Array 5 (2020) 100015

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

D4I - Digital forensics framework for reviewing and investigating cyber attacks

Athanasios Dimitriadis [a], Nenad Ivezic [b], Boonserm Kulvatunyou [b], Ioannis Mavridis [a,*]

[a] University of Macedonia, Thessaloniki, Greece
[b] National Institute of Standards and Technology, Gaithersburg, MD, USA

ARTICLE INFO

Keywords:
Digital forensics framework
Artifacts categorization and mapping
Examination and analysis
Digital reviewing and investigation

ABSTRACT

Many companies have cited lack of cyber-security as the main barrier to Industrie 4.0 or digitalization. Security functions include protection, detection, response and investigation. Cyber-attack investigation is important as it can support the mitigation of damages and maturing future prevention approaches. Nowadays, the investigation of cyber-attacks has evolved more than ever leveraging combinations of intelligent tools and digital forensics processes. Intelligent tools (e.g., YARA rules and Indicators of Compromise) are effective only when there is prior knowledge about software and mechanisms used in the cyber-attack, i.e., they are not attack-agnostic. Therefore, the effectiveness of these intelligent tools is inversely proportional to the number of the never-seen-before software and mechanisms utilized. Digital forensic processes, while not suffering from such issue, lack the ability to provide in-depth support to a cyber-attack investigation mainly due to insufficient detailed instructions in the examination and analysis phases. This paper proposes a digital forensics framework for reviewing and investigating cyber-attacks, called D4I, which focuses on enhancing the examination and analysis phases. First, the framework proposes a digital artifacts categorization and mapping to the Cyber-Kill-Chain steps of attacks. Second, it provides detailed instructing steps for the examination and analysis phases. The applicability of D4I is demonstrated with an application example that concerns a typical case of a spear phishing attack.

1. Introduction

To realize the ultimate vision of Industrie 4.0 or digitalization, manufacturing devices, equipment, and software systems have to be highly-interconnected. These connected things cannot be confined to the four walls of a manufacturing enterprise because of today's nature of highly-distributed manufacturing, both physically and virtually, through internal and external software services. Therefore, cyber-attacks are imperative threats to smart manufacturing systems that every company need to be wary of [1]. Manufacturing companies have to protect sensitive data including intellectual property, financial information, and personally identifiable information (PII) that can be manipulated and leveraged for malicious purposes. Despite many efforts in this area, the continued advances in technologies and changes of tactics by perpetrators have made the cyber-attackers seemingly invincible [2].

Security functions include protection, detection, response and investigation [3]. Sophisticated tools such as YARA rules [4] and Indicators of Compromise (IoCs) [5] were developed to assist primarily in the prevention, detection and response [6]. They are mainly created or matured based on the outcome of an investigation and they contain pieces of forensics data [6,7]. Their role in the investigation is to identify trace-s/evidence of an attack giving suggestions from where the investigation should start whenever an attack is detected [6,8]. Structured Threat Information Expression (STIX) defined by the OASIS Cyber Threat Intelligence (CTI) TC is a structure language for describing cyber threat information in JSON schema [5]. STIX enhanced IoCs so that they can include the step of a generalized attack model – Cyber-Kill-Chain that they belong to Ref. [5]. In addition to that, it provides objects that can be used to describe an attack such as TTPs and Observables [5]. However, both YARA and IoCs cannot be used as a forensics procedure to guide an investigation of a cyber-attack. Additionally, they are effective only if the software and mechanism used in the attack are known a priori [9,10]. In other words, they are not attack-agnostic and are sensitive to new or modified threats, such as in the case of zero-day attacks. In particular, they are of limited effectiveness if a cyber-attack uses completely new software and mechanisms in every one of its steps [6]. Therefore, these tools have generated few results for the investigation of new cyber-attacks.

* Corresponding author.
E-mail address: mavridis@uom.gr (I. Mavridis).

https://doi.org/10.1016/j.array.2019.100015
Received 24 October 2019; Received in revised form 18 December 2019; Accepted 20 December 2019
Available online 26 December 2019

On the other hand, digital forensics processes have been proposed to help with finding and analyzing the facts related to an incident [11,12]. They are based on generalized phases that include Collection, Examination, Analysis, and Report, and so they can be used in attack investigation while being attack-agnostic [11]. As they are based on generalized phases, they are also inadequate because they do not describe the examination and analysis phases of a cyber-attack investigation with sufficient details for the digital forensics examiner to easily follow. Moreover, the exact details of these steps may also vary depending on many needs; policies, guidelines and procedures [11,12].

Taken into consideration all the above, it may seem the perpetrators are always a step ahead of the digital forensic examiners regardless of the technology that is being used during an investigation [13]. That may be true if all the digital forensics examiners choose to continue using processes that lack to provide adequate support. As such, it is with no doubt that there is the need for a new approach in reviewing and investigating cyber-attacks by providing digital forensics examiners with support during the critical investigation phases, viz examination, and analysis [12]. This paper proposes a digital forensics framework called D4I (Digital FOrensics framework for Reviewing and Investigating cyber-attacks) whose aim is to enhance the examination and analysis phases of the digital forensics process. The linchpin of the D4I is firstly the proposed artifacts categorization and their mapping to the Cyber-Kill-Chain steps of attacks, and secondly the proposed step-by-step instructing method for examining and analyzing cyber-attacks. D4I is designed to complement and enhance, not replace, other digital forensics processes. In this way, forensic examiners can choose the digital forensics process they prefer and conduct the examination and analysis phases to review and investigate a cyber-attack by following the proposed D4I framework.

The paper is organized as follows: Section 2 presents related work and introduces the theoretical background of this research. Section 3 describes the proposed framework, while section 4 illustrates an application example of the D4I framework on a typical case of a spear phishing attack. Section 5 interprets, describes the work and compares it to existing ones and finally, Section 6 summarizes and discusses future work.

2. Background

"Digital forensics is the application of informatics to assure proper presentation of computer crime evidentiary data into a court by mainly preserving the integrity of them and maintaining a strict chain of custody" [11,14]. The ultimate goal of digital forensics is to obtain evidence so that the 5Ws and How (5WH) questions can be answered [15–17]. The 5WH questions include What happened, Who was involved, When did it take place, Where did it take place, Why did that happen, and How an incident occurred [18]. Answering these questions leads to confirming or refuting allegations of an incident [18–20].

In order for the aforementioned questions to be answered, the digital artifacts of a system have to be examined and analyzed by following one of the digital forensics processes discussed in subsection 2.1. Although there is not in the literature a formal definition of the term "digital artifact" [21], it is widely accepted that its definition should be based on the notion of "artifact" in archaeology. That is, artifact is "an object made by a human being, typically one of cultural or historical interest" [22]. Finally, an artifact has also been defined as "an object of digital archaeological interest" [23,24].

2.1. Related work

To accomplish the digital forensics goal, the 5WH questions are answered following a digital forensics process [25–27]. Numerous processes have been proposed in the literature to date without one universally accepted as the best practice [28]. These processes typically start with the data acquisition and end with the evidence reporting phases [11]. Based on existing surveys, all of them include one (analysis) or two (examination and analysis) phases during which the artifacts related to the cyber-attack should be identified and analyzed [12] [29–31] [32]. Evidently, these two phases are of great importance not only because they are common among all digital forensics processes but also because in them the actual investigation takes place [29,30,33]. Based on existing surveys in digital forensics processes, the majority of the processes do not elaborate examination and analysis in detail and so there is a dearth of guidance and limited assistance on conducting these phases [25,29,32,34]. In the following of this subsection, the processes whose examination and analysis phases are further elaborated are discussed.

The Systematic Digital Forensic Investigation Model (SRDFIM) focuses on the investigation of cybercrime and cyber-fraud [14]. It consists of eleven phases, including the examination and analysis. According to SRDFIM, the examination phase aims at searching of evidence related to the case, making it visible and preparing it in a form suitable for analysis. To this purpose, SRDFIM suggests data filtering, validation, pattern matching, searching techniques, recovering ASCII and non-ASCII data as well as finding unusual hidden files or directories, file extension and signature mismatches etc. The analysis phase is a technical review of the data acquired and extracted from the examination step to identify relationships between data, determine its significance, reconstruct events and draw conclusions. To this purpose, SRDFIM suggests time frame analysis, hidden data analysis, application analysis, file analysis, identification of relationships between fragments of data and analysis of hidden data etc. It is evident therefore that the model is technique-centric without providing a structured and a step-by-step way to conduct the examination and analysis phases.

The Integrated Digital Forensics Process Model (IDFPM) proposes a four-step model to aid investigators in following a uniform approach in investigation of cyber-attacks [35]. IDFPM consists of the "Preparation", "Incident", "Digital forensics investigation" and "Presentation", phases. The "Digital forensics investigation" phase includes the examination and analysis. The examination focusing on acquiring hidden, obfuscated, deleted or visible digital evidence/data and transforming it into a human readable form. The analysis aims at identifying data relevant to the case/hypothesis. As data can be quite large, the IDFPM proposes utilizing techniques, such as hashes, to find known data. It also proposes digital evidence with similar identifying patterns to be grouped together to help identification of evidence faster. A proposed method to do so, is to utilize known classifications created in past similar incidents. In this way, however, it requires prior knowledge and therefore it is not attack-agnostic neither it is focused on artifacts. Finally, during analysis, the organized data is proposed to be tested against the hypothesis formulated which is a high-level recommendation.

The Cyber Forensic Field Triage Process Model (CFFTPM) proposes an approach for identifying, analyzing and interpreting digital evidence in a short time frame [36]. The model focuses on decreasing the time needed to investigate a crime on scene which is considered to be a critical factor. The model proposes a series of phases that should be conducted to gather information from a Windows system. The phases include: planning, triage, usage/user profiles, chronology/timeline, Internet activity, and case specific evidence. The phases relevant to our work are the usage/user profiles, chronology/timeline, Internet activity. The name of each phase is derived from the information that can be gained by examining and analysis specific artifacts of a windows system belonging to this phase. Although it seems to be an artifact categorization it is not clearly defined and it is a work relevant to work of SANS (subsection 2.2). Also, CFFTPM does not specify how the artifacts and the categorization of them can be leveraged into investigation. Finally, the phases seem to provide details on what is needed to be examined but not on how a case can be investigated by utilizing them.

In Ref. [11], a high-level digital forensics process is defined by National Institute of Standards and Technology (NIST) which consists of the following phases (Fig. 1):

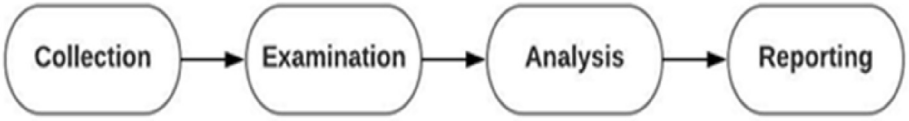

Fig. 1. Digital Forensics Process proposed by NIST.

- Collection, whose purpose is to identify any potential sources of data relevant to the incident and then to label and record them. Afterwards, the data located in those sources should be acquired while preserving the integrity of the sources.
- Examination, which involves assessing the acquired data from the Collection phase and extracting the data relevant to the incident while preserving its integrity.
- Analysis, which involves studying the information extracted by the examination to answer the 5WH questions or determine that no or partial conclusion can be drawn.
- Reporting, which is the process of preparing and presenting the procedure, methods and tools utilized in the investigation along with the results from the analysis phase.

In the following sections, we adopt the digital forensics process of NIST, without limiting the ability to apply D4I along with other digital forensics processes in order to further elaborate their corresponding examination and analysis phases. More details about how the D4I can fit into any other digital forensics process to achieve this goal are presented in the subsection 3.2 and in particular in Fig. 3.

2.2. SANS artifacts categorization

SANS (SysAdmin, Audit, Network and Security) has released the poster termed "Windows Forensic Analysis – Poster: You can't protect What You Don't Know About" [37] the aim of which is to "help investigators of cyber-attacks rapidly determine a clear picture of which user was involved, what the user was doing, when the user was doing it, and why" [37]. To this purpose, the artifacts that can be found on a Windows operating system (OS) were mapped into eight categories based on what activity they describe.

Table 1 depicts these categories, each named by the action that can be determined by examining the artifacts the category contains. For instance, if a forensic examiner is to identify the USB devices mounted on a system, they should examine and analyze the artifacts belonging to the category "External Device/USB usage". Be advised that one artifact can belong to multiple categories depending on the context the category defines. Ultimately, the poster can be utilized as a guide to help forensic examiners focus their analysis on specific areas in Windows Systems that can "best help them answer simple but critical questions" [37].

The SANS's categorization of artifacts can help forensic examiners focus their effort on specific areas in Windows. However, it lacks guidance on how the investigation (examination and analysis) should be conducted.

Table 1
Artifacts categorization by SANS [37].

Category Name	Artifacts
File download	Open/Save MRU, Email Attachments, Skype History, Browser Artifacts, Downloads, ADS Zone.Identifier
Program Execution	User Assist, Windows 10 Timeline, RecentApps, Shimcache, Jump Lists, Amcache.hve, System Resource Usage Monitor (SRUM), BAM/DAM, Last-Visited MRU, Prefetch
File/Folder Opening	Open/Save MRU, Recent Files, Jump Lists, Shell Bags, Shortcut (LNK) Files, Prefetch, Last-Visited MRU, IE|Edge file://
Deleted File or File Knowledge	XP Search – ACMRU, Thumbscache, Thumbs.db, IE|Edge File://, Search–WordWheelQuery, Win7/8/10 Recycle Bin, Last-Visited MRU, XP Recycle Bin
Network Activity/ Physical Location	Timezone, Cookies, Network History, WLAN Event Log, Browser Search Terms, System Resource Usage Monitor (SRUM)
External Device/USB usage	Key Identification, First/Last Times, User, PnP Events, Volume Serial Number, Drive Letter and Volume Name, Shortcut (LNK) Files
Account Usage	Last Login, Last Password Change, RDP Usage, Services Events, Logon Types, Authentication Events, Success/Fail Logons
Browser Usage	History, Cookies, Cache, Flash & Super Cookies, Session Restore, Google Analytics Cookies

2.3. Cyber Kill Chain

The Cyber Kill Chain (CKC) is an intelligence-driven model proposed by Lockheed Martin to be followed in the identification and prevention of cyber-attacks [6]. It adapts the United States military's kill chain process to the digital era to describe the following phases the adversaries pass through to achieve their objectives (Fig. 2):

1. Reconnaissance (R): Attackers usually scan the internet to find, identify, choose and gather information about their target.
2. Weaponization (W): An apparently legitimate file to be sent to the target is developed. This file is used to infect the target by a payload (malicious code) tailored to one or more vulnerabilities.
3. Delivery (D): The attacker sends the above file to the target.
4. Exploitation (E): The payload is executed by exploiting vulnerabilities in the operating system or the installed applications.
5. Installation (I): The payload is installed in a specific location in the victim's system to grant permanent existence (persistence)
6. Command and Control (C2): The payload establishes a covert communication channel (e.g. using DNS queries) with its creator to gain access to the target.
7 Actions on Objective (A): Attackers accomplish their objectives.

The CKC model serves two purposes [6]. It can be used for actionable intelligence so that defensive capabilities can be aligned to the steps an adversary follows and for analyzing intrusions. The analysis of intrusion, however, assumes that the detection of a cyber-attack was based on an IoC. Once an IoC is found, then the analysis should start from the phase that this IoC belongs to (since STIX IoCs can contain the CKC) and going back to prior phases as it is assumed that they have been executed already. Hence, it is evident that CKC and IoCs can be used together in investigation provided that there is prior-knowledge about a cyber-attack, i.e. at least one IoC needs to be found. Moreover, IoCs are not a framework to be used in conducting an investigation so they can no guide it but only support it.

3. The proposed D4I framework

In this section, the proposed D4I framework for reviewing and investigating cyber-attacks is presented. D4I is designed to complement and enhance, not replace, existing digital forensics processes. Consequently, digital forensics examiners can follow their preferred digital forensics process in conjunction with the D4I during the examination and analysis phases [12]. The D4I framework provides a step-by-step and a semi-automatic way of cyber-attack investigation regardless of nature, type and sophistication of the attack.

The D4I framework has two pillars. First is the proposed

Fig. 2. The phases of the Cyber Kill Chain.

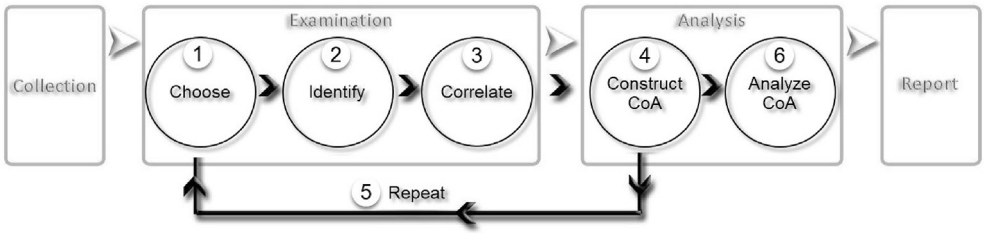

Fig. 3. The proposed step-by-step instructing method.

categorization artifacts and their mapping to CKC as presented in the next subsection. Second is the proposed step-by-step instructing method for the examination and analysis phases, which is based on the above categorization and mapping of artifacts. Hence, a detailed sequence of simple tasks an examiner can follow is provided. D4I aims at reviewing and investigating cyber-attacks with the same sequence of steps they have occurred, so as to easily and rapidly identify their traces, i.e. artifacts they have created.

For the presentation of D4I elaborate on Windows OS artifacts as Windows is the most used operating system nowadays, except Android in Mobile devices [38]. It is also popular in the Industry and its potential vulnerabilities could more likely become subject to exploitation [39]. Windows workstations are also popular in networked control systems (NCSs) in Industry [40]. Microsoft technologies, such as Windows 10, Azure, Microsoft HoloLens and Surface, are used to allow manufacturers to keep up with their end customer needs [41]. The convergence of information technology (IT) and Operational Technology (OT) is an opportunity for attackers to move laterally across a manufacturing network [39]. There are many famous cases targeted Industrial Control Systems in which vulnerabilities in Windows OS were exploited by Advanced Persistent Threats (APT) groups to accomplish their goals. Some famous examples are the "Stuxnet" [42], "NotPetya", "Duqu/Flame/Gauss" and "Night Dragon" [43]. However, artifacts of other kinds of systems can also be categorized and mapped in a similar manner, such as artifacts of other operating systems (e.g. Android, Unix and iOS), IoT (Internet of Things) devices or even Industrial Control Systems [44].

3.1. Categorization and mapping of digital artifacts

In the NIST's examination phase [11], the examiner extracts and assesses the acquired data from the compromised system while preserving the data integrity. However, a system might contain thousands of data and OS files; identifying those relevant to the attack, viz its traces, and so investigating the attack can be a highly demanding task.

To cope with this problem, artifacts have been categorized and mapped into the phases of the CKC. In this way, digital forensics examiners will be able to identify all the traces/artifacts that the attack has left/created in each phase of CKC (NIST's examination phase). Utilizing the proposed categorization and mapping of artifacts in conjunction with the step-by-step instructions described in the next subsection, analysts can focus their effort only on correlating artifacts between CKC phases. Therefore, the identification of those relevant to the attack being investigating becomes a straightforward task.

Table 2 illustrates a CKC-based mapping of artifacts identified in the SANS Categorization. In addition to SANS artifacts, our research has also identified and categorized other Windows artifacts. They are included in the subrow termed "D4I" in Table 2 and mapped to the CKC-phases. Each artifact may belong to multiple categories depending on the context being examined and analyzed. For instance, artifacts regarding USB devices can provide information about the devices used to deliver malware (malicious software) or exfiltrate data and so they belong to "Delivery" and "Actions on Objective" stage respectively. The categorization can then be used in the step-by-step instructing method proposed in the next subsection.

Table 2
Mapping artifact categories to CKC phases.

Phases	Artifacts Categories	
R	SANS:	WLAN Event Log
	D4I:	ICMP (windows events, netstat, firewall/IDS logs, PCAP traffic both live and from RAM)
W	SANS:	–
	D4I:	File used to deliver a malware and its metadata (e.g. infected document's metadata can reveal the tool used to develop the malware embedded into it – payload of the document)
D	SANS:	File/Folder Opening, File Download, External Device/USB usage
	D4I:	Files/Folders where applications store attachments or files downloaded (e.g. viber.db file, Folder where uTorrent saves the files),
E	SANS:	Program Execution, Windows Application Log Files, File opening/creation, Account Usage
	D4I:	Vulnerable applications identified by vulnerability assessment itself or as a part of Risk Management, Files/Folders where applications store temporary files or auto save files (e.g. C:\Documents and Settings\<username>\Application Data\Microsoft\Word)
I	SANS:	ADS Zone Identifier
	D4I:	Boot Sectors, MFT Slack, Start-up locations (e.g. registry run keys)
C2	SANS:	Program Execution, Network History, Network History, Shortcut (LNK) Files, Last-Visited MRU, Jump Lists, Open/Save MRU
	D4I:	Network Connections (e.g. netstat), PCAP traffic both live and from RAM (e.g. DNS queries might be used to exfiltrate data)
A	All Windows OS and applications artifacts, and Audit log	

As mentioned in beginning of Section 3, D4I is not limited to Windows OS and can be expanded to other OS, such as Linux. In Linux, for instance, artifacts relevant to the ones being categorized and mapped into the phases of the CKC can be found as well. For example, the file "/etc/init.d" is used to run an application at startup of Linux. This file can be categorized to start-up locations and mapped into the Installation CKC phase. Another example is the file/var/log/kern.log which stores information about the USB devices connected to a Linux workstation. This artifact is categorized to "External Device/USB usage" which is mapped to the Delivery CKC phase.

3.2. Step-by-step instructing method for examination and analysis

The proposed step-by-step instructing method for the NIST's

examination and analysis phases consists of the following six steps (Fig. 3):

1. Choose: Choose a CKC phase.
2. Identify: Identify all artifacts belonging to the chosen CKC phase (examination) based on the proposed artifacts categorization.
3. Correlate: Find correlations between the artifacts of the chosen CKC phase with artifacts belonging to the same, previous or next CKC phase (NIST's examination). Artifacts can be correlated by either their attributes (e.g. timestamp, name) or content (e.g. code of a Microsoft Word VBScript and ADS of a file).
4. Construct Chain of correlated Artifacts (CoA): Keep every artifact that has any kind of correlation with artifacts belonging to the same, previous or next CKC phase and add it to a chain. In effect, analysis is being performed since conclusions are already started being drawn.
5. Repeat: Repeat the procedure (1–4 steps) for all the phases of the CKC.
6. Analyze CoA: Analyze the CoA to determine if it describes an attack (NIST's analysis). As an attack follows the phases described in the CKC, this chain of artifacts is the trace the attack left behind.

4. Application example

In this section, the D4I framework is applied on a case of a spear phishing attack in which an email containing a document attachment infected by a malicious code was sent to the victim. According to FireEye [45], Spear phishing is a targeted form of a phishing email attack. Attackers focus their effort on carefully selected victims, disguising themselves to appear as a trustworthy party that they can persuade their victims about the legitimacy of an email [45]. Doing so they can trick their victim into visiting a link or downloading/opening an attachment of the email so that they can gain access to the computer system or steal sensitive information [45].

This type of spear phishing attack has been chosen because of its wide presence. Tripwire reports three-quarters of organizations suffered from phishing attacks in 2017 [46]. PhishMe states 91% of cyber-attacks begin with a spear-phishing email in 2016 [47]. Wombat estimates 83% of organizations claim they were targets of phishing attacks in 2018 [48]. Verizon determines 92.4% of malware is delivered via email and phishing is the top threat action [49,50]. Gartner states that, through 2020, email remains the primary targeting method of advanced attacks [51]. Additionally, there are several well-known cases focused on industry in which spear phishing attack was utilized by APT groups to achieve their objectives. Some famous examples are: i) the "Havex" case a widespread espionage campaign targeting industrial control systems in Europe and the United States performed [52,53], ii) "Industroyer or Crashoverride" which is the biggest threat to power grids since Stuxnet [54]. This attack started by targeting IT workers and system administrators who was persuaded to download an infected Word attachment [54], iii) "Ukraine Power Grid" infected an Ukrainian power company and it is the first known attack to power-grid [55]. In this attack, Spear-phishing was used along with a malware exploiting the macros in Microsoft Excel documents (xls) [55], iv) "Night Dragon" targeted global oil, energy, and petrochemical companies [43]. In this attack, among others social engineering and spear phishing attack were utilized [43].

The modus operandi of applying D4I on a spear phishing attack is described below.

1. Reconnaissance: The attacker finds the IP address of the targeted organization's website using "whois" databases and "tracert". Then she visits the website and downloads a Microsoft Office document (e.g., an Excel file). Afterwards, she leverages data breaches to harvest the emails of the employees of the organization. She chooses a particular employee and gathers information about him using a usual search engine and social media sites. Finally, the attacker scans the network of the organization trying to map it and to find potential vulnerable services.
2. Weaponization: The attacker examines the downloaded document and detects an unknown (zero-day) vulnerability that she can leverage (most APT groups exploit zero-day vulnerabilities, namely vulnerabilities that have not yet identified by the security community neither published in vulnerability databases, like NIST's National Vulnerability Database). Afterwards, she develops a malware tailored to the particular vulnerability and creates an apparently legitimate file containing this malware to be sent to the victim.
3. Delivery: The attacker sends an email to the victim, pretending a trusted third party and having attached the above malware. To do so, the attacker has leveraged information about the victim gathered in the Reconnaissance CKC phase.
4. Exploitation: The employee receives email, opens the attached file, the malware exploits the vulnerability and executes itself.
5. Installation: The malware creates an ADS (Alternate Data Stream), copies its code into it and grants permanent persistence to the hosting system by installing a registry key (Run registry key) which starts the ADS in every reboot of the system.
6. Command and Control: The malware establishes a covert communication channel between the compromised system and its creator and starts sending image screenshots.
7. Actions on Objective: The attacker's goal is completed, e.g., data exfiltration or moving forward to compromise Industrial Control Systems (this occurred in many famous APT attacks like in "Ukraine Power Grid" case [55])

Although the attack described above might use never-seen-before tools (e.g., a zero-day vulnerability in a Microsoft Office document downloaded from the target's website) to overcome security measures, the modus operandi of the attack is the one described above. So, when the company finds out that sensitive data, such as a part design data, has been exfiltrated, an investigation is to be conducted. Following the framework, the steps might be the following:

1. Starting the investigation from the Installation CKC phase (D4I - Choose), artifacts belonging to this phase are identified based on the proposed categorization and mapping (D4I - Identify). Among them, it is determined that there is a Run registry key created that starts a code located into an ADS. The key and the ADS stream were created at X1 timestamp (D4I - Correlate). At this point, the chain of correlated artifacts contains a registry key and an ADS belonging to the Installation CKC phase (D4I - Construct CoA).

   CoA: [−], [−], [−], [−], [Run Registry key, ADS], [−], [−]

2. Afterwards, the artifacts belonging to Exploitation CKC phase (D4I - Choose) are identified (D4I - Identify). Having the X1 timestamp, it is found that almost the same time an xls file was run by examining the folder where Microsoft Office creates temporary files (D4I - Correlate). At this point, the chain of correlated artifacts contains a registry key, an ADS and an xls file (D4I - Construct CoA).

   CoA: [−], [−], [−], [xls file], [Run Registry key, ADS], [], []

3. Artifacts belonging to the "Delivery" CKC phase (D4I - Choose) are identified based on the proposed categorization and mapping (D4I - Identify). Having all these artifacts identified, it is found that this xls is attached to an email (Email attachments, see the Delivery phase of the Table 2) (D4I - Correlate). By analyzing this email, the IP address, say IP2, is found. At this point, the chain of correlated artifacts contains a registry key, an ADS, an xls file and an email (D4I - Construct CoA).

   CoA: [−], [−], [email], [xls file], [Run Registry key, ADS], [], []

4. As the Weaponization phase (D4I - Choose) usually takes place in the attacker's facilities, no artifacts belonging to this phase might be found on the system being investigated. However, we can determine how the attacker created this xls file and if it contains a malware by analyzing this xls file. Having done the latter, it is determined that the xls file contains a malware which contains the code found in the ADS stream.
5. Artifacts belonging to the Command and Control phase (D4I - Choose) are identified (D4I - Identify). A covert communication channel with the IP1 address using DNS protocol to transfer image screenshots is revealed based on the ADS code existing in the CoA. PCAP files extracted from RAM revealed image files sent from the compromised system to the IP1 address (D4I - Correlate). At this point, the chain of correlated artifacts contains a registry key, an ADS, an xls file, an email, and an IP address (PCAP) (D4I - Construct CoA).

   CoA: [−], [−], [email], [xls file], [Run Registry key, ADS], [IP], []

6. Reconnaissance phase is selected (D4I - Choose), and its artifacts are identified by following the proposed categorization and mapping of artifacts. IP1 address from "Windows Firewall log files" are identified and IP2 is also found on the web server's log files (D4I - Correlate). At this point the CoA is:

   [Log files], [−], [email], [xls file], [Run Registry key, ADS], [IP], []

7. Actions on Objectives (D4I - Choose): PCAP files extracted from the RAM (Identify) shows exfiltration of numerous image files which proves the conclusion made on step 5 (D4I - Correlate). The CoA is:

   [Log files], [−], [email], [xls file], [Run Registry key, ADS], [IP], [image files]

This section showed that the attack was investigated in a step-by-step way applying the D4I framework. It was found that a phishing email attack took place with the purpose of exfiltrating data by taking screenshots of the compromised system. The described procedure can be accomplished automatically by implementing an algorithm finding correlations and visualizing the results to help forensics examiners.

5. Discussion

Following the D4I framework, an attack can be revealed in a step-by-step way, as every phase is a direct consequence of the previous one accomplished. As the possibility for two artifacts to be correlated is higher when they belong to the same or adjacent CKC phases than when they belong to distant phases, the examiner can rapidly correlate them and develop an understanding of the cyber-attack in the NIST's analysis phase. For instance, the timestamp of opening a document containing a malicious VBScript and the timestamp of the creation of a start-up registry key used as a persistent mechanism of a malware is usually almost the same (once a malicious VBScript is run, a registry key is usually created).

With the proposed artifact categorization and mapping, digital forensics examiners are able to identify (NIST's examination phase) all the traces/artifacts that an attack has left/created in each phase of CKC. As the traces/artifacts are associated with CKC phases, the examiners can rapidly correlate them and develop a thorough understanding of cyber-attacks (NIST's analysis phase). For instance, a digital forensics examiner may decide to start the investigation beginning with the artifacts belonging to CKC's Installation Phase based on the fact that in order for malware to run after a system reboot it has to be installed on a start-up location. This way, he can find a registry key containing malicious code. The timestamp of this registry key can point an application run in the system (e.g., Microsoft Office). This application can be found by analyzing the artifacts belonging to the CKC's Exploitation phase (e.g., Program Execution category). Moving to the CKC's Delivery phase and utilizing the all the forenamed information found (name of the application, registry key, timestamp) the investigation can continue in the same manner.

Finally, the result can synthesize a graph where nodes are the artifacts of the different phases (traces of the attack in this phase) and the links are the relationship between them in terms of correlation points, such as timestamps, IP addresses, and processes. Essentially, this graph will depict the modus operandi of the attack and its corresponding traces get left behind. Therefore, the D4I can also be used for attack visualization purposes in terms of constructing attack graphs and signatures. Fig. 4 is a sample high-level graphical representation of an outcome of this process.

Considering all the above, by following this framework not only can the attack be investigated, but the modus operandi and the signature of the attack can also be determined. As the signature is created using artifacts, the attack is contextualized with them. Taking all the above into consideration, the D4I framework can be used for:

1. Examination and analysis of cyber-attacks in a step-by-step way.
2. Determining the modus operandi.
3. Conceptualization of attacks using artifacts.

Compared to D4I, no other digital forensics process focuses on leveraging CKC and artifacts to provide a way to conduct investigation of cyber-attacks while being attack-agnostic. In addition to that, they do not offer the level of details that the D4I offers. The processes that tried to provide more details on the examination and analysis are presented in Section 2.1. Compared to D4I, the SRDFIM is limited to providing the techniques that a digital forensics examiner can use during the examination and analysis. Also, it does not take into consideration the phases CKC neither corresponding artifacts. The IDFPM focuses on leveraging previous attacks to investigate new ones and so it does not attack-agnostic as D4I. Also, compared to D4I, the IDFPM does not focus on CKC neither on artifacts. Moreover, the IDFPM offers a high level of details in examination and analysis. Another existing work is the CFFTPM model. CFFTPM tried to leverage an artifact categorization to provide steps on examination and analysis. However, it is limited to categorize artifact as SANS has done. The work of SANS however is much more detailed. Compared to D4I, the steps of CFFTPM is limited to analyzing artifacts themselves and not how to leverage them into investigation as D4I does. In this way, it seems to be myopic regarding the investigation of cyber-attacks.

6. Conclusion

In this paper, we proposed a digital forensics framework called D4I, providing a systematic approach for reviewing and investigating cyber-attacks. The D4I framework has two folds. First, it proposes a digital artifacts categorization and mapping to the generalized steps of attacks known as Cyber-Kill-Chain. Second, it provides detailed instructing steps for the examination and analysis phases. As a result, the D4I framework

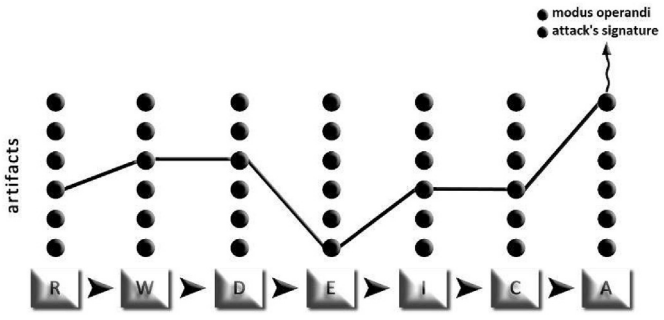

Fig. 4. D4I framework visualization.

provides a step-by-step way to investigate cyber-attacks that is not only attack agnostic but also provides sufficient details for repeatable and effective investigation. Moreover, the D4I framework is designed so that it can be scaled to other types of systems such other Windows versions, other OS (e.g., Android, Unix and iOS) as well as systems operating in Smart Manufacturing, such as SCADA, by creating similar categorizations and mapping of artifacts into CKC phases. In addition, the D4I can be used in conjunction with the NIST Cyber Security Framework (CSF) [3] and more specifically it can be utilized as an Informative Reference of the subcategory "RS.AN-3: Forensics are performed" of the outcome function "Respond (RS)". The D4I framework is not a complete forensics process nor does it replace other forensics processes, such as the one proposed by NIST, but elaborates the most critical phases of an investigation of a cyber-attack, namely examination and analysis. Therefore, digital forensics examiners can follow their preferable digital forensics process and apply D4I during the examination and analysis phases which are common within most of digital forensic processes.

Our future research effort aims at mapping the attacks into CKC using ontologies of digital artifacts, with the ultimate goal of developing a prototype tool used to support investigations.

Disclaimer

Any mention of commercial products is for information only; it does not imply recommendation or endorsement by NIST.

CRediT authorship contribution statement

Athanasios Dimitriadis: Conceptualization, Methodology, Writing - original draft. **Nenad Ivezic:** Methodology, Writing - original draft. **Boonserm Kulvatunyou:** Writing - original draft, Validation. **Ioannis Mavridis:** Conceptualization, Methodology, Writing - review & editing.

References

[1] University of Cambridge. Cyber risk outlook 2018 [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf. [Accessed 5 September 2019].

[2] Coats DR. Worldwide threat assessment of the US intelligence community. 13 2 [Online]. Available: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf. [Accessed 17 March 2019].

[3] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. Gaithersburg: National Institute of Standards and Technology; 2018.

[4] Culling C. Which YARA rules rule: basic or advanced?, SANS insitute. 6 July [Online]. Available: https://www.sans.org/reading-room/whitepapers/tools/paper/38560. [Accessed 5 June 2019].

[5] OASIS Cyber Threat Intelligence (CTI) TC. STIX™ version 2.0. Part 2: STIX objects. OASIS Cyber Threat Intelligence (CTI) TC, [Online]. Available: http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html#_Toc496714313. [Accessed 15 October 2019].

[6] Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. [Accessed 19 January 2019].

[7] Tixteco MdCP, Tixteco LP, Sánchez Pérez G, Toscano LK. Intrusion detection using Indicators of compromise based on best practices and windows event logs. In: Cimp 2016 : the eleventh international conference on internet monitoring and protection; 2016. Valencia, Spain.

[8] Robertson C. Indicators of compromise in memory forensics. February[Online]. Available: https://www.sans.org/reading-room/whitepapers/forensics/indicators-compromise-memory-forensics-34162. [Accessed 7 February 2019].

[9] ENDGAME. Mind the Detection Gap. Three things SOC teams must consider for earliest detection of unknown threats [Online]. Available: https://www.endgame.com/sites/default/files/Mind%20the%20Protection%20Gap.pdf. [Accessed 5 August 2019].

[10] Sabry S. Serious threat hunting: hunting for advanced adversaries without Indicators of compromise. Abu Dhabi: RSAConference; 2016.

[11] Grance T, Dang H, Kent K, Chevalier S. Guide to integrating forensic techniques into incident response. Gaithersburg: National Institute of Standards and Technology; 2006.

[12] Sachowski J. Implementing digital forensic readiness. Elsevier; 2016.

[13] Kohn M, Olivier MS, Eloff JH. Framework for a digital forensic investigation. In: ISSA; 2006. p. 2006.

[14] Agarwal A, Gupta S, Gupta S, Gupta M. Systematic digital forensic investigation model. Int J Comput Sci Secur 2011;5(1):118–30.

[15] Årnes A. Digital forensics. WILEY; 2017.

[16] Association of Chief Police Officers. Practice advice on core investigative doctrine. Centrex; 2005.

[17] Owen B. Exploiting digital evidence artefacts: finding and joining digital dots. semanticscholar; 2018.

[18] Ieong RS. FORZA: digital forensics investigation framework that incorporate legal issues. In: DFRWS (digital forensics research conference). Lafayette; 2006.

[19] Anson S, Bunting S, Johnson R, Pearson S. Mastering windows network forensics and investigation. SYBEX; 2012.

[20] Bryant R, Bryant S. Polishing digital crime. England: Ashgate; 2014.

[21] Harichandran VS, Walnycky D, Baggili I, Breitinger F. CuFA: a more formal definition for digital forensic artifacts. In: Digital forensics research conference. DFRWS); 2016.

[22] Lexico - artefact. OXFORD, [Online]. Available: https://www.lexico.com/en/definition/artefact. Accessed 1 5 2019.

[23] Van der Waag-Cowling N, Leenen L. ICCWS 2019 - proceedings of the 14th international conference on cyber warfare and security. Stellenbosch - South Africa; 2019.

[24] Shumba R. Exploring the use of graph databases to catalog artifacts for client forensics. In: ADFSL conference on digital foreniscs. Security and Law; 2018.

[25] Du X, Le-Khac N-A, Scanlon M. Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv. Cornell University; 2017. 5 August.

[26] Hassan NF, Jaber HM. Offline vs. Online digital forensics of cloud-based services20. Journal of Al-Nahrain University; 2017. p. 117–24. December 4.

[27] ISACA. Overview of digital forensics [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/overview-of-digital-forensics.aspx. [Accessed 15 July 2019].

[28] Arshad H, Jantan AB, Abiodun OI. Digital forensics: review of issues in scientific validation of digital evidence. J Inform Process Syst 2018;14(2):346–76.

[29] Patil PS, Kapse AS. Survey on different phases of digital forensics investigation models. Int J Innov Res Comput Commun Eng 2015;3(3). March.

[30] Selamat SR, Yusof R, Sahib S. Mapping process of digital forensic investigation framework. IJCSNS Int J Comput Sci Netw Secur 2008;8(10):163–9. October.

[31] Yusoff Y, Ismail R, Hassan Z. Common phases of computer forensics investigation models. Int J Comput Sci Inf Technol 2011;3(3). June.

[32] Kyei K, Zavarsky P, Lindskog D, Ruhl R. A review and comparative study of digital forensic investigation models. In: International conference on digital forensics and cyber crime; 2012. Berlin.

[33] Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digit Invest 2005;2(2):147–67. June.

[34] Peasah K, Quayson E, Agyei O, Danso Ansong E. Survey of digital forensic models and proposed thematic scheme. Int J Comput Appl 2017;169(11):975–8887.

[35] Kohn M, Eloff M, Eloff J. Integrated digital forensic process model. Comput Secur 2013;38:103–15.

[36] Rogers MK, Goldman J, Mislan R, Wedge T, Debrota S. Computer forensics field triage process model. J Digital Foren Secur Law 2006;1(2).

[37] SANS Institute. Windows forensics analysis [Online]. Available: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download. [Accessed 21 August 2019].

[38] statcounter-GlobalStats [Online]. Available: https://gs.statcounter.com/os-market-share/desktop-tablet-console/worldwide/#monthly-201810-201910. [Accessed 11 December 2019].

[39] Trend Micro Research. Security in the era of industry 4.0: dealing with threats to smart manufacturing environments. 3 3 TRENDMICRO 2019 [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments. [Accessed 11 December 2019].

[40] Gaj P, Skrzewski M, Stój J, Flak J. Virtualization as a way to distribute PC-based functionalities. IEEE Trans Indus Inform 2015;11(3):763–70.

[41] Pidgeon E. Powering the industry 4.0 revolution in manufacturing with windows 10 and Microsoft cloud," Microsoft. 24 3. 2017 [Online]. Available: https://www.microsoft.com/en-us/microsoft-365/blog/2017/04/24/powering-the-industry-4-0-revolution-in-manufacturing-with-windows-10-and-microsoft-cloud/. [Accessed 11 December 2019].

[42] Falliere N, Murchu LO, Chien E. W32.Stuxnet dossier. Symantec; 2011.

[43] Hemsley KE, Fisher E. History of industrial control system cyber incidents. United States: Idaho National Lab. (INL); 2018.

[44] Assante MJ, Lee RM. The industrial control system cyber kill chain. October [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. [Accessed 9 May 2019].

[45] FireEye. Spear-Phishing Attacks Why they are successful and how to stop them [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf. [Accessed 19 April 2019].

[46] Bisson D. Three-quarters of organizations experienced phishing attacks in 2017, report uncovers. January[Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/three-quarters-organizations-experienced-phishing-attacks-2017-report-uncovers/; 2018. 24 Accessed 11 April 2019.

[47] PhishMe. 2019 state of the phish report protect your organization from phishing attacks. PhishMe; 2019.

[48] Wombat Security Technologies. State of phish 2019 report. 2019. Wombat.

[49] Verizon. 2018 data breach investigations report. 2018. Verizon.

[50] Verizon. 2019 data breach investigations report. 2019. Verizon.

[51] Gartner. Gartner fighting phishing - 2020 foresight. 19 7[Online]. Available: https://www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight. [Accessed 1 September 2019].
[52] Piggin R. Industrial systems: cyber-security's new battlefront [Information Technology Operational Technology. Eng Technol 2014;9(8):70–4.
[53] Nelson N. The impact of dragonfly malware on industrial control systems. United States: SANS Institute; 2016.
[54] Virsec. Virsec hack analysis: deep dive into industroyer (aka crash override). virsec, [Online]. Available: https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/. [Accessed 9 December 2019].
[55] Whitehead DE, Owens K, Gammel D, Smith J. Ukraine cyber-induced power outage: analysis and practical mitigation strategies. In: 70th annual conference for protective relay engineers. CPRE); 2017. p. 1–8.