BÁO CÁO BÀI TẬP

**Môn học: Cơ chế hoạt động của mã độc**

**Tên chủ đề: Advanced Virus Techniques**

*GVHD: Phan Thế Duy*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.O21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 2 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 3 | Phạm Ngọc Nhung | 21521248 | 21521248@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu a | 100% |
| 2 | Yêu cầu b | 100% |
| 3 | Yêu cầu c | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Tìm hiểu nguyên lý phát hiện sandbox (thí dụ như Cuckoo Sandbox,…). Trình bày ngắn gọn các kỹ thuật nhận diện sandbox để trốn tránh cho mã độc.**
2. **Tìm hiểu nguyên lý phát hiện sandbox:**

* **Sandbox** là một môi trường ảo được sử dụng để phân tích hành vi của phần mềm, đặc biệt là mã độc, trong một môi trường an toàn mà không gây ảnh hưởng đến hệ thống thực. Cuckoo Sandbox là một trong những hệ thống phổ biến để phân tích mã độc. Nguyên lý hoạt động cơ bản của sandbox bao gồm:
  + **Cách ly:** chạy mã trong một môi trường ảo, tách biệt với hệ thống thật.
  + **Giám sát:** Theo dõi và ghi lại mọi hành động của mã độc, bao gồm thao tác với file, registry, mạng và bộ nhớ.
  + **Phân tích:** sử dụng dữ liệu thập được để phân tich và đánh giá hành vi của mã độc.
* Mã độc có thể kiểm tra một số đặc điểm hệ thống để nhận diện nếu nó đang chạy trong môi trường sandbox, ví dụ:
  + **Tên hệ thống**: Sandbox thường có tên hệ thống cụ thể như “Cucko”, “Sandbox”, v.v
  + **File hệ thống và registry**: Nhiều sandbox để lại các dấu hiệu đặc trưng trên hệ thống.
  + **Hoạt động hệ thống**: Sandbox thường mô phỏng hành vi người dùng với một mức độ hạn chế, thiếu sự tương tác thực sự.

1. **Các kỹ thuật nhận diện sandbox để trốn tránh cho mã độc**

Mã độc thường sử dụng nhiều kỹ thuật để phát hiện xem nó có đang chạy trong môi trường sandbox hay không và từ đó thay đổi hành vi của nó nhằm trốn tránh bị phát hiện. Các kỹ thuật này bao gồm:

* **Kiểm tra các tài nguyên hệ thống:**
  + **Tên máy chủ và người dùng:** Kiểm tra tên máy hoặc tên người dùng để phát hiện các tên mặc định thường được sử dụng trong môi trường sandbox.
  + **Phần cứng:** Kiểm tra thông tin phần cứng như số lượng CPU, dung lượng RAM, và các đặc điểm phần cứng khác mà thường có giới hạn môi trường ảo.
* **Kiểm tra sự tương tác của người dùng:** Mã độc có thể kiếm tra xem có sự tương tác của người dùng thực sự hay không (như di chuyển chuột, gõ phím, v.v). Nếu không có sự tương tác, mã độc có thể nghĩ rằng nó đang chạy trong một môi trường sandbox và do đó không thực hiện hành vi độc hại.
* **Kiểm tra thời gian chạy:** Mã độc có thể kiểm tra thời gian chạy của chính nó. Nếu thời gian chạy quá ngắn, mã độc có thể nghĩ rằng nó đang chạy trong một môi trường sandbox và do đó không thực hiện hành vi độc hại.
* **Kiểm tra thời gian hệ thống**: Kiểm tra thời gian hệ thống để phát hiện sự chậm trễ bất thường trong các hoạt động hệ thống, vốn có thể chỉ ra rằng mã đang chạy trong một môi trường ảo bị giám sát.
* **Kiểm tra các tiến trình chạy song song**: Mã độc có thể kiểm tra xem có các tiến trình khác đang chạy song song hay không. Nếu có quá ít tiến trình, mã độc có thể nghĩ rằng nó đang chạy trong một môi trường sandbox và do đó không thực hiện hành vi độc hại.
* **Kiểm tra kết nối mạng**: Xác minh sự tồn tại của các kết nối mạng bất thường hoặc các giao diện mạng ảo thường được sử dụng trong môi trường sandbox.
* **Dò tìm các phần mềm giám sát**: Tìm kiếm các tiến trình, dịch vụ hoặc driver đặc trưng của các công cụ giám sát như Cuckoo Sandbox, VMware Tools, hay VirtualBox Guest Additions.
* **Thay đổi hành vi**:
  + **Trì hoãn hành vi độc hại:** Tạm hoãn các hành vi độc hại trong một khoảng thời gian dài để vượt qua giai đoạn phân tích ngắn hạn của sandbox.
  + **Hành vi có điều kiện:** Chỉ thực hiện hành vi độc hại khi thỏa mãn một số điều kiện nhất định, ví dụ như một tập hợp các file hoặc cấu hình hệ thống cụ thể mà thường không có trong sandbox.

1. **Hiện thực lại mã độc chống phân tích động khả năng nhận biết môi trường (environmental sensivity) (trang bị thêm cho payload ban đầu của các bài tập trước).**

Các nhóm sinh viên CHỌN 2 KỸ THUẬT TRONG SỐ 3 KỸ THUẬT: anti-debugging, anti-VM và anti-sandbox để hiện thực tính năng:

+ Nhận biết đang chạy trong môi trường máy ảo,

+ Nhận biết đang chạy trong môi trường sandbox,

+ Nhận biết, phát hiện đang bị gỡ lỗi (debugging),

Một khi nhận biết đang bị đặt trong môi trường phân tích, nó sẽ không thực hiện hành vi, không thể hiện bản chất của mình (vd: payload không thực thi đoạn mã mục tiêu cho trước, dừng chương trình…).

*\*\*\*Lưu ý: Quay video demo tương ứng và đính kèm link video trong báo cáo nộp để minh chứng (trong video có thông tin của nhóm).*

1. **Nâng cao: Tìm hiểu kỹ thuật Environmental Keying – một trong những cơ chế trốn tránh phát hiện của mã độc:**

+ Nhóm sinh viên tìm hiểu cách thức hoạt động của kỹ thuật này thông qua phân tích các trường hợp báo cáo điển hình được thống kê trên MITRE. Ví dụ: Tìm hiểu cách thức hoạt động của một trong các loại mã độc sau: Equation, InvisiMole, Ninja, PowerPunch, APT41,…

+ Trình bày báo cáo yêu cầu này dưới dạng sơ đồ lây nhiễm (kèm giải thích ngắn gọn qui trình), nhấn mạnh vào vai trò của kỹ thuật Environmental Keying.

**Environmental Keying** là một kỹ thuật giúp mã độc tránh bị phát hiện bằng cách chỉ kích hoạt trong môi trường phù hợp, tránh các môi trường sandbox hoặc phân tích.

**Phân tích cách thức hoạt động của kỹ thuật này thông qua năm mã độc: Equation, InvisiMole, Ninja, PowerPunch, và APT41:**

**1. Equation**

* Equation là một loại mã độc tinh vi được phát triển bởi nhóm APT (Advanced Persistent Threat) Equation Group.
* Cách thức hoạt động:
  + Bước 1: Phishing email được gửi đến nạn nhân, chứa liên kết tải xuống mã độc.
  + Bước 2: Mã độc được tải xuống và cài đặt trên máy tính nạn nhân.
  + Bước 3: Mã độc sử dụng kỹ thuật Environmental Keying để thu thập thông tin về môi trường mạng của nạn nhân, bao gồm địa chỉ IP, tên miền, và thông tin về hệ điều hành.
  + Bước 4: Mã độc sử dụng thông tin thu thập được để tạo ra một khóa mã hóa duy nhất cho nạn nhân.
  + Bước 5: Mã độc mã hóa dữ liệu trên máy tính nạn nhân và yêu cầu tiền chuộc để giải mã.
* Vai trò của Environmental Keying: Kỹ thuật này cho phép mã độc Equation thu thập thông tin về môi trường mạng của nạn nhân, từ đó tạo ra một khóa mã hóa duy nhất và tăng khả năng mã hóa dữ liệu.

Sơ đồ lây nhiễm:

Phishing email → Tải xuống mã độc → Cài đặt mã độc → Thu thập thông tin môi trường → Tạo khóa mã hóa → Mã hóa dữ liệu → Yêu cầu tiền chuộc

**2. InvisiMole**

* InvisiMole là một loại mã độc được phát triển bởi nhóm APT InvisiMole.
* Cách thức hoạt động:
  + Bước 1: Phishing email được gửi đến nạn nhân, chứa liên kết tải xuống mã độc.
  + Bước 2: Mã độc được tải xuống và cài đặt trên máy tính nạn nhân.
  + Bước 3: Mã độc sử dụng kỹ thuật Environmental Keying để thu thập thông tin về môi trường mạng của nạn nhân, bao gồm địa chỉ IP, tên miền, và thông tin về hệ điều hành.
  + Bước 4: Mã độc sử dụng thông tin thu thập được để tạo ra một kênh liên lạc với máy chủ điều khiển.
  + Bước 5: Mã độc thực hiện các hoạt động gián điệp, bao gồm thu thập thông tin, ghi lại các hoạt động của nạn nhân, và truyền dữ liệu về máy chủ điều khiển.
* Vai trò của Environmental Keying: Kỹ thuật này cho phép mã độc InvisiMole thu thập thông tin về môi trường mạng của nạn nhân, từ đó tạo ra một kênh liên lạc với máy chủ điều khiển và thực hiện các hoạt động gián điệp.

Sơ đồ lây nhiễm:

Phishing email → Tải xuống mã độc → Cài đặt mã độc → Thu thập thông tin môi trường → Tạo kênh liên lạc → Thực hiện hoạt động gián điệp

**3. Ninja**

* Ninja là một loại mã độc được phát triển bởi nhóm APT Ninja.
* Cách thức hoạt động:
  + Bước 1: Phishing email được gửi đến nạn nhân, chứa liên kết tải xuống mã độc.
  + Bước 2: Mã độc được tải xuống và cài đặt trên máy tính nạn nhân.
  + Bước 3: Mã độc sử dụng kỹ thuật Environmental Keying để thu thập thông tin về môi trường mạng của nạn nhân, bao gồm địa chỉ IP, tên miền, và thông tin về hệ điều hành.
  + Bước 4: Mã độc sử dụng thông tin thu thập được để tạo ra một kênh liên lạc với máy chủ điều khiển.
  + Bước 5: Mã độc thực hiện các hoạt động gián điệp, bao gồm thu thập thông tin, ghi lại các hoạt động của nạn nhân, và truyền dữ liệu về máy chủ điều khiển.
* Vai trò của Environmental Keying: Kỹ thuật này cho phép mã độc Ninja thu thập thông tin về môi trường mạng của nạn nhân, từ đó tạo ra một kênh liên lạc với máy chủ điều khiển và thực hiện các hoạt động gián điệp.

Sơ đồ lây nhiễm:

Phishing email → Tải xuống mã độc → Cài đặt mã độc → Thu thập thông tin môi trường → Tạo kênh liên lạc → Thực hiện hoạt động gián điệp

**4. PowerPunch**

* PowerPunch là một loại mã độc được phát triển bởi nhóm APT PowerPunch.
* Cách thức hoạt động:
  + Bước 1: Phishing email được gửi đến nạn nhân, chứa liên kết tải xuống mã độc.
  + Bước 2: Mã độc được tải xuống và cài đặt trên máy tính nạn nhân.
  + Bước 3: Mã độc sử dụng kỹ thuật Environmental Keying để thu thập thông tin về môi trường mạng của nạn nhân, bao gồm địa chỉ IP, tên miền+ Bước 4: Mã độc sử dụng thông tin thu thập được để tạo ra một khóa mã hóa duy nhất cho nạn nhân.
  + Bước 5: Mã độc mã hóa dữ liệu trên máy tính nạn nhân và yêu cầu tiền chuộc để giải mã.
* Vai trò của Environmental Keying: Kỹ thuật này cho phép mã độc PowerPunch thu thập thông tin về môi trường mạng của nạn nhân, từ đó tạo ra một khóa mã hóa duy nhất và tăng khả năng mã hóa dữ liệu.

Sơ đồ lây nhiễm:

Phishing email → Tải xuống mã độc → Cài đặt mã độc → Thu thập thông tin môi trường → Tạo khóa mã hóa → Mã hóa dữ liệu → Yêu cầu tiền chuộc

**5. APT41**

* APT41 là một nhóm APT được biết đến với nhiều loại mã độc, bao gồm DoublePulsar, ShadowBrokers, và FruityArmor.
* Cách thức hoạt động:
  + Bước 1: Phishing email được gửi đến nạn nhân, chứa liên kết tải xuống mã độc.
  + Bước 2: Mã độc được tải xuống và cài đặt trên máy tính nạn nhân.
  + Bước 3: Mã độc sử dụng kỹ thuật Environmental Keying để thu thập thông tin về môi trường mạng của nạn nhân, bao gồm địa chỉ IP, tên miền, và thông tin về hệ điều hành.
  + Bước 4: Mã độc sử dụng thông tin thu thập được để tạo ra một kênh liên lạc với máy chủ điều khiển.
  + Bước 5: Mã độc thực hiện các hoạt động gián điệp, bao gồm thu thập thông tin, ghi lại các hoạt động của nạn nhân, và truyền dữ liệu về máy chủ điều khiển.
* Vai trò của Environmental Keying: Kỹ thuật này cho phép mã độc APT41 thu thập thông tin về môi trường mạng của nạn nhân, từ đó tạo ra một kênh liên lạc với máy chủ điều khiển và thực hiện các hoạt động gián điệp.

Sơ đồ lây nhiễm:

Phishing email → Tải xuống mã độc → Cài đặt mã độc → Thu thập thông tin môi trường → Tạo kênh liên lạc → Thực hiện hoạt động gián điệp.

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)