BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Lỗ hổng bảo mật thanh địa chỉ trình duyệt Chrome cho Android

Theo 9to5Google, nhà phát triển Jim Fisher đã chứng minh rằng một trang web có thể dễ dàng thay thế thanh địa chỉ và giao diện thẻ của trình duyệt Chrome trên hệ điều hành Android, chỉ đơn giản thông qua một số thủ thuật thiết kế web.

Về cơ bản, khi người dùng cuộn xuống bất kỳ trang nào trong trình duyệt Chrome dành cho Android, giao diện người dùng phía trên với thanh địa chỉ và các thẻ sẽ bị ẩn khỏi chế độ xem. Điều mà Fisher tìm thấy là có thể bẻ khóa trong quá trình cuộn trang, cho phép cuộn lại trang mà không cần trình duyệt hiển thị lại giao diện người dùng.

Tiếp theo, khi người dùng cuộn lên, trang có thể hiển thị hình ảnh của thanh địa chỉ giả ở đầu màn hình với một URL hoàn toàn khác, bao gồm cả biểu tượng ổ khóa bảo mật cho biết trang này ở trạng thái an toàn.

Để củng cố những lập luận của mình, Fisher đã thực hiện một minh họa trực quan về việc khai thác thanh địa chỉ trong thực tế. Trong video minh họa, người dùng có thể thấy thanh địa chỉ thực hiển thị trang web jameshfisher.com đã bị đổi thành trang giả mạo có địa chỉ của ngân hàng hsbc.com.

Hiện tại, cách tốt nhất để kiểm tra xem thanh địa chỉ trang web có bị giả mạo hay không là khóa điện thoại, sau đó mở khóa lại. Thao tác này sẽ buộc Chrome trên Android hiển thị thanh địa chỉ thực.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng hệ điều hành Android cần kiểm tra cẩn thận trình duyệt Chrome khi sử dụng và cập nhật ngay khi có phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/lo-hong-bao-mat-thanh-dia-chi-trinh-duyet-chrome-cho-android-1076709.html

2. Đến lượt GitHub bị tấn công đòi tiền chuộc

Càng ngày những cuộc tấn công dữ liệu càng tăng lên, những dịch vụ nổi tiếng đình đám cũng từng ít nhất 1 lần bị các hacker đánh cắp dữ liệu. Mới đây GitHub, nền tảng chia sẻ và lưu trữ code trực tuyến lớn nhất trên thế giới, đã bị tấn công khiến hàng trăm nhà phát triển mất toàn bộ kho lưu trữ code và commit.

Các hacker đã "ngang nhiên" để lại lời nhắn tới khoảng hơn 390 nạn nhân như sau: "Để khôi phục lại kho code của bạn và tránh bị rò rỉ, gửi chúng tôi 0,1 Bitcoin (BTC - khoảng 566USD) vào ví Bitcoin địa chỉ: ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA. Liên hệ qua email admin@gitsbackup.com với tài khoản đăng nhập Git của bạn và bằng chứng của việc trả tiền (Proof of Payment). Nếu bạn không chắc chúng tôi đang có dữ liệu của bạn, hãy liên hệ và chúng tôi sẽ gửi bạn bằng chứng. Kho code của bạn đã được tải xuống và sao lưu trên dịch vụ của chúng tôi. Nếu chúng tôi không nhận được khoản thanh

toán trong 10 ngày tới, chúng tôi sẽ công khai kho code của bạn hoặc sử dụng chúng với mục đích khác."

Bên cạnh đó một số dịch vụ khác như GitLab và Bitbucket cũng chịu thảm cảnh tương tự, khoảng hơn 1.000 tài khoản BitBucket bị ảnh hưởng. Cuộc tấn công này diễn ra trong vòng 1 ngày và đã được ngăn chặn kịp thời. Điều may mắn hơn đó là các code không bị xóa mà chỉ bị thay đổi phần header của commit nên dễ dàng khôi phục lại.

Trước tình trạng trên, Giám đốc bảo mật của GitLab, Kathy Wang đã đưa ra lời khuyên với các tài khoản nên dùng các công cụ quản lý mật khẩu để lưu trữ mật khẩu, tăng tính bảo mật hơn thay vì lưu chúng dưới dạng plaintext (dạng văn bản không mã hóa) trên kho chứa có liên quan. Một số nhà phát triển khác cũng khuyên các nạn nhân cần liên hệ với nhóm hỗ trợ của GitHub, GitLab và Bitbucket trước khi trả bất kỳ khoản tiền chuộc nào cho hacker.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng dịch vụ Gibhub nên dùng các công cụ quản lý mật khẩu để lưu trữ mật khẩu tăng tính bảo mật cho nội dung lưu trữ của mình.

Link tham khảo: https://quantrimang.com/den-luot-github-bi-tan-cong-doi-tien-chuoc-163479

3. Google gỡ một số ứng dụng độc hại khỏi Play Store

Cụ thể, 6 ứng dụng có chứa tính năng chèn quảng cáo và thu thập dữ liệu người dùng trái phép này bao gồm: Camera Selfie, Total Cleaner, Smart Cooler, RAM Master, Omni Cleaner và AIO Flashlight, đều được phát triển bởi nhà sản xuất DU Group từ Trung Quốc. Các chuyên gia bảo mật của Google cho biết, cả 6 ứng dụng đều được tích hợp tính năng đánh lừa người dùng nhấn vào quảng cáo và thu thập dữ liệu người dùng

Các chuyên gia bảo mật nhận định, các ứng dụng trên còn hoạt động thu thập dữ liệu người dùng một cách bí mật. Chúng hoạt động kể cả khi người dùng không mở ứng dụng, khiến thiết bị tiêu hao pin và dữ liệu di động nhiều hơn. Theo số liệu, chỉ riêng ứng dụng Camera Selfie của DU Group đã có tới hơn 50 triệu lượt tải xuống. Trong khi đó, 5 ứng dụng còn lại cũng đạt hơn 10 triệu lượt tải xuống với vị trí cuối cùng là AIO Flashlight có 1 triệu lượt tải. Do đó, nguy cơ về số lượng người dùng bị ảnh hưởng bởi các ứng dụng trên là không hề nhỏ.

Sau khi phát hiện hành vi trái phép trên từ 6 ứng dụng của DU Group, Google đã gỡ bỏ cả 6 ứng dụng khỏi kho phần mềm Play Store. Tuy nhiên, Google không tiết lộ chi tiết về cách xử lý triệt để đối với mối nguy hại tiềm tàng này. Trên thực tế, kho phần mềm Play Store của Google hiện có tới hàng triệu ứng dụng khác nhau tới từ rất nhiều nhà phát triển phần mềm trên thế giới. Tuy nhiên, trong những năm qua, Play Store vẫn đang tồn tại một số lượng không nhỏ ứng dụng độc hại dưới vỏ bọc là những phần mềm tiện ích, trò chơi thu hút một số lượng lớn người dùng tải về.

Google dường như vẫn chưa tìm ra phương cách quản lý triệt để ngay từ bước đầu khi đăng tải phần mềm lên Play Store. Hiện tại, tất cả chỉ dừng ở việc phát hiện và xóa bỏ sau đó. Nếu mối nguy hại này không có phương án xử lý triệt để, người dùng sẽ khó có thể yên tâm khi sử dụng các thiết bị Android trong thời gian tới.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần gỡ bỏ các ứng dụng nêu trên để đảm bảo an toàn thông tin.

Link tham khảo:

http://www.antoanthongtin.vn/Detail.aspx?NewsID=38dfdb8a-bd32-4b78-bdab-f41045a588e4&CatID=c74b5c11-1141-471b-95c8-a05fe6e7d3a6

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	IBM	CVE-2019-6155 CVE-2019-4092 CVE-2018-1729 CVE-2019-4222 ...	Nhóm 15 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Apache	CVE-2019-0218 CVE-2018-1328 CVE-2019-0186 CVE-2019-0223 CVE-2018-1317 …..	Nhóm 06 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Chưa có thông tin xác nhận và bản vá
3	Oracle	CVE-2019-2602 CVE-2018-3123 CVE-2019-2587 ……..	Nhóm 160 lỗ hổng dựa trên một số sản phẩm của Oracle (MySQL, Weblogic, data server, jdk, ..) cho phép kẻ tấn công có quyền truy cập vào hệ thống qua nhiều giao thức khác nhau gây ra chậm treo, Dos của hệ thống.	Đã có thông tin xác nhận và bản vá.
4	Google	CVE-2019-2027 CVE-2019-2028 CVE-2019-2030 CVE-2019-2026 ……	Nhóm 19 lỗ hổng dựa trên một số sản phẩm của Google (Androi, Tensorflow) cho phép một ứng dụng độc hại thực, sử dụng tệp được tạo đặc biệt thi mã tùy ý trong hệ thống. Sử dụng tensorflow trong google làm tràn bộ nhớ đệm trong quá trình biên dịch.	Đã có thông tin xác nhận và bản vá.
5	Linux	CVE-2013-7470 CVE-2011-3151 CVE-2019-11486 CVE-2019-11487 …….	Nhóm 07 lỗ hổng dựa trên một số sản phẩm của Linux () Config_NetLabel bị vô hiệu hóa cho phép kẻ tấn công gây ra lỗi từ chối dịch vụ,	Đã có thông tin xác nhận và chưa có bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	localhost.localdomain
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	43trfdsds.com
6	iuefgauiaiduihgs.com
7	bszotsjovih.com
8	strikotunrev.top
9	analilaofr.com
10	dnshkjashsdk3d11144d.ru

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:

- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.