**Khoa an toàn thông tin**

**Môn học: Mật Mã học nâng cao**

**ĐỀ TÀI BÀI TẬP NHÓM**

**XÂY DỰNG LẠI MÃ ĐỘC TỐNG TIỀN RANSOMWARE VÀ DEMO**

Tên thành viên nhóm:

* Nguyễn Khuyến – B13DCAT071
* Nguyễn Đức Thuận – B13DCAT091
* Cao Thị Diệp – B13DCAT053
* Lê Tiến Thành – B13DCAT088
* Nguyễn Ngọc Trường Sơn – B13DCAT119

1. Phân tích cơ chế hoạt động của RANSOMWARE (mã hóa file và tống tiền)
2. Xây dựng kịch bản demo
3. Giấu ransomware vào file doc, pdf, .. đánh lừa nạn nhân là file tài liệu rồi gừi, phát tán qua email, hoặc download (nghiên cứu sâu hơn để có thể qua được các trình diệt virus, scan của gmail,…) .
4. Nạn nhân tải về rồi bật, ransomware được kích hoạt và mã hóa toàn bộ/ một phần tài liệu trong máy nạn nhân.
5. Sau khi mã hóa xong sẽ thay đổi màn hình nền máy tính nạn nhân để thông báo và chứa các hướng dẫn giải mã (thông tin để tống tiền) và gửi các thông tin sinh khóa bí mật dùng cho mã hóa (sử dụng thuật toán AES) đến cho server quản lý (nguyên tắc là không gửi chính xác khóa bí mật lên server).
6. Server có các nhiệm vụ như sau:
   * + Nhận thông tin đăng kí của 1 nạn nhân (lưu khóa bí mật + victimID vào CSDL).
     + Tiếp nhận phương thức thanh toán của nạn nhân (giao diện web) và kiểm tra, nếu thanh toán thành công thì trả về khóa bí mật cho nạn nhân giải mã.
     + Cung cấp phần mềm giải mã cho nạn nhân.
     + Kiểm tra hạn của khóa bí mật, nếu trong 1 khoảng thời gian xác định mà nạn nhân vẫn không đưa tiền chuộc thì có thể cảnh báo hoặc xóa khóa bí mật.
7. Nạn nhân sau khi bị tác động sẽ làm theo hướng dẫn trên màn hình nền để truy cập đến server và tiếp tục làm theo hướng dẫn.
8. Demo