

Mã độc chiếm quyền màn hình trên điện thoại Android và giải pháp xử lý tận gốc

10:21 07/06/2026

Nhiều người dùng điện thoại thông minh hệ điều hành Android tại Việt Nam đang đối mặt với một loại hình tấn công mạng gây hoang mang dư luận. Theo các phản ánh thực tế, thiết bị của nạn nhân bất ngờ bị khóa toàn bộ màn hình giao diện, không thể thực hiện các thao tác cảm ứng thông thường, kèm theo đó là những thông báo đe dọa đòi tiền chuộc từ tin tặc.



Hệ điều hành Android tại Việt Nam đang đối mặt với một loại hình tấn công mạng gây hoang mang dư luận

Tuy nhiên, các chuyên gia an ninh mạng khẳng định đây không phải là loại mã độc tống tiền (ransomware) nguy hiểm có khả năng mã hóa dữ liệu chuyên sâu, mà bản chất chỉ là một ứng dụng độc hại lợi dụng sơ hở của người dùng để chiếm quyền hiển thị.

Phương thức chiếm quyền điều khiển thiết bị thông qua tệp cài đặt apk

Kịch bản tấn công thường bắt đầu khi người dùng có nhu cầu tìm kiếm và tải về các ứng dụng nằm ngoài kho chính thống. Tin tặc đã chủ động phát tán các ứng dụng độc hại này dưới định dạng tệp .apk thông qua các trang web giả mạo hoặc các đường link tải ngẫu nhiên trên Internet.

Trong quá trình cài đặt, ứng dụng này sẽ liên tục yêu cầu người dùng phê duyệt hàng loạt quyền truy cập hệ thống nhạy cảm, điển hình như: quyền hiển thị trên các ứng dụng khác, quyền hoạt động toàn màn hình hoặc quyền kiểm soát một số chức năng cốt lõi của thiết bị. Khi người dùng sơ hở chấp thuận, ứng dụng sẽ ngay lập tức kích hoạt mã độc, liên tục đề các cửa sổ thông báo toàn màn hình với nội dung như "Thiết bị đã bị hack" hoặc "Điện thoại đã bị khóa".

Để gây áp lực tâm lý, tin tặc để lại số điện thoại liên hệ nhằm ép buộc nạn nhân phải mua mã mở khóa với số tiền giao dịch từ 150.000 đến 500.000 đồng, đi kèm lời đe dọa nếu mang máy ra cửa hàng sửa chữa sẽ bị xóa sạch dữ liệu. Do ứng dụng độc hại này được thiết lập quyền tự khởi chạy cùng hệ thống nên ngay cả khi người dùng thực hiện thao tác tắt đi bật lại máy, giao diện tống tiền vẫn tiếp tục hiện ra, tạo cảm giác điện thoại đã bị kiểm soát hoàn toàn.

Quy trình gỡ bỏ mã độc bằng tính năng Safe mode (Chế độ an toàn)

Do mã độc này chỉ can thiệp ở lớp bề mặt hiển thị chứ không thể mã hóa sâu vào cấu trúc tệp tin của hệ điều hành Android, người dùng hoàn toàn có thể tự xử lý và khôi phục thiết bị về trạng thái bình thường mà không cần phải chi trả bất kỳ khoản tiền chuộc nào cho tin tặc. Giải pháp kỹ thuật tối ưu nhất là kích hoạt tính năng Safe mode (Chế độ an toàn) của điện thoại theo các bước cụ thể:

- **Bước 1 (Tắt nguồn thiết bị):** Thực hiện nhấn và giữ nút nguồn vật lý của điện thoại, sau đó chọn lệnh "Tắt nguồn" để đưa máy về trạng thái tắt hoàn toàn.
- **Bước 2 (Kích hoạt Safe mode):** Tiến hành nhấn và giữ đồng thời nút nguồn cùng nút giảm âm lượng. Ngay khi màn hình thiết bị vừa sáng lên, người dùng thả ngón tay ở nút nguồn ra nhưng vẫn tiếp tục duy trì việc giữ chặt nút giảm âm lượng cho đến khi giao diện màn hình khóa của máy xuất hiện. Nếu quy trình thao tác chính xác, dòng chữ "Chế độ an toàn" hoặc "Safe mode" sẽ hiển thị rõ ở góc dưới màn hình.
- **Bước 3 (Gỡ bỏ ứng dụng độc hại):** Khi vận hành ở chế độ Safe mode, hệ điều hành Android sẽ tự động vô hiệu hóa toàn bộ các ứng dụng của bên thứ ba và chỉ khởi chạy các ứng dụng mặc định của hệ thống. Lúc này, app độc hại sẽ bị đóng băng hoàn toàn và không thể chiếm quyền màn hình. Người dùng thực hiện mở khóa máy, truy cập vào mục Quản lý ứng dụng

trong phần Cài đặt, tiến hành rà soát để tìm và gỡ bỏ tận gốc các ứng dụng lạ hoặc ứng dụng vừa mới tải về trước khi máy bị khóa.

- **Bước 4 (Khởi động lại):** Sau khi hoàn tất công tác xóa bỏ phần mềm lừa đảo, người dùng chỉ cần thực hiện khởi động lại điện thoại để đưa máy về chế độ vận hành thông thường.

Cần lưu ý rằng sau khi thoát khỏi trạng thái Safe mode, một số dòng smartphone Android có cơ chế tự động kích hoạt chế độ máy bay (Airplane mode). Người dùng cần kiểm tra và tắt tính năng này để bảo đảm các kết nối mạng dữ liệu di động và sóng liên lạc không bị gián đoạn.

Các nguyên tắc bảo mật cốt lõi để bảo vệ thiết bị Android

Hệ sinh thái thiết bị đa dạng, lượng người dùng khổng lồ cùng cơ chế mở của Android luôn là mảnh đất màu mỡ để tin tặc săn tìm và khai thác các lỗ hổng bảo mật. Để chủ động bảo vệ dữ liệu cá nhân, người dùng cần tuân thủ nghiêm ngặt các nguyên tắc an toàn thông tin:

- **Tuyệt đối tin dùng kho ứng dụng chính ngạch:** Người dùng chỉ nên thực hiện cài đặt các phần mềm trực tiếp từ kho ứng dụng Google Play. Đối với các ứng dụng đặc thù bắt buộc phải cài qua tệp .apk, chỉ lựa chọn tải về từ những nền tảng website có tên tuổi và uy tín lớn, tuyệt đối không bấm vào các kết quả tìm kiếm không rõ nguồn gốc.
- **Tỉnh táo trước các đánh giá giả mạo:** Ngay cả trên môi trường Google Play, một số ứng dụng rác chứa mã độc ẩn giấu vẫn có thể lọt qua hàng rào kiểm duyệt của Google. Trước khi quyết định tải về, người dùng cần đọc kỹ các nhận xét của cộng đồng. Nếu phát hiện các tài khoản đánh giá có dấu hiệu ảo, nội dung khen ngợi chung chung được lập trình tự động, người dùng nên lập tức dừng việc cài đặt.
- **Cập nhật hệ điều hành định kỳ:** Việc thường xuyên kiểm tra và nâng cấp các bản vá bảo mật cũng như các phiên bản Android mới nhất từ nhà sản xuất là lá chắn hữu hiệu giúp vá các lỗ hổng kỹ thuật, ngăn chặn từ sớm các nguy cơ xâm nhập trái phép của tin tặc.

Tâm An