INTISARI

Meningkatnya penggunaan teknologi informasi telah menyebabkan meningkatnya kejahatan dunia maya, yang biasa disebut dengan serangan siber salah satunya adalah malware xinchao. Malware adalah perangkat lunak yang dibuat dengan niat jahat untuk menyusup ke dalam suatu sistem dan melakukan berbagai tindakan yang merugikan pemiliknya. Dampak negatif yang disebabkan oleh malware dapat bervariasi, mulai dari mengurangi kinerja sistem hingga merusak atau bahkan menghancurkan data penting yang disimpan dalam sistem. Berdasarkan masalah tersebut peneliti melakukan proses analisis terhadap malware menggunakan teknik reverse engineering untuk mengidentifikasi dan memahami perilaku malware tersebut pada mesin virtual tertutup. Dalam penelitian ini system operasi windows 10 tidak terinfeksi oleh malware xinchao. Teknik reverse engineering efektif karena untuk membongkar dan memahami struktur malware daripada analisis statis. Saran yang dapat diberikan untuk penelitian selanjutnya yaitu analisis malware menggunakan teknik reverse engineering dapat dilakukan menggunakan tools seperti IDApro agar lebih banyak fitur dan informasi yang diektrak dari malware.

Kata kunci: Malware, Reverse engineering, Analisis

ABSTRACT

The increasing use of information technology has led to an increase in cybercrime, commonly referred to as cyber attacks, one of which is the xinchao malware. Malware is software created with malicious intent to infiltrate a system and carry out various actions that are detrimental to its owner. The negative impacts caused by malware can vary, from reducing system performance to damaging or even destroying important data stored in the system. Based on this problem, researchers carried out an analysis process for malware using reverse engineering techniques to identify and understand the behavior of the malware on closed virtual machines. In this research, the Windows 10 operating system running in VirtualBox was not infected by the Xinchao malware. Reverse engineering techniques are effective because they dismantle and understand the structure of malware rather than static analysis. Suggestions that can be given for further research are that malware analysis using reverse engineering techniques can be carried out using tools such as IDApro so that more features and information can be extracted from the malware.

Keywords: Malware, Reverse engineering, Analysis