



School of Design and Informatics

BSc Ethical Hacking, 2022/23

An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses

Author: Martin Georgiev

Supervisor: Natalie Coull
Head of Division of Cybersecurity Abertay

Note that the information contained in this document is for educational purposes.

Contents

Table of Figures.....	iv
Table of Tables	v
Abbreviations.....	vi
Acknowledgements.....	vii
Abstract	viii
1 Introduction	1
1.1 Background and Context	1
1.2 Aims and Research Questions	2
1.3 Scope of Project	3
1.4 Structure	4
2 Literature Review.....	5
2.1 Literature Review Introduction	5
2.2 Cyber-attacks and Incident Response	5
2.2.1 Incidents and Incident Response Plans	5
2.2.2 Significance of Incident Response	6
2.2.3 Advantages and Disadvantages of IRPs	8
2.3 Cyber-Attack Analysis	9
2.3.1 Malware Analysis	9
2.3.2 Digital Forensics	11
2.3.3 Signature Scanning.....	12
2.4 Literature Review Summary	12
3 Methodology	14
3.1 Methodology Introduction.....	14
3.2 Generalised Cyber Incident Response Plan	14
3.3 Simplified Methodology.....	16
3.3.1 Tools and Techniques	16
3.3.2 Data Analysis	17
3.3.3 Use of Obtained Data	18
3.4 Implementation	19
3.4.1 Malware Types and Samples	19

3.4.2	Testing Environment.....	20
3.4.3	Static Analysis	21
3.4.3.1	AV Vendor Scans.....	21
3.4.3.2	String Extraction	21
3.4.3.3	PEStudio and ExeInfoPE	23
3.4.4	Dynamic Analysis	25
3.4.4.1	Detonation Symptoms and Conditions.....	25
3.4.4.2	Network-Based Indicators	27
3.4.4.3	Host-Based Indicators.....	28
3.4.5	Utilising Yara for Signature Scanning.....	31
3.5	IRP Module Creation.....	31
3.6	Questionnaire Development.....	32
3.7	Methodology Summary.....	34
4	Results	35
4.1	Results Introduction	35
4.2	Malware Analysis Methodology	35
4.3	Incident Response Plan and Modules	36
4.4	Questionnaire Results	37
4.5	Results Summary	39
5	Discussion.....	40
5.1	Discussion Introduction	40
5.2	Existing Research Data	40
5.3	CIRP Development	42
5.3.1	Generalised Incident Response Plan	42
5.3.2	Attack-specific Modules.....	43
5.4	Methodology Development.....	44
5.5	Limitations.....	46
5.6	Discussion Summary	47
6	Conclusion	48
6.1	Conclusion	48
6.2	Future Work	49

7	References.....	51
8	Appendices.....	55
	Appendix A – Extracted Malware Strings	55
	Appendix A1 – FileTour Strings.....	55
	Appendix A2 – Jigsaw Strings	57
	Appendix A3 – NotPetya Strings	58
	Appendix A4 – SnakeKeylogger Strings	59
	Appendix B – Memory Forensics.....	60
	Appendix B1 – Privileges	60
	Appendix B2 – Malfind	61
	Appendix B3 – Netscan.....	62
	Appendix C – Yara Rules	63
	Appendix C1 – FileTour.yara	63
	Appendix C2 – Jigsaw.yara.....	64
	Appendix C3 – NotPetya.yara.....	65
	Appendix C4 – SnakeKeylogger.yara.....	66
	Appendix D – Malware Analysis Reports and Methodology	67
	Appendix E – Generalised CIRP	69
	Appendix F – Response Modules	70
	Appendix G – GDPR Data Sign-Off Form.....	72

Table of Figures

Figure 1.1 - Average Weekly Attacks per Organisation by Industry in 2021 and 2020. . .	1
Figure 3.1 - Virtual Machine Testing Environment.....	20
Figure 3.2 - Host-Only Network Settings.	20
Figure 3.3 - Hash Identification.....	21
Figure 3.4 - VirusTotal Results for Jigsaw.	21
Figure 3.5 - Error Generated by Floss by Some Samples.	22
Figure 3.6 - FileTour Malicious Functions.....	22
Figure 3.7 - NotPetya Ransom Message.....	23
Figure 3.8 - SnakeKeylogger PEStudio Analysis.....	23
Figure 3.9 - Custom Function in Second Stage Payload of FileTour (PBrowFile15). ...	24
Figure 3.10 - Custom self-modifying section in Jigsaw.....	24
Figure 3.11 - Recent Debug Time of SnakeKeylogger.	25
Figure 3.12 - Identified URLs and Other Hidden Data in Jigsaw.	25
Figure 3.13 - Jigsaw Visible Ransom.	26
Figure 3.14 - NotPetya Ransom Message.....	26
Figure 3.15 - Screen Recorder Launched by FileTour.....	27
Figure 3.16 - SnakeKeylogger Web Address Access.	27
Figure 3.17 - FileTour Third-Stage Payloads.....	28
Figure 3.18 - NotPetya Attempting to Interrogate the Server.....	28
Figure 3.19 - Drpbx.exe File Used for Encryption.....	29
Figure 3.20 - Frfx (firefox.exe) File Used for Persistence.	29
Figure 3.21 - Fake Disk Repair Message by NotPetya.....	29
Figure 3.22 - FileTour Second-Stage Payloads.....	30
Figure 3.23 - SnakeKeylogger Second-Stage Payload.	30
Figure 3.24 - NotPetya Yara Rule.	31
Figure 3.25 - NotPetya Yara Rule Test.....	31
Figure 3.26 - Severity Guidance Section for the FileTour Module.	32
Figure 3.27 - Methodology Section of the Questionnaire.....	33
Figure 4.1 - Methodology Documentation.....	35
Figure 4.2 - First Two Pages of Base IRP.	36
Figure 4.3 - Part of SnakeKeylogger's Module.	37

Table of Tables

Table 2.1 - Causes of incident response failure.....	7
Table 2.2 - Malware Types.	10
Table 2.3 - Six stages of analysis based on the EDRM framework.	12
Table 3.1 - Generic Response Plan Sections.	16

Abbreviations

Abbreviation	Meaning
SME	Small and Medium-sized Businesses.
MA	Malware Analysis.
DF	Digital Forensics.
IR/IRP	Incident Response/Incident Response Plan.
CIRP	Cyber Incident Response Plan.
CIRT	Cyber Incident Response Team.
SOTER	“cyberSecurity Optimisation and Training for Enhanced Resilience” (Onwubiko and Ouazzane, 2020).
EDRM	Electronic Discovery Reference Model.
MCFF	Mobile Cloud Forensics Framework.
C&C Server	Command-and-control Server.

Acknowledgements

I would like to extend my gratitude to Dr Natalie Coull, my supervisor, for her unwavering support and guidance throughout this study. Her invaluable feedback and expert direction were crucial in shaping the outcome of this thesis.

I would also like to express my deepest appreciation to my family and friends. Their constant encouragement and support have been a source of strength and inspiration throughout my academic journey. I am grateful for their unwavering love and compassion, which helped me navigate the ups and downs of my studies.

Last but not least, I wish to acknowledge the faculty and staff of the School of Design and Informatics at Abertay University for their knowledge and assistance during my degree program. Their expertise and commitment to education have been instrumental in my academic growth.

Abstract

Due to the Covid-19 pandemic and the exponential growth of devices, there has been a significant rise in the usage and variety of interconnected devices and services. Along with the usage surge, cyber-attacks have become more widespread and continue to increase annually. Many organisations have implemented incident response plans (IRPs) to limit the damage caused by such attacks. However, most IRP templates are not user-friendly or efficient. Although larger corporations can effectively utilise them, response plans remain too technical and complex for small and medium-sized enterprises (SMEs) without an IT department.

The paper investigates different methods to enhance the accessibility of IRPs for SMEs. The primary objective is to devise, prototype and assess a modular approach to incident response plans. This tailored approach provides a set of actions against specific cyber incidents. The response modules are coupled with a straightforward but effective attack analysis methodology that can be used to analyse an incident and formulate response modules based on the results.

To successfully meet the project's objectives, the researcher conducted extensive research on cyber-attacks, incident response, and attack analysis techniques such as MA, DF, and signature scanning. The information gathered provided an overview of the current advantages and disadvantages of CIRPs, which were then used to develop a modular CIRP solution. This new solution enables organisations to conduct swift attack analysis, identify the malicious software, and select or create a response module for that specific malware.

As it was not possible to test the prototype artefacts in a real-life cyber incident, the researcher designed a questionnaire aimed at cybersecurity professionals. The results revealed that the solution may still be too complex for staff without prior IT knowledge. However, third-party cybersecurity providers could use it to train their staff and respond rapidly and efficiently to cyber incidents. Such a swift response would significantly reduce the damage caused by malware and potentially mitigate adverse outcomes for SMEs. Future studies could focus on accessibility enhancement by thoroughly testing

the modular incident response plans and creating a centralised web application for advice, automated analysis, and exchange of response modules.

1 Introduction

1.1 Background and Context

As people increasingly rely on internet connectivity, particularly due to the Covid-19 pandemic, remote work and entertainment have expanded corporate networks. While this provides more freedom and flexibility, it also creates more attack opportunities for cybercriminals and significantly increases malicious activity across various sectors. Every year, more companies are affected by cyber-attacks, as evidenced by Checkpoint's 2022 report (CheckPoint, 2022) (Chart 1.1), which shows weekly attacks on Education, Gov/Military, Communications, and ISP/MSP sectors increasing by 66%, 42%, 45%, and 59%, respectively, compared to Q2 2021. In recent years, there has been a significant rise in cyber-attacks globally, posing a greater risk to private users and corporations. These attacks not only threaten their security and reputation but also their physical safety. The analysis of 2022 statistics in relation to previous years revealed a discernible escalation in both the frequency and severity of these attacks, emphasising the urgency for improved cybersecurity measures. According to CrowdStrike's 2023 assessment (Baker, 2023), cybercriminals commonly use automated approaches, such as malware, to infiltrate, damage, or steal a firm's data or assets.

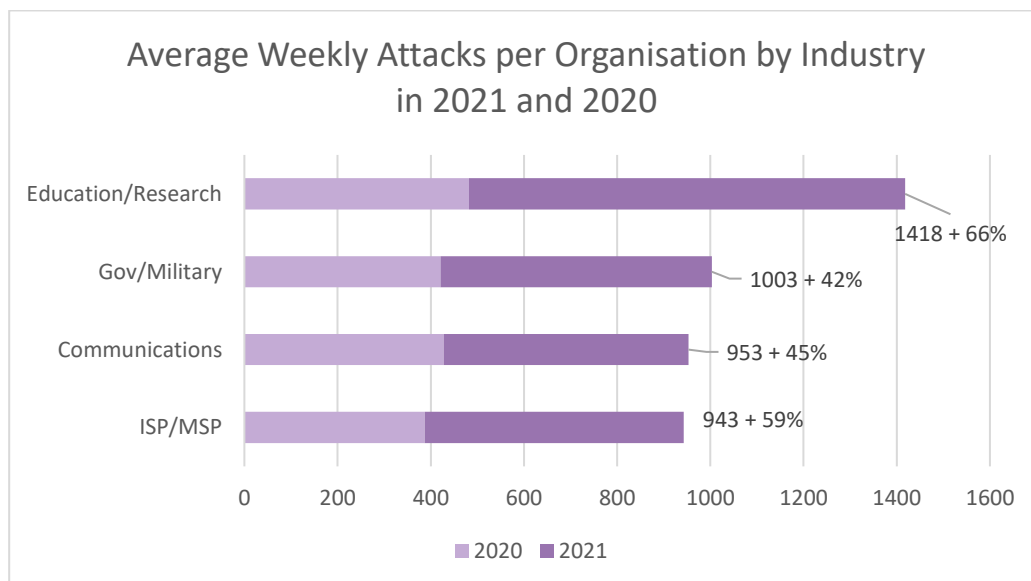


Figure 1.1 - Average Weekly Attacks per Organisation by Industry in 2021 and 2020.

Malware is a term that covers several types of software designed to carry out harmful actions for malicious purposes. The diverse strains include wipers, spyware, ransomware, Trojan horses, and fileless malware (Sudhakar and Kumar, 2020). Each type of malware can cause distinct types of damage, such as encrypting, deleting, or stealing data, opening backdoors for unauthorised access, or obstructing bandwidth. Moreover, some malware employ multiple capabilities or adopt disguises to mimic other types of malicious software. It could significantly complicate the identification and appropriateness of a response and may even pose a risk to the organisation's infrastructure if the malware is misidentified. These attacks can have significant consequences for corporations, their users, and the data they store, resulting in financial losses and legal action on national or international scales. Moreover, the varied strains of malware could make managing the attack considerably more complex and sophisticated, which could result in additional damages or even litigation from third-party organisations or users. With the number of malware attacks increasing each year (PurpleSecurity, 2023), organisations have developed strategies to minimise the impact of infections and respond effectively. These strategies are known as Incident Response Plans.

To address the increasing threat, many organisations have created Incident Response Plans (from here on IRPs) that provide detailed instructions on preventing and responding to attacks in pre-, peri-, and post-infection scenarios. However, in practice, many companies fail to review and update their IRPs regularly, relying on external digital forensic experts to assess the situation before taking preventative action. This reactive approach can result in delays and unexpected damage since malware can disguise itself or rapidly spread across networks. Therefore, it is also essential for companies to create an official cybersecurity plan in place to minimise panic and mitigate potential damage when an attack occurs. A way to enhance the accessibility and efficacy of incident response even further is to employ a **modular version of IRPs**.

1.2 Aims and Research Questions

The project **aims to develop a modular incident response plan tailored to various cyber-attacks**. The modules will primarily modify the response section of a generic IRP to provide a clear set of actions that companies, or their Cyber Incident

Response Team (CIRP) can take to respond to an incident efficiently. The project will compare the effectiveness of the modular plans to general IRPs in terms of the response process and evaluate the results critically. Based on this, the project identified the following objectives:

- Review generalised incident response plans with their advantages and disadvantages.
- Prototype multiple modules for incident response plans based on malware samples.
- Provide a simple malware analysis and digital forensics methodology.
- Analyse four malware samples for the module prototypes (SnakeKeyLogger, BitcoinBlackmailer, FileTour and NotPetya).
- Prototype Yara rules for signature scanning and malware identification based on the analysed samples.

The aim and objectives were tackled with the help of the following research questions:

- **What are the differences between generic incident response plans and their modular variants?**
- **How can modular IRPs optimise response time and efficiency for cyber incident mitigation?**
- **What advantages do modules for separate malicious software provide in terms of response performance?**
- **How can signature scanning combined with modular IRPs affect cyber incident mitigation?**

1.3 Scope of Project

Unlike previous research on malware analysis, this project will combine that knowledge with incident response and attempt to create a more accessible way of responding to cyber-attacks. While there may be anti-virus solutions and malware for all major operating systems, the research will solely focus on malicious software targeting Microsoft Windows as it is the most prevalent operating system used by both organisations and private users.

1.4 Structure

To accurately relay the research and its results, the paper was made with the following sections:

- **Literature Review** – Analysis of academic and industry data that discusses cyber-attacks and incident response.
- **Methodology** – The methodology section provides an in-depth overview of the practical work conducted by the researcher.
- **Results** – A summary of the collected data and practical results of the project – analysis papers, base IRP and malware-based modules, malware analysis methodology and questionnaire results.
- **Discussion** – The results are critically evaluated and compared to the aims in **Section 1.2 Aims and Research Questions** and **Section 2 Literature Review**.
- **Conclusion** – The final section determines whether the project was successful and discusses any planned future work.

2 Literature Review

2.1 Literature Review Introduction

The review aimed to identify how SMEs can deal with cyber-attacks using malware analysis, digital forensics, and incident response plans. This is a critical area due to the increasing number of attacks on smaller businesses with weaker security, often unreported, and with victims paying ransoms to attackers. The review covered distinctive features of IRPs and various methodologies for malware analysis and digital forensics, based on academic research and industry data. Topics included in the review are:

- Incident Response – importance, plans, and advantages/disadvantages.
- Cyber-Attack Analysis – Malware Analysis, Digital Forensics and Signature Scanning.

2.2 Cyber-attacks and Incident Response

2.2.1 Incidents and Incident Response Plans

With the development of personal electronic devices and mass movement to online work environments due to the pandemic, criminals have been continuously shifting their attention towards cybercrime. Computers and the Internet are involved in numerous personal and corporate activities daily, constantly being used for communication and to perform numerous personal (entertainment, exchange of goods, etc.) and business (transactions, intellectual property, services, etc.) actions (Prosise and Mandia, 2003). The constant flow of information is a perfect target for cybercriminals.

Cyberattacks and breaches of confidentiality have become common occurrences. Despite the academic literature and media coverage, no significant research is assessing those attacks' risks and trends (Edwards, Hoffmyer, Forrest 2016; Biener, Eling, and Wirfs 2014). Based on Romanosky's research (Romanosky, 2016), malicious incidents remained constant at around 60% of the cases. Organisations may also be scared to publicly communicate the incident and may not take any legal action against the adversaries. Half of 1700 recorded legal actions were brought in as private civil actions, while only 17% were regarded as criminal actions.

Depending on the scale of the attack and the affected organisation, such attacks could not only significantly damage the company's reputation and intellectual and physical assets but may also endanger human lives. To mitigate or reduce the risk and damages of such attacks, business owners should be able to appropriately respond to incidents. This can be achieved with Incident Response Plans (IRPs).

IRPs are documents used by a company to guide them through a cyber-attack. Such plans have been developed by various organisations, establishing flexible frameworks that can be altered to suit the company's work model and infrastructure. The most well-known and efficient IR frameworks were developed by NIST (Cichonski, 2012) and SANS (Kral, 2012) and can be used as the foundation for an IT team's incident-handling strategies. While it cannot be said which framework is better (as it is heavily dependent on the organisation's assets), IRPs are certainly significant for efficient cyber incident retaliation.

2.2.2 Significance of Incident Response

Incident Response (IR) is crucial to a company's security. Efficient protection and detection measures against attacks and infections will not be able to resolve an incident without appropriate incident response planning. Protection measures are always a part of the human error factor, and adversaries can find exploitable backdoors. In case of an attack, consistent detection methodologies will show the time, scale, and damage by an attack but what would happen afterwards?

Organisations might miss critical aspects of the response process without a comprehensive plan, leaving them vulnerable to newer attack methodologies, human error, panic, and hasty decisions. Effective incident response requires detection, containment, eradication, recovery, and rapid communication. Failure in any one of these phases can lead to a catastrophic outcome. Target's data breach in 2013, where debit/credit card track data was leaked, is an example of this (Krebs, 2013). Despite the severity of the incident, Target failed to communicate with its users, damaging its reputation. Without effective communication channels, an organisation's incident response could appear ineffective to any external entity, leaving them with a long-lasting negative perception of the corporation.

There are multiple reasons why a company's response might appear or even be insufficient in case of an attack. Lack of planning, management support, and leadership are the main causes of ineffective plans (Thompson, 2018) (**Table 2.1**):

Cause	Description
Lack of Planning	Key parts of the response methodology may be missing or lacking an appropriate description.
Lack of Preparation	Preparation is an important part of incident response. The lack of knowledge and practice could lead to uncertainty in the security team and continuous consultation with the plan to find the correct steps for an adequate response. As this will significantly increase the response time, it may also result in a potential failure to resolve the crisis.
Lack of Leadership	Depending on the severity and scale of the incident, individuals may panic and/or forget crucial parts of the response methodology. Such behaviour may affect the remainder of the team negatively if the IR team lacks appropriate leadership which can deal with such issues.
Lack of Management Support	Executives may disagree with critical decisions of the security team (such as shutting down crucial systems) as this will affect the normal operation of the business and its profits. They need to trust their response team and support their recommendation when sufficient reasoning is provided.

Table 2.1 - Causes of incident response failure.

In 2022 (Department for Digital, Culture, Media & Sport), 38% of micro and small businesses experienced cyber-attacks, 20% of which resulted in negative outcomes. Phishing (82%) and more sophisticated attacks (i.e., malware, denial of service - 25%) were identified. However, only 18% have a formal incident management plan and 22% have a cyber security strategy. Less than half sought external data, have outsourced providers, and only 6% have a Cyber Essentials certification or assessed wider supply chain risks. The survey shows that micro-businesses and SMEs are not prepared to respond to cyberattacks.

To handle critical situations effectively, IR teams and executives must receive training. Successful incident response requires leadership and regular practice, to

ensure that organisations can efficiently mitigate damage, and communicate with external partners and users.

2.2.3 Advantages and Disadvantages of IRPs

Despite being a significant part of an organisation's security, Incident Response Plans are not perfect. They have various advantages and disadvantages that may vary depending on the company's structure, architecture, and experience.

Regarding its strengths, IRPs are an effective method for defence preparation. As each company can customise it based on its asset infrastructure, creating the plans can show them various weaknesses and what they need to focus on during an attack. Many IRPs contain information about the preparation, identification, containment, eradication, and recovery phases of the response process; others have sections to help with communication throughout the incident (whom to contact depending on the severity, etc.). The data is handled gradually, ensuring the business can react to a cyberattack in multiple stages. Each step will also contain technical and non-technical actions to be undertaken throughout the incident handling.

In terms of the disadvantages, IRPs are too broad, so organisations create playbooks for specific attacks. such as **NIST**, **NCSC (National Cyber Security Centre)**, and **SOTER** (Onwubiko and Ouazzane, 2020). SOTER is useful for larger firms because it splits work into three hierarchical structures - Bronze, Silver, and Gold. Playbooks offer a technical view of attacks and are useful for creating attack-specific countermeasures, but they can be complicated for SME owners without technical experience. IRPs may also cause damage, as modern malware can disguise itself as a different type, as seen in the **NotPetya** attack in 2017 (Bisson, 2017), which caused severe damage globally. Due to its false ransom message and the Master Boot Record (MBR) encryption, the malware destroyed the data in numerous drives without data recovery.

IRPs may be inefficient for SMEs due to being developed primarily for larger corporations or those with internal CIRTs and may be too general. While playbooks can help, SME executives without technical experience may still struggle. Therefore, a combination of technical actions presented in an easy-to-understand language is

necessary for effective incident response in SMEs and is explored further in the dissertation.

2.3 Cyber-Attack Analysis

Investigating a cyber-attack is essential for effective incident response. Analysis can provide valuable information that may change initial response actions, but the inspection methodology varies based on the company's infrastructure. Combining malware analysis (MA) and digital forensics (DF) is typically the most efficient approach, allowing a firm to dissect malicious software and identify the adversary's actions and potentially their identity.

2.3.1 Malware Analysis

Malware is the common name for malicious software used to attack organisations or individuals. Malicious software can be split into multiple categories depending on its capabilities and how it would affect a potential victim. Examples of such categories can be seen in **Table 2.2** (Baker, 2023):

Type	Functions
Ransomware	Ransomware encrypts the victim's data and demands payment. Paying the ransom is not advised as ransomware groups often do not provide the decryption keys.
Spyware	Spyware is a type of malware that remains silent on the victim's machine and collects their data. The information is then sent to the adversary using the software. Spyware can be used in phishing/spearfishing campaigns or to steal user credentials and session tokens.
Trojan	The Trojan is a reference to the Trojan horse used by the Greeks to infiltrate the city of Troy. Such malware disguises itself as legitimate software (or uses a vulnerable application with injected malicious code) to bypass Anti-Virus (AV) alerts. Its capabilities may vary but such malware is often used in establishing remote code execution (RCE) connections on the target's machine.
Adware	Adware monitors victims' activity and generates pop-up ads based on their browser data, which can cause bandwidth issues. It was initially considered spyware and requires identifying its accessed information and usage to effectively differentiate.

Worm	Worms are one of the oldest types of malware that replicate on other machines, potentially across networks. They may have additional capabilities, such as encryption or RCE, and can cause network bandwidth issues.
Fileless Malware	Fileless Malware refers to a modern form of malicious software that operates without installing any payloads. It bypasses AV software by altering native and legitimate apps to the operating system (PowerShell). As edited files cannot be recognised, such malware is more covert and up to ten times more successful.

Table 2.2 - Malware Types.

Malware analysis is used to identify the malicious software's capabilities and create signatures for detection (used in AV and other systems such as intrusion detection systems (IDS)). Analysts successfully conduct investigations by following two common methodologies (Gandotra, Bansal and Sofat, 2014) – static and dynamic analysis.

Static analysis is a powerful methodology for examining malware code without execution, divided into basic and advanced techniques. Basic techniques rely on tools to analyse strings, file packers, blacklisted functions, and creation/debugging timestamps. Advanced techniques require manual reverse-engineering skills and a deep understanding of low-level programming languages, OS infrastructure, and processes. Manual reverse-engineering uncovers valuable intel, such as obfuscated data, killswitches, encryption code, and zero-day exploits. If a killswitch is identified, researchers could potentially debug and prevent the malware from detonation.

Dynamic analysis is used to examine the impact of malware on a system or network. However, this type of analysis is unsafe and requires specialised analysis labs with monitored connections to prevent it from propagating to networks. Execution, function calls, network communications, altered files, services, registries, and data observation can be applied to analyse malware behaviour. This methodology provides more resilience than static analysis because it reveals the natural behaviour of the malware. However, some malicious software can detect virtual environments and change their detonation process or not execute under certain conditions, making this methodology time-intensive and challenging to scale due to resource constraints.

Analysts commonly use a Hybrid Analysis methodology to combat the advanced evasion and propagation techniques in modern malware. This approach combines static analysis of the file and volatile data, such as runtime execution and RAM usage. Some organisations have also developed sophisticated artificial intelligence tools that employ advanced machine learning algorithms (Ucci, Aniello and Baldoni, 2019), such as malware family and category similarity analysis, to automate the identification of malicious software. This combination of techniques allows for extracting as much data as possible from samples, making it a powerful tool in the fight against malware.

2.3.2 Digital Forensics

Digital Forensics (DF) follows principles of Identification, Preservation, Analysis, Documentation, and Presentation for data from digital sources, and includes subcategories like mobile, computer, and network forensics. Unlike malware analysis, which focuses on malware behaviour, DF obtains information about the entire incident by examining assets such as network traffic, hidden/deleted files, and stolen data. One example of an investigation process is the use of the six main stages based on the Electronic Discovery Reference Model (EDRM) (Casey, 2013). However, other frameworks may be more appropriate depending on the case and affected devices or data, such as NIST's D4I, Mobile Cloud Forensic Framework (MCFF) and others. The EDRM stages can be seen in **Table 2.3**:

Stage name	Actions
Information Management	Identify and mitigate risks and expenses if data acquisition becomes an issue.
Identification	The beginning of a forensic case. The stage aims to identify electronically stored information (ESI), its location, range, format, and relevance to the case.
Collection and Preservation	Acquisition of any ESI (electronic data, devices, drive images, etc.) and its preservation using write blockers to prevent evidence alteration.
Processing, Analysis, and Review	Filtering of the acquired information based on relevance, file types, date range, etc. The data is then analysed and reviewed to ensure that they are useful for the case.

Production	The production stage focuses on extracting the relevant data in native form (documents, images, encoded/encrypted files with decoding/decryption) which will later be used for the presentation.
Presentation	In this stage, researchers are required to present the obtained evidence in forensically accurate documentation either to the victim or at a trial. The data is presented in a native format but parts of it may be highlighted or omitted depending on their importance or sensitivity.

Table 2.3 - Six stages of analysis based on the EDRM framework.

2.3.3 Signature Scanning

Signature scanning, also called signature mapping, is a widely used technique for endpoint security. This approach is simple, fast, effective, and employed by anti-virus vendors and intrusion detection systems (IDS). Depending on the technique used by an analyst, signature scanning can be hash-based or string/rule-based. Hash-based approaches are successful only if the malware does not change, as it uses the hash of the malicious file for comparison. If the malware undergoes any changes, so will the hash value, making it difficult to detect. Conversely, string/rule-based techniques are more modern and have a higher success rate.

Yara is an example of a powerful malware classification and identification framework, using a sophisticated pattern-matching engine for large data samples. By combining signature scanning, malware analysis, and digital forensics, researchers could create comprehensive rules for detecting malware. Yara maps data to match strings or binary patterns and scans network data for identifying payloads or suspicious activity. Although Yara is primarily for detecting malware files, it is a versatile tool for investigating cyber threats. However, creating and maintaining rules requires extensive technical knowledge and experience in malware analysis.

2.4 Literature Review Summary

To summarise, the literature review identified incident response as vital to an organisation. Despite this, many SMEs have not revised or even created such response plans and blindly tackle the issue whenever it occurs. Depending on the severity, the company's reputation and operation could be significantly damaged, which could also lead to its collapse. This could be prevented with the development of an IRP, frequent

technical/awareness training, and IT knowledge. SME executives could either rely on an external security organisation to ensure their security or use various forensic techniques to analyse the attack, its scale, damage, and recovery possibilities.

Employing such forensic techniques could reveal valuable information that could then be leveraged to develop targeted response modules. These modules would replace the response section of an Incident Response Plan, enabling a tailored approach to a particular malware strain and improving the response's efficiency and speed. Based on the identified accessibility issues and worrying statistics, the modular approach to incident response combined with a more accessible methodology for attack analysis would be beneficial for the security of SMEs. Such an approach could also increase the efficiency of incident mitigation while minimising the damage and negative outcomes.

3 Methodology

3.1 Methodology Introduction

Following the completion of the research phase, the practical development and implementation of the proposed incident response framework commenced. Drawing upon the findings of **Section 2 Literature Review**, the researcher identified three key areas for improvement: IRP modules, MA methodology, and signature scanning. The methodology could be split into the following main steps:

- Create a **generalised IRP template** that would later be used for the creation of IRP modules.
- Developing an accessible and effective **cyber-attack analysis methodology** by employing industry standard and user-friendly tools to enable non-technical SME executives and staff to conduct analyses during cyber incidents.
- Test the methodology by **analysing four malware** samples with various capabilities – **NotPetya**, **FileTour**, **Jigsaw**, and **SnakeKeylogger**.
- Employ the findings from the analysis into the creation of **Yara signature scanning rules** and **attack-specific incident response modules**.

In line with the identified objectives outlined in **Section 1.2 Aims and Research Questions**, the aforementioned steps would attempt to establish an effective method for detecting and mitigating future malware incidents, ultimately enhancing the overall cybersecurity posture of small and medium-sized enterprises.

3.2 Generalised Cyber Incident Response Plan

Effective Cyber Incident Response Plans (CIRPs) are crucial for any organisation, but many smaller companies either lack a plan or struggle to implement one efficiently. This could be due to several factors, including overly broad or overly technical formats. Some CIRPs are too general, providing insufficient guidance on how to address specific cyberattacks. Such plans may be designed for companies with a trained Cyber Incident Response Team (CIRT) that could supplement the plan with their expertise. For instance, the Scottish CIRT (Scottish Government, 2021) is a general plan that assumes a competent CIRT will adapt it to their needs. On the other hand, templates

like the one developed by Cyber Management Alliance (CM Alliance, 2015 – Present Day) and Microsoft/Ey/Edelman (Microsoft et al., 2022) may require a prominent level of technical knowledge, making them challenging for personnel in smaller enterprises who lack a technical background to understand.

It is essential to create a balance between providing enough detail to handle specific incidents while not overwhelming users with technical jargon. To accomplish this goal, the researcher conducted a thorough analysis of existing IRP templates and developed a new one that was both flexible and user-friendly. Unlike the Scottish CIRP, which focused primarily on a single country's jurisdiction and governmental organisations, the new template was designed to be accessible to organisations from various countries. To streamline the plan and enhance readability, certain sections were consolidated, and others were eliminated, but the overall structure of the template remained the same. This approach aimed to prevent larger documents from becoming unwieldy and difficult to navigate, especially in critical situations. The plan contained a total of five major sections to guide personnel through an incident (**Table 3.1**):

Section	Content
Introduction	This part of the template covered three sub-sections: <ul style="list-style-type: none">• Purpose – what does the template aim to achieve?• Coordination – how should the affected organisation cooperate with the respective government and governmental organisation?• Scope – the types of incidents covered by the plan.
Management Roles and Responsibilities	This section allows an organisation to specify the responsibilities of different personnel. It contains segments for the CIRT, crisis management team, an example RACI Matrix and plan update conditions. The company can change or remove the segments to suit its infrastructure.
Communications	Who should be contacted and when? The sub-sections cover the organisation's executives, HR, and third-party organisations with examples of their capabilities and contact conditions.

Response Process	A section based on the NIST's incident response methodology for pre- and peri-infection. The pre-infection phase advised on how the organisation should prepare, threat intelligence (following alerts for new cyber-attacks and updates) and training/awareness. The peri-infection phase covered the identification (attack type and data classification), incident reporting (how, when and what should be reported), analysis and assessment (how severe was the compromise and what was affected), containment (how to stop the attack), eradication (how to eliminate malware or adversary activity and access) and recovery (how to restore the network).
Further Awareness and Reporting	The section is based on SANS' incident response methodology for post-incident situation analysis and reporting. It aims to guide the personnel through effectively communicating the attack's origin and consequences. The results should be relayed to the executives for feedback and changes to the architecture, future response, and awareness campaigns.

Table 3.1 - Generic Response Plan Sections.

The researcher also incorporated two essential sections from CMA's template, recognising their value to the new plan – **Critical Apps & Systems** and **Scenarios**. The components were used to develop the CIRP modules. The modules will act as scenarios for specific situations and will follow the altered response process section of the Scottish CIRP template. Further information can be found in **Section 3.5 IRP Module Creation**.

3.3 Simplified Methodology

As previously mentioned, the researcher aimed to create an accessible and powerful analysis methodology. Its main goal was to provide SME owners with an easy-to-follow process that could extract information from a malware sample used in the attack. To achieve this, the analyst split the methodology into static analysis, dynamic analysis, and signature scanning. Each phase employed various industry-standard tools that would not require extensive knowledge.

3.3.1 Tools and Techniques

During the static analysis phase, the analyst used four tools to extract data without detonating the sample. To quickly identify if any anti-virus solutions would flag the file

as malicious, AV vendor scans (such as **VirusTotal** (VirusTotal, 2004 – Present Day) were employed. For human-readable string extraction, both **Strings** (Russinovich, 2021) and **Floss** (Ballenthin, 2016) were recommended and used. Floss also attempted to de-obfuscate and decode any hidden strings within the file. If **Floss** failed to extract the data or the file was not a binary, Strings could extract all readable data. Lastly, **PEStudio** (Fox, 2021) and **ExeInfoPE** (ASL, 2023) could obtain more detailed information about the sample - file packers, blacklisted functions/strings/libraries, embedded executables, file hashes, debug/compile data and more.

During the dynamic analysis phase, the methodology aimed to provide comprehensive information regarding the capabilities of the malicious software. The analysis began by identifying any visible detonation symptoms and the conditions required for detonation. Following this, the methodology continued with an examination of possible network-based symptoms. The researcher prioritised them over host-based ones to identify any propagation capabilities that could enable the malware to affect other machines or data. The analysis employed **TCPView** (Russinovich, 2022) to monitor open connections and **Wireshark** (Wireshark, 1997 – Present Day)/**Inetsim** (Hagenberg and Eckert, 2007) on a Remnux Linux distribution to simulate a DHCP server and internet connection and to follow any network data. Host-based indicators were analysed using **Procmon** (Russinovich, 2022) and **Volatility 3.0** (Volatility Foundation, 2020). Procmon monitored the process in real-time and displayed any service calls, registry/file manipulation, and hidden processes. Volatility 3.0 was combined with **WinPmem** (Cohen, et al., 2019) to dump any data held within RAM. The researcher then used Volatility to identify masked services with injected malicious code, what services attempted/expected connections and more.

3.3.2 Data Analysis

The malware analysis methodology could leave personnel with large amounts of unfiltered information, which could be confusing and overwhelming, particularly for individuals with limited technical experience. Data analysis, in fields such as DF and MA, requires extensive knowledge to distinguish relevant data and technical terminology that may be unfamiliar to regular personnel. Improperly filtered or misunderstood results could even lead to panic among staff members.

To make the methodology more accessible and mitigate confusion, the researcher included a list of commonly used technical terminology in malware analysis in the documentation. The technical jargon was thoroughly explained using accessible language. Additionally, each phase included extensive examples of the generated output, including recurrent functions/libraries used in different malware types, the capabilities of different malware types, and how they could affect the network and system. The documentation also provided instructions on filtering the diverse output of various tools, such as filtering in Procmon, Wireshark packet filtering, and string filtering, to ensure that personnel could accurately analyse and understand the data.

This approach aimed to simplify the complicated process of output filtering and analysis for personnel, enabling them to distinguish between several types of malware and their capabilities and understand how they would affect the infected system. By following the methodology and examples, personnel could efficiently and effectively analyse substantial amounts of data without requiring extensive technical knowledge.

3.3.3 Use of Obtained Data

After conducting a thorough analysis to identify relevant data on the malware's capabilities, the analyst developed Yara rules based on the analysed samples. The methodology's documentation included extensive examples to help personnel understand the structure, syntax, and usage. The rules were based on strings found within the malware samples that were directly associated with their functionality, such as embedded file names, suspicious URLs, embedded commands, and more.

To create the rules, the researcher specified different signatures related to the file and the necessary conditions. The rules could then be run using yara32 within FlareVM or implemented within an IDS if the organisation uses one for its network. Organisations could use those rules to scan specific files, entire directories, or network packets. If the signature matched any files, yara32 or the IDS would either list the matching files or generate an alert.

This approach aimed to enhance the organisation's capability to detect and respond to malware threats effectively. By creating Yara rules based on analysed samples, the organisation could proactively scan for and identify similar threats in the future,

potentially reducing the risk of a successful attack. The examples provided in the methodology's documentation ensured that personnel with little technical experience could understand the process and create effective Yara rules to help protect the organisation's systems and network.

3.4 Implementation

To test the methodology, the researcher applied it to four separate malware samples. The analysis of the samples could be used as a guide together with the methodology.

3.4.1 Malware Types and Samples

As seen in **Section 2.3.1 Malware Analysis**, malicious software could be split into multiple types depending on their capabilities. The researcher analysed four malware samples with varying offensive capabilities and complexities: SnakeKeylogger, Jigsaw, FileTour (AbuseCH, 2020), and NotPetya (ytsif, 2014 – Present Day). SnakeKeylogger (Zhang, 2021) is an active phishing campaign malware that attempts to steal various data types, including those from popular browsers and messaging platforms like Discord. Jigsaw, or BitcoinBlackmailer, (Ashdown, 2021) was active from 2016 to 2021 and used fearmongering techniques. It was unique in that it deleted data after a user refused to cooperate, and its live support chat suggested that its motive was not solely monetary gain.

FileTour (Stamus Labs, 2022) was a complex file packer previously used in the Stantinko (ESET, 2017) botnet for payload delivery. It used multiple stages of execution and payload delivery, with payloads capable of data theft and backdoors. The sample was heavily obfuscated. NotPetya (Ivanov and Mamedov, 2017) was a 2017 malware associated with APT Sandworm, using the EternalBlue zero-day exploit. It encrypted data with unrecoverable sophistication and launched through an accounting software update injected with the malicious sample. Some researchers categorised it as a wiper due to how it behaves.

The analysis of the samples was aided by the analysis sandbox **Any.Run** to speed up the process and led the researcher through the more complex samples (Lapshin, 2016).

3.4.2 Testing Environment

The testing environment comprised two virtual machines, FlareVM and Remnux, created in VirtualBox and connected to a host-only network (**Figure 3.1**). FlareVM, an open-source Windows-based security distribution available on GitHub, was ideal for analysing samples designed to infect Windows machines due to its extensive arsenal of analysis tools. Remnux, a Linux-based alternative to FlareVM, came preinstalled with InetSim and Wireshark - essential tools for DNS/DHCP simulation and traffic monitoring.

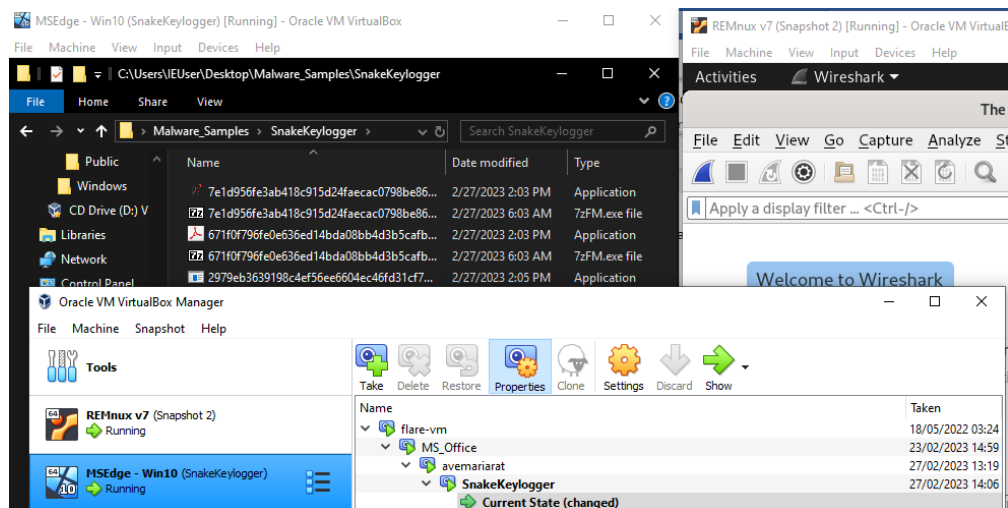


Figure 3.1 - Virtual Machine Testing Environment

The network was a simple /24 subnet without access to the physical machine or other networks (**Figure 3.2**). The subnet's size was chosen to evaluate how some samples would enumerate the subnet and whether they would attempt to move further within the network.

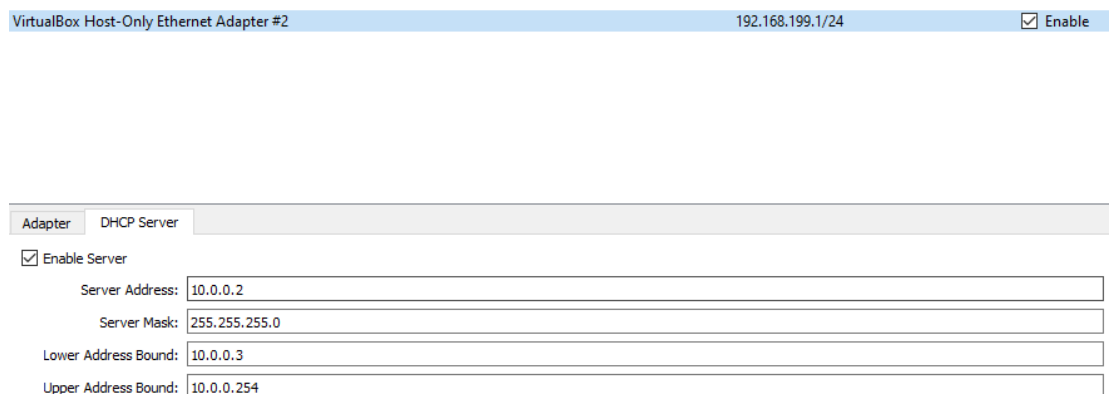


Figure 3.2 - Host-Only Network Settings.

3.4.3 Static Analysis

3.4.3.1 AV Vendor Scans

The static analyses began by identifying the MD5 and SHA256 hashes of the samples (**Figure 3.3**). Researchers could utilise the hashes in platforms such as VirusTotal for identification, statistical, and awareness purposes. Upon analysis, all four samples' hashes were flagged as malicious, providing unambiguous evidence that they were malware. The vendor results were highly accurate, with some even indicating the name of the malicious software. (**Figure 3.4**)

```
C:\Users\IEUser\Desktop\Malware_Samples\Jigsaw
λ md5sum.exe jigsaw.exe
2773e3dc59472296cb0024ba7715a64e *jigsaw.exe

C:\Users\IEUser\Desktop\Malware_Samples\Jigsaw
λ sha256sum.exe jigsaw.exe
3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7 *jigsaw.exe
```

Figure 3.3 - Hash Identification.



Figure 3.4 - VirusTotal Results for Jigsaw.

3.4.3.2 String Extraction

This phase of the analysis was carried out with the tools “Strings” and “Floss”. Floss was unable to properly extract the strings from some of the identified binaries, due to heavy obfuscation which caused issues within the script (**Figure 3.5**).

```

C:\Users\IEUser\Desktop\Malware_Samples\FileTour_Adware
λ floss FileTour.exe > strings.txt
WARNING:envi.codeflow:parseOpcode error at 0x004254c1 (addCodeFlow(0x425468)): InvalidInstruction("ffffff010000002a000000" at 0x4254c1,)
WARNING:visect.base.cb_opcode(0x417553): LOCATION ALREADY EXISTS: loc: 'PTR: 0x0041755d'
WARNING:visect.base.cb_opcode(0x417558): LOCATION ALREADY EXISTS: loc: 'PTR: 0x0041756c'
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x422844, opva: 0x42284f, op: inc eax, err: HIT LOCTYPE 4 AT 0042284d
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x401018, opva: 0x40108f, op: mov dl,66, err: HIT LOCTYPE 4 AT 0040108e
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x40edf8, opva: 0x40ee49, op: js: 0x0040ee4c, err: HIT LOCTYPE 2 AT 0040ee3c
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x40edcc, opva: 0x40ee1d, op: inc ebp, err: HIT LOCTYPE 2 AT 0040ee0c
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x420618, opva: 0x42068f, op: inc edx, err: HIT LOCTYPE 4 AT 0042068d
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x41d3c8, opva: 0x41d434, op: outsb edx,byte [esi], err: HIT LOCTYPE 2 AT 0041d424
WARNING:visect.impemu.emulator:Emulator prehook failed on fva: 0x422704, opva: 0x42270c, op: adc al,16, err: HIT LOCTYPE 4 AT 0042270c
WARNING:visect.base.cb_opcode(0x40ee3c): LOCATION ALREADY EXISTS: loc: "EmptyWorkingsSet\\x00"
WARNING:visect.base.cb_opcode(0x40ee9f): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverBaseNameA\\x00"
WARNING:visect.base.cb_opcode(0x40eea0): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverBaseNameA\\x00"
WARNING:visect.base.cb_opcode(0x40ee98): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverBaseNameA\\x00"
WARNING:visect.base.cb_opcode(0x40ee75): LOCATION ALREADY EXISTS: loc: "InitializeProcessForWMatch\\x00"
WARNING:visect.base.cb_opcode(0x40ee5c): LOCATION ALREADY EXISTS: loc: "InitializeProcessForWMatch\\x00"
WARNING:visect.base.cb_opcode(0x40eec0): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverFileNameA\\x00"
WARNING:visect.base.cb_opcode(0x40eeca): LOCATION ALREADY EXISTS: loc: "GetMappedFileNameW\\x00"
WARNING:visect.base.cb_opcode(0x40eeb4): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverFileNameA\\x00"
WARNING:visect.base.cb_opcode(0x40ee8c): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverBaseNameA\\x00"
WARNING:visect.base.cb_opcode(0x40eeef): LOCATION ALREADY EXISTS: loc: "GetDeviceDriverBaseNameA\\x00"
WARNING:visect.base.cb_opcode(0x40eec9): LOCATION ALREADY EXISTS: loc: "GetMappedFileNameW\\x00"
WARNING:visect.base.cb_opcode(0x40f234): LOCATION ALREADY EXISTS: loc: "Module32First\\x00"
WARNING:visect.base.cb_opcode(0x40f23f): LOCATION ALREADY EXISTS: loc: "Module32First\\x00"
WARNING:visect.base.cb_opcode(0x40f25a): LOCATION ALREADY EXISTS: loc: "Module32FirstW\\x00"
WARNING:visect.base.cb_opcode(0x40f265): LOCATION ALREADY EXISTS: loc: "Module32NextW\\x00"
WARNING:visect.base.cb_opcode(0x40f254): LOCATION ALREADY EXISTS: loc: "Module32FirstW\\x00"
WARNING:visect.base.cb_opcode(0x40f246): LOCATION ALREADY EXISTS: loc: "Module32Next\\x00"
WARNING:envi.codeflow:parseOpcode error at 0x0041a9e9 (addCodeFlow(0x41a9e0)): InvalidInstruction("ffffff10000000506c65617365207365" at 0x41a9e9,)
WARNING:envi.codeflow:parseOpcode error at 0x0041e7c5 (addCodeFlow(0x41e7c0)): InvalidInstruction("ffffff020000005b690000fffffffff02" at 0x41e7c5,)

```

Figure 3.5 - Error Generated by Floss by Some Samples.

The extracted strings provided valuable evidence about the malicious software samples such as blacklisted libraries and distinctive names/text (**Figure 3.6**). The libraries allowed for a broader idea of the malware's capabilities. Other artefacts such as embedded software, ransom messages, file system locations, languages, and file extensions further proved its capabilities (**Figure 3.7**). They also showed key investigation evidence that would aid the further analysis of the situation. More information can be found in **Appendix A**.

```

RegQueryInfoKeyA
RegOpenKeyExA
RegEnumKeyExA
RegCreateKeyExA
LookupPrivilegeValueA
GetUserNameA
shell32.dll
ShellExecuteExA
ShellExecuteA
cabinet.dll
FDIDestroy
FDICreate
ole32.dll
OleInitialize
CoTaskMemFree
CoCreateInstance
CoUninitialize
CoInitialize
shell32.dll
SHGetSpecialFolderLocation
SHGetPathFromIDListA
SHGetMalloc
SHChangeNotify

```

Figure 3.6 - FileTour Malicious Functions.


```

0123456789abcdef
Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
CHKDSK is repairing sector
Please reboot your computer!
Decrypting sector
Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.
We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:
If you already purchased your key, please enter it below.
Incorrect key! Please try again.

```

Figure 3.7 - NotPetya Ransom Message.

3.4.3.3 PESTudio and ExeInfoPE

With PESTudio, the analyst could successfully conduct a more in-depth static analysis and identify several indicators pointing to malicious behaviour (**Figure 3.8**). The tool provided valuable data on blacklisted strings, functions, libraries, metadata, and file sections. While the libraries used by the malware varied based on their capabilities, some were consistent across multiple samples, such as kernel32.dll and user32.dll. However, not all libraries were marked as banned, as they were also present in numerous legitimate software applications.

property	value
md5	40CD711112184320F0E523340B823519
sha1	2A8EDE6329419CC071412AE33A8EDF192D5047E6
sha256	D76E0F9F10F5589DE72E43D07B1C20F5DDB1E6A1834556637BC9B225EAF61479
entropy	7.999
file-offset	0x0000AC00
size	248087 (bytes)
signature	Nullsoft
first-bytes-hex	04 00 00 00 EF BE AD DE 4E 75 6C 6C 73 6F 66 74 49 6E 73 74 42 3E 00 00 17 C...
first-bytes-text Nullsoft\instB >]
file-ratio	84.93 %

Figure 3.8 - SnakeKeylogger PESTudio Analysis.

The researcher also observed that the samples employed functions from the accessed libraries. Others implemented custom functions with obfuscated names

(**Figure 3.9**), which could be a crucial lead for more advanced static analysis techniques such as reverse engineering.

functions (13)	namespace (3)	blacklist (0)	ordinal (1)	library (2)
AncodntQOrHVwMgqTckbl...	-		-	mscorlib.dll
koi	-		-	mscorlib.dll
gLFFatrEMIOkQA@~kMIKio...	-		-	mscorlib.dll
n/a	-		-	mscorlib.dll
System.Runtime.InteropServices...	fgregre		-	-
System.Reflection	fgregre		-	-
System	fgregre		-	-
System.IO	fgregre		-	-
System.Runtime.Versioning	fgregre		-	-
65535 (.ctor)	fgregre		x	-
System.Runtime.CompilerServicesSe...	fgregre		-	-
System.Text	fgregre		-	-

Figure 3.9 - Custom Function in Second Stage Payload of FileTour (PBrowFile15).

Furthermore, the researcher found several samples with suspicious sections within their code. Some contained self-modifying sections, while others were nameless, writable, virtualised, or executable. These sections indicated the use of sophisticated obfuscation or exploited legitimate software with injected malicious code (**Figure 3.10**).

property	value	value	value	value	value
name	!mmJJPp	text	rsrc	reloc	n/a
md5	84ED17C693B72297449986A...	25C7E782FE572BC66C5DBF4...	42554AC5ECA4608577CB97...	F73E3F2C2543C556F8D9396...	A1131D32898900E17032CE4...
entropy	7.999	5.391	3.581	0.098	0.139
file-ratio (99.65%)	73.72 %	24.87 %	0.71 %	0.18 %	0.18 %
raw-address	0x0000400	0x00034800	0x00046200	0x00046A00	0x00046C00
raw-size (289280 bytes)	0x00034400 (214016 bytes)	0x00011A00 (72192 bytes)	0x00000800 (2048 bytes)	0x0000200 (512 bytes)	0x0000200 (512 bytes)
virtual-address	0x00402000	0x00438000	0x0044A000	0x0044C000	0x0044E000
virtual-size (287044 bytes)	0x00034260 (213600 bytes)	0x00011878 (71800 bytes)	0x00000650 (1616 bytes)	0x0000000C (12 bytes)	0x00000010 (16 bytes)
entry-point	-	-	-	-	0x0004E00A
characteristics	0xE0000040	0x60000020	0x40000040	0x42000040	0x60000020
writable	x	-	-	-	-
executable	x	x	-	-	x
shareable	-	-	-	-	-
discardable	-	-	-	x	-
initialized-data	x	-	x	x	-
uninitialized-data	-	-	-	-	-
unreadable	-	-	-	-	-
self-modifying	x	-	-	-	-
virtualized	-	-	-	-	-
file	n/a	n/a	n/a	n/a	n/a

Figure 3.10 - Custom self-modifying section in Jigsaw.

Regarding the metadata, the analyst discovered information about the file's creation and last debugging. Three of the samples had their final debugging dates in 2016 and 2017. Conversely, SnakeKeylogger was recently debugged on 27th Feb (**Figure 3.11**), indicating that the malware is still active and there were newly created samples to bypass AV detection.

name (15)	size (bytes)	location (address)	location (section)	time-stamp
export-table	0x00000000 (0)	0x00000000	n/a	n/a
import-name	0x00000104 (260)	0x00019594	.rdata	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
resource	0x000001E0 (480)	0x00023000	.rsrc	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
exception	0x00000000 (0)	0x00000000	n/a	n/a
security	0x00000000 (0)	0x00000000	n/a	n/a
relocation	0x000019FC (6652)	0x00024000	.reloc	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
debug	0x00000038 (56)	0x00017470	.rdata	0x63FC6AFC (Mon Feb 27 08:34:04 2023 UTC)
architecture	0x00000000 (0)	0x00000000	n/a	n/a
global-pointer	0x00000000 (0)	0x00000000	n/a	n/a
thread-storage	0x00000000 (0)	0x00000000	n/a	n/a
load-configuration	0x00000040 (64)	0x000190A8	.rdata	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
bound-import	0x00000000 (0)	0x00000000	n/a	n/a
import-address	0x00000428 (1064)	0x00017000	.rdata	0x00000000 (Thu Jan 01 00:00:00 1970 UTC)
delay-loaded	0x00000000 (0)	0x00000000	n/a	n/a
.NET	0x00000000 (0)	0x00000000	n/a	n/a

Figure 3.11 - Recent Debug Time of SnakeKeylogger.

Lastly, the identified strings showed undiscovered data that Floss, and Strings, did not extract. PEStudio displayed various URLs and other critical data hidden within the sample (**Figure 3.12**). By combining the information obtained from all three tools, the researcher was able to extract as much data as possible to aid in our analysis.

indicator (45)	detail	level
strings > blacklist	count: 17	1
functions > blacklist	count: 3	1
section > blacklist	section: ???mmUPp	1
section > first > writable	section: ???mmUPp	1
entry-point > suspicious > location	section: :0x0004E00A	1
sections > writable > executable	count: 1	1
URL > pattern	url: http://btc.blockr.io/api/v1/	1
sections > nameless	count: 1	2
file > name > original	name: BitcoinBlackmailer.exe	3

Figure 3.12 - Identified URLs and Other Hidden Data in Jigsaw.

3.4.4 Dynamic Analysis

3.4.4.1 Detonation Symptoms and Conditions

One of the analysed samples, NotPetya, required specific conditions for successful detonation as it was transferred as a .bat file through an exploited accounting software update. It could not be executed through double-clicking, requiring a specific command in a terminal window. The researcher could conventionally detonate the other malware samples.

Symptom-wise, two samples (Jigsaw (**Figure 3.13**) and NotPetya (**Figure 3.14**)) made visible changes by encrypting data and displaying a ransom message, while FileTour and SnakeKeylogger had partially hidden and completely covert symptoms, respectively. The lack of C&C servers may have contributed to FileTour's partially

visible indicators (**Figure 3.15**), and SnakeKeylogger's design as spyware reinforced its stealth capabilities.

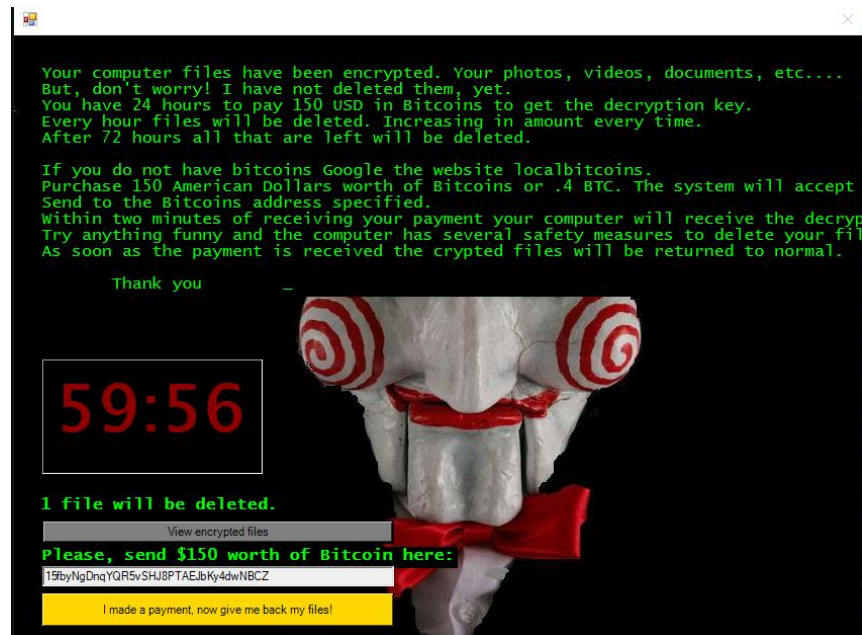


Figure 3.13 - Jigsaw Visible Ransom.

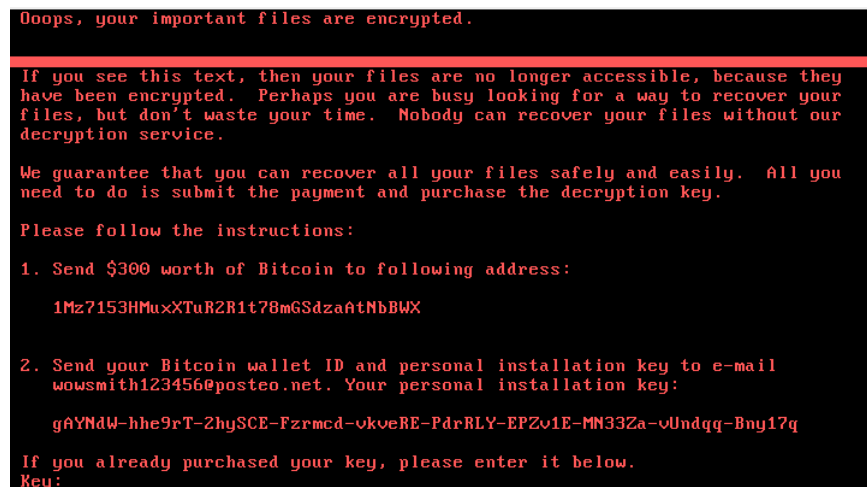


Figure 3.14 - NotPetya Ransom Message.

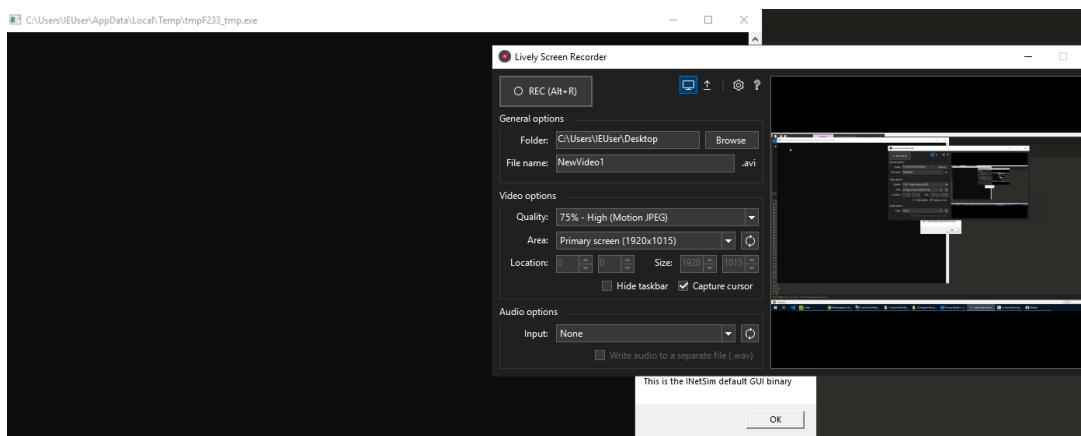


Figure 3.15 - Screen Recorder Launched by FileTour.

3.4.4.2 Network-Based Indicators

The researcher examined different network behaviours in each sample. Jigsaw communicated with web addresses only when the victim attempted to pay the ransom (**Figure 3.14**). The ransomware did not attempt to access any other addresses and did not use any complex propagation mechanisms. SnakeKeylogger tried to contact two web addresses, including a possible C&C server on Telegram (**Figure 3.16**). The first web address attempted to obtain more information on the victim - such as IP address, geolocation, etc. The researcher could not identify the exact use of the Telegram server, but the malware might have sent the stolen data to it as a message.

```

▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;)\r\n
    Host: checkip.dyndns.org\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://checkip.dyndns.org/]
    [HTTP request 1/1]
    [Response in frame: 29]
  
```

Figure 3.16 - SnakeKeylogger Web Address Access.

FileTour's network activity was integrated into its second-stage payloads, trying to download third-stage executables – sonia30.exe and Xtect12.exe (**Figure 3.17**). The researcher could not analyse the capabilities of the former executable, but they could assume that the latter binary tested Anti-virus solutions based on the URL. The malware also obtained information about the IP and the country of the infected. NotPetya had the most complex network capabilities, utilising worm-like functionality and EternalBlue

to enumerate the entire subnet and exploit machines and servers to propagate (**Figure 3.18**). The malware aggressively tried to traverse through the network and checked the status of the connected systems (whether they were infected or not). Combining it with the zero-day exploit (**EternalBlue**), it could effortlessly traverse networks and cause considerable damage.

354	8.335512172	10.0.0.4	10.0.0.3	HTTP	137 GET /files/sonia30.exe HTTP/1.1
357	8.337471906	10.0.0.3	10.0.0.4	HTTP	312 HTTP/1.1 200 OK (text/html)
368	8.344740544	10.0.0.4	10.0.0.3	HTTP	210 GET /antivirustesting/Xtect12.
374	8.369962982	10.0.0.3	10.0.0.4	HTTP	150 HTTP/1.1 200 OK (x-msdos-prog
381	8.374625835	10.0.0.3	10.0.0.4	HTTP	150 HTTP/1.1 200 OK (x-msdos-prog
418	8.795322059	10.0.0.4	10.0.0.3	HTTP	199 GET /ip HTTP/1.1
421	8.804393797	10.0.0.3	10.0.0.4	HTTP	312 HTTP/1.1 200 OK (text/html)
437	11.158670329	10.0.0.4	10.0.0.3	HTTP	250 GET /msdownload/update/v3/stat
440	11.168301261	10.0.0.3	10.0.0.4	HTTP	312 HTTP/1.1 200 OK (text/html)
461	12.187804736	10.0.0.4	10.0.0.3	HTTP	250 GET /msdownload/update/v3/stat
464	12.197518790	10.0.0.3	10.0.0.4	HTTP	312 HTTP/1.1 200 OK (text/html)
465	12.197518790	10.0.0.3	10.0.0.4	HTTP	250 GET /msdownload/update/v3/stat

Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3				
Transmission Control Protocol, Src Port: 50357, Dst Port: 80, Seq: 1, Ack: 1, Len: 83				
Hypertext Transfer Protocol				
GET /files/sonia30.exe HTTP/1.1\r\n				
Host: activityhike.com\r\n				
Connection: Keep-Alive\r\n				
\r\n				
[Full request URI: http://activityhike.com/files/sonia30.exe]				
[HTTP request 1/1]				
[Response in frame: 374]				

Figure 3.17 - FileTour Third-Stage Payloads.

118	49.675543810	10.0.0.4	10.0.0.255	BROWSER	216 Get Backup List Request
119	49.675606248	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
120	50.305023594	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.5? Tell 10.0.0.4
121	50.445835549	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
122	51.196619615	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
123	51.212861719	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.5? Tell 10.0.0.4
124	52.213890332	PcsCompu_e6:e5:59	PcsCompu_1e:4b:5f	ARP	60 Who has 10.0.0.3? Tell 10.0.0.4
125	52.213890683	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.5? Tell 10.0.0.4
126	52.213909317	PcsCompu_1e:4b:5f	PcsCompu_e6:e5:59	ARP	42 10.0.0.3 is at 08:00:27:1e:4b:5f
127	52.964387369	10.0.0.4	10.0.0.255	BROWSER	216 Get Backup List Request
128	52.964435453	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
129	53.730073314	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
130	54.325353713	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.6? Tell 10.0.0.4
131	54.480807125	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1b>
132	55.214611782	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.6? Tell 10.0.0.4
133	56.221755043	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.6? Tell 10.0.0.4
134	56.253718269	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1e>
135	57.014573261	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1e>
136	57.782624101	10.0.0.4	10.0.0.255	NBNS	92 Name query NB WORKGROUP<1e>
137	58.344729508	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.7? Tell 10.0.0.4
138	59.218791769	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.7? Tell 10.0.0.4
139	60.215093750	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.7? Tell 10.0.0.4
140	62.376115456	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.8? Tell 10.0.0.4
141	63.220077055	PcsCompu_e6:e5:59	Broadcast	ARP	60 Who has 10.0.0.8? Tell 10.0.0.4

Figure 3.18 - NotPetya Attempting to Interrogate the Server.

3.4.4.3 Host-Based Indicators

Each sample exhibited different host-based symptoms that impacted the victim's system in several ways. Jigsaw and NotPetya encrypted specific file extensions, but only Jigsaw had persistence mechanisms that deleted files as punishment. It also installed two more executables - one for system encryption and the other for persistence. The files used similar names of legitimate software to evade detection (drpbx and frfx)

(**Figure 3.19** and **Figure 3.20**). NotPetya restarted the machine after some time, displaying a fake drive repair message. The encryption process then began, camouflaged as a file repair service (**Figure 3.21**). Finally, the false ransom message appeared, indicating that the contents were encrypted.

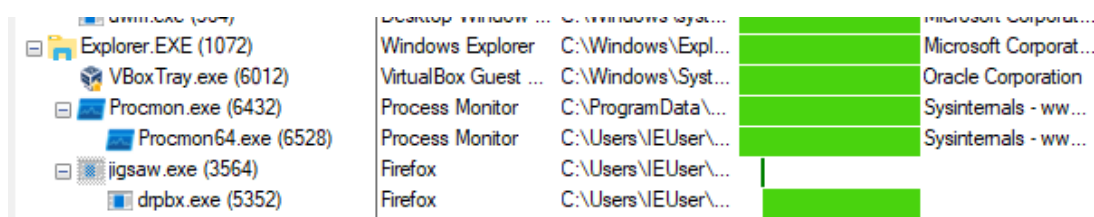


Figure 3.19 - Drpbx.exe File Used for Encryption.

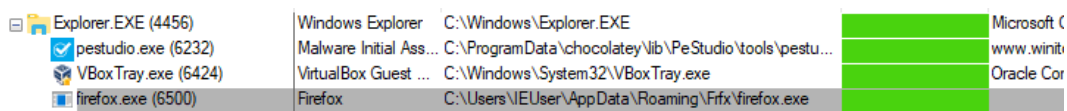


Figure 3.20 - Frfx (firefox.exe) File Used for Persistence.

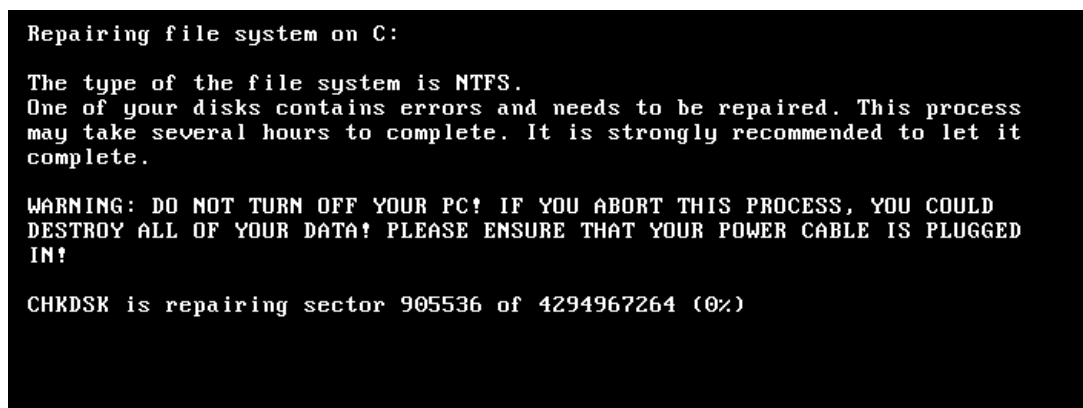


Figure 3.21 - Fake Disk Repair Message by NotPetya.

FileTour installed multiple payloads with different capabilities, including backdoor access, data theft, and encryption (**Figure 3.22**). Despite being recognised as adware, FileTour did not display any ads when the researcher used the browser. SnakeKeylogger acted covertly as typical spyware. It extracted only one executable (fzpceresm.exe) which carried out the data theft. The file accessed various registries and files that contained browser history and account details (**Figure 3.23**).

Process	Description	Image Path	Life Time	Company	Owner	Comr
FileTour.exe (5420)	SmartPDF 10.32.0...	C:\Users\IEUser\...		SmartPDF	... MSEDGEWIN10\...	"C:\U
9840432e051a6fa1192594...		C:\Program Files (...)			MSEDGEWIN10\...	"C:\P
PBrowser.exe (3808)	gsdffd	C:\Program Files (...)		gsdffd	MSEDGEWIN10\...	"C:\P
lg.exe (7552)	VNC® Viewer	C:\Program Files (...)		RealVNC Ltd	MSEDGEWIN10\...	"C:\P
Conhost.exe (4304)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	MSEDGEWIN10\...	"??C
lg.exe (6456)	VNC® Viewer	C:\Program Files (...)		RealVNC Ltd	MSEDGEWIN10\...	"C:\P
Conhost.exe (4320)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	MSEDGEWIN10\...	"??C
LivelyScreenRecS3.0.exe (8976)	Quick Screen Re...	C:\Program Files (...)		Module Art	MSEDGEWIN10\...	"C:\P
tmpECAC_tmp.exe (8976)		C:\Users\IEUser\...			MSEDGEWIN10\...	"C:\U
Conhost.exe (8984)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	MSEDGEWIN10\...	"??C
note866.exe (2192)		C:\Program Files (...)			MSEDGEWIN10\...	"C:\P
stats.exe (4860)	stats Setup	C:\Program Files (...)			MSEDGEWIN10\...	"C:\P
stats.tmp (8016)	Setup/Uninstall	C:\Users\IEUser\...			MSEDGEWIN10\...	"C:\U
Setup.exe (8692)		C:\Users\IEUser\...			MSEDGEWIN10\...	"C:\U
Conhost.exe (915)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	MSEDGEWIN10\...	"??C
SmartPDF.exe (3928)		C:\Program Files (...)			MSEDGEWIN10\...	"C:\P
cmd.exe (5428)	Windows Comma...	C:\Windows\SYS...		Microsoft Corporat...	MSEDGEWIN10\...	"cmd"
Conhost.exe (6060)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	MSEDGEWIN10\...	"??C

Figure 3.22 - FileTour Second-Stage Payloads.

SnakeKeylogger.exe (1428)	retreatism	C:\Users\IEUser\...	deforms	MSEDGEWIN10\...
fzpceresm.exe (4136)		C:\Users\IEUser\...		MSEDGEWIN10\...
fzpceresm.exe (740)		C:\Users\IEUser\...		MSEDGEWIN10\...
fzpceresm.exe (2452)		C:\Users\IEUser\...		MSEDGEWIN10\...
WerFault.exe (6632)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...
WerFault.exe (4224)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...

Figure 3.23 - SnakeKeylogger Second-Stage Payload.

As a final step, the researcher dumped the testing environment's RAM and leveraged Volatility 3.0 to identify the privileges of each malware and any hidden processes. The analysis of the four samples revealed consistent results, including injected code in legitimate software (FileTour) and elevated system-level privileges (Figure 3.24). Further information can be found in **Appendix B**.

204	9840432e051a6f	2	SeCreateTokenPrivilege	Create a token object
204	9840432e051a6f	3	SeAssignPrimaryTokenPrivilege	Replace a process-level token
204	9840432e051a6f	4	SeLockMemoryPrivilege	Lock pages in memory
204	9840432e051a6f	5	SeIncreaseQuotaPrivilege	Present Increase quotas
204	9840432e051a6f	6	SeMachineAccountPrivilege	Add workstations to the domain
204	9840432e051a6f	7	SeTcbPrivilege	Act as part of the operating system
204	9840432e051a6f	8	SeSecurityPrivilege	Present Manage auditing and security log
204	9840432e051a6f	9	SeTakeOwnershipPrivilege	Present Take ownership of files/objects
204	9840432e051a6f	10	SeLoadDriverPrivilege	Present Load and unload device drivers
204	9840432e051a6f	11	SeSystemProfilePrivilege	Present Profile system performance
204	9840432e051a6f	12	SeSystemTimePrivilege	Present Change the system time
204	9840432e051a6f	13	SeProfileSingleProcessPrivilege	Present Profile a single process
204	9840432e051a6f	14	SeIncreaseBasePriorityPrivilege	Present Increase scheduling priority
204	9840432e051a6f	15	SeCreatePageFilePrivilege	Present Create a pagefile
204	9840432e051a6f	16	SeCreatePermanentPrivilege	Create permanent shared objects
204	9840432e051a6f	17	SeBackupPrivilege	Present Backup files and directories
204	9840432e051a6f	18	SeRestorePrivilege	Present Restore files and directories
204	9840432e051a6f	19	SeShutdownPrivilege	Present Shut down the system
204	9840432e051a6f	20	SeDebugPrivilege	Present Debug programs
204	9840432e051a6f	21	SeAuditPrivilege	Generate security audits
204	9840432e051a6f	22	SeSystemEnvironmentPrivilege	Present Edit firmware environment values
204	9840432e051a6f	23	SeChangeNotifyPrivilege	Present,Enabled,Default Receive notifications of changes to files or directories
204	9840432e051a6f	24	SeRemoteShutdownPrivilege	Present Force shutdown from a remote system
204	9840432e051a6f	25	SeHotkeyPrivilege	Present Remove computer from docking station
204	9840432e051a6f	26	SeSyncAgentPrivilege	Synch directory service data
204	9840432e051a6f	27	SeEnableDelegationPrivilege	Enable user accounts to be trusted for delegation
204	9840432e051a6f	28	SeManageVolumePrivilege	Present Manage the files on a volume
204	9840432e051a6f	29	SeImpersonatePrivilege	Present,Enabled,Default Impersonate a client after authentication
204	9840432e051a6f	30	SeCreateGlobalPrivilege	Present,Enabled,Default Create global objects
204	9840432e051a6f	31	SeTrustedCredManAccessPrivilege	Access Credential Manager as a trusted caller
204	9840432e051a6f	32	SeRelabelPrivilege	Modify the mandatory integrity level of an object
204	9840432e051a6f	33	SeIncreaseWorkingSetPrivilege	Present Allocate more memory for user applications
204	9840432e051a6f	34	SeTimeZonePrivilege	Present Adjust the time zone of the computer's internal clock
204	9840432e051a6f	35	SeCreateSymbolicLinkPrivilege	Present Required to create a symbolic link
204	9840432e051a6f	36	SeDelegateSessionUserImpersonatePrivilege	Present Obtain an impersonation token for another user in the same session.

Figure 3.24 - Process Privileges for FileTour 2nd stage payload.

3.4.5 Utilising Yara for Signature Scanning

As mentioned in **Section 3.3.3 Use of Obtained Data**, the analyst used the obtained information to create Yara rules (VirusTotal, 2013) that detected the analysed samples using distinctive strings from the malware and could successfully identify each malicious software (**Figure 3.25** and **Figure 3.26**). The signature scanning rules can be found in **Appendix C**.

```
/*
NotPetya Yara Rule
Author: Martin Georgiev
Date: 27/11/22
Reference: Georgiev, M. (2022). Analysis and Comparison of WannaCry and NotPetya. [online] Github.
Available at: https://github.com/Kvdickt/Analysis\_and\_Comparison\_of\_WannaCry\_and\_NotPetya/commit/8ff0172ef1077dc6035d54375cd4e4d4de8dbf4
[Accessed 29 Nov. 2022].
*/

rule NotPetya_Wiper {
  meta:
    description = "Yara rule for detecting NotPetya wiper sample from 2017"
    author = "Martin Georgiev"
    university = "Abertay University"
    degree = "BSc Hons Ethical Hacking"
    date = "27/11/22"
    md5 = "db345b97c37d23f5eald184e3c89eb4"
    sha256 = "24d004a104d4d54034dbcfcc2a4b19a11f39008a575aa614ea04703480b1022c"

  strings:
    $s1 = "Oops, your important files are encrypted." fullword wide ascii
    $s2 = "Send your Bitcoin wallet ID and personal installation key to e-mail " fullword wide
    $s3 = "process call create \\C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\$s\\\" $1 " fullword wide // creates a process call to execute itself with rundll32.exe
    $s4 = "-d C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\$s\\\",$1 " fullword wide // runs itself with rundll32.exe on newly infected machines
    $s5 = "fsutil usn deletejournal /D %c:" fullword wide // deletes USN journal (changes on drive C)
    $s6 = "wevtutil cl Setup & wevtutil cl System" ascii //clears Setup and System logs
    $s7 = "allhost.dat" fullword wide //psnec.exe execution for local network propagation
    $s8 = "$s /node:\\$s\" /user:\\$s\" /password:\\$s\" " fullword wide //remote execution with wmic.exe
    $s9 = "schtasks $s/Create /SC once /TN \"\" /TR \"\\$s\" /ST %02d:%02d\" fullword wide //schedule system reboot at noon
    $s10 = "uts \\$s -accepteula -s " fullword wide // automatically accepts EULA upon execution to remain hidden

  condition:
    uint16(0) == 0x5a4d and filesize < 1000KB and (1 of ($s*) or any of them) // Check first byte (DOS executable), if under 1000KB and has 1 or any of $s
}
```

Figure 3.24 - NotPetya Yara Rule.

```
FLARE Tue 11/29/2022 5:11:16.22
C:\Users\IEUser\Desktop\Malware_Samples\NotPetya>ls
DLLLoader32_C17B.exe      Ransomware.NotPetya.dat.zip
NotPetya.yara             output.txt
Ransomware.NotPetya.dat   perfc.dll

FLARE Tue 11/29/2022 5:11:18.03
C:\Users\IEUser\Desktop\Malware_Samples\NotPetya>yara32 NotPetya.yara .
NotPetya_Wiper .\Ransomware.NotPetya.dat
NotPetya_Wiper .\perfc.dll

FLARE Tue 11/29/2022 5:11:22.51
C:\Users\IEUser\Desktop\Malware_Samples\NotPetya>
```

Figure 3.25 - NotPetya Yara Rule Test.

3.5 IRP Module Creation

The researcher used the obtained information and the generic Incident Response Plan (IRP) to create four response process modules tailored to each malware (**Figure 3.26**). The modules covered incident identification, severity analysis, containment, eradication, and recovery. The containment phase suggested measures like temporary infrastructure changes, stopping services, stopping the connection, or contacting specialised personnel depending on the complexity of the infection. The eradication

phase discussed decryption with third-party businesses, countering malware capabilities, checking for adversaries, and contacting law enforcement if necessary. Post-infection recovery actions included restarting services, monitoring network performance, restoring access, and requesting legal support based on the affected infrastructure and assets of the company.

1.4.3 Severity Guidance

It is important to conduct an initial triage to obtain more information about the malware and its artefacts. This includes a few subcategories – delivery, execution, and symptoms.

As previously mentioned, the malicious software's main means of propagation are through social engineering and phishing techniques – email attachments, disguised as popular freeware or pirated software. If it is delivered after an adversary obtains access to a machine, they may upload it and execute it as administrator privileges are not required. Some strains have built-in capabilities to escalate their privileges and obtain full access to the machine's resources – files, security logs, and tokens. It could also impersonate all users in the same session and any clients which connect to the machine. All evidence (IDS/IPS logs, emails, unexpected connections, memory forensics, files, and system changes) must be thoroughly documented as it can be used to identify the exact capabilities of the sample, how it ended on the system, as well as how it behaves (connections to any C&C servers, cryptographic functionalities, specific data theft, etc.)

As the FileTour samples and strains are broad, the team must look for the following (but not extensive) known SHA256 hashes:

- ab5e597bf7316bd8fcaeca8cddeec38a9585704a7929d50ea92ba603b038d7f3
- ff2fba623a5fef5ad2ab852079c88fbc33d12e48cfb0a06c90390d4a19270d2c
- e6dff8475541ebddc1f0db47a311eb2c25581b7d5e62af8066d59c283114c2d3
- 8fe6c86b038ce91a991fe6eb8a9b323bb37b554ff6b4e5c18de3fe52d4aedf6d
- aa3c8a767a538de40293e531aba50c4cfa189510927a22d028f3e34f2997bf95
- da6332feebc2a530509de0c661231bbd427327c31d6607a6a9286db710b68795
- 9c9cdb438163a2e64adcb398a6f1f1abdc81c1cf35ab5728441104a151240fd
- 4f4c2c9bdfef8a8cfbe2c8f84bf12cc86f26f59d54c277dab39f4c5e92948708
- 9453ddc4bebb87a937e3d53d38c56814907b2862496142ccdb568f48caf2d467
- 9c83561fb5253478d523e0ca20900b7e0ce87e60f686bfea25c9ca99716257c2
- 719838a1192ae6b53966159da56635e7a05754eb017f2538ca3f82c580543280
- d2d90f02ccd7c3fd1b46d667081529a1af8172e4a51feda461c8d250081c3548
- b3af0eb6e6ddce0f2e2993634d4b3edd86b3584c0c6f600c5f94379f491698d

Other samples can be found in various forums such as Malware Bazaar. Regarding the execution, as previously said, some strains do not require administrator rights. Some symptoms may not be obvious as the samples try to remain hidden and evade any sort of detection by using self-modifying code and silent scripts to install the payloads.

Figure 3.26 - Severity Guidance Section for the FileTour Module.

3.6 Questionnaire Development

Due to the nature of the project, the researcher could not test the project's potential success and reliability in real-life scenarios. The analyst developed a questionnaire in Google Forms aimed at industry professionals (**Figure 3.27**). It aimed to prove the project's efficiency or identify any underlying problems to mitigate in future work. All participants worked in the DFIR (Digital Forensics and Incident Response) and law enforcement, making their responses a valuable and significant contribution to the project's success.

Methodology

In addition to the incident response plans, the project has developed a robust malware analysis and forensics methodology that is both simple and effective. This methodology is designed to be easy to follow for SME executives who may not have extensive technical expertise in the field.

With its clear documentation and numerous examples, this methodology enables executives to analyse unknown malware samples during a cyber incident. Executives can utilise the obtained information to select an existing attack-specific module to address the incident or create their own. They can also provide the data to law enforcement or third-party incident response companies if they choose to do so. Furthermore, the methodology will also guide them in creating Yara rules and using them to scan suspicious files. To provide a comprehensive framework for this methodology, it will consist of the following sections:

1. Test Environment Setup (FlareVM and Remnux within a host-only network for communication)
2. Static Analysis - String (Floss) and in-depth (PEStudio - hashes, blacklisted functions/libraries, malicious indicators, etc.) analysis and packer identification (ExeInfoPE)
3. Dynamic Analysis and Digital Forensics - detonation symptoms, host-based forensics (procmon - file manipulation, processes, registry manipulation, evasion and persistence mechanisms), network-based forensics (TCPView, Wireshark and Inetsim for Internet/DHCP server simulation), and RAM forensics (WinPMem and Volatility 3.0)
4. Yara rule creation - identifying malware-specific signatures and using them to scan unknown files.

3. What is your opinion on the methodology? Would users with little experience be able to follow it? Would it be hard to keep it updated with the rapid development of malware? Could it be further simplified?

Your answer

4. Do you think the methodology could lead to issues? (i.e. causing additional damage if the user does not accurately follow it)

Your answer

Figure 3.27 - Methodology Section of the Questionnaire.

The researcher split the questionnaire into three separate sections. The first section aimed to familiarise the responder with the project and the response modules. The second section covered the malware analysis methodology and asked for their opinion and issues (inability to follow the analysis methodology, etc.) The final segment served as a conclusion and aimed to acquire the participants' insight – Would it raise awareness? Could it be beneficial? Would it be successful in real-life incidents?

To ensure that the participants could accurately analyse and understand the plans and malware analysis methodology, the researcher provided samples of the analysis documentation, a Yara rule, the generic IRP and a module for the malware covered in the analysis. The questionnaire was carried out in Google Forms, removing any

question restrictions, and allowing the participants to withdraw or omit any questions they would not like to answer. All responses were also anonymised unless the participant specified otherwise. The researcher handled the questionnaire results under the 1998 Data Protection law to mitigate possible ethical issues. The results of the questionnaire can be found in **Section 4.4 Questionnaire Results**.

3.7 Methodology Summary

In summary, the methodology section provided comprehensive coverage of the development process for the study's artefacts. To effectively convey the numerous details, each phase was covered separately. The methodology commenced with the generalised incident response plans, detailing their sections and accessibility considerations. It was then followed by the attack analysis methodology, which covered the tools, samples, types of analysis, and extracted intelligence utilisation. Finally, the section delved into the creation of attack-specific IRP modules based on information obtained from the malware analysis and the questionnaire, which aimed to demonstrate the project's benefits, accessibility, and effectiveness in real-life cyber incident response.

4 Results

4.1 Results Introduction

The results section of the project contains the data collected during the development stages, which were analysed to evaluate the methodology and response modules' efficiency. It was a crucial part of the project as it provides insight into the success of the project after its development and implementation.

4.2 Malware Analysis Methodology

By utilising the malware analysis methodology (**Figure 4.1**), the analyst successfully analysed the samples. Thanks to its simplicity, the analysis process was not convoluted. The analysis of each malware sample showed its behaviour within the local system and the network. The methodology aided with the identification of each sample's capabilities and distinctive features. The analysis results were presented in four separate reports, each covering one malware sample in detail. The reports covered the entire analysis process, including background, static and dynamic analysis, results, discussion, and countermeasures. Any evidence of malicious activity was filtered and compiled within multiple abstracts.

2.3.3 Network-Level Analysis

Network-Level analysis can show if malware attempts to access other machines. This could mean downloading multi-stage payloads, attempting to move to other uninfected machines or accessing links to send/receive data.

Analysts will need both machines to monitor the network. FlareVM will be used to detonate the malware, while Remnux will keep track of the activity. Open a terminal window with Ctrl+Alt+T and run Inetsim by typing Inetsim. Open a second tab from the + sign in the top left corner and type wireshark (Wireshark, 1997 – Present Day) to open the packet sniffer. It will then open a new window for the application. Click on the blue shark fin (top left) to start recording the network traffic. (**Figure 2.3.17**)

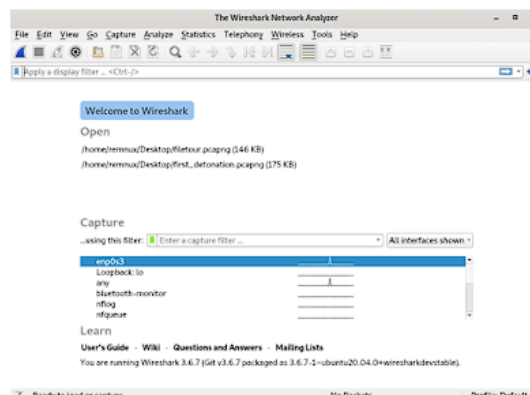



Figure 2.3.17 – Wireshark.

Figure 4.1 - Methodology Documentation

The researcher then employed the obtained evidence in creating incident response modules and Yara rules for signature scanning. The Yara rules were created using distinctive strings from the analysed samples and could successfully identify the malicious files. Using the rules with **yara32** displayed the name of the malicious files if their signatures matched the conditions. More about each analysis report can be found in **Appendix D**.

4.3 Incident Response Plan and Modules

The initial incident response plan provided a generalised approach for cybersecurity incident response. The response plan provided organisations with a broad set of actions, allowing them to identify the root cause of the attack and choose appropriate mitigation strategies. While this approach might not be as efficient in dealing with known attacks, it remains an essential component of a company's security posture and could help respond to unknown threats. **(Figure 4.2)**



School of Design and Informatics
BSc Ethical Hacking, 2022/23

An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses

Cyber Incident Response Plan
Version: 1.0

Author: Martin Georgiev

Supervisor: Natalie Coull
Head of Division of Cybersecurity Abertay

Note that the information contained in this document is for educational purposes.

VERSION CONTROL

Version No	Updated By	Reason for Update/Area Updated	Date Updated
vXX	<Group Name>	<Brief update description>	<Date of Update>

APPROVAL RECORD

Version No	Approval Body	Date of Approval	Date of Review	Effective Date
vXX	<Organisation Name>	<Date>	<Date>	<Date of Operation>
vXX	<Department Name>			

DISTRIBUTION LIST

Department Names	Personnel Positions
<Name of departments provided with the plan>	<Name of separate positions provided with the plan>

Figure 4.2 - First Two Pages of Base IRP.

After analysing each malware sample, the analyst created response modules based on the gathered data and evidence tailored to the specific capabilities of each malware.

These modules were modified versions of the response process outlined in the general IRP plan, covering the entire incident response process, including identification, analysis, containment, and eradication of the incident.

To make the technical data more accessible, the researcher provided detailed examples and comprehensive sets of actions for each section of the response modules. The researcher also acknowledged that the suggested course of action outlined in the modules might vary depending on the specific incident scenario and the organisation's infrastructure, thus making it adaptable to suit the company's requirements. Moreover, the modules recognised that some malware samples might be too sophisticated for organisations to handle, even if the company has a specialised Cyber Incident Response Team (CIRT) and advised involving law enforcement if necessary. **(Figure 4.3)** More about the response modules and the generalised plan can be found in **Appendix E** and **Appendix F**.

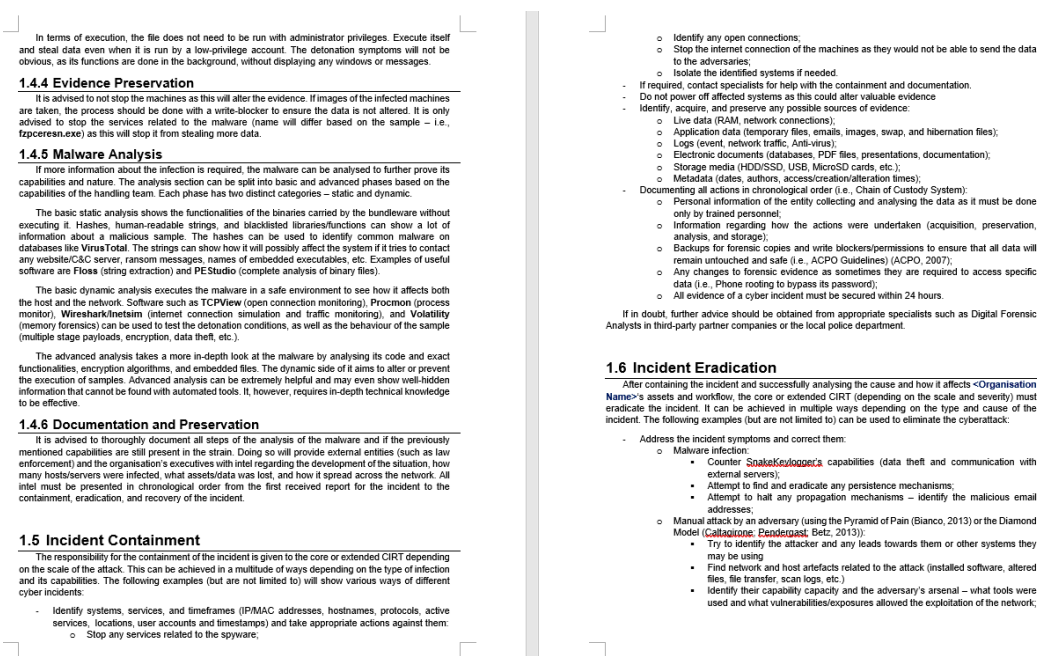


Figure 4.3 - Part of SnakeKeylogger's Module.

4.4 Questionnaire Results

Although the questionnaire received a limited number of responses, the feedback provided valuable insights into the project's potential success in real-life scenarios.

Unfortunately, only one participant completed the survey, a higher-up in the cybersecurity department of a law enforcement organisation.

While the low number of responses was a concern, the perspective of this respondent offered valuable insights into the practical applications of the project. Future research could benefit from a broader and more diverse sample of respondents to provide a more comprehensive understanding of the project's potential impact on incident response.

As mentioned in **Section 3.6 Questionnaire Development**, the core of the survey was in sections two and three. In the second section of the survey, participants were asked about their thoughts on the MA and DF methodology, including its complexity and ability to handle newer malware variants. The respondent expressed concerns that the procedure may be too difficult for users without prior IT knowledge or experience whilst being challenging to maintain for modern, more dynamic malware due to their complex behaviour and capabilities.

After being asked about the potential consequences of not accurately following the methodology, the participant noted that issues could arise. However, they also emphasised that these problems could be mitigated with appropriate support and education for users/executives.

The third section of the survey asked participants for their overall opinion of the project, including its potential for raising security awareness, benefits for the industry, and the likelihood of success. When asked about the project's impact on security awareness, the respondent expressed uncertainty about its effectiveness in helping SME owners understand the importance of adequate security for their businesses and users. As such, the project would require changes to raise awareness among executives.

However, the participant was generally positive about the project's benefits, indicating that the modular plans would appeal to SME executives and security service providers hired by SMEs. Additionally, they expressed that the project should target

said providers rather than regular companies. These modular plans could aid in providing efficient responses during incidents.

Concerning the project's potential for success in real-life incident scenarios, the respondent emphasised the importance of employing and supervising trained cybersecurity professionals. With the right expertise and oversight, the project could successfully mitigate and respond to cyber security incidents for SMEs. The **GPDR Data Sign-Off Form** can be found in **Appendix G**.

4.5 Results Summary

Following the methodology, the researcher developed and prototyped four artefacts:

- Generalised IRP.
- Cyber-attack analysis methodology.
- Signature scanning rules and attack-specific modules based on the results of the analysed malware samples.

Since it was not possible to test the project in real-life environments, the questionnaire results played a vital role in assessing the project's potential success and identifying issues that could arise in real-life scenarios. Despite the low number of responses and the identified accessibility problems, the respondent provided positive feedback regarding the project's potential benefits to SME security. The researcher then assessed the artefacts and questionnaire results against the initial aims and objectives, research questions, and literature review findings presented in **Section 2 Literature Review**. The critical evaluation can be found in **Section 5 Discussion**.

5 Discussion

5.1 Discussion Introduction

In this chapter, the researcher critically evaluated and discussed the literature review and the project's practical results, focusing on how they have helped achieve its objectives (aims and research questions). The section covered the assessment of the proposed response modules and analysis methodology, making it crucial for the effectiveness of real-life incident mitigation. The analyst also compared the developed solution to existing incident response methodologies, highlighting their respective advantages, disadvantages, and capabilities. Lastly, this section considered the need for more accessible incident response for smaller businesses, including future work and improvements based on the development data and insights from questionnaire participants.

5.2 Existing Research Data

The initial objective of this research was to analyse various incident response plans and attack analysis methodologies and evaluate their effectiveness and accessibility for Small and medium-sized enterprises. The goal was achieved through a comprehensive review of the existing research and security trends, including an in-depth analysis of cyber-attacks, incident response and the appropriate analytical frameworks (malware analysis and digital forensics).

The literature review's results on cyber-attacks and incident response were concerning, indicating a consistent increase in cyber incidents annually, while small and medium-sized enterprise (SME) owners were not sufficiently taking steps to mitigate potential threats. As mentioned in **Section 2.2.2 Significance of Incident Response**, in 2022 only 18% of UK-based SMEs had a formal cyber incident response plan, and merely 22% had a response strategy, leaving organisations vulnerable to modern malware. Such lack of preparedness could be attributed to the limited accessibility of cyber incident response plans and analysis methodologies. While such plans could be an effective means of defence preparation, they were often too broad and required technical expertise to implement effectively in incident response, making them difficult for SMEs to utilise. Additionally, their generic nature could be damaging, as they did not

address specific types of attacks or advanced malware (disguised as different types or with multiple unknown capabilities) and lack of experience could misidentify how it was affecting the system. Moreover, these plans were primarily developed for large corporations with internal cyber incident response teams, making them impractical for SMEs to adopt.

In terms of analysis methodologies, the research highlighted three key areas: malware analysis, digital forensics, and signature scanning. These approaches have shown promise in mitigating and investigating malware samples and cyber-attacks; however, their successful implementation would require substantial IT expertise, making them inaccessible to staff with limited knowledge. Consequently, SMEs face challenges in independently identifying and responding to cyber intrusions based on the nature of the attack.

The researcher could then refer to the first research question – „**What are the differences between generic incident response plans and their modular variants?**“. Generic plans could offer comprehensive security to companies with well-trained security personnel by providing a broader step-by-step guide for incident response. Alternatively, modular variants could include specific actions to limit or entirely prevent damage caused by distinct malware samples. Each module would be designed based on analysed malicious software samples (in combination with the analysis methodology), comprising a straightforward yet comprehensive response for identifying, containing, eradicating, and recovering from the incident. Such design would make them a more accessible alternative for SMEs, contrary to cyber incident playbooks.

Based on the collected data, the researcher successfully achieved the first objective and proceeded to develop a more accessible, generalised Cyber Incident Response Plan (CIRP) (**Section 5.3 CIRP Development**), response modules to enhance efficiency for specific attacks while remaining accessible (**Section 5.3.2 CIRP Module Development**), and an attack analysis methodology that was more user-friendly (**Section 5.5 Methodology Development**).

5.3 CIRP Development

5.3.1 Generalised Incident Response Plan

In the first part of the development process, the researcher focused on creating a more accessible and generalised cyber incident response plan. As complete accessibility would be difficult to achieve, the plans were created in a manner that could guide users with some experience, while attempting to explain the situation and provide advice to users with limited knowledge on what external entities should be contacted for aid.

To address the advantages and disadvantages identified in the literature review, the researcher examined three response plans templates by governmental and private organisations: the **Scottish Government**, **CM Alliance**, and **Microsoft/Ey/Edelman** CIRPs. The first plan offered a thorough and detailed approach to cyber incident mitigation, but its broad scope assumed prior knowledge of cybersecurity, making it less accessible to some users. Conversely, the second and third plans were too vague, offering only a general overview of the response process. Although these plans may be effective for incident response teams with significant cybersecurity expertise, they may be challenging for SMEs to utilise while potentially discouraging some due to the high usage of technical terminology.

The developed generic plan combined the strengths of the previously mentioned cyber incident response plans to create a more concise and user-friendly template. The broad and thorough explanations of the Scottish Government's plan were preserved, with some sections being omitted or altered/combined to make it easier to navigate. As mentioned in **Section 3.2 Generalised Cyber Incident Response Plan**, the template was split into 5 main sections, covering various parts of the CIRT integration within the organisation and the response process:

- **Introduction** – Establishing the goal and scope of the template.
- **Roles** – Various roles for handling different parts of the response process.
- **Communications** – Who and when should be contacted?
- **Response Process** – A general response process for a cyber incident.

- **Reporting and Awareness** – How to report, learn from the incident and raise awareness among the staff.

SME owners could alter or omit any section to suit the infrastructure of their company. Any parts of the Scottish CIRP that focused on the UK's jurisdiction were generalised, allowing companies from various countries to easily employ the response plan within their organisations. The roles, communication and reporting sections remained flexible, allowing companies to effortlessly adapt them for bigger or smaller CIRTs.

5.3.2 Attack-specific Modules

The incident response modules drew inspiration from the technical approach of the last two templates. The researcher created them based on the analysis of four malware from different categories. As a result, the researcher achieved the fourth objective of the study, which involved analysing different samples to determine the appropriate IRP modules.

The response modules were created from the **Response Process** section of the generic plan by altering the data to better fit the malicious software's capabilities. Each sample aimed to provide an in-depth response process for the specific malware. All created modules had the following sections:

- **Preparation** – Pre-infection actions.
- **Identification** – Infection source.
- **Reporting** – Severity, damage, and scale.
- **Analysis** – Sample hash values and analysis guide.
- **Containment, Eradication, and Recovery** – Peri- and post-infection actions.

Considering that most modern malware attacks involve social engineering and phishing attempts, the preparation section in all modules remained nearly identical, covering pre-infection countermeasures, awareness, and contact suggestions, including law enforcement and third-party cybersecurity services.

The Identification section was revised to include detailed descriptions of potential sources of infection for each specific malware, making the terminology more accessible. The Reporting section provided guidance on contacting relevant entities and

organisations based on the severity and damage caused by the infection. It was particularly important for SMEs who may require external assistance to counter highly sophisticated modern malware. By identifying the scale of the attack and its potential consequences for external entities, their users, or their country of residence, SMEs could use the modules to take appropriate action to mitigate the impact.

The Analysis section remained broad as users are expected to combine it with the developed methodology document, which will be discussed in **Section 5.4 Methodology Development**. The section would only be required if an unknown malware was identified, or a detailed report was required. It outlined the severity of the infection, the malware hashes, and instructions on how to preserve evidence and analyse the sample safely. The final three sections covered the peri- and post-infection phases, presenting a clear set of actions that users should employ to counter the malware.

With the completion of the modular plan and the attack-specific modules, the researcher successfully met the second objective of the project. The researcher could also refer to two other research questions:

- **How can modular IRPs optimise response time and efficiency?**
- **What advantages do modules for separate malicious software provide in terms of response performance.**

Combining the developed artefacts with the responses from the questionnaire, the researcher discovered that modular plans could improve the cyber incident response process. The specific actions provided in each module would allow SMEs and third-party cybersecurity providers to rapidly respond to a cyber-attack, adapting the operation as needed to suit the infrastructure of the affected organisation. This would result in a more efficient and effective response, potentially reducing the damage caused and expediting the restoration of regular business operations.

5.4 Methodology Development

To develop the attack analysis methodology, the researcher thoroughly analysed the three key areas (MA, DF, and signature scanning) identified in the literature review

to determine their most important aspects in a cyber incident scenario. This step was crucial in ensuring the methodology's simplicity and effectiveness. The researcher focused on basic static and dynamic analysis, which allowed users to extract a wealth of data from malware without the need for complex techniques. The resulting methodology document was organised into four main sections: testing environment creation, static analysis, dynamic analysis, and signature scanning.

The initial section of the methodology introduced users to the testing environment and provided a comprehensive guide on setting up the virtual machine and local network. The following section covered static analysis, utilising various tools, and providing a step-by-step guide on how to extract file hashes and strings using **Floss/strings**, as well as conducting an in-depth investigation with **PEStudio/ExeInfoPE**. Given that analysing extracted strings could be challenging for those with limited knowledge, the methodology recommended reviewing the malicious indicators provided by PEStudio and the results obtained from **VirusTotal** after performing a file hash lookup.

The third section of the methodology focused on dynamic analysis, providing users with a step-by-step guide on how to analyse the malware's behaviour after detonation. Additionally, the section included clear examples of the capabilities of specific types of malware to help users effortlessly identify malicious software. It also covered network and local-level analysis, guiding users through identifying possible propagation or communication with C&C servers, utilising tools such as **TCPView**, **Wireshark**, and **Inetsim**. For the local-level analysis, a process examination with **procmon** was suggested, including information on process trees and process filtering. As filtering was essential to classify the malicious software's capabilities, the methodology provided a table with detailed explanations, suggestions, and examples. The final part of the dynamic analysis involved **RAM** forensics using **Volatility 3.0**. The methodology guided users on obtaining a data dump and analysing it with various Volatility plugins. This step was crucial in identifying malware activity that might not be present in static or network analysis, such as hidden processes or injected code.

The methodology also covered signature scanning using Yara, explaining its usage and the structure of rules and syntax. This section aimed to highlight the significance of signature scanning in cybersecurity and guide users on creating rules using the extracted strings from analysed malware samples. The researcher successfully answered the final research question ("**How can signature scanning combined with modular IRPs affect cyber incident mitigation?**") by incorporating Yara into the malware sample analysis and creating a signature scanning section within the attack analysis methodology. With the help of effective Yara rules, the malware type could be swiftly identified, enabling incident responders to select the appropriate IRP module and interfere with the malicious software's capabilities.

Completing the attack analysis methodology allowed the researcher to successfully achieve the final two objectives of the study, which were to prototype a simple MA and DF methodology and create Yara rules for the analysed malware.

5.5 Limitations

To efficiently assess the accessibility of the modular plans and the methodology, they both had to be provided to several SME executives and test them in fictional incident exercises or actual incidents. As this was not possible, the researcher took a different approach by creating a questionnaire for experienced industry professionals.

As distinguished in **Section 4.4 Questionnaire Results**, the survey yielded limited responses, making it partially successful. Nonetheless, the questionnaire exposed critical issues that need to be addressed. Doing so would enhance the project's accessibility to individuals with limited knowledge. The development process, viewed through the lens of a cybersecurity researcher, made it challenging to identify the aspects of the cyber-attack analysis methodology that could be complicated for inexperienced personnel. According to the results, the current attack analysis methodology remained difficult for staff lacking previous IT experience. **Section 6.2 Future Work** covers potential solutions to this problem.

Although the methodology may have posed some accessibility challenges for personnel without IT backgrounds, the respondent acknowledged the project's potential to enhance the response process. As it stands, the project could cater to security

service providers by utilising the methodology to train new security analysts. Following malware identification, the providers could employ separate attack modules and receive a detailed action plan for swift response, thereby minimising damage to SMEs and reducing the risk of serious adverse outcomes. With the successfully achieved objectives, the project has effectively evaluated and prototyped incident response modules for incident mitigation.

5.6 Discussion Summary

In conclusion, the project results provided a positive insight into the potential success of the developed artefacts, having evaluated the methodology and results, and successfully achieving the outlined objectives. Although the current IRP modules and attack analysis methodology may be challenging for staff without prior IT knowledge and experience, the questionnaire respondent acknowledged the project's potential in real-life incident response scenarios. Furthermore, this section identified the primary obstacles to the methodology's lack of accessibility. Possible modifications to mitigate the accessibility issues within the modules and methodology will be discussed further in **Section 6.1 Conclusion** and **Section 6.2 Future Work**.

6 Conclusion

6.1 Conclusion

The primary objective of the honours project was to create and assess a more efficient incident response approach for small and medium-sized enterprises. To achieve this, the researcher conducted a comprehensive analysis of technical and academic literature to identify the shortcomings of current incident response plans and attack analysis methods. After conducting the research, three key issues were identified - accessibility, potential problems with disguised malware, and design. Based on these findings, the researcher developed and prototyped a modular approach to incident response plans and an attack analysis methodology suitable for large corporations and SMEs. By using this modular approach, businesses could more effectively address the identified issues in incident response planning. Additionally, the attack analysis methodology would provide a means to identify and mitigate the effects of disguised malware.

The response modules, which were derived from the examination of multiple malware samples using the analysis methodology, were designed to target the specific capabilities of the malware. Such modular plans would enable businesses or third-party security providers to mitigate the incident while reducing the likelihood of negative outcomes swiftly and effectively. By altering the response section of a generalised plan, tailored modules could be created for each specific malware, making the incident response process more efficient and effective. Overall, the approach was designed to be flexible and adaptable, allowing businesses of all sizes to respond to and mitigate future cyber incidents more efficiently.

In addition to the response modules and attack analysis methodology, the researcher created a questionnaire for incident response and digital forensics professionals. Although the survey received feedback from a single respondent, it provided valuable initial insight into the primary issue of the developed prototype: unsatisfactory accessibility.

As the artefacts were developed from a cybersecurity researcher's perspective, it was challenging to identify what could be too technical for non-IT personnel without surveying staff or testing the artefacts in real-life scenarios. Despite this, the questionnaire respondent had a positive view of the project's potential success in legitimate cases of cyber incident response. Currently, the project may not be reasonable for staff and executives without prior IT knowledge. However, third-party cybersecurity providers could use it to provide a faster and more efficient incident response service.

In conclusion, the overall project successfully met the aims and answered the research questions in **Section 1.2 Aims and Research Questions**. While the findings from the questionnaire identified potential flaws within the developed artefacts, it highlighted the need for further consideration in the incident response plan and tools development to ensure they were accessible and usable for a broader range of users. Future research could explore ways to address these issues, such as conducting usability testing with non-IT personnel or incorporating user-centred design principles into the development process. By doing so, incident response plans and tools could become more user-friendly and effective for all users, regardless of their technical expertise.

6.2 Future Work

As identified in the previous section, the developed artefacts had flaws in terms of accessibility and would require further research to make them available to a broader range of users. Given more time, the researcher could improve the response modules and attack analysis methodology by:

- Testing them in a real-life incident environment.
- Surveying non-IT personnel.
- Developing a centralised platform for the response modules.
- Creating an automated version of the analysis methodology.

Testing the artefacts in a real-life environment, be it an actual incident or test scenarios, and obtaining feedback from non-technical personnel would reveal the areas people may find challenging. Gathering a broad range of survey responses and testing

results would uncover the most ambiguous sections of the modular IRP and attack analysis methodology, enabling the researcher to make necessary modifications based on the outcome.

In addition, a centralised platform for the response modules could significantly improve the accessibility of the project. The researcher would make the platform into a web application designed to store modules for different malware and provide advice from cybersecurity professionals. Such a platform would allow staff and executives to search for specific response modules based on the type of infection.

The platform would also permit users to upload modules they have personally created. Cybersecurity professionals would then verify the modules before they become open to the public. Furthermore, the researcher could attempt to develop an automated sandbox version of the analysis methodology, which could be implemented into the web application. While similar tools already exist, they may be too expensive or require subscriptions that smaller businesses could not afford. The developed sandbox would allow users to upload malicious samples, automatically analyse them, and generate a sample report or response module that users could modify based on their needs.

In summary, thorough testing, a centralised platform, and an automated sandbox version of the analysis methodology could significantly improve the accessibility and effectiveness of the project, enabling a broader range of users to benefit from the developed incident response plan and attack analysis methodology.

7 References

Sudhakar and Kumar, S. (2020). *An emerging threat Fileless malware: a survey and research challenges*. Cybersecurity, 3(1). doi:<https://doi.org/10.1186/s42400-019-0043-x/> (Accessed: 11 October 2022).

CheckPoint (2022). *Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed*. Available at: <https://pages.checkpoint.com/cyber-security-report-2022/> (Accessed: 12 October 2022).

ytisf (2014). *TheZoo*. Available at: <https://github.com/ytisf/theZoo/> (Accessed: 15 Oct. 2022).

Ivanov, A and Mamedov, O. (2017). *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*. Available at: <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/> (Accessed: 16 October 2022).

CM Alliance (2015 – Present Day). *Cyber Incident Response Plan Template*. Available at: <https://www.cm-alliance.com/cyber-incident-response-plan-template/> (Accessed: 29 October 2022).

VirusTotal (2004 – Present Day). *VirusTotal*. Available at: <https://www.virustotal.com/gui/home/upload/> (Accessed: 15 November 2022).

Scottish Government (2021). *Cyber resilience: incident management*. Available at: <https://www.gov.scot/publications/cyber-resilience-incident-management/> (Accessed: 15 November 2022).

Ballenthin, W. (2016). *Floss*. Available at: <https://github.com/mandiant/flare-floss/> (Accessed: 20 November 2022).

Russinovich, M. (2021). *Strings v2.54*. Available at: <https://learn.microsoft.com/en-us/sysinternals/downloads/strings> (Accessed: 20 November 2022).

ASL (2023). *ExeInfoPE*. Available at: <http://www.exeinfo.byethost18.com/?i=1/> (Accessed: 24 November 2022).

Hungenberg, T and Eckert, M. (2007). *INetSim*. Available at: <https://www.inetsim.org/> (Accessed: 27 November 2022).

Russinovich, M. (2022). *TCPView v4.17*. Available at: <https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview/> (Accessed: 27 November 2022).

Wireshark. (1997 - Present Day). *Wireshark Documentation*. Available at: <https://www.wireshark.org/docs/> (Accessed: 27 November 2022).

Russinovich, M. (2022). *Process Monitor v3.89*. Available at: <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon/> (Accessed: 28 November 2022).

Fox, N. (2021). *PeStudio Overview: Setup, Tutorial and Tips*. Available at: <https://www.varonis.com/blog/pestudio/> (Accessed: 28 November 2022).

Microsoft, Ey, and Edelman (2022). *Incident Response Reference Guide*. Available at: <https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf> (Accessed: 8 December 2022).

Baker, K. (2023). *The 12 Most Common Types of Malware*. Available at: <https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/> (Accessed: 12 December 2022).

Volatility Foundation (2020). *Volatility 3.0*. Available at: <https://www.volatilityfoundation.org/3/> (Accessed: 15 December 2022).

Cohen, M., et al. (2019). *WinPmem*. Available at: <https://github.com/Velocidex/WinPmem/> (Accessed: 15 December 2022).

ESET (2017). *Stantinko Teddy Bear Surfing Out of Sight*. Available at: <https://www.welivesecurity.com/wp-content/uploads/2017/07/Stantinko.pdf> (Accessed: 14 January 2023).

Cichonski, P (2012). *Computer Security Incident Handling Guide*. Available at: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final/> (Accessed: 20 January 2023).

Kral, P. (2012). *Incident Handler's Playbook*. Available at: <https://www.sans.org/white-papers/33901/> (Accessed: 20 January 2023).

Bisson, D. (2017). *NotPetya: Timeline of a Ransomware*. Available at: <https://www.tripwire.com/state-of-security/notpetya-timeline-of-a-ransomware/> (Accessed: 27 January 2023).

Stamus Labs (2022). *Threat Detection Update*. Available at: <https://www.stamus-networks.com/stamus-labs/detection-update-2022-05-31/> (Accessed: 8 February 2023).

Ashdown, D. (2021). *Jigsaw Ransomware Analyses*. Available at: <https://www.cyberdonald.com/post/jigsaw-ransomware-analyses/> (Accessed: 12 February 2023).

Thompson, E.C. (2018). *Cybersecurity Incident Response*. Berkeley, CA: Apress. doi:<https://doi.org/10.1007/978-1-4842-3870-7/> (Accessed: 15 February 2023).

Biener, C., Eling, M. and Wirfs, J.H. (2014). *Insurability of Cyber Risk: An Empirical Analysis*. The Geneva Papers on Risk and Insurance - Issues and Practice, 40(1), pp.131–158. doi:<https://doi.org/10.1057/gpp.2014.19/> (Accessed: 15 February 2023).

Romanosky, S. (2016). *Examining the costs and causes of cyber incidents*. Journal of Cybersecurity, 2(2), p.tyw001. doi:<https://doi.org/10.1093/cybsec/tyw001/> (Accessed: 16 February 2023).

Edwards, B., Hofmeyr, S. and Forrest, S. (2016). *Hype and heavy tails: A closer look at data breaches*. Journal of Cybersecurity, 2(1), pp.3–14. doi:<https://doi.org/10.1093/cybsec/tyw003/> (Accessed: 18 February 2023).

Onwubiko, C. and Ouazzane, K. (2020). *SOTER: A Playbook for Cybersecurity Incident Management*. IEEE Transactions on Engineering Management, pp.1–21. doi:<https://doi.org/10.1109/TEM.2020.2979832/> (Accessed: 18 February 2023).

Gandotra, E., Bansal, D. and Sofat, S. (2014). *Malware Analysis and Classification: A Survey*. Journal of Information Security, 05(02), pp.56–64. doi:<https://doi.org/10.4236/jis.2014.52006/> (Accessed: 20 February 2023).

Casey, E., Altheide, C. and Al, E. (2013). *Handbook of digital forensics and investigation*. pp.63-135. Amsterdam: Academic Press. Available at: <https://dl.acm.org/doi/abs/10.5555/1822831/> (Accessed: 21 February 2023).

Ucci, D., Aniello, L. and Baldoni, R. (2019). *Survey of machine learning techniques for malware analysis*. Computers & Security, 81, pp.123–147. doi:<https://doi.org/10.1016/j.cose.2018.11.001/> (Accessed: 23 February 2023).

Prosis, C. and Mandia, K. (2003). *Incident Response & Computer Forensics. 2nd Edition ed.* pp.4–32. Available at: <https://dl.acm.org/doi/abs/10.5555/1207603/> (Accessed: 27 February 2023).

Zhang, X. (2021). *Deep Dive into a Fresh Variant of Snake Keylogger Malware*. Available at: <https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware/> (Accessed: 4 March 2023).

Krebs, E. (2013). *Target Investigating Data Breach*. Available at: <https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/> (Accessed: 11 March 2023).

Department for Digital, Culture, Media & Sport, UK Gov. (2022). *Cyber Security Breaches Survey: 2022 - Micro and Small Businesses*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089586/Cyber_Security_Breaches_Survey_2022_Infographic-Micro_Small_business.pdf (Accessed: 15 March 2023).

AbuseCH (2020). *MalwareBazaar*. Available at: <https://bazaar.abuse.ch/> (Accessed: 24 March 2023).

Lapshin, A. (2016). *Any.run*. Available at: <https://any.run/> (Accessed: 26 March 2023).

VirusTotal (2013). *Yara - The pattern matching Swiss knife for malware researchers (and everyone else)*. Available at: <https://virustotal.github.io/yara/> (Accessed: 29 March 2023).

Google (2016). *Google Forms*. Available at: <https://docs.google.com> (Accessed: 11 April 2023).

8 Appendices

Appendix A – Extracted Malware Strings

Note: The appendix contains a partial version of the extracted strings. The full versions were replaced by screenshots of the most vital parts due to the sheer volume. Each text file with extracted strings can be found in the respective malware analysis folders of the submitted artefacts and the analysis reports.

Appendix A1 – FileTour Strings

```
SmartPDF Uninstall
@%04\Uninstall.exe
@%04\Uninstall.ini
https://smartpdf.org/
SmartPDF
SmartPDF
SmartPDF 10.32.0.64.2
https://smartpdf.org/
Software/SmartPDF
installed
@%04\SmartPDF.exe
@%04\9840432e051a6fa1192594db02b80a4c1fd73456.exe
@%04\lg.exe
@%04\LivelyScreenRecS3.0.exe
@%04\note866.exe
@%04\PBrowFile15.exe
@%04\stats.exe
@%04\Visit.url
@%04\Uninstall.exe
@%04\Visit.url
@%04\9840432e051a6fa1192594db02b80a4c1fd73456.exe
@%04\PBrowFile15.exe
@%04\lg.exe
@%04\LivelyScreenRecS3.0.exe
@%04\note866.exe
@%04\stats.exe
/Versysilent
@%04\SmartPDF.exe
Welcome to the SmartPDF Setup Wizard
This wizard will guide you through the installation of SmartPDF.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Setup will install SmartPDF in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
At least 4.28 Mb of free disk space is required.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Please wait while SmartPDF is being installed. The installation will take several minutes.
Completing the SmartPDF Setup Wizard
SmartPDF has been installed on your computer.
Click Finish to close this wizard.
For installing SmartPDF on disk %s insufficiently free place. Try to choose other disk.
License Agreement
Please review the license terms before installing SmartPDF.
Choose Install Location
Choose the folder in which to install SmartPDF.
Choose a Start Menu Folder for the SmartPDF shortcuts.
Select shortcuts
Select additional shortcuts.
Ready to Install
Please wait while SmartPDF is being installed.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install SmartPDF.
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.
Launch SmartPDF
View README
Browse...
Do not create shortcuts
```

Figure 1 - Part one of the extracted FileTour strings.

Destination folder:
 Start Menu Folder:
 Additional shortcuts:
 Are you sure you want to quit SmartPDF?
 Setup needs the next disk
 Please insert disk %s and click OK.
 If the files on this disk can be found in a folder other than the one displayed below, enter the correct path or click Browse.
 Select the folder to install SmartPDF in:
 Select any additional shortcuts for SmartPDF that you would like created by the installation:
 Extracting files...
 This program must be run on
 Enter the password
 This setup is password protected.
 A password is required to begin the installation of SmartPDF. Type the password and then click "Next".
 If you do not know the password then click "Cancel" to cancel the installation.
 Installation password
 Execute the commands...
 Registering:
 Install SmartPDF is breaking.
 Creating INI entries...
 Installing
 Setup is now ready to begin installing SmartPDF on your computer.
 SmartPDF will be uninstalled from the following folder. Click Uninstall to start the uninstallation.
 Uninstall
 Uninstalling from:
 Yes, restart the computer now
 No, I will restart the computer later
 Uninstall SmartPDF
 Remove SmartPDF from your computer.
 Completed
 Uninstallation Complete
 Uninstall was completed successfully.
 Delete File:
 Please wait while each of the following components is removed...
 Remove Directory:
 SmartPDF was successfully removed. Click Finish to close this wizard.
 You really want to break removing SmartPDF?
 Unregistering:
 Setup has finished installing SmartPDF on your computer.
 To complete the installation, Setup must restart your computer. Would you like to restart now?
 Creating directories...
 Visit product uninstall web page
 Please read following information.
 Setup has finished installing SmartPDF on your computer.
 Visit product web site
 You must be logged in as an administrator when installing this program.
 This setup requires the .NET Framework version . Please install the .NET Framework and run this setup again.
 The .NET Framework cab be obtained from the web. Would you like to do this now?
 File already exists:
 Existing file:
 New file:
 Overwrite
 Overwrite all
 Skip all
 An error occurred while trying to copy a file:
 Click Retry to try again, Ignore to proceed anyway, or Abort to cancel installation.

Figure 2 – Part two of the extracted FileTour strings.

Appendix A2 – Jigsaw Strings

Congratulations. Your software has been registered. Confirmation code 994759
Email us this code in the chat to active your software. It can take up to 48 hours.
Thank you
Drpbx\drpbx.exe
Frfx\firefox.exe
System32Work\
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.
Thank you
Please, send \$
worth of Bitcoin here:
FormBackground
dataGridViewEncryptedFiles
ColumnDeleted
ColumnPath
FormEncryptedFiles
EncryptedFiles
Address.txt
You are about to make a very bad decision. Are you sure about it?
Great job, I'm decrypting your files...
Decrypting your files. It will take for a while. After done I will close and completely remove myself from your computer.
Great job
You did not sent me enough! Try again!
You haven't made payment yet! Try again!
Are you connected to the internet? Try again!
files will be deleted
Lucida Console
labelWelcome
I want to play a game
labelTask
All you have to do...
textBoxAddress
12Xspzstah37626slkwKhsKSHA
buttonCheckPayment
I made a payment, now give me back my files!
buttonViewEncryptedFiles
View encrypted files
Lucida Sans Unicode
labelCountDown
labelFilesToDelete
1 file will be deleted.
FormGame
Main.Properties.Resources
ExtensionsToEncrypt

Figure 1 – Extracted payload names and ransom message in Jigsaw.

Appendix A3 – NotPetya Strings

```
0123456789abcdef
Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
CHKDSK is repairing sector
Please reboot your computer!
Decrypting sector
Oops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.
We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:
If you already purchased your key, please enter it below.
Incorrect key! Please try again.
nt_c>8ubN
```

Figure 1 – Fake disk repair message in NotPetya.

```
FLOSS static Unicode strings
#+3;CScs
    Your personal installation key:
wowsmith123456@posteo.net.
2.    Send your Bitcoin wallet ID and personal installation key to e-mail
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
Oops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because
they have been encrypted. Perhaps you are busy looking for a way to recover
your files, but don't waste your time. Nobody can recover your files without
our decryption service.
We guarantee that you can recover all your files safely and easily.
All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1.    Send $300 worth of Bitcoin to following address:
MIIBCKCAQEAxP/VqKc0yLe9JhVqFMQGWUIT06WpXWnKSNQAYT0065Cr8PjIQInTeHkXEjf02n2JmURWV/uHB0Zr1Q/wcYJBwLhQ9EqJ3iDqmN190o7N
tyEUmbYmopcq+YLlBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29Qitf5oLu15wVLONCuEibGaNNpgq
+CXsPwfITDbDDmdrRIiUEUw6o3pt5pN0skf0JbMan2TZu6zfHzuts7KafP5UA8/0Hmf5K3/F9Mf9SE68EZjK
+cIiF1KeWndP0XfRCYXI9AJYCea0u7CXF6U0AVNNjvLe0n42LHFUK4o6JwIDAQAB
C:\Windows;
.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.
mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vm
sd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.
Microsoft Enhanced RSA and AES Cryptographic Provider
README.TXT
```

Figure 2 – Ransom message and affected extensions.

Appendix A4 – SnakeKeylogger Strings

CloseClipboard
SetClipboardData
EmptyClipboard
OpenClipboard
TrackPopupMenu
AppendMenuW
CreatePopupMenu
GetSystemMetrics
SetDlgItemTextW
GetDlgItemTextW
MessageBoxIndirectW
CharPrevW
CharNextA
wsprintfA
DispatchMessageW
PeekMessageW

Figure 1 – SnakeKeylogger clipboard manipulation and data distribution.

Appendix B – Memory Forensics

Note: The appendix contains a partial version of the malware forensics results. The full versions were replaced by screenshots of the most vital parts due to the sheer volume or similar data. Each text file can be found in the memory forensics folders within the respective malware directories of the submitted artefacts and the analysis reports.

Appendix B1 – Privileges

7816	fzpceresm.exe	2	SeCreateTokenPrivilege	Create a token object
7816	fzpceresm.exe	3	SeAssignPrimaryTokenPrivilege	Replace a process-level token
7816	fzpceresm.exe	4	SeLockMemoryPrivilege	Lock pages in memory
7816	fzpceresm.exe	5	SeIncreaseQuotaPrivilege	Increase quotas
7816	fzpceresm.exe	6	SeMachineAccountPrivilege	Add workstations to the domain
7816	fzpceresm.exe	7	SeTcbPrivilege	Act as part of the operating system
7816	fzpceresm.exe	8	SeSecurityPrivilege	Manage auditing and security log
7816	fzpceresm.exe	9	SeTakeOwnershipPrivilege	Take ownership of files/objects
7816	fzpceresm.exe	10	SeLoadDriverPrivilege	Load and unload device drivers
7816	fzpceresm.exe	11	SeSystemProfilePrivilege	Profile system performance
7816	fzpceresm.exe	12	SeSystemtimePrivilege	Change the system time
7816	fzpceresm.exe	13	SeProfileSingleProcessPrivilege	Profile a single process
7816	fzpceresm.exe	14	SeIncreaseBasePriorityPrivilege	Increase scheduling priority
7816	fzpceresm.exe	15	SeCreatePagefilePrivilege	Create a pagefile
7816	fzpceresm.exe	16	SeCreatePermanentPrivilege	Create permanent shared objects
7816	fzpceresm.exe	17	SeBackupPrivilege	Backup files and directories
7816	fzpceresm.exe	18	SeRestorePrivilege	Restore files and directories
7816	fzpceresm.exe	19	SeShutdownPrivilege	Present Shut down the system
7816	fzpceresm.exe	20	SeDebugPrivilege	Debug programs
7816	fzpceresm.exe	21	SeAuditPrivilege	Generate security audits
7816	fzpceresm.exe	22	SeSystemEnvironmentPrivilege	Edit firmware environment values
7816	fzpceresm.exe	23	SeChangeNotifyPrivilege	Present,Enabled,Default Receive notifications of changes to files or directories
7816	fzpceresm.exe	24	SeRemoteShutdownPrivilege	Force shutdown from a remote system
7816	fzpceresm.exe	25	SeUndockPrivilege	Present Remove computer from docking station
7816	fzpceresm.exe	26	SeSyncAgentPrivilege	Synch directory service data
7816	fzpceresm.exe	27	SeEnableDelegationPrivilege	Enable user accounts to be trusted for delegation
7816	fzpceresm.exe	28	SeManageVolumePrivilege	Manage the files on a volume
7816	fzpceresm.exe	29	SeImpersonatePrivilege	Impersonate a client after authentication
7816	fzpceresm.exe	30	SeCreateGlobalPrivilege	Default Create global objects
7816	fzpceresm.exe	31	SeTrustedCredManAccessPrivilege	Access Credential Manager as a trusted caller
7816	fzpceresm.exe	32	SeRelabelPrivilege	Modify the mandatory integrity level of an object
7816	fzpceresm.exe	33	SeIncreaseWorkingSetPrivilege	Present Allocate more memory for user applications
7816	fzpceresm.exe	34	SeTimeZonePrivilege	Present Adjust the time zone of the computer's internal clock
7816	fzpceresm.exe	35	SeCreateSymbolicLinkPrivilege	Required to create a symbolic link
7816	fzpceresm.exe	36	SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session.

Figure 1 – Privileges identified in the four malware samples.

Appendix B2 – Malfind

```

7496 LivelyScreenRe 0x275466e0000 0x275466effff VadS PAGE_EXECUTE_READWRITE 2 1 Disabled
00 00 00 00 00 00 00 00 .....
eb 61 fd 08 0b 72 00 01 .a...r..
ee ff ee ff 02 00 00 00 .....
20 01 6e 46 75 02 00 00 ..nFu...
20 01 6e 46 75 02 00 00 ..nFu...
00 00 6e 46 75 02 00 00 ..nFu...
00 00 6e 46 75 02 00 00 ..nFu...
0f 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 eb 61 fd 08 0b 72 00 01 ee ff ee ff 02 00 00 00 20 01 6e 46 75 02 00 00 2
7496 LivelyScreenRe 0x2755f0b0000 0x2755f0bffff VadS PAGE_EXECUTE_READWRITE 7 1 Disabled
00 00 00 00 00 00 00 00 .....
1a 99 52 f7 3f 89 00 01 ..R.?...
ee ff ee ff 02 00 00 00 .....
20 01 0b 5f 75 02 00 00 ..._u...
20 01 0b 5f 75 02 00 00 ..._u...
00 00 0b 5f 75 02 00 00 ..._u...
00 00 0b 5f 75 02 00 00 ..._u...
0f 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 1a 99 52 f7 3f 89 00 01 ee ff ee ff 02 00 00 00 20 01 0b 5f 75 02 00 00 2
7496 LivelyScreenRe 0x27561a70000 0x27561aa1fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
00 00 00 00 00 00 00 00 .....
90 3f 0b 5f 75 02 00 00 .?_u...
90 3f 0b 5f 75 02 00 00 .?_u...
00 00 0b 5f 75 02 00 00 ..._u...
00 0f a7 61 75 02 00 00 ...au...
00 10 a7 61 75 02 00 00 ...au...
00 20 aa 61 75 02 00 00 ...au...
02 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 90 3f 0b 5f 75 02 00 00 90 3f 0b 5f 75 02 00 00 00 0b 5f 75 02 00 00 e
7496 LivelyScreenRe 0x7ff47d20000 0x7ff47d20ffff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
00 00 00 00 00 00 00 00 .....
78 0d 00 00 00 00 00 00 x.....
0c 00 00 00 49 c7 c2 00 ...I...
00 00 00 48 b8 40 4a 8f ...H.@J.
ef fc 7f 00 00 ff e0 49 .....I
c7 c2 01 00 00 00 48 b8 .....H.
40 4a 8f ef fc 7f 00 00 @J.....
ff e0 49 c7 c2 02 00 00 ..I.....
00 00 00 00 00 00 00 00 78 0d 00 00 00 00 00 00 0c 00 00 00 49 c7 c2 00 00 00 00 48 b8 40 4a 8f e
7496 LivelyScreenRe 0x7ff47d210000 0x7ff47d2affff VadS PAGE_EXECUTE_READWRITE 2 1 Disabled
d8 ff ff ff ff ff ff ff .....
08 00 00 00 00 00 00 00 .....
01 00 00 00 00 00 00 00 .....
00 02 0e 03 38 00 00 00 ....8...
68 01 d7 07 0c 00 00 00 h.....
d8 5d 31 ee fc 7f 00 00 .j]1....
00 10 2f ee fc 7f 00 00 ./.....
08 4a 48 ee fc 7f 00 00 .JH.....
d8 ff ff ff ff ff ff ff 08 00 00 00 00 00 00 01 00 00 00 00 00 00 02 0e 03 38 00 00 00 e

```

Figure 1 – FileTour second stage payload with injected malicious code.

```

4424 drpbx.exe 0x2b50000 0x2b5ffff VadS PAGE_EXECUTE_READWRITE 10 1 Disabled
00 00 00 00 00 00 00 00 .....
f8 97 33 d0 80 c9 00 01 ..3.....
ee ff ee ff 02 00 00 00 .....
20 01 b5 02 00 00 00 00 .....
20 01 b5 02 00 00 00 00 .....
00 00 b5 02 00 00 00 00 .....
00 00 b5 02 00 00 00 00 .....
0f 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 f8 97 33 d0 80 c9 00 01 ee ff ee ff 02 00 00 00 20 01 b5 02 00 00 00 00 20 01 b
4424 drpbx.exe 0x1120000 0x1151fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
00 00 00 00 00 00 00 00 .....
d0 7f b5 02 00 00 00 00 .....
d0 7f b5 02 00 00 00 00 .....
00 00 b5 02 00 00 00 00 .....
c0 0f 12 01 00 00 00 00 .....
00 10 12 01 00 00 00 00 .....
00 20 15 01 00 00 00 00 .....
02 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 d0 7f b5 02 00 00 00 d0 7f b5 02 00 00 00 00 b5 02 00 00 00 c0 0f 1
4424 drpbx.exe 0x7ff42cb8000 0x7ff42cc0ffff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
d8 ff ff ff ff ff ff ff .....
08 00 00 00 00 00 00 00 .....
01 00 00 00 00 00 00 00 .....
00 00 08 01 38 00 00 00 ...8...
15 00 0e 00 0e 00 00 00 .....
50 99 fc 0c fe 7f 00 00 P.....
00 10 b9 0c fe 7f 00 00 .....
b8 ee bc 0c fe 7f 00 00 .....
d8 ff ff ff ff ff ff ff 08 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 08 01 38 00 00 00 15 00 e
4424 drpbx.exe 0x7ff42cb7000 0x7ff42cb7ffff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
00 00 00 00 00 00 00 00 .....
78 0d 00 00 00 00 00 00 x.....
0e 00 00 00 49 c7 c2 00 ...I...
00 00 00 48 b8 00 8f d3 ...H....
0d fe 7f 00 00 ff e0 49 .....I
c7 c2 01 00 00 00 48 b8 .....H.
00 8f d3 0d fe 7f 00 00 .....
ff e0 49 c7 c2 02 00 00 ..I.....
00 00 00 00 00 00 00 00 78 0d 00 00 00 00 00 0e 00 00 00 49 c7 c2 00 00 00 00 48 b8 00 8f d3 0d fe ;

```

Figure 2 – Jigsaw malicious second stage payload.

Appendix B3 – Netscan

0xba87f8c8bd70	UDPv4	0.0.0.0	*	0	7816	fzpceresm.exe	2023-02-28 16:12:31.000000
0xba87f8c8bec0	UDPv4	0.0.0.0	*	0	7816	fzpceresm.exe	2023-02-28 16:12:31.000000
0xba87f8c8bec0	UDPv6	::	*	0	7816	fzpceresm.exe	2023-02-28 16:12:31.000000
0xba87f8c8c6a0	TCPv4	0.0.0.0	5357	0.0.0.0	LISTENING	4	System
0xba87f8c8c6a0	TCPv6	::	5357	::	LISTENING	4	System
0xba87ff5fb1b0	UDPv6	fe80::c50d:519f:96a4:e108		1900	*	0	916 svchost.exe 2023-02-27 14:06:30.000000
0xba87ff5fb300	UDPv4	0.0.0.0	3702	*	0	2424	svchost.exe 2023-02-27 14:06:30.000000
0xba87ff5fb300	UDPv6	::	3702	*	0	2424	svchost.exe 2023-02-27 14:06:30.000000
0xba87ff5fb5a0	UDPv4	0.0.0.0	3702	*	0	2424	svchost.exe 2023-02-27 14:06:30.000000
0xba87ff5fb840	UDPv4	0.0.0.0	0	*	0	7816	fzpceresm.exe 2023-02-28 16:12:31.000000
0xba87ff5fc560	UDPv6	::1	1900	*	0	916	svchost.exe 2023-02-27 14:06:30.000000
0xba87ff5fc6b0	UDPv4	0.0.0.0	0	*	0	7816	fzpceresm.exe 2023-02-28 16:12:31.000000
0xba87ff5fc6b0	UDPv6	::	0	*	0	7816	fzpceresm.exe 2023-02-28 16:12:31.000000

Figure 1 – SnakeKeylogger network connections.

Appendix C – Yara Rules

Appendix C1 – FileTour.yara

```
/*
    FileTour Yara Rule
    Author: Martin Georgiev
    Date: 21/02/23
*/

rule FileTour_Bundleware {
    meta:
        description = "Yara rule for detecting FileTour malicious boundleware with SmartPDF"
        author = "Martin Georgiev"
        university = "Abertay University"
        degree = "BSc Hons Ethical Hacking"
        date = "21/02/23"
        md5 = "146d5e3ba35287954f1b61bf2ef52e24"
        sha256 =
"ab5e597bf7316bd8fcaeca8cddeec38a9585704a7929d50ea92ba603b038d7f3"

    strings:
        // NOTE: This rule has been specifically made for hash specified above.
        // Some of the $p strings may be present in legitimate files.
        // Checking the strings of the file is advised to ensure authenticity if ran on other strains.
        $p1 = "..\\sim.exe" fullword wide ascii
        $p2 = "SMART INSTALL MAKER" ascii
        $p3 = "The setup files are corrupted. Please obtain a new copy of the program." ascii
        $p4 = "inflate 1.1.4 Copyright 1995-2002 Mark Adler" ascii // Compression tool
        $p5 = "deflate 1.1.4 Copyright 1995-2002 Jean-loup Gailly" ascii // Decompression tool
        // Dropped 2nd stage payloads
        $s1 = "@$&%04\\SmartPDF.exe" fullword wide ascii
        $s2 = "@$&%04\\9840432e051a6fa1192594db02b80a4c1fd73456.exe" fullword wide
ascii
        $s3 = "@$&%04\\lg.exe" fullword wide ascii
        $s4 = "@$&%04\\LivelyScreenRecS3.0.exe" fullword wide ascii
        $s5 = "@$&%04\\note866.exe" fullword wide ascii
        $s6 = "@$&%04\\PBrowFile15.exe" fullword wide ascii
        $s7 = "@$&%04\\stats.exe" fullword wide ascii
        $s8 = "@$&%04\\Visit.url" fullword wide ascii
        $s9 = "@$&%04\\Uninstall.exe" fullword wide ascii
        $s10 = "Inno Setup Setup Data (5.5.7)" fullword wide ascii
        $s11 = "SmartPDF 10.32.0.64.2 Installation" fullword wide ascii

    condition:
        uint16(0) == 0x5a4d and any of ($p*) and all of ($s*) // Check first byte (DOS executable)and if it
has any of $p and all of $s.
}
```

Appendix C2 – Jigsaw.yara

```
/*
    Jigsaw Yara Rule
    Author: Martin Georgiev
    Date: 5/3/23
*/

rule Jigsaw_Ransomware {
    meta:
        description = "Yara rule for detecting Jigsaw Ransomware"
        author = "Martin Georgiev"
        university = "Abertay University"
        degree = "BSc Hons Ethical Hacking"
        date = "5/3/23"
        md5 = "2773e3dc59472296cb0024ba7715a64e"
        sha256 =
"3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7"

    strings:
        $s1 = "BitcoinBlackmailer" ascii
        $s2 = "Drpbx\\drpbx.exe" fullword wide ascii // 2nd stage payload #1
        $s3 = "Frfox\\firefox.exe" fullword wide ascii // 2nd stage payload #2
        $s4 = "Try anything funny and the computer has several safety measures to delete your
files." fullword wide ascii
        $s5 = "You are about to make a very bad decision. Are you sure about it?" fullword wide
ascii
        $s6 = "http://btc.blockr.io/api/v1/" fullword wide // Crypto wallet link part 1
        $s7 = "coin/info/" fullword wide // Crypto wallet link part 2
        $s8 = "coinbase" fullword wide // Crypto wallet link part 3
        $s9 = "address/balance/" fullword wide // Crypto wallet link part 4

    condition:
        uint16(0) == 0x5a4d and filesize < 1000KB and all of ($s*) // Check first byte (DOS executable), if
under 1000KB and has all of $s
}
```

Appendix C3 – NotPetya.yara

```
/*
    NotPetya Yara Rule
    Author: Martin Georgiev
    Date: 27/11/22
    Reference: Georgiev, M. (2022). Analysis and Comparison of WannaCry and NotPetya. [online]
    Github.

    Available at:
    https://github.com/Kyd1ct/Analysis_and_Comparison_of_WannaCry_and_NotPetya/commit/8ff0172ef
    1877dc6035d554379cdae4d40e8dbf4
    [Accessed 29 Nov. 2022].
*/

rule NotPetya_Wiper {
    meta:
        description = "Yara rule for detecting NotPetya wiper sample from 2017"
        author = "Martin Georgiev"
        university = "Abertay University"
        degree = "BSc Hons Ethical Hacking"
        date = "27/11/22"
        md5 = "db349b97c37d22f5ea1d1841e3c89eb4"
        sha256 =
            "24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c"

    strings:
        // Generic Ransomware messages
        $p1 = "Oops, your important files are encrypted." fullword wide ascii
        $p2 = "Send your Bitcoin wallet ID and personal installation key to e-mail " fullword
        wide

        // NotPetya related commands
        $s1 = "process call create \"C:\\Windows\\System32\\rundll32.exe
        \\\"C:\\Windows\\%s\\\" #1 " fullword wide // creates a process call to execute itself with rundll32.exe
        $s2 = "-d C:\\Windows\\System32\\rundll32.exe \"C:\\Windows\\%s\\\",#1 " fullword
        wide // runs itself with rundll32.exe on newly infected machines
        $s3 = "fsutil usn deletejournal /D %c:" fullword wide // deletes USN journal (changes on
        drive C)
        $s4 = "wevtutil cl Setup & wevtutil cl System" fullword wide ascii //clears Setup and
        System logs
        $s5 = "dllhost.dat" fullword wide //psexec.exe execution for local network propagation
        $s6 = "%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" " fullword wide //remote
        execution with wmic.exe
        $s7 = "schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d" fullword
        wide //schedule system reboot at noon
        $s8 = "u%s \\\\%s -accepteula -s " fullword wide // automatically accepts EULA upon
        execution to remain hidden
```

Appendix C4 – SnakeKeylogger.yara

```
/*
    SnakeKeylogger Yara Rule
    Author: Martin Georgiev
    Date: 25/3/23
*/

rule Jigsaw_Ransomware {
    meta:
        description = "Yara rule for detecting SnakeKeylogger spyware"
        author = "Martin Georgiev"
        university = "Abertay University"
        degree = "BSc Hons Ethical Hacking"
        date = "25/3/23"
        md5 = "6f0d31986bdac094d0903a1a44cc5432"
        sha256 = "7e1d956fe3ab418c915d24faecac0798be86b86a4244580ebf8af91bc01f752f"
        note = "This yara rule works only for the specified sample. The sample did not contain
any obvious strings which can be found in other SnakeKeylogger variants."

    strings:
        // Generic Nullsoft strings
        $p1 = "Nullsoft" fullword wide ascii
        $p2 = "\\Microsoft\\Internet Explorer\\Quick Launch" fullword wide ascii // IE related

    registry
        $p3 = "Software\\Microsoft\\Windows\\CurrentVersion" fullword wide ascii //
CurrentVersion registry
        // Clipboard functions
        $s1 = "CloseClipboard" ascii
        $s2 = "SetClipboardData" ascii
        $s3 = "EmptyClipboard" ascii
        $s4 = "OpenClipboard" ascii
        // Retrieve messages from windows on the current thread and dispatch them.
        $s5 = "PeekMessageW" ascii
        $s6 = "DispatchMessageW" ascii

    condition:
        uint16(0) == 0x5a4d and filesize < 1000KB and any of ($p*) and all of ($s*) // Check first byte
(DOS executable), if under 1000KB and has any of $p and any of $s
}
```

Appendix D – Malware Analysis Reports and Methodology

Note: The appendix contains a partial version of the documents. Large parts were omitted due to their sheer volume. The methodology and analysis reports can be located as within the main folder (Methodology.docx) and the respective malware analysis directories of the submitted artefacts.

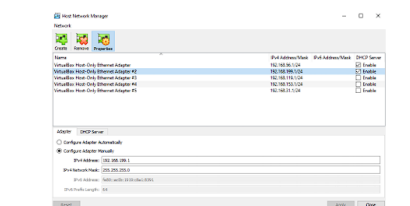


Figure 2.3.1 – Host Network Manager.

A new adapter can be created from the create button. It should have the following data in the adapter (Figure 2.3.2) and DHCP Server (Figure 2.3.3) tabs:

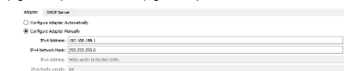


Figure 2.3.2 – Adapter tab.



Figure 2.3.3 – DHCP Server tab.

The analyst should then right-click on the imported FlareVM and Remnux machines and open Settings (the top option). Once the Settings window is opened, open the network tab and change the 'Attached to:' setting to 'Host-only Adapter' and the 'Name:' to the name of the newly created adapter. (Figure 2.3.4) This will allow the machines to communicate.

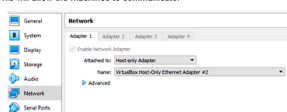


Figure 2.3.4 – Network settings of the machines.

The final action the analyst needs to take is to launch FlareVM and edit the network adapter's settings. This can be achieved by opening the Control Panel (press the Windows key and type Control Panel) and then clicking on 'View network status and tasks' (Figure 2.3.5).



Figure 2.3.5 – Network tab in Control Panel.

Once the window opens, click on 'Change adapter settings' located on the top left. (Figure 2.3.6)

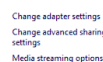


Figure 2.3.6 – Change adapter settings.

Right-click on the Ethernet adapter and open the properties. (Figure 2.3.7)

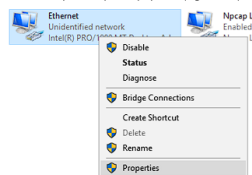


Figure 2.3.7 – Opening properties of the ethernet adapter.

Afterwards, the analysts need to double-click on the Internet Protocol Version 4 option and change the preferred DNS address to 10.0.0.3. (Figure 2.3.8 and Figure 2.3.9)

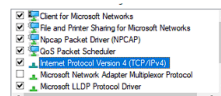


Figure 2.3.8 – IPv4 option.

Figure 1 – Network setup in the attack analysis methodology.

2.2.3 In-depth Inspection

The analysis proceeded with PEStudio. PEStudio is a tool speeding up the initial malware analysis process and making it easier. The tool conducts a complete static analysis of the file and provides researchers with indicators, imports, libraries, and file entropy (randomness of data hinting at hidden/suspicious data).

Loading the sample into the tool revealed the entropy level (7.9 out of 8), indicating that the data within it is heavily obfuscated. Based on the compiler stamp, this specific binary was created on the 25th of September, 2021. The tool then showed five critical and four high indicators - blacklisted strings/functions, URL patterns, embedded files, virtualised spps8093 and invalid checksums (Figure 2.2.5)

indicator (5)	detail	level
strings > blacklist	count: 37	1
file > embedded	signature: Nullsoft; location: offset: 0x0000AC00; size: 240807	1
functions > blacklist	count: 35	1
URL > pattern	url: http://msdn.net/NGS_Error	1
URL > pattern	url: 25.50.84.7	1
overlay > file-ratio	value: 84.93%	2
functions > anonymous	count: 1	2
checksum > invalid	expected: 0a00548ff	2
section > virtualized	section: .mdta	2
manifest > name	value: Nullsoft.NGS.exehead	3
entry-point > location	section: .text(0x00005040)	3

Figure 2.2.5 – Malicious indicators.

In terms of the libraries, the tool identified seven libraries, none of which were blacklisted. This, however, did not exclude that they could be used for malicious purposes (Figure 2.2.6)

library (7)	blacklist (0)	type (3)	functions (165)	description
advapi32.dll	-	implicit	13	Advanced Windows 32 Base API
shell32.dll	-	implicit	6	Windows Shell Common Dll
ole32.dll	-	implicit	5	Microsoft OLE for Windows
comctl32.dll	-	implicit	6	Common Controls Library
user32.dll	-	implicit	6d	Multi-User Windows USER API Client DLL
gdi32.dll	-	implicit	8	GDI Client DLL
kernel32.dll	-	implicit	65	Windows NT BASE API Client DLL

Figure 2.2.6 – List of libraries.

The tool discovered a total of thirty-five blacklisted functions. As mentioned in the previous section, they allowed the malware to alter the registries/clipboard, execute shell commands, and obtain information (file paths, names, etc.). There were also some non-blacklisted functions that were suspicious - custom function used to delete all pointers, object manipulation and image creation (Figure 2.2.7)

functions (165)	blacklist (35)	ordinal (1)	library (7)
RegEnumKeyW	x	-	advapi32.dll
RegSetValueExW	x	-	advapi32.dll
RegDeleteValueW	x	-	advapi32.dll
RegDeleteKeyW	x	-	advapi32.dll
AdjustTokenPrivileges	x	-	advapi32.dll
LookupPrivilegeValueW	x	-	advapi32.dll
OpenProcessToken	x	-	advapi32.dll
SetFileSecurityW	x	-	advapi32.dll
SHGetSpecialFolderLocation	x	-	shell32.dll
SHFileOperationW	x	-	shell32.dll
SHBrowseForFolderW	x	-	shell32.dll
SHGetPathFromIDListW	x	-	shell32.dll
ShellExecuteExW	x	-	shell32.dll
SHGetFileInfoW	x	-	shell32.dll
OpenClipboard	x	-	user32.dll
SetClipboardData	x	-	user32.dll
CloseClipboard	x	-	user32.dll
SystemParametersInfoW	x	-	user32.dll
ExitWindowsEx	x	-	user32.dll
EmptyClipboard	x	-	user32.dll
GetExitCodeProcess	x	-	kernel32.dll
WriteFile	x	-	kernel32.dll
GetTempFileNameW	x	-	kernel32.dll
RemoveDirectoryW	x	-	kernel32.dll
CreateProcessW	x	-	kernel32.dll
SetEnvironmentVariableW	x	-	kernel32.dll
SetFileAttributesW	x	-	kernel32.dll
GetCurrentDirectoryW	x	-	kernel32.dll
MoveFileW	x	-	kernel32.dll
SearchPathW	x	-	kernel32.dll
MoveFileExW	x	-	kernel32.dll
WritePrivateProfileStringW	x	-	kernel32.dll
FindNextFileW	x	-	kernel32.dll
FindFirstFileW	x	-	kernel32.dll
DeleteFileW	x	-	kernel32.dll
RegCreateKeyExW	x	-	advapi32.dll
RegQueryValueExW	x	-	advapi32.dll

Figure 2.2.7 – Partial list of functions utilised by the malware.

The analyst then checked whether the malware was packed using one of the commonly found packers such as UPX1 to evade detection. This was achieved with ExeinfoPE. Loading the file into the tool revealed that the EP section was in .text, indicating that no specific packer was used. 'Text' is the section of an executable that contains its code. (Figure 2.2.8)

Figure 2 – PEStudio analysis of SnakeKeylogger.

2.3 Dynamic Analysis

Dynamic analysis of malware is achieved by detonating the sample in a safe environment (or surveying an already compromised environment) to see how it behaves on a local and network level. This may be dangerous if the safe environment is not properly set up as it may allow the malicious software to propagate to the physical machine, the user's network, and possibly even other connected networks.

2.3.1 Detonation Symptoms

In Section 2.2.2 String Extraction, the researcher identified that a different approach was needed to execute the wiper. The analyst used the command found during the strings analysis to launch the binary, specifically: "rundll32 Ransomware.NotPetya.dll, #1". This command utilised the rundll32.dll (Microsoft, 2021) to execute the malware with an entry point of 1. While there were no visible signs of infection after the malicious file removed itself upon detonation, the tester decided to reboot the machine. However, the boot process was unsuccessful, and a fake error message appeared on the disk (Figure 2.3.1). Despite attempting to repair the device, the process was unsuccessful, and in the end, the ransom message was displayed (Figure 2.3.2). The fake repair message and the ransom message had the same fonts, and the repair message showed unrealistic sector numbers – over 4 billion for an 80GB drive. An 80GB drive should have around 167,772,160 sectors, approximately 4.1 billion less than what was displayed. Furthermore, during the fake repair process, the malware caused additional damage to the system.

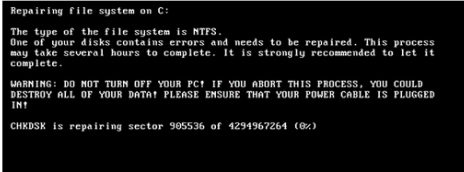


Figure 2.3.1 – Fake disk repair message.

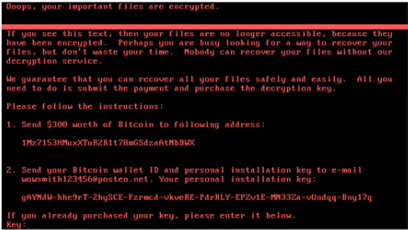


Figure 2.3.2 – Ransom message after unsuccessful "repair".

To prevent the malware from executing fully, the analyst created a file named "perfc" in the "C:\Windows" directory. A similar file name was found in the Floss output, but the file had a .dat extension. Several analysts discovered this local killswitch and provided different files for the vaccine, including perfc.dll, and perfc.dat. While all three files were successful, the first two produced an error indicating that the .dll file had no such entry point (Figure 2.3.3). The killswitch files successfully prevented the ransomware from executing. However, the system was infected if the malware was run again after the researcher deleted the previously noted files. Notably, running NotPetya as a regular user encrypted the files (Figure 2.3.4) without damaging the Master Boot Record, meaning that victims could still access their machine while losing the affected files.

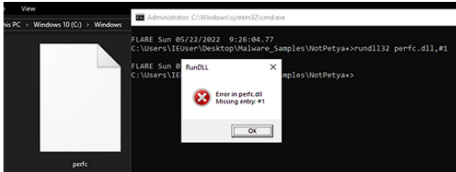


Figure 2.3.3 – Killswitch results.

Figure 3 – NotPetya dynamic analysis.

4 Discussion

4.1 General Discussions

Analysing the sample revealed that it successfully encrypted the user's files. Compared to other ransomware variants, Jigsaw does delete the files of users if they do not comply with its demands. The static and dynamic analysis showed the behaviour of the sample, as well as how it would behave in both local and external environments. The lack of a propagation mechanism was expected as it is known that the ransomware mainly propagated through phishing emails.

The sample did not use any payloads downloaded over the internet, nor did it have any communications with a C&C server. Some of the other strains may have different behaviour as there have been identified variants with live support chats for the victims controlled by the attackers.

4.2 Countermeasures

4.2.1 Pre-infection Countermeasures

The most effective way to protect a system from infection would be before it becomes infected. As some of the modules contain cryptography functions, a fully working sample could encrypt the victim's files. This, in most cases, would not allow them to retrieve their files.

4.2.1.1 Frequent Security Updates

One of the reasons why malware is successful is the lack of security patches or users refusing to apply the newest updates to their operating systems and/or anti-virus applications. Keeping your system and anti-virus software up to date would ensure that publicly known vulnerabilities could not be exploited, and the AV may have updated signature databases to detect the sample.

4.2.1.2 Distinguishing Spam

As the malware is primarily distributed through social engineering, users must be able to distinguish spam emails from real ones. This also applies to legitimate and fake websites and/or files. Users should not open any links or execute files unless they know the sender and the nature of the link or file. Additionally, users should look for bad grammar, fearmongering, rushed actions or similar addresses to legitimate ones.

4.2.1.3 Blacklisting Unknown Applications and Anti-Virus Software

System administrators could put restrictions on users by blacklisting unknown software. This way they would not be able to execute suspicious applications and provide the system/network with damage control to prevent any harm. It could be achieved with Anti-Virus software and integrated browser protection.

An updated Anti-Virus software could be used to perform system scans or simply scan newly generated files. Some may even prevent the malicious software from executing itself if they recognise specific code patterns or behaviours.

4.2.1.4 File Scanners and IDS

Intrusion Detection Systems will alert security analysts if they detect any suspicious behaviour – phishing emails, specific signatures, etc. Some of them can also be combined with file scanners such as Streika for greater detection accuracy. This way the internal SOC team could notice the threat before it causes any harm to the system.

4.2.2 Post-infection Countermeasures

4.2.2.1 Data Backups

As some of the payloads contained cryptography-related libraries and functions, it would be beneficial to keep data backups. With such, the company could wipe the infected drive and simply replace it with the information they have stored elsewhere. It is also advised to keep such data in physical storage if possible or in locations which are not directly connected to the network of the infected machine as some malware could propagate to it and destroy the backups.

4.2.2.2 Refuse Ransom Payments

Ransom payments should NOT be considered even in dire situations. In the case of encrypted files, the adversary may attempt to fearmonger the victim by threatening them to publicly post their data or delete it. Paying the ransom does not guarantee that the data can be recovered as the attacker may send a fake decryption key or they may not send one at all.

4.2.2.3 Possible Decryption

Multiple analysts discovered that the ransomware could be decrypted for free. After reverse-engineering the sample and identifying how its encryption algorithm works, they created a decryptor. To use it, the infected users must first terminate the firefox.exe and drpbx.exe processes from the Task Manager to prevent further deletion of files. The victims must then open the start-up tab within the Task Manager to disable firefox.exe (Figure 4.2.1).

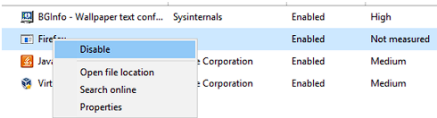


Figure 4.2.1 – Disabling the start-up process.

Afterwards, the users can download the decryptor from websites such as [BleepingComputer](#). Depending on the strain, such decryptors may also result in further deletion or they may not even work. Victims are suggested to first consult themselves with a professional. Using such tools must be done at their own risk.

Figure 4 – Jigsaw countermeasures.

Appendix E – Generalised CIRP

Note: The appendix contains a partial version of the document. Large parts of the generalised CIRP have been omitted due to its sheer volume. The plan can be located as **CIRP.docx** within the main folder of the submitted artefacts.

Criticality Levels	Description
Criticality 1	Enterprise-Wide Resources (Vital Services, Network Devices, DNS, Firewall, etc.).
Criticality 2	Critical Data – Confidential Data (Intellectual Property, Blueprints, etc.).
Criticality 3	Critical Systems (AD Servers, Web Services, etc.).
Criticality 4	Sensitive Data – Restricted Data (Corporate Information, Financial Documentation, User Data, etc.).
Criticality 5	Non-Critical Systems (File Servers and other systems that are not vital for the organisation's workflow).
Criticality 6	Regular Data and Separate Systems.

Table 4.4.2 – Criticality levels based on the Scottish CIRP Template.

The threat and criticality levels provided above are examples and can be altered to <Organisation Name>'s needs. When the two components are created and thoroughly discussed, their impact can then be shown with the help of a risk matrix. The incident's severity can be assessed when the separate components are placed in the matrix provided below (Table 4.4.3). This will provide the CIRT with an estimate of the attack's severity.

Criticality Level	Threat Level					
	1	2	3	4	5	6
1	Critical	Critical	Critical	High	High	Medium
2	Critical	Critical	High	High	Medium	Medium
3	Critical	High	High	Medium	Medium	Medium
4	High	High	Medium	Medium	Medium	Low
5	High	Medium	Medium	Medium	Low	Low
6	Medium	Medium	Medium	Low	Low	Low

Table 4.4.3 – Risk Matrix based on the Scottish CIRP Template.

Severity Level	Impacts	IR Characteristics
Critical	<p>Highest level of severity. The impact can potentially be catastrophic for the company and its employees, including loss of business, public trust and/or impact on its operations. The following implications are indicators of this degree of severity:</p> <ul style="list-style-type: none"> - Threat to life or physical safety of customers, public or personnel. - Significant destruction of IT assets (hardware and software). - Significant disruption of business operations for a long period. - Significant damage to <Organisation Name>'s reputation. - Significant destruction of corporate capabilities. - Risks of considerable financial loss. - Loss/Leakage of confidential information. 	<p>Due to the nature of this severity level, immediate and continual action from the CIRT is required. Such incidents have the highest impacts on the organisation and involve extensive and persistent operations, which often use complex attacks that are hard to counter. This severity level will trigger the policies of the Cyber Defence Departments of the country where <Organisation Name> is based. Possible indicators for such incidents are:</p> <ul style="list-style-type: none"> - Potentially involving law enforcement. - Potentially involving multiple media outlets and support from multiple organisations. - <Organisation Name>'s executives will have an immediate and continual interest in the incident and its development. Possible requirement for multiple levels of reporting (regulatory and/or compliance).
	<p>Substantial impact affecting the proper operations of <Organisation Name>'s business operations, public trust, and impacts on their personnel. The following impacts are indicators of this severity level:</p> <ul style="list-style-type: none"> - Large loss of confidential data, restricted information, and public confidence. - Destruction of corporate 	<p>Albeit milder than the previous severity level, this one also requires the immediate attention of both the Core and extended CIRT. It may require extended work hours or even around-the-clock response activities. Such incidents have substantial negative impacts on operations and involve persistent and sophisticated attacks. Such attacks require large amounts of resources to contain, control and counter them. This</p>

Figure 1 – Risk assessment.

4.5 Incident Containment

The responsibility for the containment of the incident is given to the core or extended CIRT depending on the scale of the attack. This can be achieved in a multitude of ways depending on the type of infection and its capabilities. The following examples (but are not limited to) will show various ways of different cyber incidents:

- Identify systems, services, and timeframes (IP/MAC addresses, hostnames, protocols, active services, locations, user accounts and timestamps) and take appropriate actions against them:
 - o Remove users from critical infrastructures;
 - o Remove elevated privileges of users;
 - o Stop any affected services;
 - o Isolate any of the identified systems if needed.
- Isolate connections with external networks to prevent further spread.
- If required, contact specialists for help with the containment and documentation.
- Do not power off affected systems as this could alter valuable evidence
- Identify, acquire, and preserve any possible sources of evidence:
 - o Live data (encrypted files, RAM, network connections);
 - o Application data (temporary files, emails, images, swap, and hibernation files);
 - o Logs (event, network traffic, Anti-virus);
 - o Electronic documents (databases, PDF files, presentations, documentation);
 - o Mobile phones (call logs, contacts, emails, SMS, and appropriate application data);
 - o Storage media (HDD/SSD, USB, MicroSD cards, etc.);
 - o Metadata (dates, authors, access/creation/alteration times);
 - o Navigation data (GPS data).
- Documenting all actions in chronological order (i.e., Chain of Custody System):
 - o Personal information of the entity collecting and analysing the data as it must be done only by trained personnel;
 - o Information regarding how the actions were undertaken (acquisition, preservation, analysis, and storage);
 - o Backups for forensic copies and write blockers/permissions to ensure that all data will remain untouched and safe (i.e., ACPO Guidelines) (ACPO, 2007);
 - o Any changes to forensic evidence as sometimes they are required to access specific data (i.e., Phone rooting to bypass its password);
 - o All evidence of a cyber incident must be secured within 24 hours.

If in doubt, further advice should be obtained from appropriate specialists such as Digital Forensic Analysts in third-party partner companies or the local police department.

Figure 2 – Incident Containment.

Appendix F – Response Modules

Note: The appendix contains a partial version of the documents. Large parts have been omitted due to their sheer volume. The modules can be located as within the respective malware analysis folder of the submitted artefacts.

1.4.1 Severity Assessment

One of the best ways to identify the criticality of an incident and its implications is by using a risk matrix. To create the matrix, this CIRP will use threat levels (types of threat in hierarchical order based on severity) and criticality levels (importance of systems/information in hierarchical order). Both can be found in descending order in Table 4.4.1 and Table 4.4.2 respectively. The tables are based on the examples in the Scottish Cyber Incident Response Plan Template.

Threat Levels	Description
Threat 1	Full compromise controlled by a human: <ul style="list-style-type: none">External personnel without appropriate authorisation (cyber intrusion).External stakeholders with inappropriate authority.Internal staff exceeding intended authority.
	Close-Access Breach (physical penetration of a site) <ul style="list-style-type: none">Fake Wi-Fi network.Router pivoting (redirection of traffic).
	Partial compromise controlled by a human: <ul style="list-style-type: none">External personnel without appropriate authorisation (cyber intrusion).External stakeholders with inappropriate authority.Internal staff exceeding intended authority.
Threat 3	Automated full compromise controlled by malware
Threat 4	Automated partial compromise controlled by malware
Threat 5	DoS (Denial of Service, affecting connectivity)
Threat 6	Directed Scanning (vulnerability and open port identification) or malware not controlled by a command-and-control server.

Table 4.4.1 – Threat types converted to levels based on the Scottish CIRP Template.

Criticality Levels	Description
Criticality 1	Enterprise-Wide Resources (Vital Services, Network Devices, DNS, Firewall, etc.).
Criticality 2	Critical Data – Confidential Data (Intellectual Property, Blueprints, etc.).
Criticality 3	Critical Systems (AD Servers, Web Services, etc.).
Criticality 4	Sensitive Data – Restricted Data (Corporate Information, Financial Documentation, User Data, etc.).
Criticality 5	Non-Critical Systems (File Servers and other systems that are not vital for the organisation's workflow).
Criticality 6	Regular Data and Separate Systems.

Table 4.4.2 – Criticality levels based on the Scottish CIRP Template.

Jigsaw is a type of malicious software which encrypts various file extensions and attempts to feignomerge its victims. As there are no identified automated ways of propagation and it does not install a backdoor or attempt to elevate its privileges, the incident can be placed as **Medium** or **High** depending on the affected data.

Criticality Level	Threat Level					
	1	2	3	4	5	6
1	Critical	Critical	Critical	High	High	Medium
2	Critical	Critical	High	High	Medium	Medium
3	Critical	High	High	Medium	Medium	Medium
4	High	High	Medium	Medium	Medium	Low
5	High	Medium	Medium	Medium	Low	Low
6	Medium	Medium	Medium	Low	Low	Low

Table 4.4.3 – Risk Matrix based on the Scottish CIRP Template.

1.4.2 Severity Guidance

Based on the capabilities of the malware and the fashion it operates in, it would be difficult to affect the entire corporate network of the organisations. Based on the scale of the damage, multiple media outlets may be involved, and the organisation's executives may require multiple levels of frequent reporting. In terms of damage, depending on the role of the infected machine, it can destroy/leak a lot of valuable data or affect a low-level computer with little to no vital information on it. Due to the **Medium** or **High Severity Level** of the incident, the organisation should assign the response duty to the entire CIRT if deemed necessary. It can also be escalated to law enforcement.

Severity Level	Impacts	IR Characteristics
High	Substantial impact affecting the proper operations of <Organisation Name>'s business operations, public trust, and impacts on their personnel. The following impacts are indicators of this severity level: <ul style="list-style-type: none">Large loss of confidential data, restricted information, and public confidence.Destruction of corporate assets and capabilities with a large impact.Substantial disruption of the normal operation process.Large damages to the reputation.Risk of large financial loss.	Albeit milder than the previous severity level, this one also requires the immediate attention of both the Core and extended CIRT. It may require extended work hours or even around-the-clock response activities. Such incidents have substantial negative impacts on operations and involve persistent and sophisticated attacks. Such attacks require large amounts of resources to contain, control and counter them. This level will also trigger policies from the local Cyber Defence Department. Possible indicators of this incident are: <ul style="list-style-type: none"><Organisation Name>'s executives will have an immediate and continual interest in the incident and its development. Possible requirement for multiple levels of reporting (regulatory and/or compliance).Potentially involve law enforcement, engagement by some

Figure 1 – Jigsaw severity assessment.

1.5 Incident Containment

The responsibility for the containment of NotPetya is given to the entire CIRT due to the severity of the infection. This can be achieved in a multitude of ways. It is highly recommended to contact law enforcement and third-party cybersecurity providers due to the severity of the attack. The following examples (but are not limited to) will show an example of how the incident should be contained (RedGoat, 2022):

- Quick actions – NotPetya is a type of malware which can cause severe destruction to a company's data. Speed is a key requirement for damage minimisation.
- Identify systems, services, and timeframes (IP/MAC addresses, hostnames, protocols, active services, locations, user accounts and timestamps) and take appropriate actions against them:
 - Remove users from critical infrastructures;
 - Remove elevated privileges of users;
 - Stop any affected services;
 - Isolate any of the identified systems if needed;
 - Blacklist email/domain used by an attacker if the sample was delivered through social engineering.
- Isolate connections with external networks to prevent further spread. Infecting external partners/organisations will cause further issues and more work for the CIRT, making them less efficient.
- If required, contact specialists for help with the containment and documentation.
- Do not power off affected systems as this could alter valuable evidence and will encrypt the drive's Master Boot Record.
- Identify, acquire, and preserve any possible sources of evidence:
 - Live and volatile data (encrypted files, network communications);
 - Application data (temporary files, system logs, hidden files);
 - Other logs (event, network traffic, Anti-virus/Yara detection);
 - Storage media (HDD/SSD, USB, MicroSD cards, etc.);
 - Metadata (dates, file access/creation/alteration times).
- Documenting all actions in chronological order (i.e., Chain of Custody System):
 - Personal information of the entity collecting and analysing the data as it must be done only by trained personnel;
 - Information regarding how the actions were undertaken (acquisition, preservation, analysis, and storage);
 - Backups for forensic copies and write blockers/permissions to ensure that all data will remain untouched and safe (i.e., ACPD Guidelines);
 - Any changes to forensic evidence (system shut down or any system changes to restore operations)
 - All evidence of a cyber incident must be secured within 24 hours.

If in doubt, further advice should be obtained from appropriate specialists such as Digital Forensic Analysts in third-party partner companies or the local police department.

Figure 2 – NotPetya containment.

1.2 Identification

It is important that the staff can properly identify the type of incident as reporting a false type would potentially result in more damages while the CIRT is attempting to mitigate and analyse the wrongly reported attack. Possible incident types for a FileTour-related infection are provided in Table 4.2.1 below this paragraph.

No	Incident Type Name	Incident Description
1	Phishing	Phishing can have two different incidents. The first type covers personnel from the organisation who receive suspicious emails from someone who claims to be a specific individual/organisation. The second type covers third-party individuals who receive an email from someone who claims to work in <Organisation Name> without being a part of the organisation.
2	Social Engineering	Attempts to gain access to the <Organisation Name>'s data or systems by deceiving or extorting users – customers, staff or external contractors.
3	Installation and/or execution of unknown software.	Any attempts or actual execution of unknown software on <Organisation Name>'s devices. This covers both detections from anti-virus software and/or whitelisting software.
4	Loss, theft, or damage of company assets.	Any cases of loss, theft and/or damage of <Organisation Name>'s data and devices. This includes removable media (external drives, USBs, etc.) and work devices (computers, IoT devices, etc.)
5	Impersonation	Any cases of account compromise/hijacking. It covers attacks on the <Organisation Name>'s authentication capabilities, password sharing, suspicious login cases, accounts without a verifiable owner (zombie accounts), etc.
6	Privilege escalation	Any cases of users being moved to a group with more privileges or gaining excessive privileges through exploits or account switching.
7	Questionable use of legitimate privileges	Any case of a user abusing their privileges (accessing large amounts of data, sending data to unknown recipients, moving data to removable devices or inappropriate locations on the network).
8	Inappropriate use of devices	Any cases of illegal activity of staff members through company assets. This includes browsing inappropriate websites, threatening/obscene/harassing communications, access/storage

Figure 3 – FileTour incident identification.

1.4.3 Malware Identification

It is important to use the initial triage to obtain additional intel regarding the malware and its appropriate artefacts. This includes a few subcategories – delivery, execution, and symptoms.

As previously mentioned, the malware is delivered through social engineering attempts. With this, suspicious emails containing urgent/fearmongering messages will be the most common means of infection. All evidence (network and IDS/IPS logs, emails, unexpected connections) must be thoroughly documented as it can be used to identify how it was delivered from where, and where it has propagated in the organisation's network. As there are numerous samples of the Keylogger showing each day, it is hard to provide a complete list of hashes. Examples of hashes from February 2023 are:

- e8e100895fa60d667eb81cc2fb660ac12dd998f8f20aa6d7e0ea942854dc831f
- 7e1d956fe3ab418c915d24faecac0798be86b86a4244580ebf8af91bc01f752f
- ae1c76298164414736639b05b24e5c12078d7c9fb85163b92cde019d943a62d5
- 2cc5b915835368d59f7a46adb02593d468bfa0cd63eea856e9e4cd55b29f8afb
- dfe752002f955e1facba9518dc6ac3854b9aa6ec196fcc22068f41e4f5c87cf3
- bde58e12d41cd833eb907de3955528c3ba4ea45f7e825b6ca038f74eaf594d26

In terms of execution, the file does not need to be run with administrator privileges. Execute itself and steal data even when it is run by a low-privilege account. The detonation symptoms will not be obvious, as its functions are done in the background, without displaying any windows or messages.

Figure 4 – SnakeKeylogger malware identification.

Appendix G – GDPR Data Sign-Off Form



GDPR Research Data Management Data Sign Off Form

For undergraduate or postgraduate student projects supervised by an Abertay staff member.

This form MUST be included in the student's thesis/dissertation. Note that failure to do this will mean that the student's project cannot be assessed/examined.

Part 1: Supervisors to Complete

By signing this form, you are confirming that you have checked and verified your student's data according to the criteria stated below (e.g., raw data, completed questionnaires, superlab/Eprime output, transcriptions etc.)

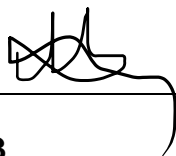
Student Name:	Martin Georgiev		
Student Number:	1901560		
Lead Supervisor Name:	Dr Natalie Coull		
Lead Supervisor Signature	NC		
Project title:	An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses		
Study route:	PhD <input type="checkbox"/>	MbR <input type="checkbox"/>	MPhil <input type="checkbox"/>
	Undergraduate <input checked="" type="checkbox"/>	PhD by Publication <input type="checkbox"/>	

Part 2: Student to Complete

	Initial here to confirm 'Yes'
I confirm that I have handed over all manual records from my research project (e.g., consent forms, transcripts) to my supervisor for archiving/storage	MG
I confirm that I have handed over all digital records from my research project (e.g., recordings, data files) to my supervisor for archiving/storage	MG

I confirm that I no longer hold any digital records from my research project on any device other than the university network and the only data that I may retain is a copy of an anonymised data file(s) from my research	MG
I understand that, for undergraduate projects, my supervisor may delete manual/digital records of data if there is no foreseeable use for that data (with the exception of consent forms, which should be retained for 10 years)	MG

**Student
signature :** _____



Date: 16.05.2023

Proof of authorisation:

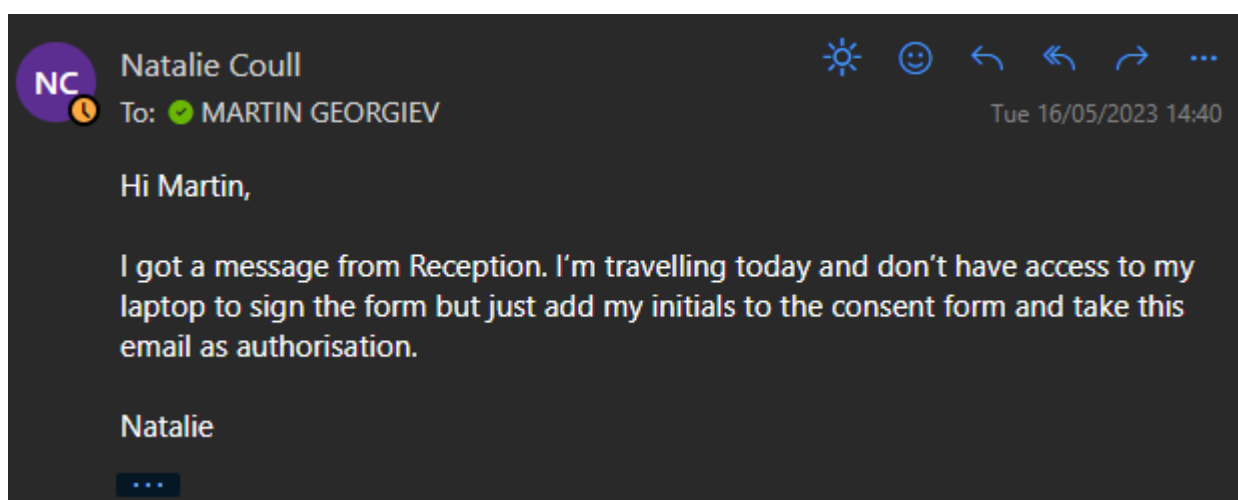


Figure 1 – Email from supervisor authorising usage of initials.