Nội dung ôn tập

Môn học: NT230 – Cơ chế hoạt động của mã độc

1. Cấu trúc và nguyên lý hoạt động của tập tin thực thi – PE file
2. Phân loại các loại mã độc phổ biến
3. Các kỹ thuật lây nhiễm (infection) của virus
4. Sâu máy tính – computer worm
5. Botnet
6. Các kỹ thuật nén – mã hóa của mã độc (packed/encrypted virus)
7. Cơ chế tạo biến thể khi lây nhiễm của mã độc (đa hình, dị hình, siêu hình)
8. Các kỹ thuật chống phân tích của mã độc (anti-debug, anti-VM, anti-sandbox)
9. Tấn công tràn bộ nhớ đệm (buffer overflow), tấn công ROP (return oriented programming), khai thác lỗ hổng FormatString

Cập nhật: 23.06.2021