TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

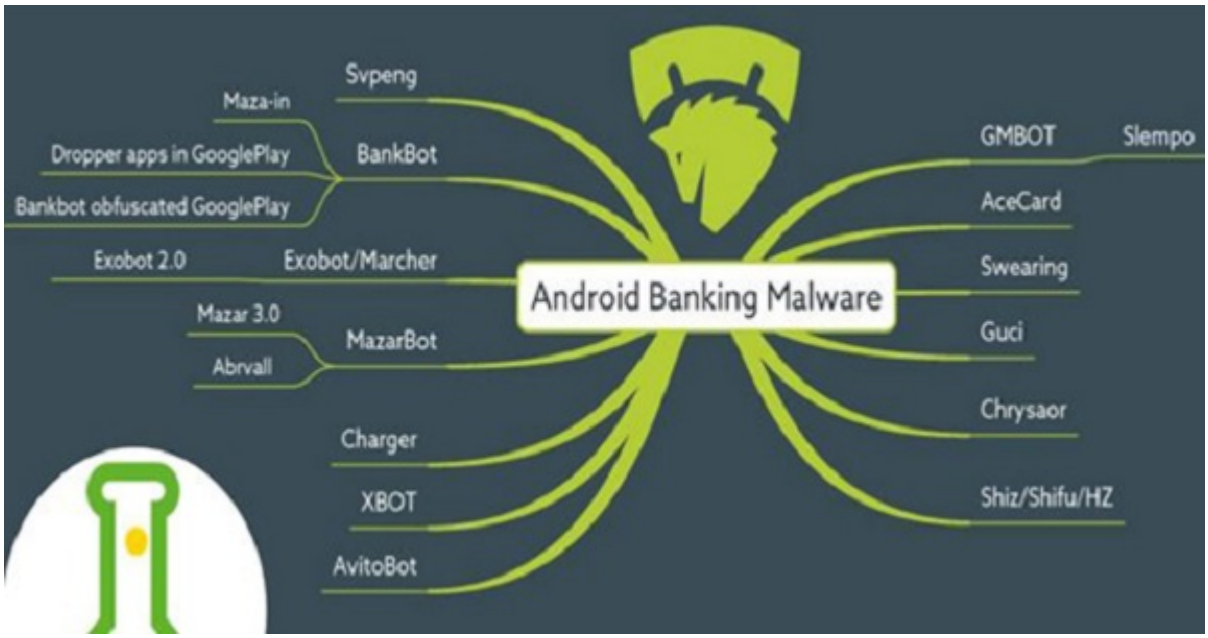
Cảnh báo mã độc Red Alert 2.0 tấn công ứng dụng ngân hàng trực tuyến

05:53 21/09/2017

Ngày 20/9, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã có công văn 490/CATT-TĐQLGS cảnh báo các tổ chức tài chính, ngân hàng thương mại về mã độc Red Alert 2.0 trên nền tảng Android tấn công ứng dụng ngân hàng trực tuyến.

Mã độc Red Alert 2.0 "ăn trộm" thông tin

Giữa tháng 9/2017, Cục An toàn thông tin đã cảnh báo về một loại mã độc ngân hàng mới gọi là Red Alert 2.0 đã được rao trên thị trường chợ đen với giá thuê 500 USD/tháng. Khác với các mã độc ngân hàng khác được phát triển từ mã nguồn của các mã độc cũ hơn, Red Alert 2.0 là một mã độc được viết lại từ đầu. Với khả năng “ăn trộm” thông tin đăng nhập, tin nhắn SMS, thu thập danh sách liên lạc, giả mạo và hiển thị phủ lên các ứng dụng hợp pháp đã cài đặt trên điện thoại của người dùng, mã độc Red Alert đang tiềm ẩn nhiều nguy cơ khó lường đối với hệ thống tài chính, ngân hàng của Việt Nam.



Các dòng mã độc ngân hàng trên nền tảng Android đã được phát hiện (Nguồn ảnh: Cục An toàn thông tin)

Thêm vào đó, mã độc Red Alert 2.0 có khả năng chặn và ghi lại các cuộc gọi từ ngân hàng và các tổ chức tài chính tới người dùng, làm cho người dùng không thể nhận được các cảnh báo tài khoản bị tấn công từ phía ngân hàng. Theo các chuyên gia công nghệ, có ít nhất 60 ứng dụng ngân hàng trực tuyến và mạng xã hội đang là mục tiêu tấn công của mã độc này.

Đề cập đến phương thức phát tán và tấn công người dùng của mã độc Red Alert 2.0, Cục An toàn thông tin cho biết, mã độc này có khả năng xâm nhập vào một số cửa hàng ứng dụng của bên thứ ba bằng cách sử dụng nhiều kỹ thuật để ngụy trang các ứng dụng nổi tiếng, hợp pháp ví dụ như: WhatsApp, Viber… cũng như giả mạo các bản cập nhật Flash Player.

Sau khi người dùng tải và cài đặt ứng dụng đã bị chèn mã độc Red Alert 2.0 trên thiết bị di động, mã độc này sẽ đợi người dùng mở một ứng dụng ngân hàng. Khi phát hiện đây là ứng dụng có giao diện mà nó có thể mô phỏng, mã độc này sẽ giả lập ứng dụng ban đầu bằng giao diện người dùng giả mạo. Giao diện giả mạo sẽ đưa ra thông báo cho người dùng về việc có lỗi trong khi đăng nhập và yêu cầu người dùng xác thực lại tài khoản của mình.

Ngay khi người dùng nhập thông tin đăng nhập vào giao diện người dùng giả mạo, Red Alert 2.0 sẽ ghi lại và gửi thông tin này tới máy chủ điều khiển và chiếm quyền kiểm soát tài khoản. Đặc biệt, kể cả đối với các ứng dụng sử dụng xác thực 2 bước (qua SMS, cuộc gọi) mã độc Red Alert 2.0 vẫn có thể vượt qua với chức năng chặn tin nhắn, cuộc gọi trên các thiết bị di động bị nhiễm mã độc.

Mã độc Red Alert 2.0 được viết hết sức tinh vi với các tính năng để ăn trộm thông tin của người dùng một cách dễ dàng, lại đang rao trên chợ đen nên có khả năng nhiều đối tượng sẽ mua để thực hiện các chiến dịch tấn công khác nhau.

Thận trọng khi cài đặt ứng dụng

Để bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công bởi mã độc, Cục An toàn thông tin khuyến nghị người dùng không tải và cài đặt ứng dụng thông qua các kho lưu trữ, liên kết không rõ nguồn gốc. Đồng thời mọi người cần kiểm tra bản quyền ứng dụng trước khi cài đặt bất kỳ ứng dụng nào.

Người dùng không nên tùy tiện trả lời những câu hỏi yêu cầu thông tin người

dùng, mật khẩu đăng nhập, thông tin tài chính, thẻ tín dụng. Đặc biệt cần lưu ý khi các thông điệp yêu cầu đó hiển thị dưới dạng hình ảnh phủ trên nền ứng dụng đang chạy.

Bên cạnh đó, người dùng nên cài đặt ứng dụng chống mã độc của nhà cung cấp có uy tín để có thể hạn chế nguy cơ bị lây nhiễm mã độc; thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin nhằm đối phó kịp thời với các nguy cơ tấn công mạng.

Đối với ngân hàng và các tổ chức tài chính, Cục An toàn thông tin khuyến nghị các đơn vị này cần kiểm tra, rà soát các ứng dụng trực tuyến đã đăng tải trên các kho ứng dụng, các ứng dụng cài đặt trên máy người dùng để tránh trường hợp giả mạo, cảnh báo đến người dùng đang sử dụng các ứng dụng do ngân hàng, tổ chức mình phát triển; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin nhằm đối phó kịp thời với các nguy cơ tấn công mạng.

Công văn của Cục An toàn thông tin cũng nêu rõ, khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, đơn vị có thể liên hệ với Cục An toàn thông tin theo số điện thoại: 024.3943.6684, thư điện tử ais@mic.gov.vn để được phối hợp, hỗ trợ.

Từ đầu năm 2017 đến nay, các chuyên gia an toàn thông tin đã phát hiện và ghi nhận nhiều chiến dịch tấn công nhằm vào ứng dụng trên nền tảng Android, đặc biệt là ứng dụng ngân hàng trực tuyến. Sự chuyển đổi mục tiêu tấn công các ứng dụng trên nền tảng Windows sang nền tảng Android liên quan đến một thực tế là ngày càng nhiều giao dịch trực tuyến được sử dụng trên thiết bị di động thay vì máy tính cá nhân.

Tại Việt Nam, nhiều ngân hàng đã phát triển ứng dụng ứng dụng ngân hàng trực tuyến trên nền tảng di động để phục vụ khách hàng, đơn cử như Ngân hàng Thương mại cổ phần Ngoại thương Việt Nam (Vietcombank), Ngân hàng Thương mại cổ phần Đầu tư và Phát triển Việt Nam (BIDV), Ngân hàng Nông nghiệp và Phát triển nông thôn Việt Nam (Agribank), Ngân hàng Thương mại cổ phần Kỹ thương Việt Nam (Techcombank)...

Hoan Nguyễn