CHAPTER I

INTRODUCTION

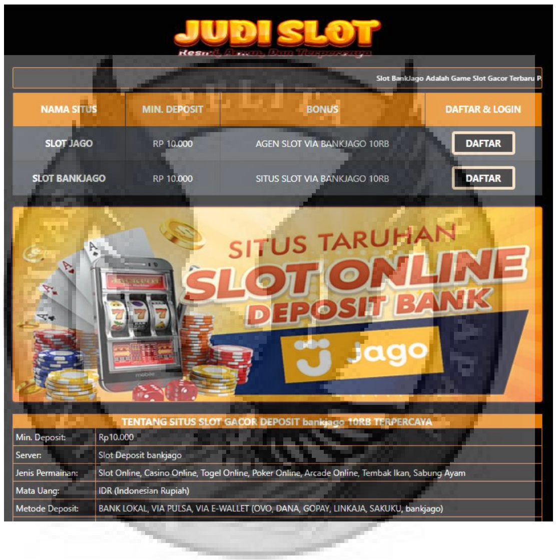
1.1. Background

In today's rapidly advancing digital world, cybersecurity is pivotal in safeguarding sensitive information and ensuring the integrity of computer systems. The increasing reliance on digital communication tools accentuates the role of forensic analysis in cybersecurity. This field is crucial for understanding and countering cyber threats through the collection, preservation, analysis, and legal presentation of digital evidence after cyber incidents.

The critical area of this research is not focused on forensic analysis against Trojans but rather on Static Analysis, Dynamic Analysis, Code Reverse Engineering, and Malware Signature Extraction. This research aims to delve into these techniques as the primary methods for identifying, analyzing, and addressing malware. By prioritizing these approaches, the research seeks to develop more effective strategies for detecting and analyzing malware, without engaging in aspects of Data Recovery and Artifact Analysis, Timeline Analysis, Memory Forensics, or Network Analysis. Concentrating on these areas is expected to provide deeper insights into the characteristics and behaviour of malware, as well as improve the ability to tackle malware threats more efficiently.

This thesis also explores advanced malware analysis, which goes beyond simple threat identification to examine the characteristics, origins, and impacts of malicious software. Malware types, including viruses, trojans, and other harmful software, pose serious risks to data integrity and confidentiality. In-depth malware analysis, therefore, is critical in developing effective defence strategies and pre-emptive measures against future threats. This approach is integral to shaping proactive cybersecurity strategies.

Recent trends, such as the increase in online gambling *web* defacement incidents, highlight significant security challenges. This research draws attention to the rapid proliferation of online gambling content on government and educational *web*sites, a phenomenon reported by Budi Arie Setiadi, Minister of Communication and Information Technology. Despite governmental countermeasures, the persistence of these attacks suggests systemic vulnerabilities and a need for more robust security protocols .



Slot BankJago Adalah Game Slot Gacor Terbaru P

NAMA SITUS	MIN. DEPOSIT	BONUS	DAFTAR & LOGIN
SLOT JAGO	RP 10.000	AGEN SLOT VIA BANKJAGO 10RB	DAFTAR
SLOT BANKJAGO	RP 10.000	SITUS SLOT VIA BANKJAGO 10RB	DAFTAR

TENTANG SITUS SLOT GACOR DEPOSIT bankjago 10RB TERPERCAYA	
Min. Deposit:	Rp10.000
Server:	Slot Deposit bankjago
Jenis Permainan:	Slot Online, Casino Online, Togel Online, Poker Online, Arcade Online, Tembak Ikan, Sabung Ayam
Mata Uang:	IDR (Indonesian Rupiah)
Metode Deposit:	BANK LOKAL, VIA PULSA, VIA E-WALLET (OVO, DANA, GOPAY, LINKAJA, SAKUKU, bankjago)

Figure 1. 1 *Web*sites that have been infiltrated with online gambling content

Figure 1.1 depicts a screenshot of a website that appears to have been infiltrated with online gambling content, specifically promoting a slot machine gambling service. The top section of the site contains navigation options such as "Home," "Minimum Deposit," "Bonus," and "Register & Login," alongside the name of the site. A prominent graphic in the center showcases the branding for "Situs Taruhan

Slot Online Deposit Bank," which translates to "Online Slot Betting Site Bank Deposit." The site emphasizes a low minimum deposit and advertises various slot games, suggesting that it targets users interested in online gambling.

According to data from the Financial Transaction Reports and Analysis Center (PPATK), during the period 2017-2022 there were approximately 157 million online gambling transactions in Indonesia with a total value of money turnover reaching Rp190 trillion (*Tren Judi Online Di Indonesia Terus Meningkat, Nilainya Tembus Rp100 T Pada 2022*, n.d.)

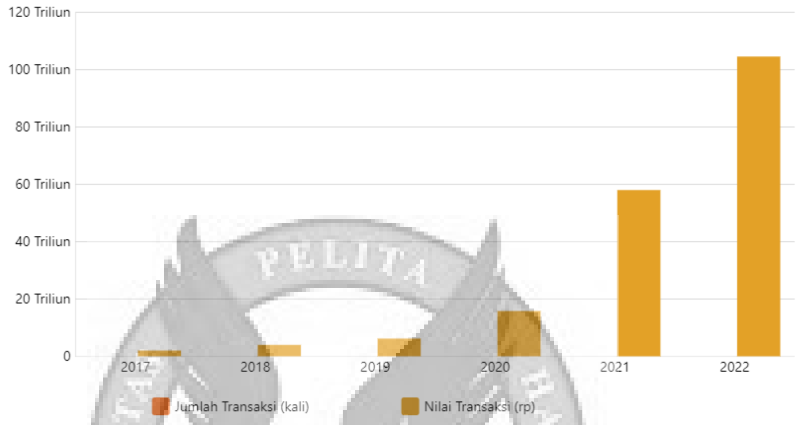
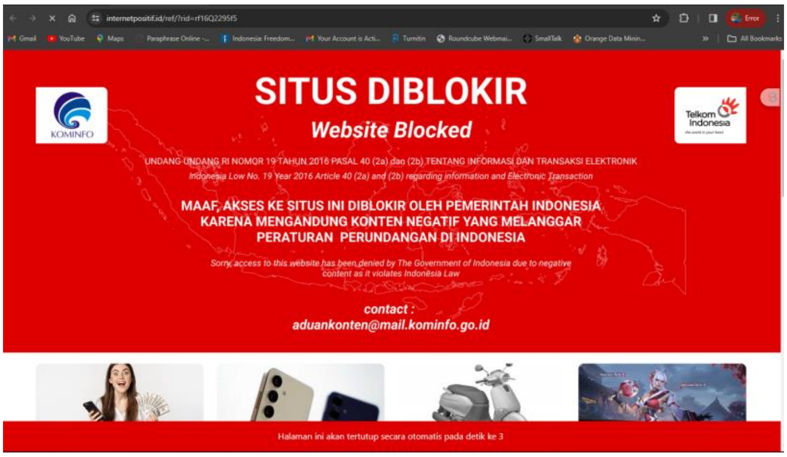


Figure 1. 2 Number and Value of Online Gambling Transactions in Indonesia per Year (2017-2022)

Figure 1.2 presents a bar graph depicting the number and value of online gambling transactions in Indonesia from 2017 through 2022. The graph uses two sets of bars to represent the data; the darker bars indicate the number of transactions (counted in occurrences), while the lighter bars represent the value of these transactions (in Indonesian Rupiah). Over the six-year span, there's a notable upward trend in both the number and value of transactions. The year 2022 shows a significant spike, indicating a steep increase in the value of transactions compared to previous years.

The Ministry of Communication and Information declared an online gambling emergency and blocked nearly 800 thousand online gambling contents, the online gambling mafia switched to utilizing government-owned domains (go.id) and academic sites because the site address would not be blocked by Kominfo (KOMINFO, n.d.)



SITUS DIBLOKIR

Website Blocked

UNDANG-UNDANG RI NOMOR 19 TAHUN 2016 PASAL 40 (2a) dan (2b) TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK
Indonesia Low No. 19 Year 2016 Article 40 (2a) and (2b) regarding information and Electronic Transaction

MAAF, AKSES KE SITUS INI DIBLOKIR OLEH PEMERINTAH INDONESIA KARENA MENGANDUNG KONTEN NEGATIF YANG MELANGGAR PERATURAN PERUNDANGAN DI INDONESIA

Sorry, access to this website has been denied by The Government of Indonesia due to negative content as it violates Indonesia Law

contact :
aduankonten@mail.kominfo.go.id

Halaman ini akan tertutup secara otomatis pada detik ke 3

Figure 1. 3 *Web*site that has been infiltrated with online gambling content

The figure 1.3 shows a web page indicating that access to the site has been blocked by the government of Indonesia due to the presence of negative content that violates Indonesian regulations. The blocking notice is prominent, with the text "SITUS DIBLOKIR" and "Website Blocked" in large, bold letters. The message apologizes for the inconvenience and explains that the site contains content that is considered negative according to local laws. There is a contact email provided for inquiries or complaints, suggesting a channel for communication regarding the block.

According to the data, there are 3 million government sites infiltrated by online gambling and 1.2 million online gambling *web* pages are also infiltrated into academic sites. Online gamblers have developed a Trojan-type malicious software (malware) that acts like an 'uninvited visitor' (dmi, n.d.). This Trojan takes over the system and uses it to promote online gambling content through compromised *web*sites and change the appearance of *web*sites containing online gambling content, which is often called *web* defacement. This is a serious threat to Indonesia as online gambling attacks on government and academic *web*sites can cause significant losses to both the government, academic institutions, and the public such as the cost of repairing system damage the cost of replacing lost or stolen data and the cost of paying and can cause disruption to the services provided by government and academic *web*sites by government and academic *web*sites academic activities, such as the learning process, research.

This research focuses on handling online gambling defacement incidents using the National Institute of Standards and Technology (NIST) SP 800-61 Rev 2 standard. Particular emphasis is given to the detection and analysis phase, involving server log retrieval, malware scanning with Thor Lite Scanner, and malware sample analysis using static, dynamic, hybrid, code, and function analysis, as well as entropy analysis methods. The eradication step includes lessons learned from the incident to prevent similar occurrences in the future, implementing the Apache *Web* Application Firewall.

1.2. Problem Identification

The primary issue identified is the widespread anomalous attacks on the *web*sites of the Southeast Minahasa Regency government, where several servers have been infected by trojan backdoors. This infection allows for the persistent insertion of online gambling content, meaning that even if this content is removed, it reappears on the server.

1.3. Limitations of The Study

a. This research only focuses on online gambling trojans identified on the *web*site of the Minahasa Tenggara Regency Government.

b. The object of the research is the data of the Virtual Private Server (VPS) server which has installed the attendance application and is infiltrated with online gambling trojan content.

c. Log analysis and trojan classification will only identify and evaluate attack anomalies based on logs and create attack clustering in the 2023 server log sample.

d. This research will only analyse the types of trojans found on servers that are infiltrated with trojans and will not analyse other types of malware.

e. The analysis will only focus on the unique characteristics of each type of trojan and its potential impact on applications and servers.

f. The tools used for trojan analysis are only Thor Lite Scanner, Event Log Analyser, YARA Rules, IDA Pro, VirusTotal.com, and Hybrid-Analysis.com, and no other tools are used.

g. This research will test the effectiveness of using Apache *Web* Application Firewall (WAF) using Acunetix, Berp Suite, and Zed Attack Proxy (ZAP) tools.

h. In malware analysis, there are generally eight methods used to understand the behaviour, characteristics, and impact of malware on systems and networks. These methods are crucial for conducting effective malware forensic analysis, which involves the systematic examination of malware samples. However, in this research, only specific methods will be discussed, namely Static Analysis, Dynamic Analysis, Code Reverse Engineering, Malware Forensic Analysis, and Malware Signature Extraction. Other methods, such as Network Analysis, Memory Forensics, Timeline Analysis, and Data Recovery and Artifact Analysis, will not be elaborated upon.

- Static Analysis involves examining the structure, code, and metadata of a malware sample without executing it. This includes analyzing file headers, strings, embedded resources, and assembly code.

  Techniques: File analysis tools, disassemblers, hex editors, and static code analysis.

- Dynamic Analysis involves executing malware samples in a controlled environment, such as a virtual machine or sandbox, to observe their behaviour and interactions with the system.

  Techniques: Sandboxing, behaviour analysis tools, monitoring system calls, and network traffic.

- Code Reverse Engineering I will schedule some time for us to connect. Cross code reference involves analyzing and understanding the functionality of malware code, including its logic, algorithms, and encryption methods.

  Techniques: Disassembly, decompilation, debugging, and code tracing.

- Malware Signature Extraction involves identifying unique patterns or signatures within malware samples that can be used to detect and classify them.

  Techniques: Signature-based detection, YARA rules, and pattern matching algorithms.

which include Network Analysis, Memory Forensics, Timeline Analysis, and Data Recovery and Artifact Analysis, will not be conducted in this research. This decision is based on specific considerations related to resources, time, or a more specific research focus on the key elements mentioned. Nevertheless, the selected techniques and elements still provide a solid foundation for forensic analysis of malware, allowing for thorough identification and understanding of the researched malware samples.

i. This research will only conduct a trial of the Apache *Web* Application Firewall (WAF) plugin in countering attack anomalies on the server.

1.4. Problem Statement

a. This research investigates the problem of online gambling trojans targeting government *web*sites, specifically focusing on the case of the Minahasa Tenggara Regency Government *web*site.

b. Limited research exists on the specific methods and impacts of online gambling trojans targeting government *web*sites, especially in the context of Indonesia.

c. Therefore, this research aims to answer the following questions:

d. What types of online gambling trojans have infiltrated the Minahasa Tenggara Regency Government *web*site?

e. What are the unique characteristics and potential impacts of these trojans on the *web*site's applications and servers?

f. Can existing tools and methodologies effectively detect and analyse these trojans in the context of government *web*sites?

g. Is the Apache *Web* Application Firewall (WAF) effective in mitigating the identified attack anomalies caused by these trojans?

h. By addressing these questions, this research aims to contribute to a better understanding of the specific threats posed by online gambling trojans to government *web*sites, and to develop effective detection, analysis, and mitigation strategies.

1.5. Research Purpose

The primary purpose of this research is to :

- Addressing Online Gambling Trojan Issue, Specifically tackle the issue of online gambling trojans targeting government and academic websites in Indonesia, focusing on the forensic examination of the Minahasa Tenggara Regency Government website following a Trojan backdoor attack.
- Deepening Understanding of Attacks, deepening understanding of the scope, entry points, characteristics, origins, and impacts of this malicious software to contribute to the development of more effective cybersecurity defences.
- Evaluating Apache Web Application Firewall (WAF). Assess the effectiveness of the Apache Web Application Firewall (WAF) in preventing future infiltrations and defacements, thereby offering valuable insights to improve security protocols against similar cyber threats.
- Contributing to Cybersecurity.

  The primary goal is not only to mitigate the direct threats posed by online gambling trojans but also to enhance the overall resilience of government and academic institutions' digital infrastructures against a broad range of cybersecurity challenges.

The flowchart in Figure 1. 4 below depicts a structured research process that begins with the identification of a specific problem and concludes with an overall enhancement of cybersecurity, through a series of interconnected steps.

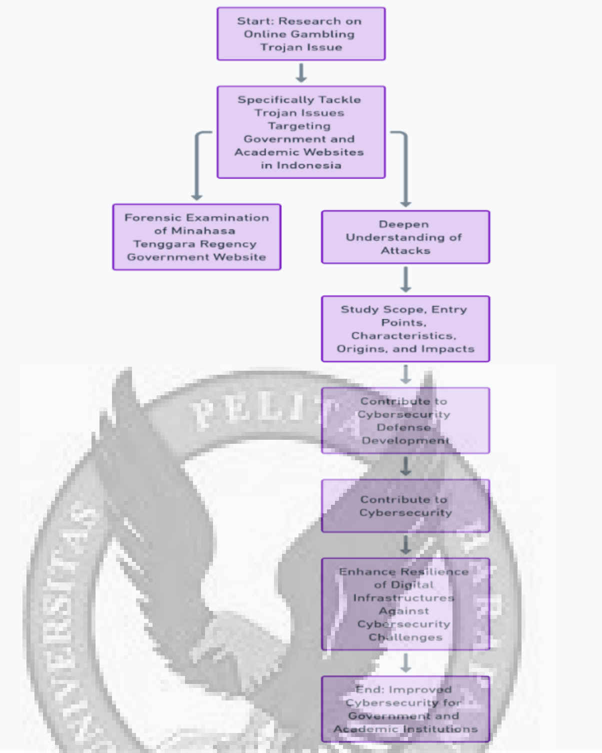

Start: Research on Online Gambling Trojan Issue
Specifically Tackle Trojan Issues Targeting Government and Academic Websites in Indonesia
Forensic Examination of Minahasa Tenggara Regency Government Website
Deepen Understanding of Attacks
Study Scope, Entry Points, Characteristics, Origins, and Impacts
Contribute to Cybersecurity Defense Development
Contribute to Cybersecurity
Enhance Resilience of Digital Infrastructures Against Cybersecurity Challenges
End: Improved Cybersecurity for Government and Academic Institutions

Figure 1. 5 Research Flowchart on the Issue of Online Gambling Trojans Targeting Government and Academic Websites in Indonesia

1.6. Research Objectives

- Classifying I will schedule some time for us to connect. Clustering types of attacks on servers by analyzing server logs to identify specific attack patterns.
- Identifying MD5 Hashes and Distribution of Malware files and Score

- Identifying and analyzing online gambling trojans targeting servers, focusing on their distribution methods and impact on system security.
- Conducting malware analysis using Static Analysis, Dynamic Analysis, Hybrid Analysis, Reference Analysis, and Entropy Analysis techniques to understand their behaviours and dissemination strategies.
- Evaluating the effectiveness of Apache *Web* Application Firewall (WAF) in mitigating online gambling attacks through a series of penetration tests designed to assess the system's resilience to such attacks.

Figure 1.5 below Cybersecurity is Analysis Process Flowchart. This figure illustrates the steps taken in analyzing and responding to security threats on server systems, culminating in the evaluation of the Apache Web Application Firewall's effectiveness.

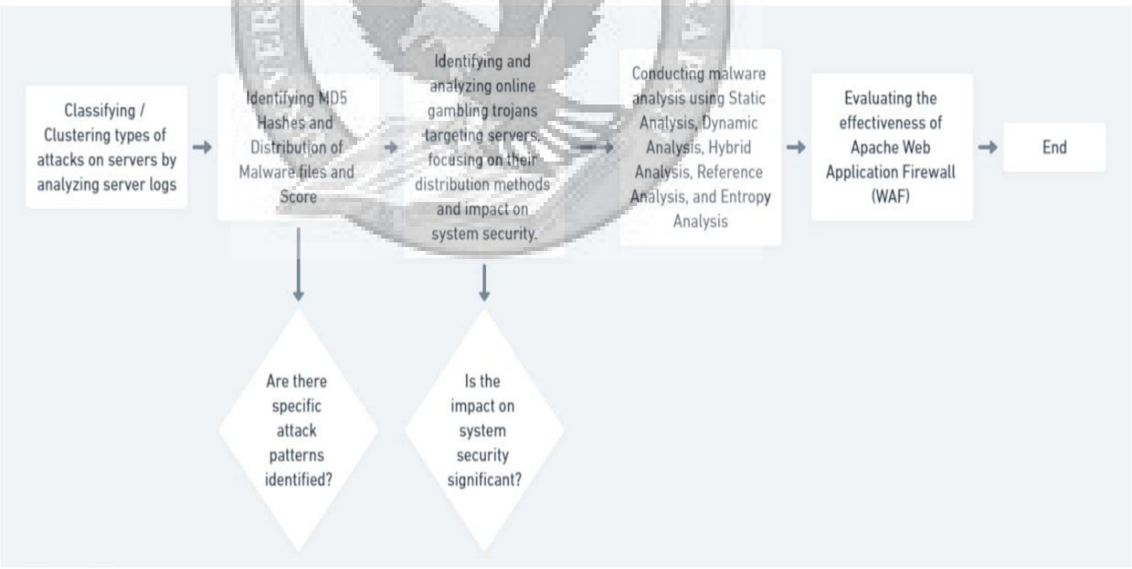

Classifying / Clustering types of attacks on servers by analyzing server logs
Identifying MD5 Hashes and Distribution of Malware files and Score
Identifying and analyzing online gambling trojans targeting servers, focusing on their distribution methods and impact on system security.
Conducting malware analysis using Static Analysis, Dynamic Analysis, Hybrid Analysis, Reference Analysis, and Entropy Analysis
Evaluating the effectiveness of Apache Web Application Firewall (WAF)
End
Are there specific attack patterns identified?
Is the impact on system security significant?

Figure 1. 6 Research Objectives Flowchart

1.7. Writing Structure

CHAPTER I INTRODUCTION

The introduction sets the stage for the study by outlining the increasing significance of cybersecurity in the face of evolving threats. It identifies specific challenges within malware detection and analysis, delineating the scope and acknowledging the limitations inherent in the research. The problem statement clarifies the gap in existing methodologies for detecting and analyzing malware, leading to the articulation of the study's purpose and objectives. This chapter aims to establish a clear foundation for the research, highlighting its relevance and the anticipated contribution to the field of cybersecurity.

CHAPTER II LITERATURE STUDY

This chapter delves into a comprehensive review of existing literature on malware analysis techniques and cybersecurity threats, including log analysis, static, dynamic, and hybrid malware analysis methods. It evaluates various tools and approaches, such as Thor Lite Scanner, Event Log Analyser, and YARA Rules, among others, for their effectiveness in identifying and analyzing malware. The discussion extends to specific cybersecurity threats like SQL injection, cross-site scripting, and others, providing a critical analysis of current methodologies and identifying gaps that the current research aims to address.

CHAPTER III RESEARCH METHODOLOGY

The methodology chapter outlines the systematic approach taken in this research, from data collection through various malware samples and log files to the detailed analysis using selected tools and techniques. It describes the stage methodology, including the use of tools like Thor Lite Scanner, IDA Pro, and online platforms such as VirusTotal.com and Hybrid-Analysis.com for malware analysis. The chapter also explains the rationale behind choosing specific analytical methods for log analysis, static, dynamic, and hybrid analysis, as well as entropy analysis and penetration testing, ensuring a comprehensive approach to understanding and combating cybersecurity threats.

CHAPTER IV RESULTS AND DISCUSSION

In this chapter, the results of the malware distribution analysis and the clustering of attack types through server log analysis are presented. It offers an in-depth examination of the findings from static, dynamic, and hybrid analyses of various malware samples, discussing the implications of these results in the context of the literature reviewed in Chapter II. The discussion provides insights into the effectiveness of the employed methodologies, the characteristics of the analysed malware, and the patterns of cyberattacks, contributing valuable knowledge to the field of cybersecurity and malware analysis.

CHAPTER V CONCLUSION AND RECOMMENDATION

The final chapter synthesizes the research findings, underscoring the study's contributions to improving malware detection and analysis methodologies. It draws conclusions from the research, reflecting on the significance of the results for cybersecurity practices. Recommendations for practitioners are provided, suggesting actionable strategies based on the study's outcomes.