Integrating digital forensics as a core component of enterprise incident management.

Alioune Ben Mor DIANKHA (adiankha@aimsammi.org)
African Institute for Mathematical Sciences (AIMS)

Supervised by: DIAO Dr. Oumar
African Institue of Mathematical Sciences , SENEGAL

April 11, 2023

Abstract

The paper discusses the symbiotic relationship between incident response and digital forensics in organizational information security. Incident response is crucial for identifying and mitigating security incidents, while digital forensics aims to preserve and analyze digital evidence to reconstruct events. Mastering both disciplines is essential for effective incident management.
This thesis combines standards and best practices to propose enterprise policies that enhance incident management by integrating digital forensics. The concept of forensic readiness is introduced to enable organizations to respond more effectively to incidents, deter unauthorized actions, and reduce investigation costs. This work will be beneficial to digital investigators, security researchers, and policy analysts seeking to understand and implement forensic policies in enterprise environments.

Keywords

Incident management, Digital forensic, malware analysis, corporate investigation, digital evidence.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Alioune B. M. DIANKHA , 24 October 2019

Contents

1. Introduction

The primary obligation of any company is to ensure its survival, allowing it to fulfill its commitments to stakeholders, maintain its operations, and generate profits. However, unforeseen events, whether natural disasters or man-made incidents, can disrupt business operations. In response, organizations have developed strategies such as incident response, awareness training, disaster recovery, and business continuity planning to mitigate risks and ensure continuity.

Beyond the operational challenges, such events can also give rise to legal, regulatory, and financial ramifications. Digital evidence plays a crucial role in investigating incidents within organizations that rely on IT infrastructure. Every interaction with information systems leaves a digital trail, making digital forensics indispensable in uncovering the events leading to an incident, such as data breaches or security breaches.

The importance of digital forensic capabilities extends beyond individual organizations to the broader legal system. Without a robust forensic capability, organizations risk overlooking critical evidence, potentially leading to miscarriages of justice or disruptions in legal proceedings. Moreover, as cybercrime continues to proliferate, understanding digital evidence has become essential for both victims and perpetrators alike.

Digital forensics, once the domain of law enforcement agencies, has now become accessible to a wide range of stakeholders, including private sector companies, organizations, attorneys, and individuals. Most individuals conduct some form of incident analysis on their own without formal training, and many security teams work through similar processes as they conduct investigations without realizing that they are, in fact, engaged in forensic process. When forensic experts conduct investigation, it is based on a formalized process, principles and good practices that have been captured over the years

This paper provides an overview of digital forensics as a core component of enterprise incident management. It is structured into three sections: establishing foundational concepts, integrating forensic processes into incident response management, and leveraging forensic tools to mitigate external threats. By proposing enterprise policies to enhance incident response through digital forensics, this thesis aims to equip organizations with the tools and insights needed to effectively respond to incidents and bolster their resilience in the digital age.

2. Foundation

2.1 Terminology and definitions

This section lays the groundwork by defining key terms necessary for understanding the subsequent discussions within this document.

2.1.1 Events and Incidents

In an organizational context, events occur regularly within systems or networks, but not all qualify as incidents. An incident is generally defined as an adverse event that has caused or has the potential to cause damage to an organization's assets, reputation, or personnel, affecting its computer and network security or its ability to conduct business.

Incidents often begin with minor anomalies that require further investigation. They can be challenging, exciting, and even frustrating, often interrupting normal operational procedures and causing stress among involved parties. While intrusions are a common form of incident, not all incidents involve unauthorized access to systems.

Defining an incident requires careful analysis and triaging of events. Not all unusual occurrences qualify as security incidents, but universally recognized types include unauthorized data access, illegal building access, malicious code infections, data breaches, and any violation of the law. This paper focuses specifically on computer security-related adverse events, which may also have non-technical causes.

2.1.2 What is incident response?

Incident response refers to the set of processes and procedures initiated to address a potential security incident once it has been identified. It is a critical security function aimed at managing incidents in a timely and cost-effective manner.

Effective incident response allows organizations to limit the damage caused by incidents and expedite recovery efforts. To facilitate this, organizations establish incident response capabilities within their existing policies, procedures, and processes, often including documented plans, multidisciplinary teams, and predefined processes and techniques.

An incident may elicit various reactions, but a swift and efficient response is crucial for controlling its effects and restoring normal business operations. In enterprise environments, responders follow a systematic approach to assess incident severity and determine the likelihood of successful response for damage limitation.

The initial stage of incident response involves confirming whether an incident has occurred, typically prompted by a user report or management notification. Once verified, the response team initiates actions to restore affected services or systems to normal levels. Depending on the severity, incidents may require comprehensive investigation and mitigation efforts, with the response team guiding and supporting the process until resolution.

2.1.3 What is Digital Forensics?

Within the realm of computer security, various sub-disciplines have emerged, with one notable area being computer forensics. Forensics, in essence, applies scientific methods to legal matters, and computer forensics combines investigative techniques with computer security principles to address crimes committed via digital mediums.

The rigorous investigative approach used in traditional forensics is equally applicable to computer forensics, although primarily employed in criminal cases, it can extend to civil matters as well. Digital forensics, a subset of forensic science, deals specifically with crimes occurring in digital environments. It involves employing computer investigation and analysis techniques to ascertain potential legal evidence.

Digital forensics is often used interchangeably with computer forensics but may encompass a broader range of devices beyond conventional computers. As a scientific process, it must be replicable by any third party and yield consistent results.

Given the widespread use of electronic devices in business and personal contexts, investigations frequently encounter digital evidence. Digital forensics plays a vital role in civil and criminal investigations, particularly within enterprises where it is integral to incident response efforts.

In the corporate setting, digital investigations prioritize timely response and damage assessment while adhering to evidentiary standards. Despite varied investigation types, the sources of evidence remain consistent, encompassing numerous devices such as workstations, laptops, and servers.

Digital forensics is chiefly employed in investigations likely to culminate in legal proceedings, emphasizing the importance of evidence integrity and legal admissibility. Apart from supporting criminal cases, it aids in data recovery and internal administration tasks like abuse monitoring.

Moreover, digital forensics tools and techniques contribute to incident response procedures within enterprises. Although often conflated, incident response and digital forensic investigation serve distinct roles. While digital forensics delves into technical aspects and identifies root causes, incident response encompasses broader actions aimed at mitigating incidents and restoring operations.

Balancing thorough forensic analysis with operational continuity poses a challenge in incident response. While a meticulous forensic approach may yield valuable insights, it can prolong operational downtime. Response teams must navigate this balance, prioritizing evidence collection while minimizing disruptions to business operations.

By preparing for legal and technical challenges in evidence collection, response teams can leverage digital evidence to uncover incident root causes and facilitate organizational recovery.

2.2 The need for Digital Forensics

While forensic science has a rich history spanning over a century, digital forensics emerged more recently with the advent of personal computers in the 1980s. Unlike traditional forensics, which deals with physical evidence, digital forensics focuses on investigating crimes committed using digital devices and mediums. This evolving field serves both public and private sectors, aiding in investigations related to cybercrimes, policy violations, civil litigations, and more.

In today's digital age, where transactions and interactions often occur in digital formats, organizations rely heavily on digital evidence to substantiate events or failures. People leave digital footprints of their activities, and this information can be crucial in various legal processes, including discovery, depositions, and litigation. Digital evidence can support legal defenses, intellectual property claims, verification of commercial transactions, and internal disciplinary actions.

Almost every criminal activity leaves a digital trail, necessitating the expertise of forensic investigators to uncover, process, and present evidence. While not every investigation ends up in court, it's essential to gather evidence in a manner that meets legal standards to withstand scrutiny. Digital forensic inves-

tigation involves employing best practices and procedures to produce compelling evidence for building a solid case.

Forensic investigators possess a unique blend of investigative, legal, and computing skills required to navigate complex digital environments. While digital forensics is not always accurate, experienced specialists can often uncover more evidence than anticipated. These investigations encompass processes, techniques, and tools aimed at combating computer abuse and crime, addressing incidents such as data recovery, identity theft, malware investigations, and corporate espionage.

In some cases, organizations may opt to involve law enforcement to prosecute computer crimes. However, many prefer to handle matters internally to minimize operational disruptions. Regardless of the approach, legal considerations, including privacy laws, industry regulations, and corporate policies, must be carefully navigated throughout the investigation process.

Time is of the essence in digital forensic investigations to prevent evidence destruction or compromise and minimize operational downtime. Once launched, investigations must proceed swiftly to restore operations and recover any losses incurred. Ultimately, digital forensic investigation serves as a vital deterrent to cybercrimes, contributing to improved network security and reduced crime rates in digital environments.

3. Integrating Forensic into Incident management

Incidents, whether intentional or accidental, arise from a multitude of human and non-human factors. Actual high-profile digital breaches have underscored the critical need for effective incident response and forensic capabilities. These incidents not only disrupt major networks and agencies but also incur significant financial losses, both directly and indirectly. Moreover, they erode public trust in affected companies, amplifying the overall impact.

In today's digital landscape, every major corporation, governmental agency, and online-operating organization must be equipped to respond to unexpected or malicious attacks on their networks and infrastructure. Recognizing malicious adversarial attacks as an inevitable risk, organizations must proactively plan to ensure ongoing operations in the face of such events. This begins with senior leadership acknowledging the significant risk and committing to understanding and addressing potential incidents for informed decision-making.

Incident management involves developing and maintaining the capability to manage incidents within an organization, mitigating their impact on business operations and achieving recovery within specified time objectives. While understanding the incident response process is crucial, building capability requires attention to elements such as personnel, policies, and procedures. A robust response capability enables effective management of response expenses, enhances risk assessment accuracy, and improves user training and awareness in computer security.

Traditionally, IT incident response in the private sector focuses on restoring IT infrastructure defenses, patching vulnerabilities, and cleaning up damage, often relegating digital forensics to a peripheral role. However, the incident landscape has evolved to become more complex and global, involving multiple organizations. Positioning digital forensics as a central component of incident response offers significant benefits and mitigates increasing risks associated with leaving it peripheral.

In incident response, forensic science applies scientific principles to investigative matters. Forensic teams may be tasked with acquiring and analyzing digital evidence using specialized tools and techniques. To ensure the admissibility of evidence in court, digital forensics examiners must understand legal issues and nuances of the forensic process. Establishing a forensic capability within an organization, with diverse team members, becomes essential when multiple forensic tasks are required. However, if the focus is primarily on supporting incident response investigations, starting with an incident-focused role within the forensic team is advisable.

3.1 Establishing a Forensic capability

Incident response is a crucial method that organizations employ to identify and recover from incidents with minimal impact on business operations. Digital forensics, on the other hand, involves a scientific investigation into the causes of incidents with the aim of bringing perpetrators to justice, resolving litigation, or enforcing policy. While these two disciplines have a close and complex relationship, they are both essential when an incident occurs.

One of the significant challenges in computer forensics is the need for a paradigm shift in responding to computer incidents. Often, organizations prioritize resuming production over collecting evidence, potentially destroying valuable information in the process. However, it's essential to realize that systems

may contain evidence and should not be tampered with until proper steps have been taken to preserve any potential evidence. Legal rules for evidence collection and preservation form the basis by which evidence can be admitted or excluded during legal proceedings.

Digital forensics plays a critical role in incident response capability by facilitating timely response, damage assessment, and maintaining evidentiary standards. The forensic aspect should be integrated into incident management rather than treated as an afterthought. Different types of incidents, such as criminal incidents, policy violations, industry-specific incidents, civil litigation activities, and accidents, may require varying levels of forensic investigation.

It may be beneficial for organizations to outsource specialized forensic services, especially if they are not conducted frequently. However, developing an in-house forensic team is advocated for building organizational response capabilities.

Organizations should undertake preparatory measures to effectively apply digital forensics investigations to incidents. This includes building and maintaining forensic-related skills within the incident response team, facilitating communication and coordination throughout the organization, and acquiring necessary forensic tools and resources.

There is no one-size-fits-all approach to incident response and forensic capability. The incident type and organization's needs will dictate the most suitable combination of incident response and forensic models and approaches.

3.1.1 Policies to Enhance Forensics

Policies play a crucial role in enhancing digital forensics investigations. They provide the foundation for security programs and activities, including designing controls, establishing user access controls, conducting risk analysis, and disciplining workers for security violations. These policies must be enforced by management to be effective.

Senior management support is crucial for defining corporate incident response policies and procedures, which ensure proper digital evidence collection and preservation. Clear roles and responsibilities must be defined, especially concerning other corporate staff, during response efforts and subsequent investigations.

While digital forensic investigation is part of the response process, it must be rigorous enough to capture evidence admissible in a courtroom. Forensics capability should be designed or added-on with enforcement mechanisms to collect and preserve digital evidence correctly.

Specifying forensic system properties through policies can have several benefits, including assisting in the design of systems and networks to meet forensic requirements, clarifying capabilities needed to meet policies, and allowing for formal verification of an organization's forensic capabilities.

Forensic policies should be tailored to an organization's security requirements and exposure to risk. They may be written as an inclusive policy or documented separately to address specific concerns. Integration with other policies related to security teams is essential.

In addition to response policies, organizations should develop and implement forensic-based policies for forensic activities conducted by corporate forensic teams. These policies and procedures should cover various activities performed during forensic investigations, ensuring user compliance and utilization.

Ultimately, an evidence-based approach is crucial for organizations to gather and use digital evidence effectively, thereby enhancing their ability to respond to incidents and deter computer crime.

The necessity of gathering and utilizing digital evidence has been emphasized in recent literature. Yasinsac and Manzano (2001) advocate for a set of policies to aid enterprises in deterring computer crime and improving their ability to conduct computer and network forensics effectively. They propose five categories of policies aimed at enhancing systems and network forensics in enterprises.

1. **Retaining Information:**
   - Implement a policy for systematically storing and retaining application and user files as potential evidence.
   - Establish a corresponding policy to protect the use of backups as evidence in court.
   - Clarify to employees that they have no expectation of privacy regarding company files and equipment usage.
   - Define acceptable use policies for company equipment with no expectation of privacy.
   - Maintain records of network events, such as login/logout activities and network service access, for potential evidence.
2. **Planning the Response:**
   - Establish a dedicated Forensics Team consisting of members from upper management, Human Resources, technical staff, and external experts.
   - Develop an Intrusion Response Procedure to guide employees in suspected attack scenarios.
   - Formalize Investigative Procedures to ensure a standardized approach when intrusions are detected.
3. **Training:**
   - Provide training to all personnel on company security policies and forensic procedures.
   - Conduct specialized training for the response team members to prepare them for decision-making in various scenarios.
   - Ensure the investigative team possesses the necessary computer forensics skills to follow investigative procedures effectively.
4. **Speeding up the Investigation:**
   - Prohibit personal file encryption to ensure accessibility during investigations.
   - Disallow the use of disk scrubbing tools and file shredding software to prevent delays in file recovery.
   - Utilize data indexes and information fusion techniques to expedite data inspection and correlation.
   - Prevent anonymous activity while balancing privacy concerns with investigation needs.
   - Require date, time, and user stamps in files to track modifications and deletions accurately.
   - Implement strong user authentication and access control mechanisms to restrict unauthorized access.
5. **Protecting the Evidence:**
   - Enforce strict control over administrative access to systems containing potential evidence.
   - Encrypt evidence files and connections to maintain their integrity and authenticity.

- Apply robust integrity checking technology periodically to ensure evidence remains uncorrupted.

Adhering to these policies can significantly enhance an organization's ability to respond to incidents effectively and conduct forensic investigations with integrity and accuracy.

The necessity of integrating Forensics into Incident response activities is highlighted in the guidance document SP 800-86. According to NIST, forensic policies should permit authorized personnel to monitor systems and networks and conduct investigations for legitimate reasons under appropriate circumstances. Organizational policies should address several considerations related to forensics:

1. **Defining Roles and Responsibilities:**
   - Clearly define the roles and responsibilities of individuals involved in the organization's forensic activities.
   - Specify internal teams and external organizations to contact under different circumstances.
2. **Guidance for Forensic Tool Use:**
   - Establish policies outlining the reasonable and appropriate use of forensic tools under various circumstances.
   - Describe necessary safeguards for sensitive information recorded by forensic tools and requirements for handling inadvertent exposure.
3. **Supporting Forensics in the Information System Life Cycle:**

Incorporate forensic considerations into the information system life cycle, including:

- Regular backups and maintenance of previous backups.
- Enabling auditing on workstations, servers, and network devices.
- Forwarding audit records to secure centralized log servers.
- Configuring applications for auditing and maintaining records of file hashes and network/system configurations.
- Establishing data retention policies supporting historical reviews and compliance with legal requirements.

Organizations must also develop guidelines and procedures for performing forensic tasks, including general methodologies for investigating incidents and step-by-step procedures. These guidelines should support the admissibility of evidence into legal proceedings and ensure the reliability and integrity of electronic records. Regular review and maintenance of these guidelines are essential to keep them accurate.

The forensic policy aims to capture digital evidence while preserving its forensic integrity for legal purposes, addressing both reactive and proactive requirements. Policies should focus on supporting the prosecution of criminal acts associated with specific assets rather than preserving data for all assets, which could be wasteful.

Given the reactive nature of incident response, digital forensic investigations often occur reactively. However, current ad hoc approaches may not be scalable to address a significant number of incidents efficiently. There is a need for a fundamentally different approach to computer security response—one that quickly detects and reacts to incidents in an efficient and cost-effective manner.

The development, integration, and implementation of proactive forensics standards, including organizational policies, are crucial. Forensic Readiness represents the integration of digital forensics as a core component of enterprise incident management. It requires a plan, resources, and means of identifying sources of useful data before incidents occur. This proactive approach aims to create more efficient and effective digital forensic processes.

3.2 Forensic Readiness

In many organizations, while incident response plans are diligently developed for post-incident investigations, little attention is paid to preparing systems and procedures beforehand. This proactive approach, termed digital forensic readiness, involves identifying, preserving, and storing digital evidence. Essentially, forensic readiness equips an entity to efficiently capture and utilize digital evidence. Although acknowledged within the digital forensics research community (Endicott-Popovsky and Frincke (2006) ; Tan (2001); Yasinsac and Manzano (2001)), the specification and implementation of forensic readiness lack consistency Endicott-Popovsky and Frincke (2006).

Typically, a forensic investigation is initiated as a response to a serious security breach or criminal incident, commencing when a crime is committed or discovered, and investigators seek to seize evidence. However, there are numerous instances where organizations could benefit from gathering and preserving digital evidence before an incident occurs. Forensic readiness entails an organization's capability to collect, preserve, protect, and analyze digital evidence effectively for legal, disciplinary, or court proceedings. It ensures maximizing the utilization of digital evidence while minimizing investigation costs.

Forensic readiness differs from preventative and recovery measures, focusing on enabling the use of digital evidence rather than preventing incidents. While security programs emphasize prevention and detection, there are various scenarios where having access to digital evidence before an incident proves beneficial. Digital forensics primarily addresses post-incident investigations, but recent research emphasizes proactive measures through forensic readiness plans.

Transitioning from a reactive to proactive stance necessitates a paradigm shift in information security disciplines to include digital forensics. It requires revisiting existing security policies, procedures, and tools to comply with stringent evidence collection and storage standards for legal admissibility. While many organizations prioritize disaster recovery and business continuity plans, recognizing the importance of forensic readiness planning is essential. Relying solely on reactive approaches can disrupt operations, compromise evidence, and incur unnecessary costs.

Forensic readiness entails pre-identifying evidence categories, establishing acquisition procedures, and ensuring preparedness through staff training, tools, and external support. It facilitates swift action during incidents, evidence collection, investigation, and communication with relevant parties. Moreover, it enhances risk management, increases efficiency, and reduces incident response costs.

Incorporating forensic readiness into organizational processes leverages incident response, business continuity, and crime prevention activities. Effective forensic readiness ensures the maintenance and collection of both digital and physical evidence, preventing its loss or compromise. Organizations need to actively gather digital evidence, prioritize resources, and make informed decisions to preserve potential evidence effectively.

Ultimately, comprehensive evidence gathering can act as a deterrent, support efficient investigations, extend information security coverage, and improve legal outcomes. Preparation involves enhanced monitoring, data security measures, staff training, legal guidance, and collaboration with law enforcement,

ensuring adherence to evidential standards and legal sensitivities.

3.2.1 Implement Forensic Readiness

Many organizations, as part of their broader information security, incident response, and crime prevention efforts, already undertake some activities essential for effectively collecting and utilizing electronic evidence. However, what is often lacking is a systematic and proactive approach to gather and preserve evidence to meet their business needs. Legal advisors can offer additional insights and suggest measures to justify the progression to formal actions, ensuring cost-effectiveness and favorable outcomes for the company. Although the decision on how to proceed typically occurs post-incident, significant legal preparation is necessary beforehand.

Forensic readiness complements and enhances existing information security activities, closely intertwining with incident response and business continuity to preserve evidence and ensure continuity. Establishing a forensic readiness plan ensures the availability of digital evidence in a usable format when needed, necessitating staff training and proper policies for compliance. It's vital to integrate forensic readiness seamlessly into incident management and other related business planning activities to avoid inefficiencies and conflicts.

For organizations intending to manage forensic work internally, forensic readiness entails ensuring the necessary capabilities for successful investigations are in place, with a focus on fully training and empowering potential investigators in digital forensics. Thus, forensic readiness fosters a corporate approach to digital evidence, requiring trained staff familiar with evidence sensitivities, company investigation policies, and external interfaces. Implementing forensic readiness involves understanding evidence sources, legal and cost-effective evidence gathering, escalating suspicious events to formal investigations, and collaborating with law enforcement agencies when necessary.

While work has begun to define elements of forensic readiness, the investigative process remains laborious, time-consuming, and complex, often requiring specialized expertise. Efficiency in digital forensics is measured in terms of cost, with significant costs associated with systems lacking forensic readiness. Although various studies have discussed forensic readiness characteristics Endicott-Popovsky and Frincke (2006) ; Tan (2001); Yasinsac and Manzano (2001), there's no universal methodology or approach to enable it within systems or enterprises.

Implementing forensic readiness policies may require new procedures and policies but should generally involve incremental enhancements to existing ones, such as data retention, incident response, and information security. These policies should address all aspects necessary before any forensic-related security incidents occur, including data collection, preservation, and cost reduction for later prosecutions. By proactively specifying what data should be preserved and what is unnecessary, organizations can efficiently utilize resources and clarify which events require forensic action.

A clear forensics policy should categorize events into those requiring forensic action and those that do not, streamlining the preservation process and avoiding unnecessary data collection. Authors have emphasized the importance of forensic readiness, highlighting the need for organizational readiness alongside technical considerations. Implementing a forensic readiness plan involves risk assessment, identifying evidence sources, legal capabilities, storage and monitoring policies, staff training, and legal review assessments.

The necessity of implementing a Forensic Readiness plan has been underscored by numerous authors. Rowlingson (2004) not only examines forensic readiness from a technical standpoint but also emphasizes the importance of organizational preparedness through specific procedures and processes. The central thesis of this paper asserts that forensic readiness holds significance from a business perspective and

can lead to cost savings in the event of an investigation. Enterprises are advised to proactively gather potential evidence, such as log files, network traffic records, emails, and telephone records, before any involvement in an investigation. This proactive approach forms the basis of a forensic readiness policy, encompassing elements like risk assessment, identification of evidence sources, legal capabilities, storage and monitoring policies, staff training, and legal review assessment.

The proposed ten steps to achieve forensic readiness contextualize digital evidence within a business framework and outline practical approaches necessary for organizations to develop forensic readiness capabilities:

1. **Define the business scenarios requiring digital evidence:** Conduct a risk assessment to identify scenarios where digital evidence may be required to mitigate the impact of computer-related crimes, comply with legal constraints, support disciplinary issues, contractual agreements, or dispute resolution.

2. **Identify available evidence sources:** Understand the potential sources of evidence within organizational systems, categorizing evidence into background (gathered for normal business reasons) and foreground (specifically collected for detecting crimes).

3. **Determine evidence collection requirements:** Conduct a cost-benefit analysis to determine the cost of collecting required evidence and its utility, considering factors like metadata, corroboration, redundancy, associations, storage duration, evidence size, and hardware.

4. **Establish a capability for secure evidence gathering:** Ensure that evidence is collected and preserved authentically, adhering to legal requirements and security measures to prevent tampering or manipulation.

5. **Establish a policy for secure evidence storage and handling:** Develop policies and procedures for securely storing and handling evidence to maintain its authenticity and integrity, ensuring compliance with legal standards like continuity of evidence or chain of custody.

6. **Implement targeted monitoring to detect major incidents:** Monitor evidence sources to detect potential incidents in a timely manner, akin to Intrusion Detection Systems, and develop policies for suspicion detection and reporting.

7. **Specify circumstances for escalating to a formal investigation:** Review suspicious events to determine if escalation to management or formal investigation, potentially utilizing digital evidence, is warranted based on the severity of the event and potential business impact.

8. **Train staff in incident awareness:** Provide comprehensive training to staff involved in incident response and evidence handling to understand their roles, legal sensitivities, and decision-making processes.

9. **Document evidence-based cases:** Develop policies for assembling evidence-based cases describing incidents and their impacts, ensuring thorough documentation for future reference.

10. **Conduct legal review for response actions:** Seek legal advice at various stages of case collation to assess the strength of the case and determine appropriate follow-up actions, ensuring justification, cost-effectiveness, and favorable outcomes for the organization.

These steps assume the presence of appropriate preventative security measures based on a comprehensive risk assessment. Implementing digital forensics standards faces challenges due to the evolving nature of investigation procedures, lack of standardization in the industry and academia.Another difficulty in implementing digital forensics standards is the complexity of the information security legal background.

4. Experiments

4.1 Malware Analysis

Malware Analysis Malware serves as a versatile tool for cybercriminals and adversaries targeting corporations or organizations. In today's evolving landscape, merely detecting and removing malware artifacts is insufficient; it's crucial to understand their operations to grasp the context, motivations, and objectives behind breaches.

This section offers heuristics for analyzing malware behavior and interpreting the results while exploring the tools utilized. By doing so, readers gain a solid understanding of these methods, enabling them to interpret analysis outcomes effectively within the context of incident investigations. While malware analysis is a deeply specialized field, this section provides effective steps for identifying and understanding malware to support incident response and forensic investigation efforts. From an incident responder perspective, understanding malware behavior and identifying affected systems are key issues that need addressing.

During incident response, forensic analysts often encounter the challenge of identifying potentially malicious code that ran on an impacted system. Several online services offer free malware sample analysis, providing automated reports regarding sample behavior. These services maintain databases compiled from thousands of analyzed samples, threat intelligence feeds, antivirus signatures, and other data sources to offer context around observed behaviors and indicators.

In cases where using a third-party service is not appropriate, maintaining an in-house automated malware analysis sandbox system is recommended. The open-source Cuckoo project, available at https://cuckoosandbox.org, stands out as a popular tool for automating routine tasks during behavioral analysis.

Despite the risks associated with modern security mechanisms, malware remains a popular weapon in adversaries' arsenals. While incident responders may lack the training or time to fully analyze each encountered malware sample, performing behavioral analysis to determine actionable indicators of compromise is well within the reach of all forensic and incident response teams. Building and utilizing automated sandboxes and malware analysis platforms enable analysts to understand malware encounters and take appropriate investigative and preventive actions.

The most technically intensive analysis in most incidents involves analyzing the malware involved. Two basic techniques, static and dynamic analysis, are used for understanding malware behavior. Basic static and dynamic analysis skills are essential for every incident responder and forensic analyst. Both types of analysis offer advantages, and incident response analysts should be familiar with both methodologies.

In dynamic analysis, the analyst runs malware in a controlled monitored environment to observe its behavior. The key to dynamic analysis is having a safe environment to execute the malware while collecting good telemetry. The most common technique for dynamic analysis is using a sandbox, which typically runs a sample on a purpose-built system, often in a virtual machine isolated from the internet. By allowing the sandbox to perform routine analysis tasks, analysts can review reports and focus on areas of interest for additional manual analysis as needed.

Another form of analysis involves understanding malware at the code level without running it, using tools like disassemblers. However, full reverse engineering requires significant effort.

Forensic identification is the practice of identifying infected hosts by looking for unique evidence of

malware in memory, on disk, or in the operating system. Even the stealthiest malware needs to persist in some manner, making evidence of compromise essential. In the initial parts of an incident response investigation, it is unknown how many systems are likely compromised by the same malware.

Dynamic malware analysis involves detonating malware in a controlled environment or malware sandbox. During this analysis, responders gain insights into indicators of compromise (IoCs) associated with the malware and can better identify other impacted systems.

While dynamic analysis provides insights into malware actions, it is less time-consuming than static analysis. Responders often need to identify IoCs associated with the malware to craft additional detective and preventive controls to contain incidents and mitigate damage. Understanding these IoCs provides responders with deeper insights into malware behavior and its relationship to the incident.

The research methodology adopted in this study is based on experiments and observations. An experiment conducted in February 2023 aimed to determine the artifacts created by a suspicious program on a compromised system.

Upon receiving notifications, the incident response team must verify if a threat truly exists. Various methods, including platforms like VirusTotal, aid in determining threat severity based on collective experiences.

Figures 4.1 through 4.6 display sample results obtained by uploading the suspicious file to VirusTotal, providing insights into initial analysis outcomes and behavioral patterns. Figure 4.1 shows the results of the analysis of the suspicious file, indicating that some virus engines detected the file as malicious. The results for the first 13 engines are shown in Fig. 4.1.

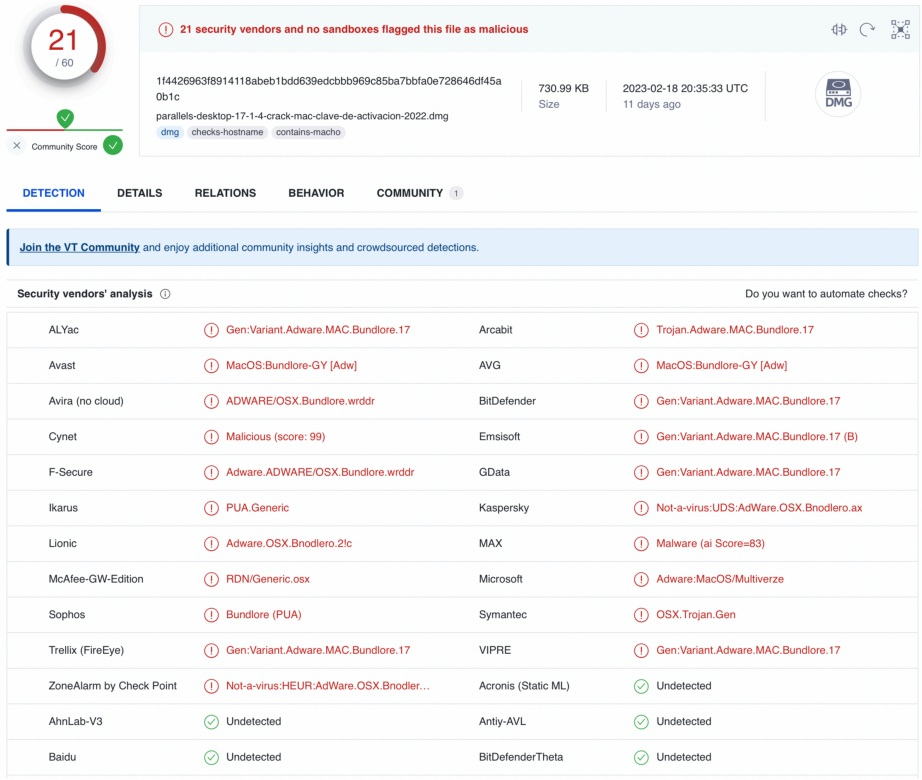

Figure 4.1: illustrates the initial results obtained from the analysis conducted on VirusTotal

Figures 4.2 to 4.6 show the results of the behavior analysis tab.

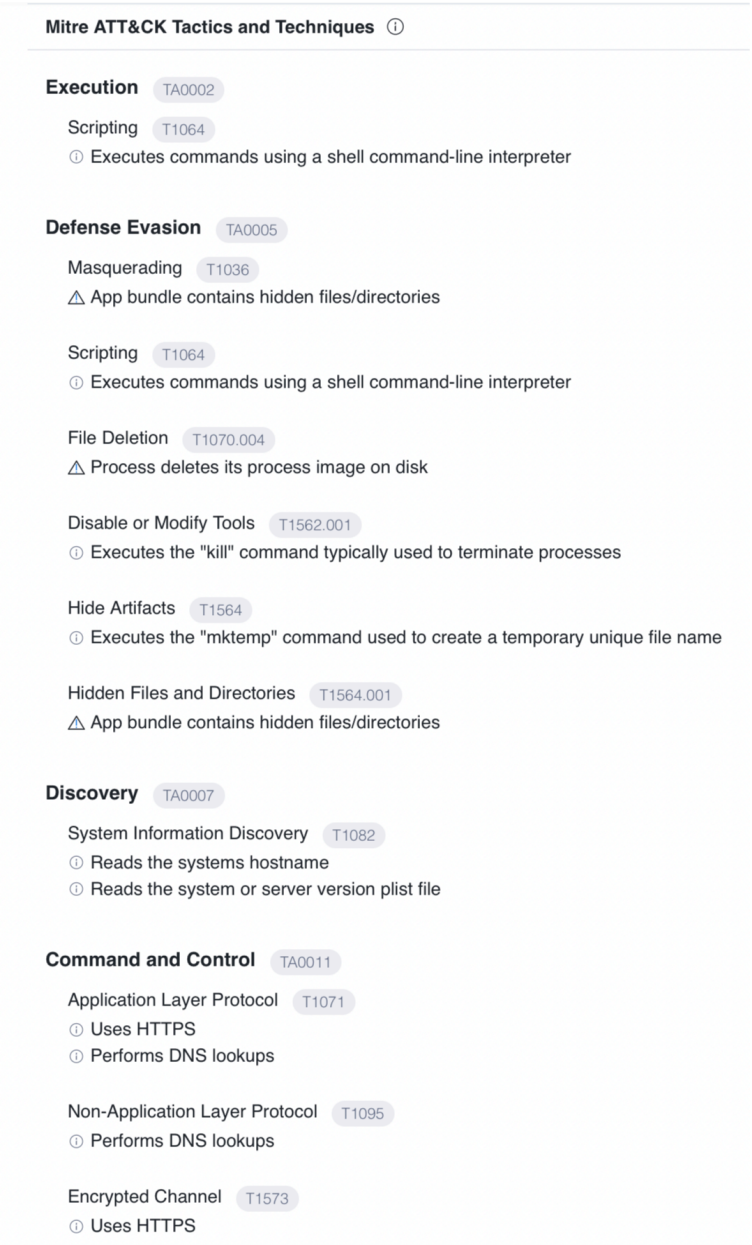

Figure 4.2: presents the Mitre ATT&CK Tactics and Techniques employed by the suspicious file.

Mitre ATT&CK serves as globally accessible knowledge base of adversaries' tactics and techniques gleaned from real-world observations. According to Mitre ATT&CK analysis, the suspicious file is indicative of containing concealed files/directories. This behavior aligns with that of a Trojan, which typically initiates the command line interpreter, retrieves system host names and versions, establishes Command and Control (C2) communication through encrypted protocols, ensures persistence by creating temporary files, and ultimately terminates all processes to evade detection.

Contacted Domains (2)

Domain	Detections	Created	Registrar
api.apple-cloudkit.com	0 / 88	2015-01-29	NOM-IQ Ltd dba Com Laude
gateway.fe.apple-dns.net	0 / 88	2014-05-28	CSC CORPORATE DOMAINS, INC.

Contacted IP addresses (27)

IP	Detections	Autonomous System	Country
104.73.64.163	0 / 88	16625	US
17.248.175.201	0 / 87	714	US
17.248.175.233	0 / 88	714	US
17.248.175.243	0 / 87	714	US
17.248.175.247	0 / 87	714	US
17.248.185.201	0 / 88	714	US
17.248.185.238	0 / 87	714	US
17.248.241.12	0 / 87	714	US
17.248.241.17	0 / 87	714	US
17.248.241.208	0 / 88	714	US
17.248.241.209	0 / 88	714	US
17.248.241.243	0 / 88	714	US
17.248.241.40	0 / 87	714	US
17.248.241.47	0 / 87	714	US
17.250.102.106	0 / 87	714	US
17.250.102.107	0 / 88	714	US
17.250.102.19	0 / 87	714	US
17.250.102.82	0 / 87	714	US
17.253.17.207	0 / 87	6185	US
17.253.7.201	0 / 87	6185	US
17.56.48.13	0 / 88	714	US
23.216.85.132	0 / 88	16625	US
23.62.24.145	0 / 88	16625	US
255.255.255.255	1 / 88	-	-
67.195.204.56	0 / 88	26101	US
72.21.91.29	0 / 88	15133	US
8.8.8.8	0 / 88	15169	US

Figure 4.3: illustrates the IP addresses contacted by the file using UDP or TCP protocol.

According to VirusTotal, the suspected file exhibits connections to a range of IP addresses and communicates with the DNS server over port 88.

Bundled Files (1)

Scanned	Detections	File type	Name
2023-02-19	25 / 62	Mach-O	/Skim's PDF

SHA-256 c9f322d3d2fe865f5bca73c8624e7291617011dd85923e77a9ae61b3278147d6
File Size 32.28 KB

Dropped Files (4)

Scanned	Detections	File type	Name
2023-02-19	25 / 62	Mach-O	Skim's PDF
?	?	file	1fc5b47a52c429092b8d61bb1692b2f25e47e6802f812e355f33eec703026861
?	?	file	4ce60ddcf11b93693a22d7fccad259f2c998203f5740272ca020b7c95bbf754b
?	?	file	ef4878d21da1d07bca4ffd6f89c36d6abd58d6a197ad90b3dca077f10b93d933

Figure 4.4: showcases four files dropped by the suspicious file on the operating system, one of which is a bundled Mach-O file flagged as malicious by several sites.

Figure 4.4 illustrates that the suspicious file initiates the opening of multiple files, including one bundled executable. These serve as indicators that the incident response team can utilize.

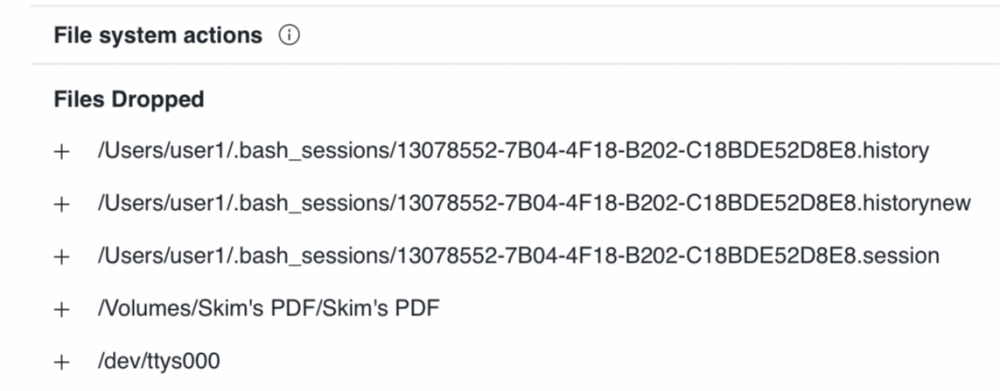

Figure 4.5: provides snippets of files that were written and moved by the suspicious file.

Figure 4.6: displays the process and service actions of the suspect file along with the loaded modules, extracted only.

The suspicious file executed a Mach-O file called "Skim's PDF," which functions as a shell script. This script creates a temporary file, invokes a binary file, executes it, terminates any spawned processes, and ultimately erases all traces of its activity.

Cuckoo Sandbox is a free tool designed to automate the analysis of potentially malicious files. By simply uploading a suspicious file, Cuckoo can quickly generate a detailed report outlining the file's behavior within a secure, isolated environment. Analysts can utilize a local version of Cuckoo to upload malware copies and conduct dynamic analyses on their own servers. This enables them to review the generated report in detail. In the following example, we will use it to conduct a review of the suspected file that can be obtained from this link.

1. Navigate to the Cuckoo Sandbox interface and select the suspicious file for analysis. Submit the file to initiate the analysis process. In the example provided, we're analyzing a file named "parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg."

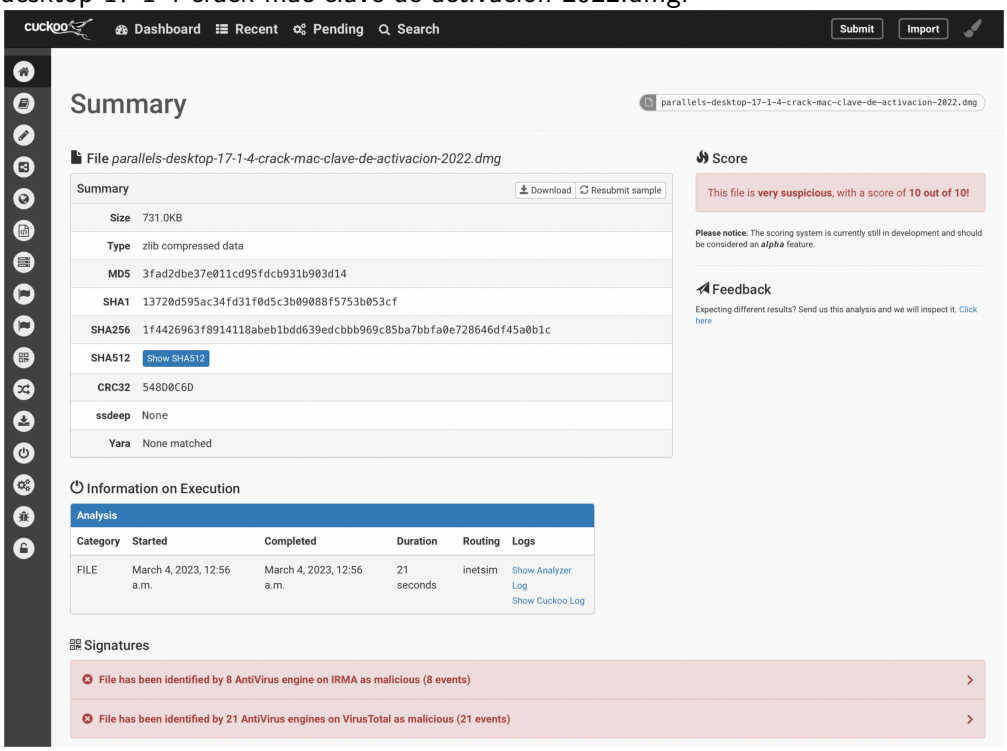

Figure 4.7: presents a summary analysis of the suspect file conducted by the Cuckoo sandbox.

Once submitted, the analysis begins, and you'll be presented with a summary window, as shown in Figure 4.7. A review of the analysis results, which include both static and dynamic elements such as behavioral and network indicators.

2. Navigate to the "Static Analysis" section. Here, analysts can access specific items such as strings and imported elements within the DLL file. In the "Static Analysis" section, there is a subsection called "Antivirus," which provides a breakdown of the VirusTotal results for the downloaded sample (as seen in the previous analysis section).Click on "IRMA" (Incident Response and Malware Analysis), which is a flexible content analysis orchestration platform. This platform offers an overview of content across various antivirus OS providers. Below is a screenshot illustrating this:

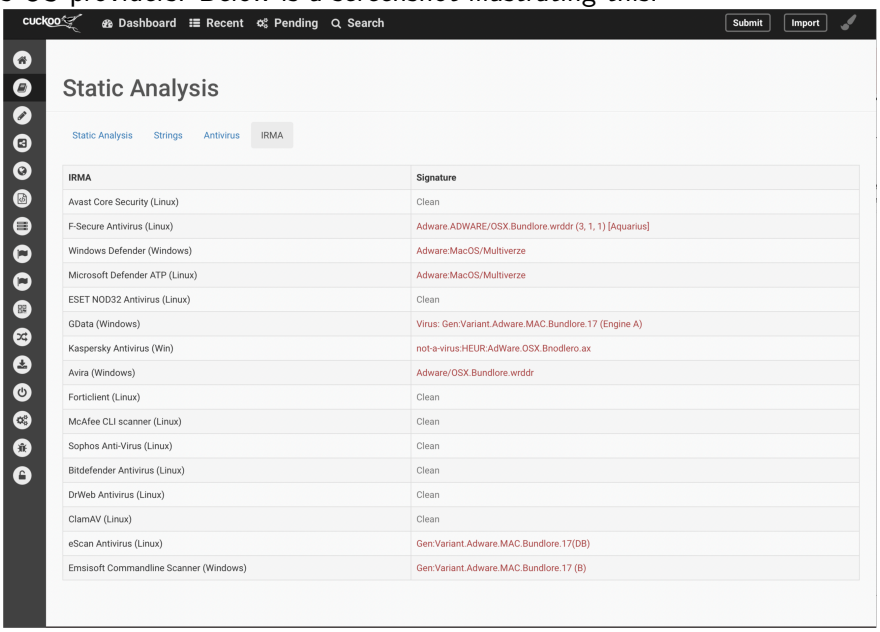

Figure 4.8: illustrates the static analysis of the suspect file conducted by various antivirus operating system providers on different operating systems.

3. Proceed to the "Behavioral Analysis" section. Here, you will find detailed descriptions of the specific behaviors exhibited by the files. A process tree is provided, breaking down the sequence of events that occurred after the malware was executed. While we discussed this in the previous section, we will not include a screenshot here. Additionally, malware often drops other files as part of its infection process. In the Cuckoo Sandbox, analysts can explore these dropped files by accessing the "Dropped Files" section. The purpose of this analysis is to identify Indicators of Compromise (IoCs). Cuckoo Sandbox offers two tools to extract these IoCs: IRMA and IntelMQ. Below is a screenshot illustrating these tools:

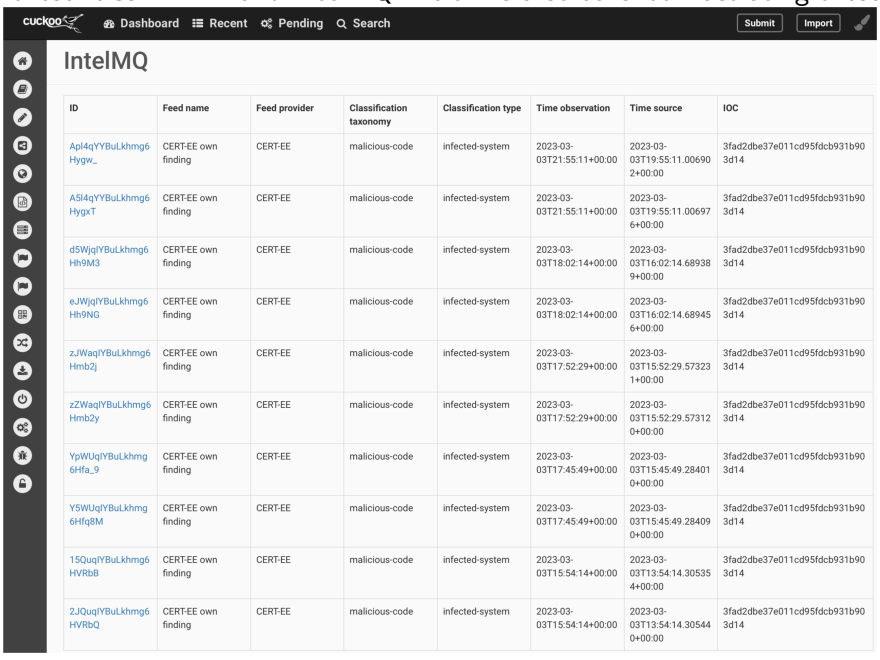

Figure 4.9: showcases the platform used to gather process threat intelligence, displaying 10 indicators of compromise (IoCs) associated with the suspect file.

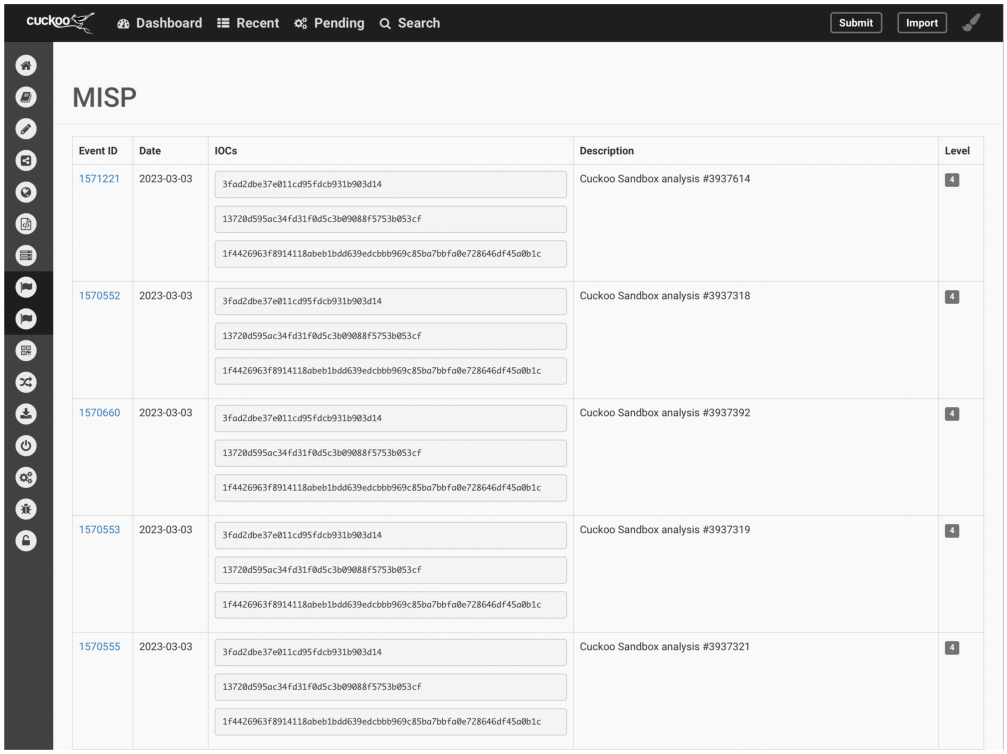

Figure 4.10: exhibits the content analysis orchestration platform, presenting 9 indicators of compromise (IoCs) related to the suspect file, shown as a snippet..

4.2 Study results

Understanding malware is essential due to its prevalence among adversaries. Malware analysis techniques, including static and dynamic analysis, offer responders valuable tools for extracting crucial data points. Additionally, the utilization of sandboxing systems enables responders to swiftly gain insights into malware behavior and attributes under controlled conditions.

The analysis indicates that the detected threat likely constitutes a Trojan. This sophisticated attack employs multiple layers and operations, leveraging social engineering vulnerabilities to deceive users into installing seemingly innocuous software containing hidden malicious executables. The Trojan establishes encrypted connections to compromised devices within the network, masquerading as command-and-control (C2) communication, and potentially exfiltrating sensitive data.

The Trojan's primary objective is to sustain communication with compromised devices post-exploitation. Each stage of the malware's lifecycle is scrutinized, yielding specific forensic data crucial for detection (IoCs).

This advanced Trojan employs self-deleting downloaders to fetch additional malicious components while remaining covert during execution. The downloaders and droppers execute batch scripts (e.g., Command Prompt), utilize rootkit techniques for concealment in the /usr/libexec/pkd directory, create temporary file systems, download payloads, and establish communication channels on compromised computers. The VirusTotal and Cuckoo Sandbox results for the analyzed malware can be accessed via the provided link.

This section merely scratches the surface of malware analysis, indicating the substantial effort required to master this specialized area of digital forensics. Despite its challenges, possessing a foundational understanding of malware analysis is crucial, given the increasing sophistication of cyber threats employed by malicious actors and nation-states.

5. Conclusion

As society becomes increasingly reliant on technology, the security of computer systems becomes paramount. In an age where essential functions like voting and air traffic control are managed digitally, incidents pose significant risks. Preventive measures alone are insufficient; there is a pressing need to effectively manage incidents, and digital forensics serves as the gateway to achieving this goal.

Integrating forensics into incident management is a complex task. As the field evolves, there is a need for advancements in specifying, implementing, and verifying forensic capabilities. Standardized properties must be defined and accepted within the forensic community to establish agreed-upon methods for implementation and formal verification of systems meeting these criteria.

Key points highlighted in this thesis include the benefits of proactive planning in digital forensic investigations, the crucial role of incident management in an organization's business continuity, the legal significance of implementing forensic capabilities, the indispensability of forensic readiness in incident management, and the importance of anticipating and planning for unforeseen disruptions.

The increased awareness of incidents, driven by widespread security breaches and attacks, underscores the necessity for basic infrastructure and standardized processes for incident handling. Forensic processes are integral to the incident response lifecycle, and organizations must view incident response as an integrated and critical component of daily security operations.

The integration of forensics into enterprise incident management is recognized as a vital research area and a promising market for practitioners. Despite ongoing efforts to secure computer systems and prevent incidents, incidents will inevitably occur. When they do, forensic techniques are essential for mitigation, learning, recovery, and legal proceedings.

This paper acknowledges the informal nature of current forensic policies, leading to ambiguity and potential inconsistencies. Future work will focus on formalizing forensic policies to enhance precision and clarity in policy definition, alongside the development of comprehensive and rigorous policy sets.

As efforts to secure critical infrastructure systems focus primarily on preventative measures, the need for forensic readiness capabilities remains significant. Collaboration between government, the private sector, and academia is essential for enhancing forensic capabilities and developing methodologies and tools to support forensic incident response.

The field of computer forensics is poised for increased demand for its services in the coming years. Preparedness is paramount, as incidents are a matter of when, rather than if, they will occur.

Acknowledgements

For my supervisor, in the words of Einstein, “It is the supreme art of the teacher to awaken joy in creative expression and knowledge. ”I thank you for being patient and making me a passionate person. Your lectures have impacted me and allowed me to grow a love for forensics.

To my mother, who, despite the fact that I am always sitting in front of my computer, has always had faith in me and understands in her own way that what I do is somehow important, and that I will achieve great things. To my brother, Thank you both, without your support this thesis might never have seen the light of day.

This thesis is my first attempt to be part of the academic discussion of humanity.

I almost gave up, I found myself in a long period of existential doubt and depression, before finally deciding that I had something to say.

I would like this work to be clear proof that efforts are always bearing fruit.

References

Endicott-Popovsky, B. and Frincke, D. Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. *Proceedings of the 2006 IEEE workshop on information assurance: computer forensics*, 2006.

Jones, N., George, E., Insa Mérida, F., Rasmussen, U., and Völzow, V. *Electronic evidence guide A basic guide for police officers, prosecutors and judges*. CyberCrime@IPA, EU/COE Joint Project on Regional Cooperation against Cybercrime, 2020. Available from https://rm.coe.int/0900001680a22757.

Kent, K., Chevalier, S., Grance, T., and Dang, H. *Guide To Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology Special Publication, 2006.

Lucas, J. and Moeller, B. *The effective incident response team*. Addison-Wesley, 2003.

Rowlingson, R. *A Ten Step Process for Forensic Readiness*. Phd, International Journal of Digital Evidence, 2004.

Sule, D. Importance of forensic readiness. Available from https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness, 2014.

Tan, J. Forensic readiness. *Cambridge, MA: Stake*, 2001.

Williams, J. *Electronic Evidence published*. Association of Chief Police Officers (ACPO) in the United Kingdom, Version 5. Available from https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.

Yasinsac, A. and Manzano, Y. Policies to enhance computer and network forensics. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 2001.