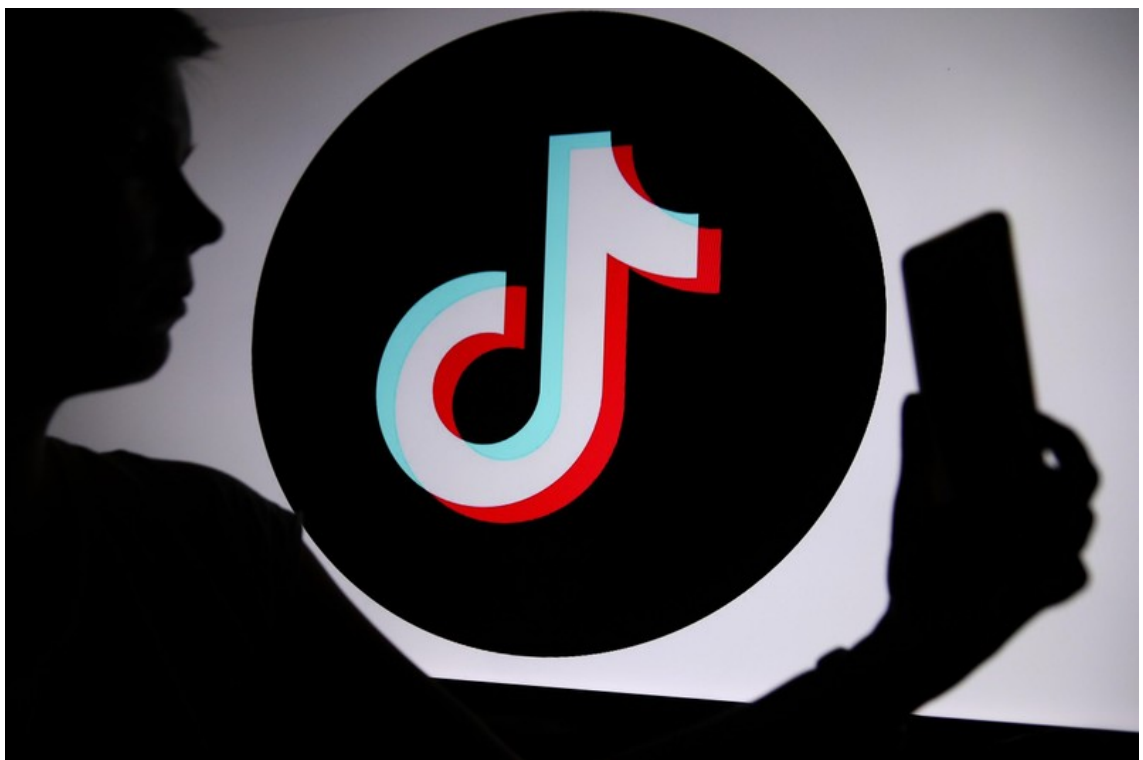


Cảnh báo mã độc trên TikTok: Video AI dụ người dùng tự chạy virus để hack tài khoản

08:02 23/10/2025

Một làn sóng video lừa đảo mới do Trí tuệ nhân tạo (AI) tạo ra đang lan truyền nhanh chóng trên TikTok, nhắm đến người dùng trẻ tuổi. Những video này dụ dỗ người xem chạy một đoạn mã độc trên máy tính để được truy cập miễn phí các dịch vụ trả phí như Netflix, Spotify. Tuy nhiên, hành động này sẽ ngay lập tức kích hoạt virus Aura Stealer, đánh cắp toàn bộ mật khẩu và dữ liệu ví tiền điện tử.



Một làn sóng video lừa đảo mới do Trí tuệ nhân tạo (AI) tạo ra đang lan truyền nhanh chóng trên TikTok, nhắm đến người dùng trẻ tuổi

Các video lừa đảo này đưa ra lời hứa hấp dẫn về việc truy cập miễn phí các dịch vụ trả phí như Microsoft 365, Adobe Photoshop hay CapCut Pro. Giọng nói robot trong video hướng dẫn người xem thực hiện "vài thao tác đơn giản" để vượt qua hệ thống thanh toán.

Tuy nhiên, yêu cầu cốt lõi là người dùng phải sao chép và chạy một đoạn mã PowerShell trên máy tính của mình. Chuyên gia bảo mật Xavier Mertens nhận định đây là một biến thể mới của cuộc tấn công "ClickFix", thao túng người dùng tự phá vỡ hệ thống bảo mật của chính họ.

Thay vì mở khóa phần mềm, chuỗi lệnh này ngay lập tức tải xuống phần mềm độc hại Aura Stealer. Loại mã độc này được thiết kế chuyên để đánh cắp dữ liệu:

Đánh cắp toàn bộ thông tin Aura Stealer nhanh chóng thu thập mật khẩu được lưu trong trình duyệt, thông tin đăng nhập, cookie và đặc biệt là khóa riêng tư của các ví tiền điện tử.

Gửi dữ liệu về máy chủ từ xa nên toàn bộ dữ liệu nhạy cảm này sau đó được gửi về một máy chủ do tin tặc kiểm soát, có thể được dùng để thực hiện các cuộc tấn công mạng tiếp theo hoặc chiếm đoạt tài khoản ngân hàng.

Điều đáng báo động là làn sóng tấn công này sử dụng nội dung do AI tạo ra hàng loạt, khiến chúng trông có vẻ thuyết phục. Nhiều video đã thu hút hàng trăm nghìn lượt thích và hàng trăm lượt chia sẻ, cho thấy mức độ lan truyền nhanh chóng.

Khuyến cáo quan trọng nhất dành cho người dùng là không bao giờ chạy bất kỳ tập lệnh, lệnh hoặc mã nào được tìm thấy trên TikTok, Discord, diễn đàn hay bất kỳ mạng xã hội nào khác, cho dù lời hứa hẹn có hấp dẫn đến đâu.

Nếu nghi ngờ mình đã bị lừa, người dùng cần ngay lập tức thay đổi tất cả mật khẩu quan trọng, đặc biệt là mật khẩu ngân hàng và ví tiền điện tử.

Tâm An (t/h)