International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2025.0902/259

Research Article Vol. 9 issue 2 Jul-Dec 2025

Incident Response: Analyzing Forensic Techniques Prevalent in Malware Attacks

Hafiz Ahmad Mujtaba [1], Gohar Mumtaz [1]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan

Corresponding Author: hafizxholics178@gmail.com

Received: 15 ,2025; **Accepted:** Nov 20,2025; **Published:** Nov 27,2025

ABSTRACT

The growing intensity and frequency of malware attacks underscore the necessity of powerful and effective incident response and digital forensic measures. In this paper, Incident Response: Analyzing Forensic Techniques Prevalent in Malware Attacks, the researcher examines major forensic techniques that have been employed in the detection, analysis, and prevention of malware attacks. It is specialized in file system, memory, network, and malware forensics, analyzing Windows registry documents, prefetch files, Amcache, volatile memory, and IDS/IPS logs. The paper illustrates the use of forensic methods in detection of command-and-control (C2) communications and propagation of ransomware through case studies of WannaCry and NotPetya. It contrasts the approaches to analysis: static, dynamic and hybrid analysis with the emphasis on the importance of sandboxing and behavioral analysis. The results show that although forensics continues to play a crucial role in attribution and evidence collection, the problem of anti-forensic measures, data loss, and structural complexity make it less visible. Also highlighted in the study is the value of documentation, preservation and inter agency cooperation in conserving the integrity and accountability of evidence.

Keywords: Digital Forensics, Incident Response, Malware Analysis, File System Forensics, Memory Forensics, Network Forensics, Ransomware, Command-and-Control (C2), Forensic Readiness, Cyber security.

1. INTRODUCTION

The modern era of technology brings more cyber threats to organization which not only attack their critical infrastructure but also damages their reputation and encrypt their data. The cyber-attacks ranges from ransomware attack, phishing attack, APT's and insider threats. They cause a lot of damage, disrupt businesses and cause financial losses, and regulatory penalties. To minimize the risk of such attacks the organization are using Incident response plans and procedures to mitigate these attacks. IR process uses the methodology that help the organization to maintain the processes and business continuity during cyber-attack Also it help the organization to recover in minimum time and minimizing the risk of cyber damage[1].

IR is a critical aspect of cyber security as it helps the organization to establish a quick plan to detect, isolate, analyze and respond to the cyber-attack before it becomes a larger crisis. To establish IR, plan the National Institute of Standards and technology provides a comprehensive an incident response program that ensures a coordinated approach for handling cyber-attacks and to improve the security posture of organization.[2].

The main aspect of NIST is to not only manage the cyber-attacks but also to improve the resilience, prevent further damages, and improve the policy implementation of an organization. According to Nist, a typical cycle of IR plan consist of many phases like preparation which involves the preparation of an organization to develop its strategies, methods and tools, then if an attack occurs their IR team able to analyze it and contain it and after they isolate the systems and start the eradication process[3][4].

2. LITERATURE SURVEY

2.1 Evolution of Incident Response Practices:

2.1.1. Early Approaches to Security Incident Handling:

In early 19's the disruption in computers like viruses, malwares and misconfigurations were managed by the system administrators. There were no dedicated teams present for this task or any widely available tools for these types of attacks. If any such attack happen the troubleshooting is performed by case to case, and this includes with or without proper documentations [6] in 1988 a Morris worm was the perfect example of handling security incident. At early as the worm was spreading through the network and fragmented with the system admin try to contain them the lack of coordination made recovery slow [7]. This highlights the importance of IR /CERT Team.

2.1.2. Emergence of Formal Incident Response Frameworks:

Long response to a cyber-attack was a scramble. Lacking a definite plan, business organizations used their IT personnel to improvise things based on the fast-thinking and personal experience. It was a reactive, ad hoc process which differed dramatically in each incident. As the cyber threats became more advanced and prevalent it became excruciatingly obvious that this would not be an effective method it would not be a sustainable approach. Companies require a universal playbook, a standardized method of dealing with breaches that would make them efficient and accountable. This was not a purely technical push towards formal Incident Response (IR) frameworks, as it was also motivated by increasing knowledge of the devastating business, legal, and regulatory consequences that result in the aftermath of a security incident [8].

This development also redefined the incident response perspective of companies. No longer has IT issued, but more of a business continuity issue. Contemporary models promote cooperation in the organization at large, uniting teams of IT, legal, public relations, compliance and top leadership.

This all-encompassing approach stresses the learning of each incident and applying those lessons to keep on improving policies, tools and training [9].

2.13. Integration of Incident Response with Enterprise Risk Management

Monolithically, modern organizations integration of their cyber security incident response is being woven into their business risk strategy. Previously, the incident response of the IT team was an airplane who came in as a technical bulldozer and went about identifying and repairing the security breaches once they occurred. However, with the increased sophistication of cyber-attacks and the possible consequences being more severe, a significant change is occurring. Companies have realized that security incident is not an IT issue, but a business risk of the magnitude. By linking incident response to enterprise risk management, companies will be able to view a cyberattack as a real threat to their fundamental goals, their capacity to act, and even follow the law[10][11]. This is a step in being proactive. Companies are not relying on their risk management principles to respond to emergencies but rather take the lead in anticipating problems. They will be able to request: according to our business objectives, what threats are the most important? This will enable them to focus on their activities and invest their time and money well because of incidents that may be detrimental to the business [12].

2.2 Phases of Incident Response in Literature:

2.2.1. Preparation: Policy, Training, and Infrastructure Readiness

Imagine training to have a cyber-incident just as if one would do a fire drill. You would not leave it to the alarm to let you know where the exits were, would you? This is also the case with cyber security. Everything is prepared, the stuff out of which a bad situation is made a complete catastrophe. Unless one has a proper strategy, a security attack will soon turn into a mess, and its effects will be much more devastating and more time-consuming to address [13].

2.3 Tools and Technologies Supporting Incident Response:

Advanced tools and technologies are critical in incident response to identify, understand and deal with security threats efficiently. These tools are useful in making organizations recognize the incidence promptly, reduce losses, and restore systems rapidly.

Table 1 Tool and Technologies Supporting Incident Response

Category	Tool	Developer	Function	Key features	Use case
Forensic analysis	CAINE	Open source	Digital forensic platform	Data carving, timeline analysis and disk imagining	Used for evidence collection and post-incident digital investigation
Network monitoring	Wireshark	Wireshark foundation	Packet capture and analysis	Protocol analysis and real-time traffic analysis	Identifies suspicious traffic patterns and intrusions
SIEM	Splunk	Splunk Inc.	Security Information and Event Management	Centralized log collection, alerting and visualization	Correlates logs to detect and investigate incidents
EDR	CrowdStrike Falcon	CrowdStrike	Endpoint protection and threat hunting	Behavioral analytics, real-time threat detection	Tracks endpoint activities and isolates infected systems
SOAR	Cortex XSOAR	Palo Alto Networks	Security orchestration, Automation and response	Automated workflows, case mangement	Accelerates response through automated mitigation

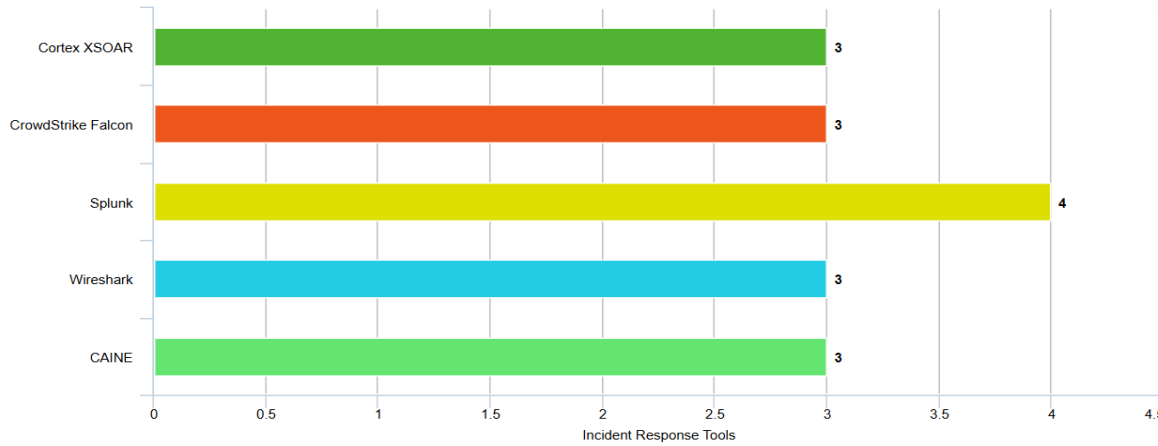

Fig 1 Comparison of tools and technologies supporting incident response

Figure 1 shows that a comparative analysis of the key incident response tools and technologies, such as CAINE, Wireshark, Splunk, CrowdStrike Falcon, and Cortex XSOAR has been made according to the number of key features they provide in order to support the activities of forensic investigation and response. The functional depth of each tool is represented by the horizontal bars, and Splunk has the most features (four) indicating its powerful feature in Security Information and Event Management (SIEM), which uses centralized logging, correlation, and automation.

2.3.1. Security Information and Event Management (SIEM) Systems:

SIEMs will include behavioral analytics and machine learning to identify anomalies that do not match set baselines to offer a better chance at identifying insider threats or attack patterns never observed before. SIEM systems are also crucial in incident response processes besides detection. There are numerous platforms that have automated response or collaborate with Security Orchestration, Automation, and Response (SOAR) solutions to quickly limit threats. As an example, in cases when a SIEM identifies a series of failed logins and a series of unusual account privileges, it may automatically execute processes to postpone or block the hacked account or the suspicious IP. This type of integrations significantly minimizes mean time to detect (MTTD) and mean time to respond (MTTR) which are two performance measures in relation to security.

2.3.2. Forensic Approaches in cyber security:

The most important concept to forensic practices is integrity and authenticity of evidence. To make sure that the digital artifacts (logs, registry files, system memory, and network packets) are not modified throughout the investigation process, investigators apply standardized procedures and tools. The chain-of-custody documentation is important because it ensures that the individual who accessed the evidence is accountable and at the right time, hence ensuring that the evidence remains admissible in a court or other regulating measures. Through the production of bit-by-bit forensic images, investigators can reconstruct deleted files, file system structures and hidden or encrypted information.

2.4 Malware Trends Shaping Forensics

2.4.1 File less malware and living-off-the-land binaries (LOLBins).

One of the primary benefits of file less malware to the attacker is that it can be executed in such a way that even after a system reboot it is still executed, such as by modifying a registry key, using a scheduled task, or an event subscription via WMI. Indicatively, advanced persistent threats (APTs) have been noted to install malicious scripts on windows registry keys to automatically run at each start. The strategies do not rely on external binaries and render the conventional disk-based forensics strategies ineffective.

2.4.2 Ransomware and Supply Chain Attacks:

Ransomware is a form of malware that encrypts the data of an organization or denies access to systems at a price and ransom is required which is usually crypto currency in exchange of decryption keys. In the last ten years, ransomware has developed as a set of opportunistic attacks on individuals to highly targeted attacks on large businesses, critical infrastructure, and government institutions. Well-known cases like WannaCry (2017) and NotPetya (2017) proved that ransomware can be as large and destructive as billions of moneys and essential services as well as affect the whole globe.

Table 2 Previous Cases on Ransomware and Supply Chain Attacks

Year	Attack Name	Target	Type of attack	Impact	Key lessons learned
2020	SolarWinds Orion Breach	Multiple U.S federal agencies and private firms	Supply chain attack	Compromised software updates used to deploy back doors	Continuous monitoring of trusted software supply chains
2021	Colonial Pipeline Ransomware	Colonial Pipeline(USA)	Ransomeware	Disrupted fuel supply across US East Coast , ransom paid Bitcoin	Need for network segmentation and stronger authentication
2021	Kaseya VSA attack	Managed Service Providers	Supply chain attack	Affected hundreds of client businesses through remote management software	Implementening multi-layered vendor risk management
2022	Costa Rica Government Ransomware	Ministry of Finance and multiple agencies	Ransomware	Shutdown of government systems, state of emergency declared	Enhancing national cyber defense and incident coordination
2023	MOVEit Data Breach	Multiple global organizations	Supply chain attack	Massive data ex-filtration and extortion cases	Importance of secure data transfer tools and patch prioritization
2024	Change Healthcare Cyber-attack	Change Healthcare (USA)	Ransomware	Disruption of healthcare payment systems nationwide	Critical infrastructure requires 24/7 threat detection and backup plans

In recent years, ransomware organizations have functioned in a so-called Ransomware-as-a-Service (RaaS) paradigm, in which developers sell ransomware tools to affiliates at a percentage of their earnings. This business-like ecosystem has decreased the barrier to entry whereby less skilled technologically inclined attackers can develop destructive campaigns.

3. METHODOLOGY

3.1 Qualitative analysis of forensic techniques

The given research assumes qualitative methods to examine forensic methodology in the framework of malware attacks response. A qualitative framework unlike quantitative methodologies focuses on the ability to explore how forensic techniques are implemented in real-world by examining their application to actual cases, their

application in context and the issues encountered by practitioners. This is more so in the field of cybersecurity, where the dynamism and variability of threats do not allow the use of rigid measurements in defining the flexibility and pragmatic usefulness of forensic tools [15].

The qualitative analysis will allow assessing the forensic methods based on the case studies, industry reports, and scholarly literature and will provide a hint on how the investigators rely on evidence of compromise, reconstruct attacker's activity, and facilitate the attribution efforts [16].

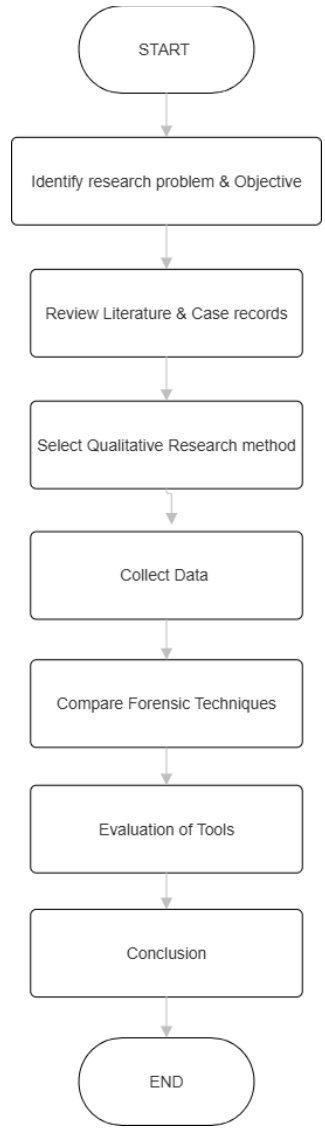

Fig 2 Flowchart of Research Methodology

The topic of memory forensics is investigated due to its ability to disclose fileless malware, dumping of credentials, and volatile artifacts that are not saved on disk. Network forensics is examined as it relates to its performance in identifying command-and-control (C2) communications, lateral movement and data exfiltration attempts. Each of the approaches is discussed in terms of its strengths, weaknesses and the situational applicability [17].

The qualitative approach is also focused on the comparative assessment of devices and methods that are typically utilized in research. Some of the tools tested include EnCase, Autopsy, Sleuth Kit, Volatility, and Rekall (disk forensics), Wireshark or Zeek (network forensics). Rather than evaluating the accuracy of the testing tool in terms of quantitative measures, the analysis explores how these tools have been used in real malware inquiries, how they can be used by the analysts and the role they play in revealing the actions of the attackers [18].

The emphasis on the chain-of-custody and legal admissibility is another aspect of qualitative analysis because the forensic process has to be integrity-oriented and accountable, so the collected evidence could be presented in the court or during the regulatory processes. In this case, qualitative assessment is based on procedural documentation and the role played by organizational policies in the development of forensic practices effectiveness.

3.2 Cyber cases, Digital Forensic reports.

Case Studies are the important source of qualitative information which provides very real-life examples of how the forensic techniques can be used in the contexts of the real malware cases. They can be enhanced-profile ransomware, supply chain, and advanced persistent threat (APT) activities. Case studies are a rich source of information about attacker strategies, tactics, and procedures (TTPs) and even the organizational forensic responses used to identify, contain, and fix such threats [20]. To illustrate, the exposure of both the WannaCry and the SolarWinds cases by the public not only show the technical remnants of the attacks but also highlights the difficulty in collecting the evidence and attributing it to the attacker by the forensic teams.

3.3 Comparative framework: evaluating file system, memory, and network forensic methods.

This study uses a comparative framework to systematically evaluate the efficacy of forensic methods to respond to malware centered incidents. The framework gives a systematic manner of assessing the contribution of various types of forensic procedures file system, memory and network to detect, analyze and control malware attacks. The framework allows equal consideration of these areas and points out the strong and weak aspects of each strategy in a situation. Investigators concentrate on persistent storage that allows them to examine artifacts of operating systems, application logs, and user data (File System Forensics). Advantages of the approach are that deleted files can be restored, attack history can be rebuilt, and persistence tools as registry keys or scheduled tasks can be identified. Godfather file system analysis is however less effective against fileless malware that are mostly memory based and do not write a lot on disk.

This technique is good at identifying malware that is stored in the memory, dumped credentials, and injected processes that are not visible in disks. If an analyst needs to reverse-engine running processes, detect loaded drivers, and steal encryption keys or plaintext credentials, tools such as Volatility and Rekall can be used. The primary drawback is the temporal nature of memory evidence after a system has been shut down or restarted, that essential evidence can be lost. Also, the large-scale enterprise environment can be difficult to acquire memory.

3.4 Limitations: access to proprietary forensic data and real-world case constraints.

File system forensics dwells on the enduring storage, and helps the investigators to examine operating system artifacts, application logs and user data. The advantages of this technique are that deleted files are recoverable; it can reconstruct timelines of the attack and identify the persistence mechanisms using registry changes or scheduled tasks. File system analysis is however not effective with fileless malware which mainly works in memory and leaves little traces in disk.

Memory Forensics fills this gap in that volatile data is captured on the RAM. The approach is effective in discovering malware in memory, dumping credentials, and injected processes which are not detected on disk. There are tools such as Volatility and Rekall that can help the analysts rebuild running processes, locate loaded drivers, and extract encryption keys or plaintext credentials. The key Achilles heel is that memory evidence is volatile and can be lost as soon as a system is shut down or rebooted, and important artifacts can be lost. Besides, large scale enterprise environments can be technically difficult in terms of memory acquisition.

The limited access to proprietary forensic data is one of the main weaknesses. When agencies are victims of malware, detailed forensic evidence, including raw memory dumps, full packet captures, and disk images, is often treated as a top-secret data by agencies because of privacy, liability, reputational risk, and similar reasons . Although these sources will be very useful, they might not be as granular as the evidence that is met in practical investigations. It is a common characteristic of case studies and other forensic reports to focus on big-time instances, like ransomware outbreaks or nation-state supply chain breaches, attracting the attention and financial aid.

4. ANALYSIS AND DISCUSSION

4.1 File System Forensics in Malware Investigations

File system forensics can be of great importance to incident response since malware can leave traces in the file system. All communication between malware and the operating system including the creation, editing of files as well as deletion of files leaves a trace that may be utilized as evidence in the forensic investigations. These pieces of evidence can assist the investigators in piecing together the chronology of the infection, what methods the malware may have employed to persist, and what the malware did to the system.

Analysis of metadata relating to files is one of the major objectives of file system forensics. The creation, modification, access, and change (widely referred to as the MACB attributes) are file timestamps that are important indicators of when malware was run and whether an attempt was made to conceal the incidents. Through the correlation of information about the timestamp, an investigator may detect patterns that would indicate tampering or a deviant system operation.

4.2 Memory Forensics for Malware Response

4.2.1 Importance of volatile data.

Volatile data also have network connections and encryption keys that malware utilizes in communication with command-and-control (C2) servers. Through the compilation of RAM, the investigator can identify IP addresses, domain names, and ports used during the time of capture. It is especially useful when tracking the continuous exfiltration operation or the lateral movement of an affected environment. Moreover, volatile data can also store encrypted keys, which are important in decrypting the affected files before they are erased by attackers in instances of ransomware. A malware tends to exploit the Local Security Authority Subsystem Service (LSASS) service to dump user credentials and session tokens. Such credentials are not necessarily found in long-term logs but can be retrieved as memory captures. With

the help of volatile data, investigators could determine hacked accounts and block further unauthorized access.

4.3 Network Forensics and Malware Containment

4.3.1 Traffic analysis, IDS/IPS logs, packet capture.

The idea of traffic analysis is to analyze traffic on the network and identify anomalies, suspicious connections, and unusual patterns of communication that are not in line with normal activity. Malware frequently interacts with command-and-control (C2) servers and analysis of traffic can show when beaconing occurs, when abnormal data exchange is taking place or when encrypted channels are being stealthily used. To illustrate, suspicious spikes of outgoing traffic or regular connections with unknown domains can be an indicator of data exfiltration that is caused by malware. Traffic analysis is also very helpful in identifying lateral movement in an organization also in phishing analysis and some URL's contain malicious websites that could harm the organization and the attackers frequently use these tactics to cut across systems by way of remote or other services[19].

4.3.2 Identifying command-and-control (C2) communication.

The detection of DGA-based traffic needs sophisticated analysis methods like entropy testing, domain name lexical analysis and correlation with threat intelligence feeds. Likewise, fast-flux DNS schemes, i.e. when IP addresses belonging to a rogue domain switch quickly, are employed to make C2 infrastructure more robust, making it harder to detecting.

4.4 Reverse Engineering and Malware Analysis

4.4.1 Static vs. dynamic analysis.

Static analysis is an analysis of the malware sample without its execution. Analysts devcodes or decompiles the code to investigate the structure, strings and libraries as well as embedded resources. The approach assists in detection of indicators like hardcoded IP addresses, suspicious API calls and use of obfuscation. The threat posed by the malware can be relatively low due to the fact that the malware is not currently active and therefore, it is less harmful to the environment of the analyst.

Dynamic analysis, however, is dedicated to tracing the malware behavior when it is executed in controlled sandbox environment. The malware can be executed, therefore, allowing investigators to track the changes in file system, registry, processes, and network activity in real time.

5. CASE STUDIES

5.1 WannaCry ransomware forensic response.

The most devastating cyber attack of all time, the WannaCry ransomware attack that happened in May 2017, impacted more than 200,000 systems in 150 countries. The EternalBlue (MS17-010) Windows vulnerability that the attack took advantage of, spread like wildfire through networks; it was a Windows vulnerability involving the Server Message Block (SMB) protocol. A best practice response to WannaCry includes a forensic analysis of file system artifacts, memory captures, network logs, and logs to recreate the order of infection, detect evidence of compromise (IoCs), and evidence to support incident remediation.

5.1.1 File System Forensic Analysis

When infected, WannaCry encrypts files with the extensions of .doc, .jpg, .xls and .ppt and adds the extension of WNCRY. This ransomware subsequently leaves ransom note files with the title of the affected directories as @PleaseReadMe@.txt. Such encrypted files, ransom notes and executables like tasksche.exe and mssecsvc.exe which belong to *the WannaCry*

payload can be revealed with file system forensics.

5.1.2 Memory Forensics

Analysis of volatile memory will be essential in identifying in-memory traces of the ransomware before they disappear. Running processes of the WannaCry or encryption keys and connections to its command-and-control (C2) servers may be observed in memory dumps. With such tools as Volatility, the process hierarchy can be revealed, injected threads can be found, and encryption routines applied when locking files can be recovered. Because the encryption keys are usually created and kept temporarily in RAM, high memory acquisition speed is necessary to raise the chances of recovery before a system goes down.

5.1.3 Network Forensics

Lateral movements of WannaCry were based on SMB (port 445) connections. Network forensics assists in the detection of these activities by the analysis of packet captures and firewall logs. Traffic analysis would be able to show the scanning of the worm as it tried to find other systems with vulnerabilities on the same network. The other notable feature of the WannaCry network activity was its kill switch domain that, in case of its registration, prevented the further propagation of the malware. Trying to identify DNS queries into this domain (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) during forensic analysis can assert that the attempts of infections or containment succeded.

5.1.4 Log Analysis and Correlation

System logs, such as Windows event logs, and SMB server logs, give an idea about the chronology of infection. Security logs can also assist in noting whether they were privileged escalated or credential stole before the encryption stage. A combination of these logs and file system and network data allows a thorough reconstruction of the attack chain

5.1.5 Incident Containment and Recovery

After forensic identification, the next phase is containment where infected machines are isolated, SMB traffic blocked over the network and the Microsoft MS17-010 patch applied. Restoration of the data should be conducted using backups instead of paying the ransom because the payment infrastructure of WannaCry was not reliable. Forensic evidence can also help to revise detection rules, firewall policy and endpoint protection systems against re-infection.

The WannaCry forensic response demonstrates the significance of fast acquisition of evidence, multi-layered analysis and patch management in current incident response. The lessons of this attack have strongly informed the way organizations are today undertaking ransomware preparedness, with proactive monitoring and forensic preparedness as an essential component of cybersecurity resiliency.

5.2 NotPetya malware outbreak and attribution.

The 2017 NotPetya malware outbreak in June is generally considered to be among the most devastating cyber incidents ever documented, resulting in many billions of dollars of worldwide economic damage. Though it seemed that it was a ransomware campaign at first, forensic studies found that NotPetya was actually a wiper malware intended to cause mayhem and not money. The virus mainly attacked organizations in Ukraine but soon spread to other parts of the world, where companies like Maersk, Merck and FedEx were all targeted

6. FINDINGS AND IMPLICATIONS

6.1 Effectiveness of forensic techniques against modern malware.

The ever-devolving nature of malware has really complicated the conventional methods of forensic investigation. Due to threat actors becoming more

advanced, including the use of fileless execution, polymorphism, encryption, and other anti-forensic methods, digital forensics needs to evolve to keep up with them. Evaluating the suitability of forensic methods in response to current malware can be achieved through examination of the capability to identify, preserve and interpolate well digital evidence in increasingly complicated threat landscapes using existing tools and processes.

6.2 Limitations and Challenges

A modern-day forensic approach, when implemented appropriately in incident response procedures, is still very effective in identifying significant points of compromise and piecing together the activity of the attacker. Disk forensics still serves as an invaluable source of information on file system modification, registry editing, and data recovery on deleted file systems. More sophisticated tools like Autopsy, FTK, and EnCase can help to detect or uncover concealed or encrypted files, persistence mechanisms, and simply match the time-stamps to rebuild the timeline.

One of the most effective methods to counter advanced malware has become memory forensics. Through volatile data analysis, investigators are able to detect malicious processes, in-memory payloads, and attempts of credential theft that cannot be detected on disk. Utilities such as Volatility and Rekall enable forensic investigators to recover running process trees, loaded DLLs, and injected pieces of code, both important in helping to identify fileless malware and living-off-the-land (LotL) attacks. Likewise, network forensics, through packet capture and intrusion detection system (IDS) logs, is still useful to track C2 communications, exfiltration of data, and intra-organizational movement in enterprise networks.

6.3 Conclusion.

The results of forensic investigations of contemporary malware outbreaks have profound practical value to Security Operations Centers (SOCs), Incident Response (IR) teams, and police departments. All these bodies are vital in detecting, inhibiting and punishing cyber-attacks, and how successful they are depending on how well forensic knowledge is integrated into operational and strategic systems.

This study has examined how forensics methods, which include file system, memory, and network analysis, are crucial in revealing the conduct and effect on the system, as well as the source of malicious software.

7. RECOMMENDATIONS

Some of the recommendations which enhance the security posture of the companies are given.

- Include forensic preparedness in organizational security activities with extensive logging and evidence gathering.
- Standardize log management and lengthen log retention time to facilitate deep forensics.
- Invest in the latest forensic and automation technologies that can be used to analyze memory, file systems, and network data.
- Regular training and practical exercises of SOC and incident response teams.
- Share timely intelligence about threats with law enforcement, CERTs, and industry teams.
- Use safe threat-sharing systems like MISP to share indicators of compromise.
- Meet the requirements of established standards including NIST SP 800-86 and ISO/IEC 27037.

8. LIMITATIONS AND CHALLENGES

Although forensic techniques can be crucial in the process of understanding and mitigating malware attacks, multiple limitations and challenges still exist in the contemporary incident response. The most important issue is the malware is constantly evolving very quickly and often it uses sophisticated methods to evade detection including encryption, polymorphism, and executing files without a file. Such techniques tend to interfere with conventional forensic methods that are based on signature detection or analysis of static files. Also, the growing popularity of anti-forensic techniques, which include data wiping, time stamping, and running in-memory, makes evidence gathering more difficult and makes recovered artifacts less reliable.

The next limitation is that volatile data is time sensitive. Memory and network data may rapidly be lost unless captured in time, influencing the thoroughness of the forensic picture. In most situations, the organization may not have the automated systems or the knowledgeable staff to save such data at the early response stage.

9. DOCUMENTATION AND PRESERVATION

The documentation and preservation are essential parts of the digital forensic and incident response process to make sure that all evidence gathered during a malware investigation is credible, verifiable, and admissible in a legal or organizational process. Documenting will give a clear account of all actions performed including the seizure of evidence and its analysis and presentation, and it will assist the investigator to ensure that the chain of custody is preserved and that the forensic process is beyond reproach.

10. REFERENCES

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson, 2019.

[2] T. Grance, K. Kent, and B. Kim, *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*, NIST, 2012.

[3] G. Killcrece, K. P. Kossakowski, R. Ruefle, and M. Zajicek, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University, SEI, 2003.

[4] R. A. Grimes, *Incident Response and Computer Forensics*. McGraw-Hill Education, 2017.

[5] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*. European Union Agency for Law Enforcement Cooperation, 2021.

[6] P. Neumann, *Computer Related Risks*. Addison-Wesley, 1995.

[7] E. Spafford, *The Internet Worm Program: An Analysis*. Purdue University Technical Report, 1989.

[8] ISO/IEC, *27035: Information Security Incident Management*. International Organization for Standardization, 2011.

[9] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. NIST, 2012.

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrating with Strategy and Performance*, 2017.

[11] ISO, *ISO 31000:2018 Risk Management – Guidelines*. International Organization for Standardization, 2018.

[12] C. Alberts, A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, *Defining Incident Management Processes for CISRTs: A Work in Progress*. Carnegie Mellon University/SEI, 2004.

[13] SANS Institute, *Incident Handler's Handbook*. 2019.

[14] R. K. Yin, *Case Study Research: Design and Methods*. Sage Publications, 2018.

[15] M. Alazab *et al.*, "Malware Analysis and Detection Techniques: A Literature Review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 26–31, 2013.

[16] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.

[17] M. H. Ligh *et al.*, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014.

[18] NIST, *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. National Institute of Standards and Technology, 2006.

[19] M. T. Suleman and S. M. Awan, "Optimization of URL-Based Phishing Websites Detection through Genetic Algorithms," *Automatic Control and Computer Sciences*, vol. 53, pp. 333–341, 2019.

[20] R. K. Yin, *Case Study Research: Design and Methods*. Sage Publications, 2018.