Analisis malware dengan metode dinamis runtime dalam sistem operasi windows 10 = Malware analysis with dynamic runtime analysis methods on windows 10 operating system

Aldi Burhanhamali, author

Abstrak

ABSTRAK
Internet dan komunikasi antar jaringan yang saat ini telah menjadi kebutuhan bagi banyak orang. Salah satu bentuk serangan keamanan komputer adalah malware. Malware (Malicious Software), merupakan perangkat lunak yang dibuat untuk atau dengan maksud dan tujuan merugikan orang lain. Malware Analysis Metode Dinamis merupakan analisis yang dilakukan terhadap malware untuk mengetahui maksud dari fungsionalitas dari suatu malware, mengetahui jenis malware, mengetahui bagaimana malware dapat tersebar, apa saja yang dapat diinfeksi oleh malware dengan mempersiapkan lingkungan khusus untuk eksekusi. Berdasarkan Threat Severity Assesstment oleh Symantec Parameter menentukan tingkat ancaman adalah sejauh mana malware berada di dunia (in-the-wild), kerusakan yang malware sebabkan jika ditemukan, dan bagaimana malware bisa menyebar di sistem. Sampel malware yang dieksekusi di dalam sistem sebanyak 17 sampel secara bergantian. Dua lingkungan virtual dibuat untuk membandingkan proses injeksinya pada sistem dengan koneksi internet dan tanpa internet. Perangkat lunak yang digunakan untuk memonitor malware adalah Regshot, Process Monitor, Autoruns, Process Explorer, TCPView, Capture BAT, Wireshark dan FakeDNS. Windows 10 mampu mengenali seluruh sampel sebagai program berbahaya. Namun hanya enam (35%) sampel yang saat berjalan mampu dihentikan Windows Defender. Lima (29%) sampel membutuhkan koneksi internet agar fungsi malware berjalan sesuai dengan jenisnya. Dari 17 sampel yang dieksekusi hanya menghasilkan 3 tingkat kategori ancaman. Enam (35%) sampel berada pada tingkat ancaman Menengah. Tiga (12%) sampel diidentifikasi sebagai kategori ancaman Rendah dan 53% lainnya dikategorikan sebagai Sangat Rendah.
<hr>
ABSTRACT
Internet and communication between networks today, has become a necessity for many people and can also threaten other people's personal or company data at the same time. Malware Malicious Software is a software created with the purpose and intent of harming others. Dynamic Malware Analysis Method is an analysis of the malware determine the intent of the functionality of the malware, knowing the type of malware, how malware spreads, anything that can be infected, by preparing special environment for execution. Based on Threat Severity Assessment by Symantec, the parameter that determines the threat level is the wild which measures to the extent in which virus is already spreading among computers, the damage which measures the amount of damage that a given infection could inflict and the distribution which measures how quickly a program spreads itself. Samples of malware that was executed are 17 samples. Two virtualization was created to compare the process on the system with an internet and without an internet. The monitoring software is Regshot, Process Monitor, Autoruns, Process Explorer, TCPView, Capture BAT, Wireshark and fakeDNS. Windows 10 recognized all samples as malware. However, six (35%) samples were terminated by Windows Defender after malware execution. Five (29%) samples require an internet in

order to perform the function as the malware type. From all samples that were executed, the result has three levels of The Threat level categories. Six (35%) samples are at Moderate Level. Three (12%) samples as Low Threat and another 53% are categorized as Very Low;;