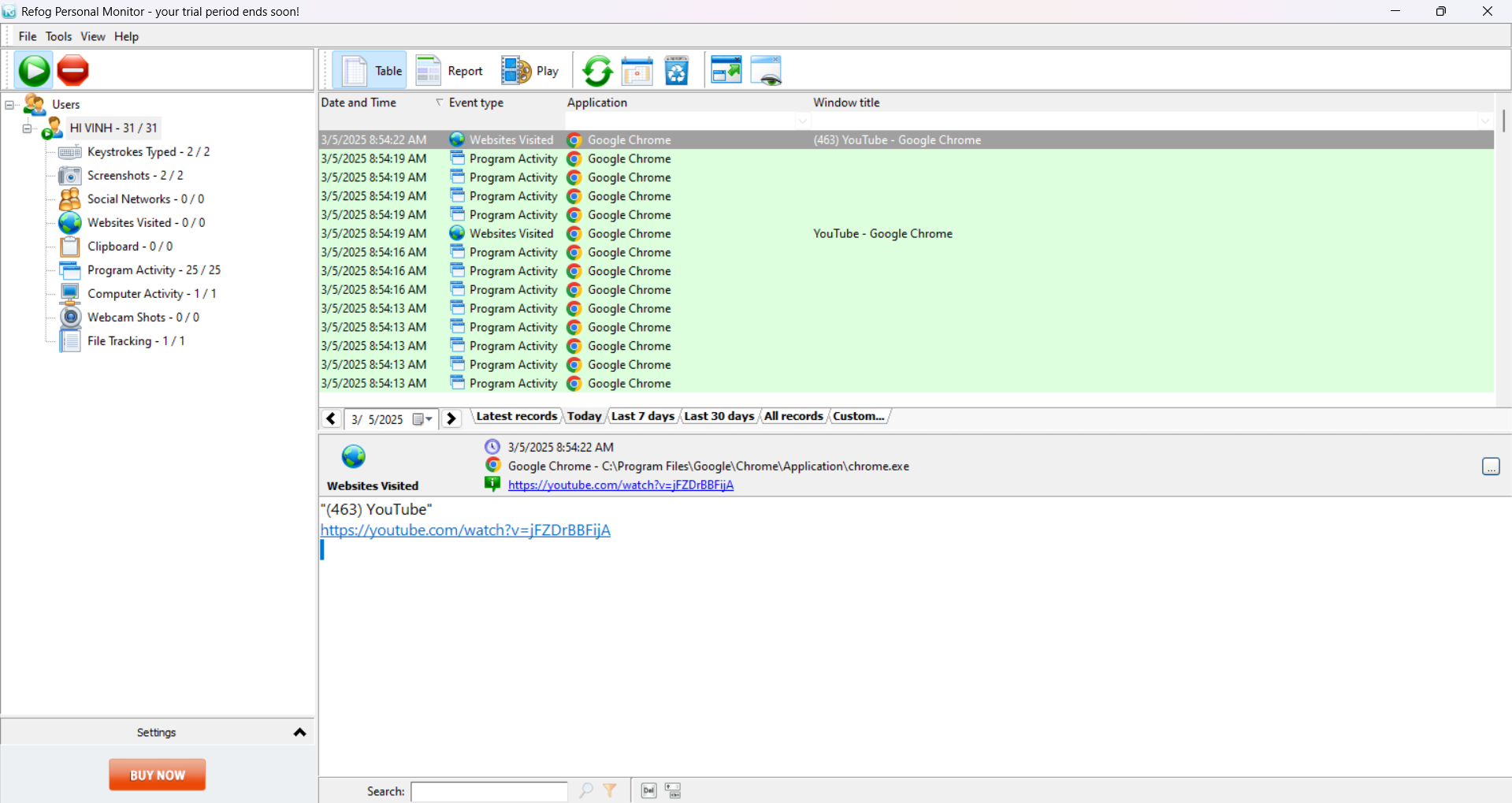
Hình ảnh sau khi tìm trình duyệt và youtube



1. Biện pháp phòng tránh và cách phát hiện Keylogger trên máy tính - điện thoại

🔹 Biện pháp phòng tránh Keylogger

Cài đặt phần mềm diệt virus & chống malware: Sử dụng Windows Defender, Malwarebytes, Kaspersky, Norton,... để quét và chặn keylogger.

Không tải phần mềm từ nguồn không rõ ràng: Chỉ tải ứng dụng từ trang web chính thức hoặc cửa hàng ứng dụng uy tín như Google Play, App Store.

Kiểm tra quyền ứng dụng: Trên điện thoại, kiểm tra xem ứng dụng có quyền truy cập bàn phím, ghi màn hình, hoặc đọc tin nhắn không.

Bật bảo vệ bàn phím ảo: Khi nhập thông tin quan trọng như mật khẩu, có thể dùng bàn phím ảo để tránh bị ghi lại phím bấm.

Sử dụng xác thực 2 lớp (2FA): Ngay cả khi bị lộ mật khẩu, hacker cũng khó xâm nhập nếu tài khoản có xác thực hai bước.

Không sử dụng bàn phím trên máy tính công cộng: Máy tính ở quán net, thư viện, hoặc quán cafe có thể đã bị cài sẵn keylogger.

🔹 Cách phát hiện Keylogger trên máy tính & điện thoại

✅ Trên máy tính:

Kiểm tra Task Manager (Ctrl + Shift + Esc): Xem có tiến trình nào lạ chạy ngầm không.

Kiểm tra chương trình khởi động (msconfig hoặc Task Manager > Startup): Keylogger thường tự động chạy khi máy khởi động.

Quét với phần mềm chống malware: Dùng Malwarebytes, Spybot Search & Destroy,... để quét và xóa keylogger.

Kiểm tra Registry (regedit): Nếu thấy các khóa lạ ở HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, có thể đó là keylogger.

Kiểm tra mạng (netstat -ano): Nếu có kết nối bất thường gửi dữ liệu ra bên ngoài, có thể là keylogger đang gửi thông tin đánh cắp.

✅ Trên điện thoại:

Kiểm tra ứng dụng cài đặt: Nếu thấy ứng dụng lạ hoặc không nhớ đã cài, cần gỡ ngay.

Kiểm tra mức sử dụng pin & dữ liệu: Keylogger thường chạy ngầm, làm tiêu hao pin và sử dụng dữ liệu mạng nhiều hơn bình thường.

Quét với phần mềm bảo mật: Sử dụng Kaspersky Mobile, Bitdefender, hay Malwarebytes để phát hiện ứng dụng độc hại.

Khởi động vào chế độ an toàn (Safe Mode): Chế độ này giúp tắt ứng dụng của bên thứ ba, cho phép phát hiện keylogger dễ dàng hơn.

2. Một số loại Keylogger trên máy tính & điện thoại

🔹 Keylogger trên máy tính

Refog Keylogger: Phần mềm giám sát bàn phím, chụp màn hình và theo dõi hoạt động máy tính.

Ardamax Keylogger: Một trong những keylogger phổ biến, có thể chạy ẩn và ghi lại mọi thao tác.

Actual Keylogger: Ghi lại tổ hợp phím, lịch sử trình duyệt và chụp màn hình.

Spyrix Free Keylogger: Dùng để giám sát trẻ em nhưng có thể bị lạm dụng vào mục đích xấu.

Hardware Keylogger: Thiết bị nhỏ cắm vào cổng USB hoặc bàn phím để ghi lại các thao tác nhập liệu.

🔹 Keylogger trên điện thoại

mSpy: Ứng dụng giám sát trẻ em, theo dõi bàn phím và ghi lại hoạt động trên điện thoại.

FlexiSPY: Một phần mềm mạnh mẽ có khả năng theo dõi bàn phím, cuộc gọi, tin nhắn, vị trí GPS.

Spyzie: Dùng để theo dõi hoạt động điện thoại từ xa, có thể bị lợi dụng để giám sát người khác mà không có sự đồng ý.

Hoverwatch: Keylogger trên Android có thể ghi lại mọi thao tác trên điện thoại.

iKeyMonitor: Ghi lại phím bấm, tin nhắn, hoạt động trên mạng xã hội, chụp ảnh màn hình.