HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



ĐỀ CƯƠNG ĐỒ ÁN

**PHÁT TRIỂN MALWARE**

**ÁP DỤNG TRÍ TUỆ NHÂN TẠO**

|  |  |
| --- | --- |
| Giảng viên hướng dẫn: | Thành viên nhóm: |
| ThS Nguyễn Anh Khôi | 1. Trần Phước An AT18N0101 2. Nguyễn Tài Nguyên AT18N0127 3. Nguyễn Minh Phong AT18N0132 4. Trần Ngọc Phong AT18N0134 5. Lê Minh Thái AT18N0145 |

*TP.Hồ Chí Minh, tháng 2 năm 2024*

1. **Thông tin chung**

Sinh viên thực hiện: 1. Trần Phước An

2. Nguyễn Tài Nguyên

3. Nguyễn Minh Phong

4. Trần Ngọc Phong

5. Lê Minh Thái

Giảng viên hướng dẫn: ThS Nguyễn Anh Khôi

Đơn vị công tác: Phân hiệu Học viện Kỹ thuật Mật mã

Đề tài: *Phát triển malware áp dụng trí tuệ nhân tạo*

1. **Đề cương đồ án**
2. **Tính cấp thiết, ý nghĩa thực tiễn của đề tài**

Trong bối cảnh công nghệ thông tin phát triển với tốc độ chóng mặt, mối đe dọa từ các phần mềm độc hại (malware) ngày càng trở nên tinh vi và khó lường. Sự xuất hiện của trí tuệ nhân tạo (AI) đã mở ra một kỷ nguyên mới trong việc phát triển và phòng chống malware. Đề tài "Phát triển Malware áp dụng trí tuệ nhân tạo" không chỉ phản ánh một thách thức lớn trong an ninh mạng mà còn đặt ra một vấn đề cấp bách cần được giải quyết, đó là làm thế nào để bảo vệ hệ thống thông tin trước những mối đe dọa ngày càng thông minh và khó đoán này.

Tính cấp thiết của đề tài này được thể hiện qua việc malware AI có khả năng tự học hỏi và thích nghi với các biện pháp phòng thủ, làm cho việc phát hiện và ngăn chặn chúng trở nên cực kỳ khó khăn. Điều này đòi hỏi cộng đồng an ninh mạng phải không ngừng nâng cao kỹ năng, công nghệ để đối phó với các mối đe dọa mới.

Mục tiêu của đề tài là tạo ra các giải pháp mới sử dụng trí tuệ nhân tạo để phát hiện và ngăn chặn các loại malware nguy hiểm, đồng thời cung cấp sự hiểu biết và công cụ cần thiết để bảo vệ thông tin và dữ liệu cá nhân của người dùng mạng. Kết quả nghiên cứu từ đề tài này không chỉ mang lại lợi ích trong việc nâng cao hiệu suất phòng chống malware mà còn đóng góp vào sự phát triển của công nghệ an ninh mạng, đảm bảo an toàn cho cả cá nhân và tổ chức, góp phần vào sự phát triển bền vững của kinh tế xã hội.

1. **Nhiệm vụ đồ án**

Các nhiệm vụ đặt ra khi thực hiện đồ án bao gồm:

1. Giới thiệu về hiện trạng tấn công mạng hiện nay (lý thuyết)

2. Phát triển malware truyền thống (lý thuyết)

3. Phát triển malware với ChatGPT (lý thuyết)

4. Phát triển malware và yêu cầu ChatGPT phân tích, giải thích (thực hành)"

1. **Dự kiến chương mục**

* Với các nhiệm vụ kể trên, chương mục dự kiến của đề tài bao gồm:

1. Giới thiệu về hiện trạng tấn công mạng hiện nay: Hiểu về hiện trạng tấn công mạng hiện nay, biết được vai trò quan trọng của malware trong các cuộc tấn công, ý nghĩa và tiềm năng của việc áp dụng trí tuệ nhân tạo trong phát triển malware.
2. Phát triển malware truyền thống: Mô tả về quá trình nghiên cứu và phát triển malware theo cách truyền thống qua các bước:
   1. Nghiên cứu và thu thập thông tin
   2. Phát triển và lập trình malware
   3. Lựa chọn kỹ thuật tấn công
   4. Thử nghiệm và điều chỉnh
   5. Triển khai và lan truyền
   6. Che giấu và duy trì truy cập
3. Phát triển malware với ChatGPT: Mô tả quá trình áp dụng trí tuệ nhân tạo vào quá trình phát triển malware, nhằm khai thác tiềm năng của trí tuệ nhân tạo để tạo ra các loại malware nguy hiểm hơn nhiều so với malware truyền thống.
   1. Thu thập dữ liệu
   2. Huấn luyện mô hình AI
   3. Phát triển malware
   4. Thử nghiệm và đánh giá
   5. Triển khai malware
   6. Một số kỹ thuật ẩn mình của malware sử dụng AI
4. Phát triển malware và yêu cầu ChatGPT phân tích, giải thích:
5. **Tài liệu tham khảo để xây dựng đề cương**
6. Marcus Hutchins, *Portable Executable Injection For Beginners*, truy cập ngày 27 tháng 2 năm 2024, <<https://www.malwaretech.com/2013/11/portable-executable-injection-for.html>>.
7. *Getting Started With Malware Development*, truy cập ngày 27 tháng 2 năm 2024, <<https://www.crow.rip/crows-nest/mal/dev/getting-started>>.

|  |  |
| --- | --- |
| **XÁC NHẬN CỦA NGƯỜI HƯỚNG DẪN**  *(Ký, ghi rõ họ tên)* | *TP.HCM, ngày ... tháng ... năm 2024*  **SINH VIÊN LÀM ĐỒ ÁN**  *(Ký, ghi rõ họ tên)* |
|  |  |