Họ và tên : Trần Lệ Uyên

Lớp : 10CNPM2

MSSV : 1050080165

Bài tập 2 lý thuyết

Câu 1 :

\*Các biện pháp :

* Sử dụng phần mềm diệt virus: Cài đặt phần mềm bảo mật mạnh như Windows Defender, Kaspersky, Bitdefender,... để quét và loại bỏ Keylogger.
* Bật xác thực hai yếu tố (2FA): Giúp bảo vệ tài khoản ngay cả khi mật khẩu bị đánh cắp.
* Không tải phần mềm không rõ nguồn gốc : Chỉ cài đặt ứng dụng từ nguồn chính thống như Microsoft Store, Google Play hoặc App Store.
* Cập nhật hệ điều hành và phần mềm thường xuyên : Các bản cập nhật giúp vá lỗ hổng bảo mật mà Keylogger có thể lợi dụng.
* Sử dụng bàn phím ảo khi nhập thông tin quan trọng : Giảm nguy cơ bị ghi lại thao tác gõ phím, đặc biệt là khi nhập mật khẩu.
* Hạn chế sử dụng máy tính công cộng: Tránh đăng nhập tài khoản quan trọng trên máy tính lạ, vì có thể đã bị cài Keylogger.
* Kiểm tra các tiến trình chạy ngầm : Định kỳ kiểm tra Task Manager (Windows) hoặc Activity Monitor (Mac) để phát hiện ứng dụng đáng ngờ.

\*Cách phát hiện Keylogger :

**Trên máy tính :**

* Kiểm tra tiến trình lạ trong Task Manager (Windows) hoặc Activity Monitor (Mac) : Nhấn Ctrl + Shift + Esc (Windows) → Tab Processes → Tìm các tiến trình lạ.
* Quét hệ thống bằng phần mềm diệt virus : Sử dụng Windows Defender hoặc phần mềm diệt virus khác để quét toàn bộ hệ thống.
* Kiểm tra phần mềm lạ trong Startup : Nhấn Win + R → nhập msconfig → Tab Startup → Tắt ứng dụng đáng ngờ.
* Sử dụng công cụ chống Keylogger : Một số phần mềm như SpyShelter, Zemana AntiLogger có thể giúp phát hiện và ngăn chặn Keylogger.

**Trên điện thoại :**

* Kiểm tra ứng dụng lạ trong cài đặt : Vào Cài đặt → Ứng dụng và tìm các ứng dụng không quen thuộc.
* Xem quyền truy cập của ứng dụng : Nếu có ứng dụng yêu cầu quyền truy cập bàn phím hoặc màn hình mà không rõ lý do, hãy xóa ngay.
* Quét virus bằng ứng dụng bảo mật : Dùng các ứng dụng như Kaspersky, Avast, Malwarebytes để quét điện thoại.

Câu 2 :

\*Phân loại Keylogger theo cơ chế hoạt động :

- Keylogger phần cứng : Là thiết bị cắm trực tiếp vào bàn phím để ghi lại thao tác gõ phím. Thường được gắn lén vào cổng USB hoặc bàn phím vật lý.

- Keylogger phần mềm : Là phần mềm chạy ẩn trên hệ thống, có thể ghi lại thao tác bàn phím, chụp ảnh màn hình và gửi dữ liệu về cho hacker.

- Keylogger dựa trên clipboard: Lưu lại dữ liệu khi người dùng sao chép (Ctrl + C) và dán (Ctrl + V).

- Keylogger dựa trên API hệ thống : Sử dụng API của hệ điều hành để ghi lại thao tác bàn phím mà không cần cài đặt sâu vào hệ thống.

- Keylogger dựa trên trình duyệt : Cài đặt vào trình duyệt để ghi lại thông tin đăng nhập khi người dùng nhập vào các trang web.

\*Một số Keylogger phổ biến trên máy tính :

- Elite Keylogger : Một trong những Keylogger nguy hiểm, có khả năng ghi lại phím, chụp ảnh màn hình, theo dõi clipboard và giám sát email.

- Spyrix Free Keylogger : Có thể ghi lại mọi thao tác nhập liệu, gửi báo cáo qua email hoặc tài khoản từ xa.

- Ardamax Keylogger : Phần mềm gián điệp được sử dụng để theo dõi máy tính, có khả năng chạy ẩn và khó bị phát hiện.

- Revealer Keylogger : Một trong những Keylogger miễn phí phổ biến, dễ sử dụng và có thể theo dõi bàn phím từ xa.

\*Một số Keylogger phổ biến trên điện thoại :

- mSpy Android, iOS : Theo dõi bàn phím, ghi lại tin nhắn, cuộc gọi, và vị trí GPS.

- Hoverwatch Android : Ghi lại thao tác bàn phím, chụp ảnh màn hình, theo dõi mạng xã hội.

- Spyic Android, iOS : Có khả năng ghi lại bàn phím và theo dõi hoạt động điện thoại mà không cần root/jailbreak.

- iKeyMonitor Android, iOS : Được thiết kế để theo dõi trẻ em nhưng có thể bị lợi dụng cho mục đích xấu.

- FlexiSPY Android, iOS : Có khả năng giám sát toàn diện bao gồm thao tác bàn phím, ghi âm cuộc gọi và theo dõi tin nhắn.

\*Cách nhận biết nếu thiết bị bị nhiễm Keylogger :

Trên máy tính :

* Hiệu suất máy chậm bất thường.
* Xuất hiện tiến trình lạ trong Task Manager.
* Bàn phím bị lag hoặc hoạt động bất thường.
* Xuất hiện phần mềm lạ trong danh sách ứng dụng.

Trên điện thoại :

* Pin tụt nhanh không rõ lý do.
* Thiết bị nóng bất thường ngay cả khi không sử dụng.
* Ứng dụng yêu cầu quyền truy cập không hợp lý.
* Xuất hiện tin nhắn hoặc email lạ gửi đi mà bạn không biết.