SCARECROW: scalable malware reporting, detection and analysis

ABSTRACT

Malware is the main computer security threat that can cause damage to user's devices and company's infrastructure. End users who want to download executable files from the Internet are currently presented by a binary choice (OK or Cancel) but there is no viable third alternative for uncertainty (Not Sure). Reporting to any security agency or company for status inquiry regarding executable files normally lack of efficiency in terms of reporting back to the users in a timely manner. As a consequence, developing a more efficient approach that provide a prompt response to the users on reported suspicious files is important in order to encourage more end users engagement in malware reporting thus ultimately reducing the number of unknown malware in the wild. This study proposes a new automatic and scalable malware analyzer that is able to quickly scrutinize and help generate report for each malware detected. The implementation of the approach includes both the client (user's system) and the backend processing (security agency). The client side provides a user friendly and integrated reporting mechanism. The backend is based on both static and dynamic analysis for comprehensive malware detection and profiling. The backend utilizes cloud computing infrastructure to scale, speed up and automate the overall analysis and feedback processes. The system provides a win-win situation for both end user and security agency by providing sustainable and successful symbiotic anti-malware eco-system.

Keyword: Malware; Malware analysis; Virtual machines; Cloud computing; Scalability