# ỨNG DỤNG SANDBOX PHÂN TÍCH MÃ ĐỘC TRÊN MÔI TRƯỜNG PHÂN TÁN

*APPLYING SANDBOX TO MALWARE ANALYSIS IN A DISTRIBUTED ENVIRONMENT*

Tác giả: *Nguyễn Tấn Khôi*, *Trần Thanh Liêm*

Tóm tắt bằng tiếng Việt:

Hiện nay, mã độc phát sinh ngày càng nhiều và càng tinh vi, khó phát hiện. Việc phân tích theo cách truyền thống là không khả thi, do đó cần có các kỹ thuật hiệu quả để phát hiện và phân tích mã độc. Để phân tích lượng mã độc lớn, ta có thể phát triển một hệ thống phân tích mã độc động sử dụng kỹ thuật sandbox tạo ra môi trường an toàn. Hệ thống này tự động thực thi một chương trình dựa trên môi trường phân tán và cho kết quả báo cáo mô tả các hành vi của chương trình. Bài báo trình bày hướng nghiên cứu và xây dựng hệ thống sandbox trên môi trường phân tán MapReduce nhằm tự động phân tích các hành vi của mã độc. Giải pháp đề xuất cho phép giảm thời gian phân tích và phát hiện chính xác mã độc.

*Từ khóa: sandbox; tính toán; song song; mã độc; phân tán; mạng; an toàn; bảo mật*

Tóm tắt bằng tiếng Anh:

Nowadays, the number of malware programs has increased more and more, appearing to be more sophisticated and difficult to detect. The traditional way for analyzing these programs is no longer feasible; therefore, it is necessary to have effective techniques for detecting and analyzing malware. To analyze large quantities of malware, we can develop a dynamic malware analysis system using Sandbox technology, thereby creating a safe environment. This system automatically executes a program based on a distributed environment and produces a report describing the program's behaviours. This paper presents an approach to research and construct a sandbox system in the distributed environment of apReduce for the automatic analysis of malware behaviours. The proposed solution makes it possible to reduce the time for the analysis and to accurately detect malware.

*Key words: sandbox; calculation; parallel; malware; distributed; network; safety; security*