HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN MÔN HỌC

**THỰC TẬP DỰ ÁN CÔNG NGHỆ**

**Đề tài: PHÁT TRIỂN MALWARE ÁP DỤNG TRÍ TUỆ NHÂN TẠO**

Sinh viên thực hiện: LÊ MINH THÁI – AT18N0145

TRẦN NGỌC PHONG – AT18N01343

NGUYỄN MINH PHONG – AT18N0132

TRẦN PHƯỚC AN – AT18N0101

*TP. Hồ Chí Minh, tháng 2 năm 2024*

**Phần I. Giới Thiệu**

Đại dịch Covid-19 xảy ra đã làm cho việc tấn công mạng trở nên phổ biến hơn do nhiều người chuyển sang làm việc, học tập, giải trí trực tuyến, dẫn đến gia tăng số lượng người sử dụng internet và mở rộng diện tích tấn công. Sự gia tăng hoạt động trực tuyến này cùng với những lỗ hổng bảo mật do nhiều doanh nghiệp, cá nhân chưa chú trọng vào việc đầu tư kiến thức, thời gian vào công tác bảo mật hệ thống nên dễ dàng bị dính vào những cạm bẫy của kẻ xấu trên mạng nhằm lừa đảo chiếm đoạt thông tin cùng nhiều tài sản quý giá.

Theo báo cáo của **Cục An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao (A05)**, Bộ Công an, trong năm 2020, đã xảy ra 10.471 vụ việc vi phạm pháp luật về an ninh mạng, tăng 15,7% so với năm 2019. Riêng trong quý 1 năm 2021, đã có 2.945 vụ việc vi phạm pháp luật về an ninh mạng, tăng 12,5% so với cùng kỳ năm 2020.

Theo **BKAV**: Trong năm 2020, Việt Nam ghi nhận hơn 27 triệu lượt tấn công mạng, tăng 25% so với năm 2019. Trong quý 1 năm 2021, đã có hơn 6,5 triệu lượt tấn công mạng vào Việt Nam.

Theo **Kaspersky**: Trong năm 2020, Việt Nam là quốc gia đứng thứ 17 về số lượng mã độc tấn công trên thế giới. Số lượng email lừa đảo liên quan đến Covid-19 tại Việt Nam tăng 350% trong năm 2020.

Hình thức tấn công đa dạng: Tấn công lừa đảo qua email, tin nhắn giả mạo cơ quan chức năng, tổ chức y tế để phát tán mã độc, đánh cắp thông tin cá nhân. Tấn công vào hệ thống mạng của các doanh nghiệp, cơ quan nhà nước để đánh cắp dữ liệu quan trọng. Tăng cường tấn công vào các hệ thống y tế, nghiên cứu khoa học liên quan đến Covid-19.

Tình hình an toàn thông tin trong thời kì dịch Covid-19 diễn ra rất phức tạp và nguy hiểm. Cần có sự chung tay của các cơ quan chức năng, doanh nghiệp và người dân để nâng cao nhận thức, đầu tư vào công tác bảo mật và tăng cường hợp tác quốc tế nhằm bảo vệ an ninh mạng trong thời đại công nghệ số.

**Malware** là viết tắt của **Malicious Software**, hay còn gọi là phần mềm độc hại. Đây là một thuật ngữ chung để chỉ các chương trình hoặc mã độc có khả năng gây hại cho hệ thống máy tính, mạng máy tính hoặc thiết bị di động. Nó đóng vai trò đáng kể trong đại dịch Covid-19, được sử dụng bởi các kẻ tấn công để khai thác tình trạng bất ổn và lo lắng của mọi người.

Những thủ đoạn mà tin tặc sử dụng malware để khai thác thông tin từ người dùng:

- **Email giả mạo**: Kẻ tấn công giả mạo các tổ chức y tế uy tín như WHO hoặc chính phủ để gửi email lừa đảo chứa mã độc.

- **Tin nhắn giả mạo**: Kẻ tấn công gửi tin nhắn giả mạo thông báo về các ca nhiễm Covid-19 hoặc các biện pháp phong tỏa để lừa người dùng tải xuống malware.

- **Trang web giả mạo**: Kẻ tấn công tạo ra các trang web giả mạo trang web của các tổ chức y tế hoặc cơ quan chính phủ để lừa người dùng nhập thông tin cá nhân hoặc tải xuống malware.

Malware là một mối đe dọa lớn trong đại dịch Covid-19. Người dùng cần nâng cao nhận thức về các mối đe dọa malware và thực hiện các biện pháp phòng chống để bảo vệ bản thân và dữ liệu của mình.