**Bài 2. a) Các phần mềm gây hại – Trojan**

**1) Khái niệm**

- Trojan là chương trình gây tổn hại đến người dùng máy tính nhằm phục vụ mục đích các nhân.

- Hoạt động bí mật khiến người dùng không nhận ra được.

- Công dụng hay gặp nhất là thiết lập quyền điều khiển từ xa cho hacker trên máy bị nhiễm Trojan.

- Không tự nhân bản như virus máy tính mà chỉ chạy ngầm trong máy bị nhiễm.

- Làm chậm tốc độ máy tính, cấm chỉnh sửa registry.

**2) Phân loại Trojan**

- Loại điều khiển từ xa (RAT):

+ Biến máy tính bị nhiễm thành 1 server để máy tính client của hacker truy cập vào và nắm quyền điều khiển.

+ Tự động kích hoạt mỗi khi phía client hoạt động.

+ Gồm 2 file, một cho server, một cho client.

+ Thường ngụy trang dưới dạng một kiểu file bình thường để giấu .exe.

+ Chạy server dưới 1 cổng riêng biệt cho phép hacker thâm nhập vào máy bị nhiễm và tiến hành điều khiển từ xa.

+ Vô hiệu hóa chỉnh sửa registry nên khó xóa trojan khỏi máy.

+ Có thể sử dụng trong việc quản lý máy tính từ xa.

+ Phổ biến: Back Orifice, Girlfriend, Netbus…

- Keyloggers:

+ Bao gồm 2 loại: phần cứng và phần mềm.

+ Nhỏ gọn, sử dụng ít bộ nhớ nên khó bị phát hiện.

+ Hoạt động đơn giản, ghi lại diễn biến của bàn phím rồi gửi lại trên máy hoặc gửi về cho hacker qua email.

+ Bao gồm 3 phần chính:

1. Chương trình điều khiển: điều phối hoạt động, tinh chỉnh các thiết lập, xem các tập tin nhật ký bằng tổ hợp phím tắt.
2. Tập tin hook, hoặc 1 chương trình monitor dùng để ghi nhận lại các thao tác từ bàn phím, capture screen.
3. Tập tin nhật ký (log) chứa đựng toàn bộ những gì hook ghi nhận được.

- Trojan lấy cắp password:

+ Ăn cắp các loại mật khẩu lưu trên máy bị nhiễm rồi gởi về cho hacker qua email.

+ Các loại phổ biến: Barri, Kuang, Barok.

- FTP trojans:

+ Mở port 21 trên máy bị nhiễm nên mọi người đều có thể truy cập máy này để tải dữ liệu.

- Trojan phá hoại:

+ Mục đích chính là phá hủy đĩa cứng, mã hóa các file.

+ Rất nguy hiểm, khó kiểm soát.

- Trojan chiếm quyền kiểu leo thang:

+ Được gắn vào một ứng dụng hệ thống nào đó và cho hacker quyền cao hơn quyền đã có trong hệ thống khi ứng dụng chạy.

**3) Một số trojan phổ biến**

- KGB SPY:

+ Có thể theo dõi các phím nhấn màn hình…

+ Có các tab trong chương trình:

1. General options
2. Password
3. Email delivery
4. Filters
5. Invisibility
6. Advanced options
7. Screenshot
8. FPT delivery
9. Alert Notifications

-Blazing Tool perfect keylogger:

+ Cho phép nhận thông tin từ máy bị nhiềm từ email hoặc fpt server.

+ Có thể lưu lại các phím nhấn, link web, nội dung chat…

- 007 Spy software

- Stealth Keylogger

- DJI RAT

- NET BUS

- HackerzRAT

**4) Phòng chống trojan**

- Chạy trojan scanner để phòng chống trojan.

- Quét các sửa đổi dáng ngờ đối với các file hệ điều hành.

**-** Quét các hoạt động mạng đáng ngờ.

- Quét những file hoặc folder đáng nghi.

- Quét các chương trình startup đáng nghi.

- Quét các dịch vụ windows đáng ngờ.

- Quét các dịch vụ driver đáng ngờ được cài đặt trên máy tính.

- Quét các mục đăng ký đáng ngờ.

- Quét những tiến trình đang chạy đáng ngờ. (công cụ: Process Viewer, Insider…)

- Quét các cổng đang mở đáng ngờ. (công cụ: Netstat, Fport, TCPView…)

- Không mở các tệp đính kèm trong mail không rõ.

- Khóa các port không cần thiết tại host và tường lửa.

- Tránh đồng ý trao đổi các chương trình trong đoạn tin nhắn khẩn.

- Tăng cường cài đặt cấu hình mặc định, yếu và vô hiệu hóa chức năng không sử dụng bao gồm các giao thức và dịch vụ.

- Giám sát lưu lượng mạng nội bộ để tìm các cổng lẻ hoặc lưu lượng được mã hóa.

- Tránh tải và giả nén các tác vụ từ các nguồn không đáng tin.

- Tải bản vá lỗi và cập nhật bảo mật cho hệ điều hành và ứng dụng.

Quest các đĩa CD và DVD với phần mềm antivirus trước khi sử dụng.

- Hạn chế quyền trong môi trường PC để ngăn cài đặt ứng dụng độc hại.

- Tránh gõ lệnh một cách mù quáng và triển khai các chương trình hoặc tập lệnh được tạo sẵn.

- Quản lí tính toàn vẹn của tệp máy trạm cục bộ thông qua tổng kiểm tra, kiểm tra hoặc quét cổng.

- Chạy phần mềm chống virus, tường lửa và phát triển xâm nhập trên máy chủ.

**5) Một số cổng đi cùng các Trojan thông dụng**

|  |  |  |
| --- | --- | --- |
| **Trojan** | **Protocol** | **Ports** |
| Back Office | UDP | 31337 hoặc 31338 |
| Deep Throat | UDP | 2140 và 3150 |
| NetBus | TCP | 12345 và 12346 |
| Whack-a-mole | TCP | 12361 và 12362 |
| NetBus 2 Pro | TCP | 20034 |
| Girlfriend | TCP | 21554 |
| Masters Paradise | TCP | 3129, 40421,40422,40423, 40426 |