Forensic Analysis as Iterative Learning

Eoghan Casey and Bruce Nikkel

1 Introduction

Protecting critical infrastructure requires up-to-date understanding of cyberattacker behavior, including their methods of approach, attack, concealment and control. Forensic analysis plays a central role in the readiness and resilience of an organization against cyberattacks; helping reduce disruption of service, data theft, financial loss, manipulation of data integrity, reputational harm, privacy violations, physical damage, and reduction of public trust. Crucially, insights gathered from forensic analysis of intrusions targeting specific organizations or an entire industry sector are invaluable for detecting and disrupting cyberattacks, and for strengthening the overall security of critical infrastructure.

Cyberattackers can compromise critical infrastructure in a number of ways, many of which are difficult to detect. In the technical domain, attackers can exploit compromised applications, rogue devices, remote access gateways, un-trusted bring your own devices (BYODs), third party outsourcing contractors, software updates and telemetry mechanisms (e.g., by modifying code on update servers of popular software products), unencrypted information in cloud environments, and weak credential management. Additionally, attackers may deploy social engineering techniques as stronger security measures strengthen the resilience of hardware and software systems. There has been a significant increase in social engineering of staff and clients of target organizations [16]. Phishing attacks can be broadly or

E. Casey (✉)
School of Criminal Sciences, University of Lausanne, Lausanne, Switzerland
e-mail: eoghan.casey@unil.ch

B. Nikkel
Bern University of Applied Sciences, Bern, Biel, Switzerland
e-mail: bruce.nikkel@bfh.ch

M. M. Keupp (ed.), *The Security of Critical Infrastructures*, International Series in Operations Research & Management Science 288,
https://doi.org/10.1007/978-3-030-41826-7_11

narrowly targeted, and implemented in different forms (e.g., email, social networks or telephone), depending on the objectives of the threat actors. The most narrowly targeted phishing attacks select particular individuals or departments within a target organization and can be crafted with personal details gathered from open sources on the Internet. With social media and open source intelligence, it is easier to prepare plausible social engineering attack scenarios. In some cases, cyberattackers hacked personal email accounts of individuals in target organizations and masqueraded as the person in order to create more convincing social engineering attacks. In other cases, cyberattackers created email filters to block or redirect responses from people attempting to check the legitimacy of the email they received. When cybercriminals use such subtle, targeted social engineering approaches, the infiltration is difficult to detect.

Case Example: Operation Sharpshooter
In late 2018, a phishing campaign called Operation Sharpshooter targeted critical infrastructure by contacting individuals under the pretext of job recruitment in order to entice them to open malicious documents that installed malware on their computers. Forensic analysis of the malicious code revealed similarities with malware used by the Lazarus (a.k.a. Hidden Cobra) group that targeted energy sectors the year before. However, forensic analysts must be careful not to jump to conclusions because different groups can reuse the same tools, and threat actors can employ misdirection. In this case, the numerous technical links to the Lazarus Group seem too obvious, and they indicate a potential for digital deception [31].

System operators should be aware that forensic analysis techniques can help neutralize these threats. Forensic analysis involves in-depth study of available evidence in a systematic and coherent manner. Employing critical thinking and bias mitigation strategies, allows analysts to gain insights into events and activities under investigation. Although incident response processes often uncover useful information, forensic analysis of the same event can yield more detailed descriptions of adversary methods and associated digital evidence that enable more effective detection of related activities. For example, a system operator or incident responder might observe that an adversary has made unauthorized use of Remote Desktop Protocol (RDP), whereas in-depth forensic analysis might find additional anomalies about that behavior that subsequently enable the victim organization to differentiate between authorized and unauthorized RDP connections.

The primary purpose of forensic analysis is to provide reliable information to support decision making. Forensic analysis is a central part of digital forensics, which is the general term used to describe the application of scientific principles and processes to recognition, preservation, examination, documentation, analysis, integration and interpretation of digital evidence for a legal context [28]. Digital evidence is any information of probative value that is stored or transmitted in binary form [33]. Key aspects of managing digital evidence include forensically

sound preservation of evidence, and maintaining chain of custody and integrity information using cryptography [25]. Examples of digital evidence may include computer drive images and other storage media, volatile memory, server log files, cloud artifacts, or other extracted digital traces.

Forensic analysis can often reveal the root causes of a cyberattack to system operators, such that insights gathered from past attacks can be used to prevent similar attacks from reoccurring. Forensic analysis also employs scientific interpretation of evidence to support important decisions such as attack attribution and public notification. Formal evaluation of the relative strength of evidence in light of alternative hypotheses is invaluable when making risk-based decisions [5]. Nonetheless, digital forensics is underutilized for securing critical infrastructures. Preparing systems from a forensic perspective can significantly enhance an organization's resilience to cyberattacks.

Digital evidence can be useful for reconstructing and understanding complex cyberattacks, including the temporal sequence of the attack, the extent to which malicious code was introduced, and the number of user accounts compromised. Further, the study of adversary techniques and objectives can help build more effective cybersecurity defenses [32]. Forensic analysis also enables intelligence-driven approaches to cyberdefense by capturing knowledge and insights gathered from past incidents to support detection, scope assessment and strategic capability enhancement [29]. Curating and sharing such forensic intelligence can help organizations enhance cybersecurity and disrupt future cyberattacks [1].

2 Forensic Defense as an Iterative Learning Cycle

To date, much past work has seen forensics as a passive and responsive tool that is deployed only after an attack has occurred. We propose an alternative view, suggesting that forensics should be seen as a process of iterative learning whose goal is to continuously advance the defensive capabilities of the organization.

Traditionally, conceptualizations of forensic analysis concentrated on reducing the business impact and recovery time of incidents [30]. For example, guidelines developed by the US National Institute of Standards and Technology (NIST) focus on incident response, with forensic analysis in a supportive capacity. The NIST document SP 800-86 *(Guide to Integrating Forensic Techniques into Incident Response*) highlights the importance of investigating security incidents in the context of incident response, but does not address the role of forensic analysis in overall cybersecurity improvement. The NIST Cybersecurity Framework defines the main functional areas of Identify, Protect, Detect, Respond, and Recover [27]. As part of risk assessment, the framework emphasizes the need to take into account current knowledge of cyberattacks, but it is not made clear that forensic analysis of security breaches is necessary to learn from past mistakes and ameliorate security weaknesses. The framework constrains forensic analysis under response activities, with the limited objective of ensuring effective response and supporting recovery activities.

It is important not to conflate forensic analysis and incident response—they are interdependent processes that serve different purposes. The purpose of incident response is to contain and recover from a cyberattack, whereas the purpose of forensic analysis is to understand what happened [6]. There is much to be gained by realizing the crucial role of forensic analysis throughout the cybersecurity risk management lifecycle. When an attack is detected, forensic analysis helps extract information that can be used to search for additional digital evidence and exposures such as compromised accounts in order to assess the scale and severity of the breach (a.k.a. scope assessment). A victim organization that favors quick reaction and containment over thorough scope assessment misses an opportunity to observe the attack in progress and understand what is happening in more detail, and potentially loses the ability to collect ephemeral digital evidence. Before attempting to clean up and carry on with normal business, performing a thorough forensic analysis of cyberattacks can uncover additional problems, can shed light on security weaknesses that need to be addressed, and can increase chances of detecting future cyberattacks more quickly. Ultimately, findings from forensic analysis feed into detection, forensic preparedness, scope assessment, cyberthreat information, and enhanced security. In the following subsections, we explain the elements of this iterative learning cycle.

2.1 Forensic Preparedness

Forensic preparedness is an organizational strategy for managing risks associated with computer misuse. Fundamentally, this involves specification of a policy that lays down a consistent approach, detailed planning against typical (and actual) case scenarios that an organization faces, identification of (internal or external) resources that can be deployed as part of those plans, identification of where and how the associated digital evidence can be gathered that will support case investigation and a process of continuous improvement that learns from experience [17]. Lack of forensic preparedness increases the risks of cyberattacks going undetected and will impair the effectiveness of response activities after a cyberattack is detected. This reactive approach is also costly as it involves the hiring of external consultants. In contrast, organizations that are prepared to gather digital evidence and employ forensic analysis in anticipation of cyberattacks put themselves in a better position to detect, investigate and neutralize attacks [15, 20]. Forensic preparedness includes producing an inventory of IT assets, prioritizing systems according to criticality, maintaining a digital evidence map [4] and developing the capability to take evasive action (e.g., changing critical account names, adding decoys). Further, it comprises the ability for intelligent logging, whereby critical systems enjoy a heightened level of monitoring, strategic ingress and egress filtering, norm deviation detection, and the capability to establish internal defense perimeters, specifically, secure communication channels which are not accessible to network intruders. These channels serve to collect and document forensic evidence and case

details during an intrusion investigation. Forensic preparedness involves having predefined processes for incident response and forensic analysis that are regularly tested and updated by a properly trained and resourced response team. Finally, forensic preparedness in organizations that operate ICS/SCADA equipment can be more challenging because these systems often use specialized data formats and network protocols. For instance, Triton malware specifically targets Safety Instrumented System controllers [21]. Such organizations may require specialized forensic acquisition and analysis methods to support their ICT/SCADA systems, and may require additional procedures to mitigate negative physical consequences resulting from cyberattacks against these systems.

2.2 Instrumenting Networks to Increase Visibility Over Cyberattacks

Two excellent data sources for detection and investigation are internal sinkholes and Netflow collectors. These mechanisms for capturing digital evidence give the greatest visibility on infections, breaches, and unauthorized activity. A private network separated from the Internet by a proxy architecture provides a higher level of security than a simple packet filtered or netted perimeter. Proxy technologies offer more possibilities for control and authentication at the application layer, and prevent any traffic from routing directly to the Internet. A proxied architecture also allows the internal propagation of a default route that ends at a special router called a sinkhole. A sinkhole will receive all internal network layer traffic destined for the Internet (something which should never happen in a proxied environment). This sinkhole traffic can be logged or monitored for possible malicious activity (e.g., malware that attempts to establish direct connections to command and control servers).

Case Example: Sinkhole
A large multinational firm implemented an internal sinkhole infrastructure. When analyzing the network traffic, they found IP packets arriving at the sinkhole destined for external Internet IP addresses. The origin of the packets was the company's perimeter infrastructure security systems (firewall/proxy). An investigation determined that the perimeter infrastructure was misconfigured to forward external packets to internal systems. The internal sinkholes enabled network level detection of a vulnerable control configuration, thus posing a risk to the firm. This misconfiguration was not detected by perimeter NIDS systems or other security detection systems.

Netflow is a standard (RFC 3954) that allows routers to collect information about network traffic. Collecting Netflow data on perimeter routers provides an historic log of all network activity, including connections to and from a network, connection time and duration, bytes transferred, IP addresses and ports, and both failed and successful connection attempts. Netflow data provides useful evidence for investigations, checking against cyberthreat information feeds, and for hunt teams looking for suspicious activity [3, 20]. Forensic analysis is empowered most when data from NetFlow and sinkhole infrastructures are correlated to gain detailed insights into cyberattacks.

Honey pots and honey tokens provide another form of visibility over cyberattacks. Honey pots can be used to redirect cyberattackers to a staged system, observe their actions, and feed them deceptive information. A honey token is a planted piece of information or fake user account that should be invisible under normal operations, but used to collect information about adversary behavior.

Organizations should use these tools to continuously improve their forensic preparedness, applying lessons learning from past security breaches. Without the productive use of insights from past breaches, defenders will not be able to avoid and prevent future similar attacks [22].

2.3 Cyberattack Detection

Detection is the use of information uncovered through forensic analysis to sweep the target network for any additional compromised systems, network segments, credentials or other IT assets [6]. Successful cyberattackers understand commonly used security systems well enough to undermine them and avoid detection. In addition, sophisticated intruders take full advantage of the lack of forensic preparedness [4]. The skill level and motivation of intruders targeting critical infrastructure has evolved to the point where gaining broad access to the target network in order to maintain unauthorized access for as long as possible without detection has become a common occurrence.

Case Example: RUAG
The Swiss company RUAG was compromised and intruders had access to internal systems for several years before being detected. The intruders used various concealment techniques on compromised systems and the network to avoid detection, and used their access to explore the RUAG network and steal substantial amounts of data. The technical report of Switzerland's Information and Security Analysis Center (MELANI) noted that 'one of the most effective countermeasures from a victim's perspective is the sharing of information about such attacks with other organizations, also crossing national borders' [18]. Several security recommendations emerged from the forensic analysis

(continued)

of this incident: to use multi-factor authentication, to implement a proxy architecture, to restrict administrator accounts and outbound connections from internal servers, to block internal direct client-to-client communication, to segment critical networks, to write-protect USB/Firewire devices, to restrict the execution of macros and unnecessary applications, and to prevent the execution of unauthorized binaries.

Results of forensic analysis can be used to detect related attacks, including static indicators such as MD5 hashes, IP addresses and domain names. Looking for static indicators of known attacks is necessary, but not sufficient for effective cybersecurity. Such static indicators are narrow and easily changed, whereas the repeated behavior patterns across related cyberattacks are more stable and difficult to change [32]. Therefore, it is also important to look for similar patterns, behaviors and anomalous activities.

The potential value of various forensic analysis results includes:

- Contextual information related to static indicators, including the location and nature of supporting digital evidence and artifacts;
- Recovered information that cyberattackers try to conceal, including deleted files, hidden processes, and encrypted data on storage media and in network traffic;
- Comprehensive event reconstruction enabling broader visibility over cyber-attacks, including correlation across data sources (e.g., file systems, volatile memory, system logs, router/firewall configuration, network traffic, backup tapes);
- Modus operandi information and behavior signature characteristics that can be used to recognize repetitions of malicious actions across different incidents, various technologies, and multiple adversary groups over prolonged time periods.

Such forensic findings can be useful for developing new and improved detection measures and defensive countermeasures.

Case Example: JSSD
A distinctive characteristic of the modus operandi of members of the JSSD (Jiangsu Province Ministry of State Security) was the use of doppelganger domain names, which involve registering and using domain names that closely resemble legitimate domain names to trick unwitting recipients of spear phishing emails. For instance, the cyberattackers registered the doppelganger domain name http://capstonetrubine.com which closely resembles the legitimate domain name of one organization that was targeted (Capstone Turbine). They also registered the domain name capstoneturbine.cechire.com to receive

(continued)

beacons from malware installed on compromised systems. An insight gathered from the forensic analysis of these cyberattacks was to monitor DNS registrations for doppelganger websites targeting specific organizations or sectors in critical infrastructure. The cyberattackers also manipulated domain registrars in order to hijack legitimate domains. After compromising the targeted organizations, the cyberattackers installed malware on some of the victimized organization's websites in order to infect computers of other organizations and thus gain unauthorized access to their systems [34]. The cyberattackers who gained unauthorized access to the Office of Personnel Management (OPM) in 2016 also used doppelganger domain names [10].

To protect an organization, it is necessary to study emerging cyberattacks, combine information and knowledge about current cyberattacks from multiple sources, and use the insights gathered to predict and prevent future attacks. The ability to find such patterns depends heavily on iterative learning using forensic analysis of digital evidence associated with cyberattacks. Victim organizations that lack visibility into cyberattacks and do not detect an intrusion for months or years have limited opportunities to learn from the situation, particularly so if digital evidence of the original attack was not forensically preserved.

2.4 Scope Assessment and Eradication

Scope assessment builds on information collected during the detection phase, and typically expands as forensic analysis uncovers additional details of a cyberattack, such as the number of systems attacked and the depth of intrusion into each system. It specifies the actually and potentially compromised systems, network segments, and credentials at a given point in time during the investigation [6]. In this context, a potentially compromised system is any device for which a cyberattacker has network access and valid credentials or remote access via installed malware.

The ultimate goal of scope assessment is to assess the scale of the attack, to determine damages and losses, and to provide information concerning the intrusion and the adversary to prepare the remediation plan of action. In addition, the scope assessment can help identify potential locations to collect digital evidence. Scope assessment requires visibility on the network, a response plan and associated personnel who have the broadest possible visibility across the cyberattack landscape. Scope assessment can also include studying related attacks or repetitive activities beyond the confines of a single organization or infrastructure. Without full knowledge about these issues, any response or containment efforts will be incomplete and not fully effective. It is worthwhile to note that existing guidelines such as NIST incident response documents do not specifically address scope assessment and coordinated

or orchestrated response. The challenge of keeping pace with evolving capabilities emphasizes the importance of using all available forensic information to understand cyberattacks and enhance cybersecurity.

As the necessary steps are taken to eradicate the attack, organizations must be careful not to disclose information to the attacker. Eradication needs to be a carefully planned and tailored operation. Modern adversaries and malwares are adept at maintaining a foothold on compromised networks, hence, quick and direct responses that attempt to block access or patch systems are unlikely to be successful. Instead, insights gained from forensic analysis should guide the eradication process. Forensic analysis is central to assessing the full scope of a cyberattack since it systematically uncovers clues that can be used to follow the cybertrail left by the attackers.

Therefore, digital forensic experts should work closely with a network of stakeholders (internal and external to an organization), correlating data from diverse sources to assess the scope of the breach [4]. Compromised systems should not always be immediately cleaned or patched, but forensically preserved and analyzed (live or offline) where feasible, followed by carefully coordinated remediation of the compromised systems. In some cases, it makes sense to delay eradication until enough evidence can be collected (traffic captures, memory dumps) and the attack and its scope can be understood more fully. Hence, the victim organization must weigh the risks of reinstalling or replacing compromised systems before understanding the scope of the problem. This is balanced against allowing the attackers to remain on the network for some time before attempting to expunge their intrusion on the network. If an intruder has already been in a network for several months or more, the organization takes on little additional risk if the malicious activity is allowed to continue for an additional few days. Taking this time between detection and eradication gives the organization an opportunity to forensically preserve and analyze sources of evidence, and to study the extent to which the attackers can access and exploit the network. This information should be the basis of a thorough, orchestrated eradication strategy.

Case Example: Financial Industry
A large financial firm was experiencing malware attacks against retail clients using the online banking portal. Forensic analysis of the attacks determined that the malware was easily scraping credential information from the HTML code and performing automated login interception. The forensic team passed this information on to the banking platform developers with a suggestion to use graphical images instead of HTML text to display credential information. Implementing this suggestion stopped an entire class of banking malware from functioning, preventing significant amounts of fraud.

In some situations, it might be more advantageous to reroute malicious activity to honey pots instead of attempting to block or disrupt the attack. Sophisticated

infections are often very resilient and difficult to clean by simple file deletion or antivirus cleaning kits. Sophisticated cyberattackers take precautions to obfuscate distinctive characteristics in their tools or execute malicious code in ways that make only minimal modifications to the compromised system, creating a need for enhanced methods and tools to search for digital evidence with minimal false positives.

Historically, it was necessary to develop customized 'antidote' tools to scan a compromised network for various versions of customized, packed malware [23]. Today, open source mechanisms such as YARA can search a network for specific digital evidence. To facilitate the use of these open source capabilities, some detailed reports of cyberattacks against critical infrastructure codify forensic findings in YARA such that organizations can automatically scan for distinctive characteristics on compromised systems. A similar capability for custom detection methods in network traffic is provided by Snort signatures.

2.5 Capability Development

Forensic insights from scrutinizing past attacks should be used to continuously develop the organization's defensive skills. Defenders should, therefore, promote prompt adoption of lessons learned from forensic analysis, through a combination of cyberrisk management processes and knowledge exchange mechanisms.

Applying insights gathered from past incidents is important since the effectiveness of defense improves with the integration of agile retrospectives [19]. In this context, lightweight agile retrospectives refer to an efficient collaborative approach to problem-solving that takes into account all stakeholder perspectives in an organization, enabling rapid improvements. A rapid reflection on the outcomes of a cyberattack can provide significant and actionable cybersecurity improvements. In some incidents, one or two security controls could have prevented a security breach from occurring. Some retrospectives revealed needed process changes or new processes to be better able to handle future cyberattacks. Senior management is crucial to implement actionable responses on the basis of such retrospection.

Case Example: The Dragonfly Attack
The Dragonfly group attacked industrial control systems through compromised computers. Although specific indicators of compromise such as IP addresses, domain names and MD5 hash values may only be useful for a limited time, forensic analysis of their activities on the targeted systems provided substantial insights into their tactics, techniques, and procedures. Defenders also learned that the group tried to conceal their activity by deleting Windows event logs. Additional concealment actions included deleting the registry key associated with terminal server client that tracks connections made to remote

(continued)

systems. After the attack was eradicated, several recommendations suggested that this forensic evidence be used to prevent future attacks. For example, one specific recommendation in the DHS/FBI report [14] is to look for this specific concealment activity by searching for event 104 on Windows system logs. Moreover, defenders learned that the attacks were facilitated by users opening malicious emails or entering their passwords on malicious websites, the absence of multi-factor authentication within the victim organizations, insufficient restrictions of administrator accounts and inadequate network segmentation of critical networks or control systems. Dragonfly also benefited from weak ingress/egress filtering, which could have detected or blocked malicious traffic. The DHS/FBI report concludes with a list of twenty-eight security measures for organizations to implement in order to prevent or disrupt similar attacks in the future.

Further, the realization of insights gathered from past incidents is facilitated by the creation of logs and databases such that one may detect commonalities across different attacks and identify patterns. When dealing with a cyberattack, it is necessary to pull together disparate data sources needed to perform forensic analysis, including timelines and link analysis. Internally, organizations can generate significant amounts of data that is useful for forensic analysis, e.g., system and application logs, perimeter NetFlow data, internal router/DNS sinkhole data, and data collected intrusion detection systems (IDS), firewalls, and anomaly detection systems (ADS). Externally, data sources may be purchased from commercial providers, collected via open source data feeds, or obtained from peer organizations facing similar threats. In many cases such external information is shared via connected software systems.

Curating such a repository of knowledge about past incidents (memory) is a crucial component of forensic intelligence. This memory is an accumulation of information, repetitions and insights gathered from past cases, which can be applied to new cases. For example, information about distinctive patterns and sequences of command line execution should be stored as it allows defenders to fingerprint attackers and to prevent future attacks.

However, any attempt to manually integrate and correlate separate data sources from various systems and formats is labor intensive, time consuming, and error-prone. Specifically, using a non-standardized system to import and format data from various sources can result in items such as date time stamps being altered, entries not being imported properly, and other errors or omissions that negatively impact forensic analysis [7]. The more time analysts spend extracting and correlating information from different sources, the less time they have left to analyze it, resulting in fewer opportunities to detect problems. These challenges are amplified when an incident spans multiple networks, and sharing of information between organizations is crucial for a successful resolution. Furthermore, without a standardized approach

to representing and sharing digital forensic information, defenders might never realize that they are investigating cyberattacks committed by the same threat actors.

As a result, the creation of useful and necessary threat information requires the ability to analyze big data effectively and efficiently. This is achieved through data analytics, which is the compilation and analysis of various types of information with the goal of using this information to drive decision-making. The analysis of complex behaviors in large scale-systems can begin to address issues of provenance, attribution, and discernment of attack patterns. Possible applications of data analytics in this field include integration of threat feeds from varying sources, automated triage, data filtering, indicator tracking, visualization, and reporting [26]. There are multiple approaches to this type of memory curation, including unstructured data to support machine learning and structured data and support for linked data analysis.

For example, the U.S. Department of Defense Cyber Crime Center (DC3) captures and reuses knowledge in intrusion-malware investigations to provide timely results and feed forensic intelligence [11]. When digital data are submitted, they are processed using automated systems that contain codified forensic knowledge accumulated from prior casework and research. Specifically, a database is maintained with the forensic analysis results from all past malware samples for future reference, functioning as institutional memory of past forensic analysis. In this way, when malware in a new case has commonality with malware that has already been encountered and processed in a previous case, the results from the prior file instances can be reused, saving time on both processing and forensic analysis. In addition, customized methods for extracting encoded information from malware samples are codified and reused to extract additional details that are not obtainable using commercial systems [12].

Further, the Malware Information Sharing Platform (MISP) is an open source threat information sharing platform that has support from the European Union. This system is growing in popularity due to the ease of use and possibilities for connecting and sharing cyberthreat information with multiple communities [24].

The Cyber-investigation Analysis Standard Expression (CASE) contributes to harmonizing disparate data sources and exchanging of cyberinvestigation in a standardized form, and maintaining provenance throughout the cyberinvestigation lifecycle, including incident response and forensic analysis [8]. The primary motivation for CASE is interoperability—to advance the exchange of cyberinvestigation information between systems, tools and countries. Such interoperability, data fusion, and information sharing can be invaluable when dealing with a single incident involving multiple data sources, and when dealing with cyberattacks against multiple organizations. CASE supports automated normalization, combination, correlation, and validation of information, which means less time extracting and combining data, and more time analyzing information [2].

For example, the DCISE (*Defense Industrial Base Collaborative Information Sharing Environment*), enables specialized analysts to find linkages between related offenses and to observe patterns across all investigations. The aim of such intelligence is to provide stakeholders with knowledge that can be useful for detecting and disrupting future attacks at both an operational and strategic level. The success of

this approach led to the development of standardized, federated computer systems that enable sharing of actionable intelligence about malware and network intrusions at machine speed. The Automated Indicator Sharing (AIS) capability maintained by the U.S. Department of Homeland Security (DHS) extended this approach, in 2015, to encompass a growing number of organizations in the private and public sector [9, 13].

Finally, this automated exchange of forensic information can be complemented by higher level organizational information exchange. For example, collaboration among banks and law enforcement is common in the fight against cybercrime activity. Modern banking malware is designed using a modular architecture allowing criminals to simultaneously target account logins at multiple banks. A single malware infection will give attackers access to bank accounts without knowing which bank the victim is using. When banks collaborate and share intelligence information about attackers, infections, and money flows, they are able to find common ways to detect attacks, block fraudulent payments, or disrupt criminal operations. Law enforcement is also involved with the banks, and intelligence sharing helps ongoing investigations and leads to additional sources of digital evidence.

While most cyberthreat information shared is sector-independent, and useful for any organization, including common infrastructure indicators of compromise (IOCs) such as hashes of malware files, botnet command and control IPs, and malicious URLs or domain names. However, some of the cyberthreat information shared is sector-specific and hence only of interest to a particular industry. For example, finance industry stakeholders share fraud indicators and information about criminal money mules, and other threat information directly relevant to their business. The automotive industry shares information specific to automotive electronics (e.g., CAN bus vulnerabilities.), and the entertainment industry focuses more on cyberthreat information related to copyright violations (e.g., peer-to-peer file sharing, DRM vulnerabilities). Managers and stakeholders must, therefore, tailor their efforts, such as ISAC memberships, to the extent to which the attacks they face are more of a general or more of a sector-specific nature.

3 Illustrative Example

The following scenario illustrates the iterative forensic learning cycle we have described in the preceding subsections. It is not intended to represent all possible steps that an organization can take when faced with a targeted cyberattack. Instead, we aim to illustrate how forensic preparedness, detection, scope assessment, agile cybersecurity retrospectives, forensic intelligence and information sharing can interact.

An organization was alerted by a government organization that known threat actors were observed accessing the organization's network. As part of its forensic preparations years before, the organization had segmented critical IT assets onto a

secured network with full network level logging/monitoring that was only accessible from certain systems within their network. However, the victim organization did not have centralized logging infrastructure, making it necessary to search logs stored on potentially compromised systems. In addition, they did not have all of their system clocks synchronized, creating added work when correlating logs. Indications of compromise were found in some logs but the organization did not have an archive of old logs, and the root cause and original date of compromise could not be determined. While assessing the scope of the intrusion, the victim organization held daily calls for members of the cyberdefense team to exchange forensic findings from compromised hosts, logs, network traffic and backups.

The team used a shared spreadsheet to track tasks as well as significant forensic analysis findings (e.g., compromised systems, accounts, external IP addresses, domains). They used a separate secure system for all electronic communications. When the cyberdefense team was satisfied that they had performed a comprehensive scope assessment, the organization executed a coordinated containment and eradication plan that removed all known compromised assets. The team maintained a heightened level of monitoring across the organization to determine whether the cyberattackers still had unauthorized access. Applying the lessons learned from the cyberattack, the organization reduced its number of Internet gateways and implemented full packet network monitoring and NetFlow at strategic points throughout the network. Realizing the value of having a mechanism to keep track of forensic analysis tasks and findings, the organization implemented a system for managing incidents to observe trends and potential links between incidents, rather than relying on a shared spreadsheet to track details of cyberattacks. This system was developed into a Forensic Intelligence platform that served internal cybersecurity operations. The organization also shared cyberthreat information with others in the industry sector to determine the full scope of the cyberattack. Industry partners used this cyberthreat information to gain more insight into cyberattacks on their networks, and developed YARA signatures that were shared back with the original organization to enable detection at all phases of the defense process.

4 Conclusion

Effective detection of cyberattacks depends on forensic findings and fuels scope assessment and forensic intelligence. Forensic preparedness, in turn, reinforces scope assessment and increases the cyberresilience critical infrastructure. It also enables rapid cyberdefense decision-making. Effective scope assessment requires organizations to resist the impulse to block or eradicate longstanding attacks until they have been more fully understood with the support of forensic analysis. An agile cycle of implementing insights gathered from forensic analysis of cyberattacks facilitates the continuous improvement of security measures. Forensic intelligence systematically keeps track of evidence and defensive measures from past cyberattacks. This repository of past knowledge (memory) is a crucial component of

forensic intelligence. Building and querying this memory must be continuous, iterative and integrated in overall cybersecurity operations. The resulting insights into threat actor Tactics, Techniques and Procedures (TTPs) and generalized behaviors provide actionable intelligence to counter targeted cyberattacks.

All in all, the iterative learning cycle proposed in this chapter should help organizations to establish a resilient and rapid cyberdefense capability. Forensic preparedness, a robust scope assessment process, an agile improvement cycle, and a strong forensic intelligence feedback loop are the tools by which this capability is created in organizational practice. This capability does not only improve the cybersecurity of the focal organization, but also contributes to a better industry-wide protection once forensic knowledge is systematically integrated and shared. For example, the particular experience of a single organization can aid law enforcement as they conduct inquiries into similar attacks.

Acknowledgement Thanks to Christopher Daywalt for his collaboration and talents investigating sophisticated network intrusions and malware.

References

1. Barnum, S.: Enabling effective cyber threat intelligence and information sharing. In: Proceedings of the International Conference on Cyber Security. Fordham University, New York (2013)
2. CASE: An international standard for sharing cyber-investigation traces. Cyber-Investigation Analysis Standard Expression (2019). https://caseontology.org/
3. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic, Waltham (2004)
4. Casey, E.: Investigating sophisticated security breaches. Commun. ACM **49**(2), 48–55 (2006)
5. Casey, E.: Standarization of forming and expressing preliminary evaluative opinions on digital evidence. Digital Investigation **32** (2020)
6. Casey, E., Daywalt, C., Johnston, A.: Chapter 4 - Intrusion investigation. In: Casey, E., et al. (eds.) Handbook of Digital Forensics and Investigation, pp. 135–206. Academic Press, San Diego (2010)
7. Casey, E., Back, G., Barnum, S.: Leveraging cybox to standardize representation and exchange of digital forensic information. Digit. Investig. **12**, 102–110 (2015)
8. Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., Nelson, A.: Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. J. Digit. Investig. **22**, 14–45 (2017)
9. Casey, E., Ribaux, O., Roux, C.: The kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. J. Forensic Sci. **64**(1), 127–136 (2019)
10. Chaffetz, J., Meadows, M., Hurd, W.: The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation. Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Congress (2016)
11. CHDS: Department of Defense Cyber Crime Center. Center for Homeland Defense and Security (2019). https://www.hsdl.org/?abstract&did=690826
12. DC3 Malware Configuration Parser (DC3-MWCP) (2020). https://github.com/Defense-Cyber-Crime-Center/DC3-MWCP
13. DHS: Automated Indicator Sharing (AIS). U.S. Department of Homeland Security, CISA (2019). https://www.us-cert.gov/ais

14. DHS/FBI: Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructures Sectors. U.S. Department of Homeland Security, CISA (2018). https://www.us-cert.gov/ncas/alerts/TA18-074A
15. Elyas, M., Ahmad, A., Maynard, S., Lonie, A.: Digital forensic readiness: expert perspectives on a theoretical framework. Comput. Secur. **52**, 70–89 (2015)
16. Europol: Internet Organized Crime Threat Assessment. Technical Report, European Cybercrime Center (2019). https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
17. Good practice guide forensic readiness. UK National Technical Authority for Information Assurance (2016)
18. GovCERT.ch: Technical Report About the Espionage Case at Ruag. GovCERT.ch (2016). https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case
19. Grispos, G., Glisson, W., Storer, T.: Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digit. Investig. **22**, 62–73 (2017)
20. Johnston, A., Reust, J.: Network intrusion investigation preparation and challenges. Digit. Investig. **3**(3), 118–126 (2006)
21. Kovacs, E.: Hackers Behind Triton ICS Malware Hit Additional Critical Infrastructure Facility, SecurityWeek (2019). https://www.securityweek.com/triton-hackers-focus-maintaining-access-compromised-systems-fireeye
22. Lee, R.: The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey. SANS (2017)
23. Malin, C., Casey, E., Aquilina, J.: Malware Forensics: Investigating and Analyzing Malicious Code. Syngress Press (2008)
24. MISP: Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Malware Information Sharing Platform (2019). https://www.misp-project.org/index.html
25. Nikkel, B.: Practical Forensic Imaging. No Starch Press, San Francisco (2016)
26. NIST: Draft NIST roadmap for improving critical infrastructure cybersecurity version 1.1. National Institute of Standards and Technology (2017). https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf
27. NIST: Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology (2018). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
28. Pollitt, M., Casey, E., Jaquet-Chiffelle, D.O., Gladyshev, P.: A framework for harmonizing forensic science practices and digital/multimedia evidence. Technical Report, The Organization of Scientific Area Committees for Forensic Science (2018)
29. Ribaux, O., Walsh, S., Margot, P.: The contribution of forensic science to crime analysis and investigation: Forensic intelligence. Forensic Sci. Int. **156**(2), 171–181 (2006)
30. Roberts, S., Brown, R.: Intelligence-Driven Incident Response: Outwitting the Adversary. O'Reilly Media, Waltham (2017)
31. Sherstobitoff, R., Malhotra, A.: Operation sharpshooter. Techical Report, McAffee (2018). https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf
32. Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., Thomas, C.: MITRE ATT&CK: Design and Philosophy, MITRE Product MP18030 (2019). Project No.: 01ADM105-PI. https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf
33. SWGDE: Swgde digital multimedia evidence glossary. SWGDE (2016). https://www.swgde.org/documents/CurrentDocuments/SWGDEDigitalandMultimediaEvidenceGlossary
34. Zhang, E.A.: Indictment: Conspiracy to Damage Protected Computers. U.D.C.S.D (2018). https://www.justice.gov/opa/press-release/file/1106491/download