

Hàng chục triệu điện thoại Android bị cài sẵn mã độc trước khi bán

16:07 12/08/2019

Hàng chục triệu điện thoại thông minh Android bị cài sẵn phần mềm độc hại nguy hiểm trước khi đến tay người dùng, nhóm nghiên cứu bảo mật của Google tiết lộ.

Rất nhiều thông tin về việc hàng triệu ứng dụng độc hại được cài đặt từ kho ứng dụng Play Store, nhưng nguy cơ này đáng gây sốc hơn nhiều. Mọi người thường tin rằng, các smartphone mới nguyên hộp đều an toàn.

Thế nhưng một số phần mềm độc hại đã được cài sẵn vào smartphone cả trước khi bán ra, nhẹ thì lợi dụng để hiển thị quảng cáo, nặng thì lấy cắp thông tin, thậm chí chiếm quyền điều khiển máy.

Maddie Stone, một nhà nghiên cứu bảo mật của Google Project Zero đã chia sẻ những phát hiện của nhóm cô tại sự kiện Black Hat hôm 8/8 vừa qua.



Hàng chục triệu smartpone Android bị cài sẵn phần mềm độc hại trước khi xuất xưởng

Khi phần mềm độc hại hoặc các vấn đề bảo mật xuất hiện dưới dạng các ứng dụng được cài sẵn, thì thiệt hại mà nó gây ra lớn hơn, Stone cho biết.

Rủi ro đến từ dự án nguồn mở của Android (AOSP), Google cho phép sử dụng hệ điều hành Android với chi phí thấp hoặc miễn phí. AOSP thường được dùng cho các smartphone giá rẻ, các nhà sản xuất lựa chọn cách này để giảm giá thành sản phẩm.

Khi đó, kẻ xấu chỉ cần thỏa hiệp với nhà sản xuất sử dụng ứng dụng của chúng để trục lợi thay vì tìm cách dụ dỗ hàng nghìn người dùng, Stone cảnh báo.

Nhóm này của Google không tiết lộ bất kỳ chi tiết nào về các thương hiệu smartphone liên quan, nhưng hơn 200 nhà sản xuất điện thoại được phát hiện cài sẵn mềm độc hại cho phép tin tặc có thể tấn công từ xa.

Android là một hệ điều hành mở, rất tốt cho tùy biến phần mềm và cài đặt nhưng tai hại khi tin tặc cũng nắm bắt cơ hội này để ngụy trang phần mềm độc hại bên cạnh các phần mềm cơ bản trên các thiết bị. Nhiều smartphone mới được cài đặt tới 400 ứng dụng từ trước khi xuất xưởng, nên nhiều ứng dụng độc hại thường bị bỏ qua trong lúc kiểm duyệt.

Google cảnh báo về 2 chủng mã độc đặc biệt là Chamois và Triada. Chamois có nhiệm vụ hiển thị quảng cáo, tải về ứng dụng nền và các plug-in, thậm chí gửi đi các tin nhắn có giá cước cao. Chỉ riêng Chamois đã được tìm thấy cài đặt sẵn trên 7,4 triệu thiết bị. Còn Triada là biến thể khác của phần mềm độc hại, cũng để hiển thị quảng cáo và cài đặt ứng dụng chứa mã độc.

Google cho biết đã tiến hành chiến dịch sàng lọc từ tháng 3/2018 đến tháng 3/2019, giúp giảm các thiết bị nhiễm Chamois từ con số 7,4 triệu xuống còn 700.000.

Tuy nhiên, theo Stone, hệ sinh thái Android rất rộng lớn với sự đa dạng các OEM, nên rủi ro với người dùng là khó tránh khỏi.

Theo Vietnamnet