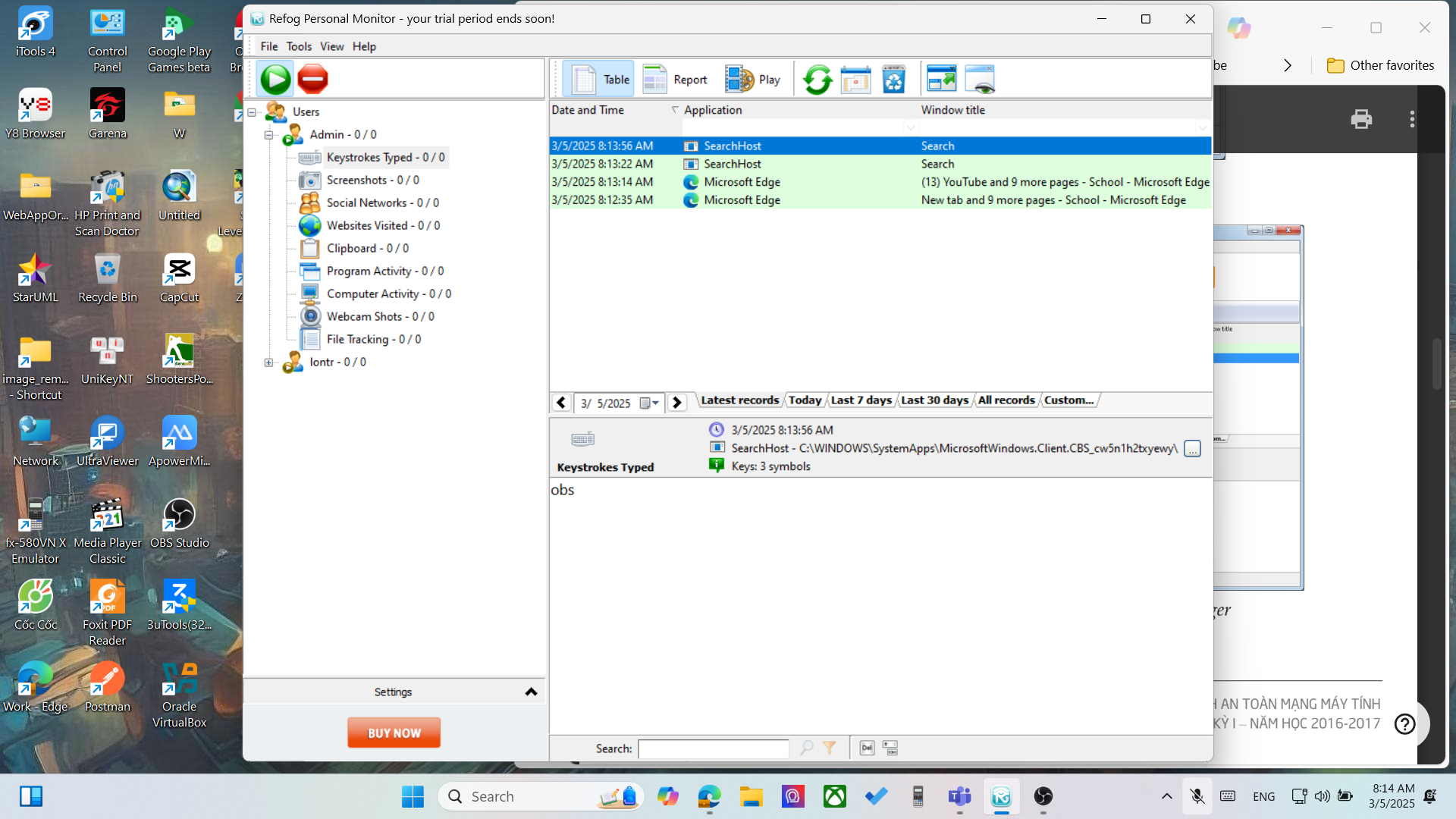
Tên: Vũ Trọng Phương

Lớp 10DHCNPM1



1. Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện thoại và minh họa nếu có thể.

Để phòng tránh keylogger trên máy tính và điện thoại, bạn cần áp dụng nhiều biện pháp bảo mật khác nhau. Dưới đây là các biện pháp chi tiết để giúp bạn giảm thiểu nguy cơ bị tấn công bởi keylogger:

1. Cập nhật phần mềm và hệ điều hành thường xuyên Máy tính: Đảm bảo hệ điều hành (Windows, macOS, Linux) và phần mềm diệt virus của bạn luôn được cập nhật. Các bản vá bảo mật giúp bịt lỗ hổng mà phần mềm độc hại có thể lợi dụng. Cập nhật phần mềm trình duyệt và ứng dụng của bạn cũng rất quan trọng, vì nhiều keylogger có thể lây lan qua các lỗi trong phần mềm. Điện thoại: Cập nhật hệ điều hành (iOS/Android) và ứng dụng trên điện thoại thường xuyên để bảo vệ khỏi các phần mềm độc hại và các lỗ hổng bảo mật.

2. Cài đặt phần mềm chống virus và chống phần mềm độc hại Máy tính: Sử dụng phần mềm bảo mật mạnh mẽ và đảm bảo tính năng quét thời gian thực (real-time scanning) luôn bật. Phần mềm diệt virus sẽ giúp phát hiện và xóa bỏ keylogger hoặc phần mềm độc hại. Các phần mềm bảo mật nổi tiếng như: Windows Defender (miễn phí trên Windows), Bitdefender, Kaspersky, Norton. Điện thoại: Trên Android, bạn có thể cài đặt phần mềm bảo mật như Avast, Malwarebytes, hoặc McAfee. iPhone thường ít bị tấn công bởi keylogger nhờ hệ sinh thái khép kín, nhưng bạn vẫn cần tải ứng dụng từ App Store chính thức để tránh rủi ro.

3. Cẩn trọng với ứng dụng và tệp tin lạ Máy tính: Đừng tải hoặc cài đặt các ứng dụng từ các nguồn không rõ ràng. Tránh mở các tệp đính kèm email lạ hoặc từ các liên kết không đáng tin cậy. Đảm bảo bạn không tải phần mềm crack hoặc phần mềm không rõ nguồn gốc từ internet, vì chúng thường kèm theo phần mềm độc hại. Điện thoại: Tránh cài đặt ứng dụng từ các nguồn ngoài Google Play Store hoặc App Store. Hãy đọc các đánh giá và quyền truy cập yêu cầu của ứng dụng trước khi cài đặt. Cẩn thận với các liên kết trong tin nhắn SMS hoặc email (phishing).

4. Sử dụng mật khẩu mạnh và xác thực 2 yếu tố (2FA) Máy tính: Sử dụng mật khẩu mạnh, kết hợp cả chữ hoa, chữ thường, số và ký tự đặc biệt. Tránh sử dụng mật khẩu đơn giản như "123456" hoặc "password". Sử dụng xác thực 2 yếu tố (2FA) cho các tài khoản quan trọng, để ngay cả khi keylogger ghi lại mật khẩu, kẻ tấn công cũng sẽ cần mã xác thực từ thiết bị của bạn. Điện thoại: Sử dụng mã PIN hoặc sinh trắc học (vân tay, nhận diện khuôn mặt) để bảo vệ điện thoại của bạn. Kích hoạt xác thực 2 yếu tố trên các dịch vụ như Google, Facebook, và các ứng dụng ngân hàng.

5. Sử dụng phần mềm chống keylogger (Anti-Keylogger Software) Cài đặt phần mềm chuyên dụng để phát hiện và bảo vệ khỏi keylogger. Các phần mềm này có thể phát hiện và ngăn chặn keylogger chạy trong nền, ví dụ như Zemana AntiLogger, Spybot Search & Destroy.

6. Tránh sử dụng Wi-Fi công cộng không bảo mật Máy tính và Điện thoại: Tránh đăng nhập vào các tài khoản quan trọng khi sử dụng Wi-Fi công cộng, vì các mạng Wi-Fi không bảo mật có thể dễ dàng bị tấn công và theo dõi. Sử dụng VPN để mã hóa kết nối của bạn khi duyệt web.

7. Kiểm tra các tiến trình và dịch vụ trên hệ thống Máy tính: Kiểm tra các tiến trình đang chạy trên máy tính và tìm các tiến trình lạ (tasklist trên Windows, top/ps trên Linux). Kiểm tra các dịch vụ và ứng dụng khởi động cùng hệ điều hành để phát hiện các phần mềm khả nghi.

8. Giám sát hoạt động của phần mềm và phần cứng Máy tính: Sử dụng phần mềm giám sát như Process Explorer (Sysinternals) để theo dõi các tiến trình và dịch vụ đang chạy. Các phần mềm keylogger có thể sử dụng quyền truy cập cao để ẩn mình. Thực hiện các quét bảo mật thường xuyên, đặc biệt nếu bạn nghi ngờ có phần mềm gián điệp

1. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính và điện thoại khác.

Keylogger là một phần mềm gián điệp được thiết kế để ghi lại tất cả các thao tác nhập liệu từ bàn phím, giúp kẻ tấn công thu thập thông tin nhạy cảm như mật khẩu, tài khoản ngân hàng, thông tin cá nhân, v.v.

Dưới đây là một số loại keylogger phổ biến trên máy tính và điện thoại. Keylogger trên Máy Tính Refog Keylogger Mô tả: Refog Keylogger là một trong những keylogger phổ biến trên máy tính, cho phép ghi lại tất cả các thao tác nhập liệu, bao gồm các mật khẩu và nội dung chat. Nó có thể ghi lại các trang web truy cập, email, và thậm chí chụp màn hình máy tính. Tính năng: Hoạt động ẩn danh, theo dõi các hoạt động mạng, có thể gửi các báo cáo qua email.

Phạm vi: Có thể hoạt động trên hệ điều hành Windows và macOS. Spyrix Keylogger

Mô tả: Spyrix Keylogger cung cấp khả năng theo dõi toàn diện, bao gồm theo dõi các hành vi trực tuyến và ngoại tuyến của người dùng, ghi lại các cuộc trò chuyện và nội dung email.

Tính năng: Chạy ẩn, có thể chụp màn hình, theo dõi các cuộc gọi VoIP và truy cập mạng xã hội.

Phạm vi: Hỗ trợ hệ điều hành Windows và macOS. KidLogger

Mô tả: KidLogger là một phần mềm keylogger được thiết kế chủ yếu để theo dõi trẻ em sử dụng máy tính. Nó ghi lại tất cả các hoạt động trên máy tính, bao gồm bàn phím, webcam, và ứng dụng sử dụng.

Tính năng: Theo dõi các ứng dụng mạng xã hội, ghi lại các cuộc trò chuyện và email, có thể gửi báo cáo qua email.

Phạm vi: Hỗ trợ Windows, macOS và các nền tảng di động như Android. Elite Keylogger

Mô tả: Elite Keylogger là một keylogger mạnh mẽ được thiết kế để theo dõi và ghi lại các hoạt động trên máy tính mà không bị phát hiện. Nó ghi lại tất cả các thao tác nhập liệu và có thể ghi lại các thông tin như mật khẩu và tin nhắn.

Tính năng: Có khả năng ghi lại các cuộc gọi VoIP (Skype, v.v.), hỗ trợ gửi báo cáo qua email hoặc FTP.

Phạm vi: Hỗ trợ Windows. Ardamax Keylogger Mô tả: Ardamax Keylogger là phần mềm gián điệp mạnh mẽ cho phép ghi lại mọi thao tác nhập liệu trên máy tính. Nó có thể ghi lại các mật khẩu, thông tin thanh toán trực tuyến và các hoạt động trên các ứng dụng mạng xã hội.

Tính năng: Hoạt động ẩn, theo dõi clipboard, chụp màn hình và gửi báo cáo qua email. Phạm vi: Hỗ trợ Windows, macOS và Android. Keylogger trên Điện Thoại mSpy Mô tả: mSpy là một trong những phần mềm giám sát điện thoại phổ biến nhất, không chỉ ghi lại các thao tác nhập liệu mà còn theo dõi các cuộc gọi, tin nhắn, vị trí GPS và các ứng dụng khác. Tính năng: Theo dõi tin nhắn, cuộc gọi, các ứng dụng mạng xã hội, vị trí GPS và lịch sử duyệt web.

Phạm vi: Hỗ trợ Android và iOS (phải jailbreak hoặc root thiết bị). FlexiSPY Mô tả: FlexiSPY là một phần mềm giám sát toàn diện, cung cấp khả năng theo dõi mọi hoạt động trên điện thoại, bao gồm việc ghi lại các thao tác bàn phím.

Tính năng: Theo dõi cuộc gọi, tin nhắn, ứng dụng mạng xã hội, email, và có thể nghe lén cuộc gọi. Phạm vi: Hỗ trợ Android và iOS (phải jailbreak hoặc root thiết bị). Spyic Mô tả: Spyic là phần mềm giám sát giúp theo dõi các hoạt động trên điện thoại, bao gồm theo dõi tin nhắn, cuộc gọi, các ứng dụng, và ghi lại các thao tác bàn phím.

Tính năng: Theo dõi các cuộc gọi, tin nhắn văn bản, các hoạt động trên mạng xã hội, và cung cấp vị trí GPS.

Phạm vi: Hỗ trợ Android và iOS (không cần root hoặc jailbreak cho iOS). iKeyMonitor

Mô tả: iKeyMonitor là một phần mềm keylogger mạnh mẽ cho phép theo dõi các hoạt động trên điện thoại, bao gồm việc ghi lại các thao tác nhập liệu.

Tính năng: Ghi lại các thao tác bàn phím, tin nhắn, cuộc gọi, vị trí GPS và các hoạt động trên ứng dụng mạng xã hội.

Phạm vi: Hỗ trợ Android và iOS (phải jailbreak hoặc root thiết bị). XNSPY Mô tả: XNSPY là một phần mềm giám sát điện thoại giúp theo dõi các cuộc gọi, tin nhắn, các ứng dụng mạng xã hội, và có khả năng ghi lại các thao tác nhập liệu.

Tính năng: Theo dõi các cuộc gọi, tin nhắn, vị trí GPS, và các hoạt động trên các ứng dụng như WhatsApp, Facebook, Snapchat, v.v.

Phạm vi: Hỗ trợ Android và iOS (phải jailbreak hoặc root thiết bị).

Các Biện Pháp Phòng Tránh Keylogger Cập nhật phần mềm: Đảm bảo hệ điều hành và phần mềm của bạn luôn được cập nhật để giảm thiểu các lỗ hổng bảo mật. Sử dụng phần mềm bảo mật: Cài đặt phần mềm chống virus mạnh mẽ để phát hiện và loại bỏ các phần mềm gián điệp. Cẩn trọng khi cài đặt ứng dụng: Không tải ứng dụng từ nguồn không rõ ràng, đặc biệt là trên điện thoại. Sử dụng mật khẩu mạnh và xác thực 2 yếu tố (2FA): Giúp bảo vệ tài khoản của bạn ngay cả khi bị keylogger ghi lại mật khẩu. Kết luận Keylogger có thể gây ra mối đe dọa nghiêm trọng đối với bảo mật của người dùng. Để giảm thiểu rủi ro, bạn nên sử dụng các phần mềm bảo mật, duy trì thói quen bảo mật tốt, và chỉ tải các ứng dụng từ các nguồn đáng tin cậy.