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**

|  |  |
| --- | --- |
| 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*

Mục lục

[Lời cảm ơn 2](#_Toc14132)

[Phần I. Giới Thiệu 3](#_Toc3014)

[Phần II. Phát triển malware bằng cách truyền thống 5](#_Toc4383)

[1. Nghiên cứu và thu thập thông tin 5](#_Toc31701)

[2. Phát triển và lập trình malware 5](#_Toc32675)

[3. Chọn lựa kỹ thuật tấn công 6](#_Toc19411)

[i. Kỹ thuật lừa đảo (Social Engineering): 6](#_Toc13862)

[ii. Kỹ thuật khai thác lỗ hổng (Exploit): 6](#_Toc18804)

[iii. Kỹ thuật tấn công chuỗi cung ứng (Supply Chain Attack): 7](#_Toc7141)

[iv. Kỹ thuật tấn công bằng phần mềm độc hại không tệp (Fileless Malware Attack): 7](#_Toc13812)

[4. Thử nghiệm và điều chỉnh 7](#_Toc20568)

[5. Triển khai và lan truyền 7](#_Toc12646)

[6. Che giấu và duy trì truy cập 8](#_Toc32700)

[Phần III. Phát triển malware bằng AI 10](#_Toc31146)

[1. Thu thập dữ liệu 10](#_Toc28860)

[2. Huấn luyện mô hình AI 10](#_Toc25057)

[3. Phát triển malware 10](#_Toc15507)

[4. Thử nghiệm và đánh giá 10](#_Toc20109)

[5. Triển khai malware 10](#_Toc27937)

[6. Một số kỹ thuật ẩn mình của malware sử dụng AI 11](#_Toc9164)

[i. Biến đổi mã 11](#_Toc22729)

[ii. Lẩn tránh các công cụ phân tích 11](#_Toc15945)

[iii. Nhắm mục tiêu tấn công 11](#_Toc4623)

[iv. Tự động hóa 11](#_Toc5339)

[Phân biệt phát triển malware bằng AI và truyền thống: 12](#_Toc12621)

**Lời cảm ơn**

Để hoàn thành báo cáo cuối kỳ đề tài “Phát triển malware áp dụng trí tuệ nhân tạo”, chúng em đã nhận được sự hướng dẫn và giúp đỡ nhiệt tình của các thầy cô, anh/chị và các bạn trong và ngoài khoa.

Trước hết, chúng em xin bày tỏ lòng biết ơn chân thành đến Ban giám đốc cùng quý thầy cô trong khoa An toàn thông tin - Học viện Kỹ thuật Mật Mã đã tận tình dạy dỗ, truyền đạt kiến thức, kinh nghiệm quý báu và tạo điều kiện thuận lợi cho chúng em trong suốt thời gian học tập.

Đặc biệt, chúng em xin chân thành cảm ơn và bày tỏ lòng biết ơn sâu sắc đến thầy Nguyễn Anh Khôi. Thầy đã dành nhiều thời gian vô cùng quý báu để định hướng và tận tình hướng dẫn, giúp đỡ chúng em trong quá trình thực hiện đề tài, để chúng em có thể hoàn thành tốt nhất đề tài của mình.

Chúng em cũng xin chân thành cảm ơn các anh/chị trong khoa và các bạn trong lớp đã giúp đỡ chúng em trong quá trình thực hiện đề tài.

Chúng em xin hứa sẽ cố gắng học tập và nghiên cứu tốt hơn nữa để có thể hoàn thành tốt các nhiệm vụ được giao trong tương lai.

**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.

Các loại malware phổ biến bao gồm virus, trojan, worm, spyware, adware và ransomware. Mỗi loại có tính chất và mục đích khác nhau, ví dụ như virus sẽ tự sao chép và lây lan từ máy tính này sang máy tính khác, trojan sẽ giả mạo thành phần mềm bình thường để xâm nhập vào hệ thống và thực hiện các hành động độc hại, spyware và adware sẽ thu thập thông tin cá nhân của người dùng hoặc hiển thị quảng cáo không mong muốn, ransomware sẽ mã hóa dữ liệu của người dùng và yêu cầu một khoản tiền chuộc để giải mã.

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.

# **Phần II. Phát triển malware bằng cách truyền thống**

Việc phát triển malware truyền thống của tin tặc thường bao gồm các bước sau:

1. **Nghiên cứu và thu thập thông tin**

Kẻ tấn công sẽ tiến hành nghiên cứu về các lỗ hổng bảo mật, cấu trúc mạng, và hệ thống phần mềm của mục tiêu dự kiến. Họ cũng thu thập thông tin về người dùng, các loại phần mềm mà họ sử dụng, và các thông tin khác có thể hữu ích cho việc tấn công. Sau khi thu thập thông tin, xác định loại malware muốn phát triển ( virus, trojan, …) từ đó xác định hướng tấn công.

1. **Phát triển và lập trình malware**

Sau khi có đủ thông tin, kẻ tấn công sẽ bắt đầu phát triển malware. Điều này có thể bao gồm việc viết mã, kiểm thử, và tối ưu hóa các chức năng của malware để đảm bảo hiệu suất và tính ổn định.

**Một số xu hướng phát triển:**

* **Phần mềm độc hại không tệp:** Loại malware này tồn tại trong bộ nhớ hoặc registry của hệ thống, khiến chúng khó phát hiện và loại bỏ hơn so với malware truyền thống. Kẻ tấn công sử dụng các công cụ hợp pháp như PowerShell để thực hiện các hành vi độc hại mà không cần tạo ra các tệp tin.
* **Tấn công ransomware:** Loại tấn công này sử dụng malware để mã hóa dữ liệu của người dùng và yêu cầu tiền chuộc để giải mã. Kẻ tấn công nhắm mục tiêu vào các doanh nghiệp lớn và yêu cầu tiền chuộc cao.
* **Tấn công Supply chain:** Loại tấn công này nhắm vào các nhà cung cấp dịch vụ để lây nhiễm  malware cho nhiều khách hàng của họ. Kẻ tấn công cài đặt malware vào sản phẩm hoặc dịch vụ của nhà cung cấp hoặc tấn công vào hệ thống của nhà cung cấp.
* **Trí tuệ nhân tạo (AI):** Kẻ tấn công sử dụng AI để phát triển malware thông minh hơn và khó phát hiện hơn. AI có thể được sử dụng để tự động hóa các quy trình tấn công, tối ưu hóa hiệu suất của malware và tạo ra các biến thể malware mới.

1. **Chọn lựa kỹ thuật tấn công**

Khi phát triển malware, kẻ tấn công cần quyết định kỹ thuật tấn công nào sẽ được sử dụng để triển khai malware vào hệ thống mục tiêu.

**Các kỹ thuật phổ biến có thể bao gồm:**

1. **Kỹ thuật lừa đảo (Social Engineering):**

* **Mục đích:** Lừa người dùng thực hiện hành động nguy hiểm, chẳng hạn như mở tệp tin đính kèm bị nhiễm malware hoặc cung cấp thông tin đăng nhập.
* **Cách thức:**
  + **Gửi email giả mạo:** Kẻ tấn công giả mạo các tổ chức uy tín để lừa người dùng mở tệp tin đính kèm hoặc nhấp vào liên kết độc hại.
  + **Sử dụng các trang web giả mạo:** Kẻ tấn công tạo ra các trang web giả mạo các trang web hợp pháp để lừa người dùng nhập thông tin cá nhân hoặc tài chính.
  + **Sử dụng các cuộc gọi điện thoại giả mạo:** Kẻ tấn công giả mạo các tổ chức uy tín để lừa người dùng cung cấp thông tin cá nhân hoặc tài chính.

1. **Kỹ thuật khai thác lỗ hổng (Exploit):**

* **Mục đích:** Khai thác các lỗ hổng bảo mật trong hệ thống để cài đặt malware.
* **Cách thức:**
  + **Quét các hệ thống mục tiêu để tìm kiếm các lỗ hổng:** Kẻ tấn công sử dụng các công cụ quét tự động để tìm kiếm các hệ thống có các lỗ hổng bảo mật.
  + **Sử dụng các công cụ khai thác:** Kẻ tấn công sử dụng các công cụ khai thác để khai thác các lỗ hổng bảo mật đã được tìm thấy.

1. **Kỹ thuật tấn công chuỗi cung ứng (Supply Chain Attack):**

* **Mục đích:** Lây nhiễm malware vào các sản phẩm hoặc dịch vụ được cung cấp bởi các nhà cung cấp uy tín.
* **Cách thức:**
  + **Cài đặt malware vào hệ thống của nhà cung cấp:** Kẻ tấn công cài đặt malware vào hệ thống của nhà cung cấp để lây nhiễm malware vào các sản phẩm hoặc dịch vụ của họ.
  + **Cập nhật phần mềm bị nhiễm malware:** Kẻ tấn cung cấp các bản cập nhật phần mềm bị nhiễm malware cho các nhà cung cấp.

1. **Kỹ thuật tấn công bằng phần mềm độc hại không tệp (Fileless Malware Attack):**

* **Mục đích:** Cài đặt malware vào hệ thống mà không cần tạo ra các tệp tin trên ổ đĩa.
* **Cách thức:**
  + **Sử dụng các công cụ hợp pháp:** Kẻ tấn công sử dụng các công cụ hợp pháp như PowerShell để thực hiện các hành vi độc hại mà không cần tạo ra các tệp tin độc hại.
  + **Lưu trữ mã độc hại trong bộ nhớ:** Kẻ tấn lưu trữ mã độc hại trong bộ nhớ của hệ thống, khiến chúng khó bị phát hiện bởi các phần mềm diệt virus dựa trên chữ ký.

1. **Thử nghiệm và điều chỉnh**

Trước khi triển khai, malware thường được thử nghiệm trong môi trường giả lập hoặc môi trường thực tế để đảm bảo tính hiệu quả và không bị phát hiện. Sau đó, kẻ tấn công có thể điều chỉnh và cải tiến malware nếu cần thiết.

1. **Triển khai và lan truyền**

Khi đã hoàn thiện, malware sẽ được triển khai vào mạng hoặc hệ thống mục tiêu thông qua các kênh tấn công đã được chọn. Mục tiêu của kẻ tấn công là để lan truyền malware một cách không bị phát hiện và gây ra tác động tiêu cực cho hệ thống mục tiêu.

**Một số phương thức lây lan:**

* **Email:** Đây là một phương thức phổ biến để lây lan malware. Kẻ tấn công giả mạo hoặc email có chứa tệp tin đính kèm bị nhiễm phần mềm độc hại.
* **Tải xuống phần mềm có nhúng malware**: Phần mềm độc hại có thể được cài đặt khi người dùng tải xuống các tệp tin từ các nguồn không đáng tin cậy.
* **Thiết bị lưu trữ ngoài**: Phần mềm độc hại có thể được lây lan qua các thiết bị lưu trữ ngoài như USB flash drive hoặc ổ cứng ngoài.
* **Lỗ hổng bảo mật**: Kẻ tấn công có thể khai thác các lỗ hổng bảo mật trong hệ điều hành hoặc phần mềm để cài đặt phần mềm độc hại.

1. **Che giấu và duy trì truy cập**

Sau khi malware đã được triển khai, kẻ tấn công có thể sử dụng các kỹ thuật che giấu và duy trì truy cập để tránh bị phát hiện và tiếp tục kiểm soát hệ thống mục tiêu.

**Một số kỹ thuật ẩn mình:**

* **Rootkit:** Rootkit là loại phần mềm độc hại có thể ẩn mình trong hệ thống để tránh bị phát hiện. Rootkit thường được sử dụng để cài đặt các phần mềm độc hại khác hoặc đánh cắp dữ liệu.
* **Polymorphism:** Polymorphism là kỹ thuật thay đổi mã của phần mềm độc hại để tránh bị phát hiện bởi phần mềm diệt virus.
* **FUD (Fully Undetectable):** FUD là loại phần mềm độc hại được thiết kế để không thể bị phát hiện bởi bất kỳ phần mềm diệt virus nào.

Với những bước trên, ta có thể thấy được ưu điểm và nhược điểm của việc tin tặc sử dụng phương pháp phát triển malware truyền thống như sau:

**Ưu điểm:**

* Chi phí phát triển thấp, tin tặc không cần quá nhiều tài nguyên để có thể phát triển ra được một phần mềm độc hại đơn giản.
* Có thể sử dụng các công cụ và kỹ thuật có sẵn để phát triển.
* Khả năng tùy biến theo ý đồ của tin tặc.

**Nhược điểm:**

* Dễ dàng bị phát hiện bởi các phần mềm diệt virus và các công cụ bảo mật khác.
* Khả năng thích ứng với các biện pháp bảo mật tân tiến thấp.
* Khó để tự động hoá các nhiệm vụ phức tạp.

# **Phần III. Phát triển malware bằng AI**

Phát triển malware bằng AI là một lĩnh vực đang phát triển nhanh chóng, với tiềm năng tạo ra các loại malware nguy hiểm hơn nhiều so với malware truyền thống.

1. **Thu thập dữ liệu**

Thu thập dữ liệu về các hệ thống mục tiêu, phần mềm bảo mật, và hành vi của người dùng.

Dữ liệu này có thể được thu thập từ nhiều nguồn khác nhau như internet, mạng xã hội, và các cuộc tấn công mạng.

1. **Huấn luyện mô hình AI**

Sử dụng dữ liệu thu thập được để huấn luyện mô hình AI có khả năng:

* Tạo mã malware mới.
* Lẩn tránh các công cụ phát hiện malware.
* Nhắm mục tiêu các hệ thống cụ thể.

1. **Phát triển malware**

Sử dụng mô hình AI đã được huấn luyện để phát triển malware mới. Malware này có thể được thiết kế để thực hiện nhiều mục đích khác nhau như:

* Đánh cắp dữ liệu.
* Khóa dữ liệu.
* Phá hoại hệ thống.

1. **Thử nghiệm và đánh giá**

Thử nghiệm malware trên các hệ thống mục tiêu để đánh giá hiệu quả của nó. Đánh giá khả năng lẩn tránh các công cụ phát hiện malware và khả năng tấn công các hệ thống mục tiêu.

1. **Triển khai malware**

Triển khai malware trên các hệ thống mục tiêu. Malware có thể được triển khai thông qua nhiều cách khác nhau như:

* Email.
* Các trang web độc hại.
* Các phần mềm bị nhiễm malware.

1. **Một số kỹ thuật ẩn mình của malware sử dụng AI**
2. **Biến đổi mã**

Sử dụng AI để tự động biến đổi mã malware, khiến cho việc phát hiện dựa trên chữ ký trở nên khó khăn.

Ví dụ: Thay đổi tên biến, hàm, hoặc sử dụng các kỹ thuật mã hóa.

1. **Lẩn tránh các công cụ phân tích**

Sử dụng AI để học cách lẩn tránh các công cụ phân tích malware.

Ví dụ: Sử dụng các kỹ thuật che giấu mã, hoặc giả mạo các tập tin hợp pháp.

1. **Nhắm mục tiêu tấn công**

Sử dụng AI để nhắm mục tiêu tấn công chính xác hơn, dựa trên thông tin thu thập về hệ thống mục tiêu.

Ví dụ: Tấn công các hệ thống sử dụng phần mềm bảo mật lỗi thời hoặc có lỗ hổng bảo mật.

1. **Tự động hóa**

Sử dụng AI để tự động hóa các bước phát triển và triển khai malware.

Ví dụ: tự động tạo mã malware, tự động lây nhiễm sang các hệ thống khác.

Dưới đây là một số ví dụ về các công cụ AI có thể được sử dụng để phát triển malware:

* Generative Adversarial Networks (GANs): GANs có thể được sử dụng để tạo mã malware mới có khả năng lẩn tránh các công cụ phát hiện malware dựa trên chữ ký.
* Reinforcement Learning: Reinforcement Learning có thể được sử dụng để huấn luyện malware tự động học hỏi cách tấn công các hệ thống mục tiêu.
* Natural Language Processing (NLP): NLP có thể được sử dụng để phát triển malware có khả năng hiểu và thao túng hành vi của người dùng.

**Phân biệt phát triển malware bằng AI và truyền thống:**

|  |  |  |
| --- | --- | --- |
| Tính năng  Loại malware | Truyền thống | AI |
| Khả năng biến đổi | Thấp | Cao |
| Hiệu quả tấn công | Trung bình | Cao |
| Quy trình phát triển | Thủ công | Tự động |
| Mức độ nguy hiểm | Trung bình | Cao |

Ví dụ:

* DeepLocker: Ransomware sử dụng AI để mã hóa dữ liệu theo cách rất khó giải mã.
* Hidden Arrow: Malware sử dụng AI để ẩn mình trong các tập tin ảnh và video.