INTISARI

Implementasi *Indicators of Compromise* (IOCs) sebagai Sarana Respon Insiden dengan Proses *Disassembly*

Kejahatan siber telah ada sejak dahulu dengan berbagai jenis upaya yang dilakukan terhadap target untuk memperoleh keuntungan. Salah satunya *malware* berupa *file* berbahaya yang telah diprogram guna mencuri data hingga merusak perangkat pengguna. Penyebaran *malware* dapat berasal dari berbagai arah seperti tautan atau dokumen yang dikirimkan melalui *email*, ataupun melalui unduhan aplikasi yang telah disisipkan suatu *malware* tertentu. Kelalaian pengguna dalam berinternet dapat menyebabkan sistem hingga jaringan terinfeksi oleh *malware* dan meningkatkan resiko kerugian. Dalam menghadapi persoalan tersebut perlu untuk melakukan analisis *malware* dengan mengidentifikasi *Indicators of Compromise* serta memahami *malware* secara mendalam yang berguna bagi tim respon insiden. *Indicator of Compromise* adalah proses pengumpulan bukti dan petunjuk digital dari insiden yang terjadi. Penelitian ini akan menggunakan *Ransomware WannaCry* sebagai sampel *malware* dan *sandbox virtual environment* yang meliputi Flare VM dan Remnux VM untuk melakukan analisis sampel secara terisolasi tanpa mempengaruhi *server host*. Analisis *malware* akan dilakukan dengan teknik statis yang berfokus pada *Indicators of Compromise* dengan mencakup *file name, string, hash, file type, file size* dan data *PE file header*. Selain itu, dilakukan analisis *malware* secara *disassembly* untuk memperoleh informasi secara detail terkait cara kerja *malware* dan penggunaannya dalam menyerang sistem dengan menggunakan alat Ghidra. Hasil analisis DLL yang terdiri dari satu fungsi user32.dll, 10 fungsi advapi32.dll, 49 fungsi msvrt.dll dan 54 fungsi kernel32.dll mengungkapkan bahwa *malware* menerapkan fungsi dan prosedur untuk beriteraksi dengan sistem operasi *windows* menggunakan standar fungsi perpustakaan C untuk mengendalikan dan merespon tindakan pengguna serta memperoleh *file* tersembunyi pada kode program melalui *reverse engineering* dengan *ratio* sebesar 98.06%.

Kata Kunci: *Malware*, *Ransomware WannaCry*, *Static Analysis, Indicators of Compromise, Disassembly*

ABSTRACT

Indicators of Compromise (IOCs) Implementation as An Incident Response Tool with Disassembly Process

Cybercrime has existed for a long time with various types of efforts carried out against targets to gain profit. One of them is malware in the form of malicious files that have been programmed to steal data and damage the user's device. The spread of malware can come from various directions, such as links or documents sent via email, or through downloading applications that have certain malware inserted. User negligence when surfing the internet can cause the system and network to be infected by malware and increase the risk of loss. In dealing with this problem, it is necessary to carry out malware analysis by identifying Indicators of Compromise and understanding malware in depth which is useful for the incident response team. Indicator of Compromise is the process of collecting digital evidence and clues from incidents that occur. This research will use the WannaCry Ransomware as a malware sample and a virtual sandbox environment including Flare VM and Remnux VM to carry out isolated sample analysis without affecting the host server. Malware analysis will be carried out using static techniques that focus on Indicators of Compromise including file name, string, hash, file type, file size and PE file header data. In addition, malware disassembly analysis was carried out to obtain detailed information regarding how malware works and its use in attacking systems using the Ghidra tool. The results of the DLL analysis consisting of one user32.dll function, 10 advapi32.dll functions, 49 msvrt.dll functions and 54 kernel32.dll functions reveal that the malware implements functions and procedures to interact with the Windows operating system using standard C library functions to control and respond to user actions and obtain hidden files in program code through reverse engineering with a ratio of 98.06%.

Keywords: *Malware, Ransomware WannaCry, Static Analysis, Indicators of Compromise, Disassembly*