

Cảnh báo từ Google về rủi ro hack tài khoản ngân hàng

05:52 08/09/2025

Mặc dù Google đã không ngừng nâng cấp hệ thống bảo mật trên Play Store, các ứng dụng chứa mã độc vẫn liên tục xuất hiện, đe dọa an ninh dữ liệu và tài chính của người dùng Android. Gần đây, Google đã loại bỏ 77 ứng dụng độc hại khỏi cửa hàng ứng dụng của mình, sau khi chúng đạt tổng cộng hơn 19 triệu lượt tải xuống.

Những ứng dụng này chủ yếu chứa các loại mã độc như Anatsa (còn gọi là TeaBot), Joker và Harly, được phân phối dưới dạng các công cụ hữu ích như trình đọc PDF, ứng dụng chăm sóc sức khỏe, bàn phím ảo hoặc ứng dụng chỉnh sửa ảnh. Theo báo cáo từ Zscaler ThreatLabz và Malwarebytes, các mã độc này không chỉ đánh cắp thông tin cá nhân mà còn thực hiện các giao dịch gian lận, dẫn đến thiệt hại tài chính nghiêm trọng.

Anatsa: Mã độc ngân hàng tinh vi với mục tiêu mở rộng

Anatsa lần đầu tiên được ghi nhận vào năm 2020 dưới dạng một trojan ngân hàng Android, chuyên đánh cắp thông tin đăng nhập, ghi lại phím bấm và thực hiện các giao dịch gian lận mà không cần sự can thiệp trực tiếp của nạn nhân. Đến nay, mã độc này đã phát triển mạnh mẽ, nhắm đến hơn 831 ứng dụng ngân hàng, ví điện tử và sàn giao dịch tiền điện tử trên toàn cầu, tăng từ con số 650 mục tiêu trước đó. Các chiến dịch gần đây tập trung vào các quốc gia như Đức, Hàn Quốc, Mỹ, Anh và châu Âu, với việc bổ sung hỗ trợ cho hơn 150 ứng dụng tài chính mới, bao gồm cả các nền tảng tiền mã hóa như Robinhood.



Cảnh báo từ Google về rủi ro hack tài khoản ngân hàng (Ảnh: internet)

Cách thức hoạt động của Anatsa rất tinh vi: Được ẩn náu trong các ứng dụng giả mạo (dropper apps) như trình đọc tài liệu hoặc công cụ quản lý file, ví dụ như "Document Reader – File Manager" từ nhà phát triển orukov5, đã đạt hơn 1.000 lượt tải trước khi bị gỡ bỏ. Sau khi cài đặt, ứng dụng yêu cầu quyền truy cập trợ năng (accessibility services) để tự động cấp phép các quyền nguy hiểm như đọc SMS, hiển thị cửa sổ hệ thống và sử dụng màn hình đầy đủ.

Tiếp theo, nó kết nối với máy chủ chỉ huy (C2 server) để tải xuống mã độc hại dưới dạng cập nhật, sử dụng mã hóa DES động và kiểm tra chống phân tích để tránh phát hiện. Mã độc sau đó quét các ứng dụng ngân hàng trên thiết bị, hiển thị giao diện đăng nhập giả mạo (overlay attacks) để thu thập thông tin đăng nhập, và truyền dữ liệu về cho hacker.

Trong một số trường hợp, nó còn thực hiện chuyển khoản tự động, gây thiệt hại trực tiếp cho tài khoản nạn nhân. Zscaler ước tính nhiều ứng dụng dropper của Anatsa đã vượt quá 50.000 lượt tải mỗi app, góp phần vào tổng số 19 triệu lượt tải của toàn chiến dịch. Malwarebytes lưu ý rằng Anatsa liên tục tiến hóa để vượt qua các biện pháp bảo vệ mới, khiến việc phát hiện trở nên khó khăn hơn.

Joker và Harly: Các mã độc quảng cáo và đăng ký gian lận

Bên cạnh Anatsa, hai loại mã độc khác là Joker và Harly cũng được phát hiện trong các ứng dụng bị loại bỏ. Joker là một trong những họ mã độc phổ biến

nhất trên Android, hoạt động như spyware và fleeceware. Nó xâm nhập qua các ứng dụng hợp pháp trên Play Store, yêu cầu quyền truy cập để thu thập tin nhắn SMS (bao gồm mã OTP), danh bạ liên lạc, thông tin thiết bị, và thậm chí chụp ảnh màn hình hoặc thực hiện cuộc gọi gian lận.

Mục tiêu chính của Joker là đăng ký thiết bị vào các dịch vụ cao cấp mà không có sự đồng ý của người dùng, dẫn đến phí phát sinh hàng tháng. Lịch sử của Joker bắt đầu từ năm 2019, và đến tháng 10/2022, nó là mã độc di động phổ biến thứ ba, sau Anubis và Hydra. Google đã loại bỏ hàng trăm ứng dụng chứa Joker, nhưng hacker liên tục tải lên các phiên bản mới, thường ẩn trong các app nhắn tin, theo dõi sức khỏe hoặc dịch thuật.

Tương tự, Harly là một trojan subscriber, được Kaspersky phát hiện từ năm 2020 trong hơn 190 ứng dụng trên Play Store, với ít nhất 4,8 triệu lượt tải (con số thực tế có thể cao hơn). Harly hoạt động bằng cách thu thập thông tin thiết bị và mạng di động, sau đó kết nối với máy chủ C2 để nhận danh sách dịch vụ cần đăng ký. Nó mở các trang web đăng ký trong cửa sổ ẩn, tiêm mã JavaScript để nhập số điện thoại, nhấn nút xác nhận và sử dụng mã từ SMS hoặc gọi điện để hoàn tất, dẫn đến phí trừ tiền mà người dùng không hay biết. Harly thường ẩn trong các app đèn pin hoặc công cụ đơn giản, như "com.binbin.flashlight" với hơn 10.000 lượt tải. Các nhà nghiên cứu từ HUMAN Security cho biết Harly tiếp tục tiến hóa, với 95 ứng dụng độc hại được phát hiện trong năm 2025.

Cách bảo vệ thiết bị khỏi các mối đe dọa này

Dù Google đã khắc phục lỗ hổng và gửi cảnh báo cho người dùng bị ảnh hưởng, các chuyên gia nhấn mạnh rằng người dùng cần chủ động bảo vệ. Trước khi tải ứng dụng, hãy kiểm tra nhà phát triển, số lượt tải, đánh giá và quyền yêu cầu – tránh cấp quyền không cần thiết như đọc SMS hoặc truy cập trợ năng. Không tải ứng dụng từ nguồn thứ ba ngoài Play Store, và gỡ bỏ các app không sử dụng. Kích hoạt Google Play Protect (mặc định bật) để quét ứng dụng trước khi cài đặt, và cập nhật hệ điều hành Android cùng các ứng dụng cốt lõi để nhận bản vá bảo mật mới nhất.

Sử dụng phần mềm bảo mật đáng tin cậy như Malwarebytes cho Android (phát hiện Anatsa dưới dạng Trojan.Banker.CPL) hoặc Kaspersky để quét và chặn mã độc. Ngoài ra, áp dụng xác thực hai yếu tố không dựa vào SMS (như app authenticator) để giảm rủi ro từ mã độc như Joker. Bằng cách này, bạn có thể giảm thiểu đáng kể nguy cơ bị hack tài khoản ngân hàng.

Lê Thanh (t/h)