Phòng chống mối nguy hại tiềm ẩn với công nghệ Data Sanitization

Ngô Minh Nhựt
Khoa Công nghệ Thông tin
Trường Đại học Khoa học Tự nhiên, ĐHQG-HCM
nmnhut@fit.hcmus.edu.vn

Tóm tắt

Các phần mềm diệt virus truyền thống phòng chống các mối nguy hại máy tính bằng cách ngăn chặn hoặc xóa những tập tin bị nhiễm mã độc, chủ yếu dựa vào định danh của virus. Mối nguy hại tiềm ẩn và các khai thác lỗ hổng zero-day ngày càng phát triển nhanh và thông minh hơn cùng với sự phát triển của Internet. Nhiều loại mã độc được chế tác theo cách thông minh hơn với nội dung biến đổi, khiến cho các chương trình diệt virus truyền thống không thể phát hiện. Bên cạnh đó, cơ sở dữ liệu virus không được cập nhật cũng có thể dẫn tới việc bỏ sót các loại mã độc mới. Hướng tới giải quyết vấn đề này, chúng tôi đề xuất một phương pháp phòng chống mối nguy hại mới với công nghệ Data Sanitization, giúp phòng chống mã độc và bảo vệ người dùng Internet.

Từ khóa: mã độc, lỗ hổng zero-day, data sanitization

Preventing Unknown Threats with Data Sanitization

Nhut Minh Ngo
Faculty of Information Technology, University of Science, VNU-HCM
nmnhut@hcmus.edu.vn

Abstract

Conventional antivirus software prevents threats by blocking or deleting infected files, usually based on virus signatures matching. Unknown threats and zero-day exploits are increasingly developing fast and wisely with the development of the Internet. Many malwares are crafted more sophisticatedly with dynamic content in a way that antivirus software cannot detect. Besides, systems with outdate antivirus database could also not detect malware promptly. Tackling this problem, we introduced a new method of preventing threats with Data Sanitization technology that can help prevent malicious threats and protect Internet users.

Key words: malicious threat, zero-day exploit, data sanitization