Studies (CSIS), Strategic Technologies Program, 2015.

Zurkus K. Threat intelligence needs to grow up; 2015.

Wiem Tounsi is a cyber security scientist and a R&D Professional. She obtained her Ph.D. degree in January 2014 from TELECOM Bretagne (Rennes, France) of Mines-TELECOM Institute. She received the Engineering degree in computer networks and telecommunications from INSA.T and the M.S. degree in electronic systems and communication networks from the Polytechnic School (EPT) in 2008 and 2009, respectively. Her research interests include cyber threat intelligence generation, reverse engineering, formal verification/analysis of security properties and management of security and privacy policies. She has authored several research papers in selective and high level international journals and conferences.

Helmi Rais is a senior professional in charge of security services, business development and R&D. He received the Engineering degree in computer networks and telecommunications from INSA.T in 2004. Reaching 15 years of expertise in cyber security, his main interests include data protection, risk assessment and cyber defense strategies building. He is a member of founding teams of ANSI, AlliaCERT, TUNCERT, OIC-CERT, AfricaCERT, DevTeam and a speaker and panelist in different IT security events (TedX, ITU, FIRST, Alliacom Events, CNIS Mag, OIC-CERT, TF-CSIRT and Securiday).