ABSTRACT

Marthen Amelius Solang (01671220002)

ANALYSIS OF ONLINE GAMBLING TROJAN BACKDOOR ATTACKS TO AID WEB SERVER STRENGTHENING, A CASE STUDY INSIGHTS ON SOUTHEAST MINAHASA REGENCY

(xix + 258 pages, 102 figures, 28 tables, 3 attachments)

From 2017 to 2022, Indonesia recorded 157 million online gambling transactions valued at Rp190 trillion. In response, the Indonesian Ministry of Communication and Information Technology blocked nearly 800,000 gambling sites by the end of 2023. However, this countermeasure led to an escalation of cybersecurity threats, with hackers increasingly targeting government and academic domains. They exploited government (.go.id) and academic (ac.id) domains, which were not blocked by the ministry's policies, to disseminate online gambling content. Consequently, over 3 million government *web*sites and 1.2 million academic sites were compromised with gambling content. The government *web*site of Southeast Minahasa Regency was also affected, with gambling content spreading through trojan backdoor *web* shell malware attacks. Hackers exploited *web*site vulnerabilities using methods such as cross-site scripting (XSS), SQL Injection, Directory Traversal, and malicious URLs to attack the target applications. Once successful, they inserted a trojan into the server, taking control as if they were the server administrators.

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.

This research provides evidence that the Apache *Web* Application Firewall (WAF) is highly effective in blocking penetration attempts, demonstrating its significant capability in reducing anomalies and filtering dangerous traffic. Furthermore, Apache WAF proves to be effective in preventing the majority of infiltration attacks, solidifying its position as a reliable *web* security solution. Overall, these findings affirm the effectiveness of Apache WAF as a robust and efficient tool for *web* security.

Keywords: Trojan Backdoor Attack, Cybersecurity, Apache *Web* Application Firewall, Online Gambling Defacement, Malware Analysis, Southeast Minahasa Regency *Web*site

ABSTRAK

Marthen Amelius Solang (01671220002)
Analisis Serangan Trojan Backdoor Judi Online, Untuk Memperkuat Keamanan Web Server, Studi Kasus di Kabupaten Minahasa Tenggara.

(xix + 258 halaman, 102 gambar, 28 tabel 3 lampiran)

Dari tahun 2017 hingga 2022, Indonesia mencatat 157 juta transaksi perjudian online senilai Rp190 triliun. Menanggapi hal ini, Kementerian Komunikasi dan Informatika Indonesia memblokir hampir 800.000 situs perjudian pada akhir tahun 2023. Namun, tindakan pemblokiran tersebut menyebabkan eskalasi ancaman keamanan siber, dimana para peretas yang semakin menargetkan domain pemerintah dan akademik. Mereka mengeksploitasi domain pemerintah (.go.id) dan akademis (ac.id), karena doaian tersebut tidak diblokir oleh kebijakan kementerian, untuk menyebarkan konten perjudian online. Akibatnya, lebih dari 3 juta situs pemerintah dan 1,2 juta situs akademik disusupi konten perjudian. Situs *web* pemerintah Kabupaten Minahasa Tenggara juga terkena dampaknya, dengan konten perjudian yang menyebar melalui serangan *malware* trojan *backdoor web shell*. Peretas mengeksploitasi kerentanan situs *web* menggunakan metode seperti *cross-site scripting* (XSS), SQL *Injection*, *Directory Traversal*, dan URL berbahaya untuk menyerang aplikasi target. Setelah berhasil, mereka memasukkan trojan ke dalam *server*, mengambil kendali seolah-olah mereka adalah administrator *server*.

Penelitian ini berfokus pada penanganan insiden perusakan perjudian *online* dengan menggunakan standar *National Institute of Standards and Technology* (NIST) SP 800-61 Rev 2. Penekanan khusus diberikan pada tahap deteksi dan analisis, yang melibatkan pengambilan log *server*, pemindaian *malware* dengan Thor Lite Scanner, dan analisis sampel *malware* menggunakan analisa statis, analisa dinamis, Analisa hibrid, kode dan fungsi, serta metode analisis entropi. Langkah pemberantasan meliputi pelajaran yang didapat dari kejadian tersebut untuk mencegah kejadian serupa di masa depan, dengan mengimplementasikan Apache *Web* Application Firewall.

Penelitian ini memberikan bukti bahwa Apache *Web* Application Firewall (WAF) sangat efektif dalam memblokir upaya penetrasi, menunjukkan kemampuannya yang signifikan dalam mengurangi anomali dan memfilter trafik yang berbahaya. Selain itu, Apache WAF terbukti efektif dalam mencegah sebagian besar serangan penyusupan, memperkuat posisinya sebagai solusi keamanan *web* yang andal. Secara keseluruhan, temuan ini menegaskan keefektifan Apache WAF sebagai alat yang kuat dan efisien untuk keamanan *web*.

Kata kunci: Trojan Backdoor Attack, Keamanan Siber, Apache *Web* Application Firewall, *Defacement* Perjudian *Online*, Analisis Malware, Situs *Web* Kabupaten Minahasa Tenggara.