BẢN TIN NỘI BỘ

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

1. Người Việt làm web về virus corona trong 12 tiếng

Nhóm kỹ sư 5 người làm việc liên tục trong 12 tiếng để xây dựng trang web về virus corona cho người Việt, dùng AI để phát hiện tin giả.

Nhóm phát triển trang web Corona.kompa.ai gồm năm người, một số kỹ sư đang làm việc tại Mỹ, số còn lại là ở Việt Nam. Theo anh Vòng Thanh Cường, trưởng nhóm, trở ngại lớn nhất khi xây dựng trang web này là làm sao kết nối được đội ngũ Data Science tại thung lũng Silicon và đội ngũ phát triển tại Việt Nam.

Ý tưởng xây dựng một trang web thuần Việt bắt nguồn từ việc các bản đồ lây nhiễm của thế giới không có phiên bản tiếng Việt. Số ca lây nhiễm, vùng có người bị bệnh ở Việt Nam không được cập nhật chi tiết. Quan trọng hơn, những tin giả về dịch bệnh trên mạng xã hội trong nước ngày càng nhiều.

Cả nhóm xác định ưu tiên phát triển những tính năng cơ bản nhưng cần thiết trước, sau đó sẽ dần nâng cấp, cập nhật sau. Trong đó nội dung quan trọng nhất là số thống kê chính thức trên thế giới cũng như tại Việt Nam. Sau đó là các thông tin, tin giả liên quan đến sự kiện. Do đó, phiên bản đầu tiên tập trung phát triển 3 tính năng gồm: Bản đồ lây nhiễm toàn cầu; Bản đồ lây nhiễm ở Việt Nam và tin tức từ những nguồn chính thống.

Khi đã xác định được hướng đi, với công nghệ, dữ liệu có sẵn, nhóm đã "ráp" tất cả vào một cách nhanh chóng.

14h ngày 30/1, nhóm kỹ sư ở Việt Nam bắt đầu thu thập tất cả đoạn hội thoại công khai trên mạng xã hội liên quan đến virus corona. Hai tiếng sau, đội Data Science tại Mỹ và kỹ sư tại Việt Nam phân tích để xác định những chủ đề người dùng quan tâm nhất dựa trên công nghệ NLP (Xử lý ngôn ngữ tự nhiên) và Big Data có sẵn của Kompa - công ty ứng dụng Dữ liệu lớn và AI.

Đến 20h cùng ngày, nhóm kỹ sư ở thung lũng Silicon gửi bản phác thảo các tính năng cần có cho bản đầu tiên và thiết kế sơ bộ vẽ tay trên giấy. Sau đó, cả nhóm tiếp tục họp để phát triển phần giao diện người dùng. Vì không có nhiều thời gian nên nhóm quyết định bỏ qua công đoạn thiết kế giao diện (UI/UX) và sử dụng luôn một mẫu được thiết kế trước đó.

Đêm 30/1, nhóm kỹ sư ở Việt Nam bắt đầu lập trình phần kết nối dữ liệu từ WHO, đồng thời sửa lại một thành phần nhỏ về thông tin trên báo chí chính thống. Kho dữ liệu về báo chí được công ty Kompa phát triển và sử dụng được hai năm nay nên không mất nhiều công đoạn lập trình. Phát sinh duy nhất lúc này là dữ liệu của Việt Nam theo WHO luôn bị chậm so với Bộ Y tế Việt Nam công bố, do đó, các kỹ sư phải mất thêm thời gian để đồng bộ dữ liệu, đặc biệt là thông tin địa phương có người nhiễm bệnh.

Vì chênh lệch múi giờ và tính gấp rút của dự án, các thành viên trong nhóm quyết định làm việc xuyên đêm. 1h sáng ngày 31/1, các kỹ sư bắt đầu ráp lại phần

giao diện và dữ liệu đã được xử lý. Sau khi đã điều chỉnh lại giao diện, dữ liệu cho đầy đủ thông tin cho cả bản PC và mobile.

"2h ngày 31/1 dự án hoàn thành, chúng tôi nhấn bấm nút 'Publish' đưa trang web lên server tại Mỹ và chính thức công bố đến người dùng", anh Vòng Thanh Cường kể. Thời gian từ lúc bắt đầu làm trang web này đến lúc công bố là 12 tiếng.

Khác biệt lớn nhất trong bản đồ lây nhiễm của Việt Nam so với thế giới là phần tin tức. Người dùng không chỉ theo dõi được số ca nhiễm bệnh mà còn có thể cập nhật nhanh những thông tin chính thống, mới nhất liên quan đến dịch bệnh, tránh bị hoang mang bởi tin giả trên mạng xã hội. Ngoài bản đồ lây nhiễm toàn cầu được cập nhật theo thời gian thực, trang web còn có thêm bản đồ lây nhiễm của Việt Nam. Tất cả được Việt hoá để người dùng dễ dàng theo dõi.

Hệ thống ứng dụng mô hình máy học (Machine Learning) để tự động cập nhật và phân loại tin tức chính thống liên quan đến sự kiện. Trên phiên bản mới nhất, nhóm đang thử nghiệm phân tích và đánh giá các bài viết có lượng tương tác cao trên mạng xã hội. Đây là nơi tin giả xuất hiện nhiều nhất khiến cộng đồng hoang mang. Tuy nhiên, hệ thống AI cũng cần thời gian để học hỏi và cải thiện độ chính xác.

Sau một tuần ra mắt, trang web liên tục đạt đỉnh về lượng truy cập. Ngoài Việt Nam, người dùng từ nhiều quốc gia khác trên thế giới cũng lên đây cập nhật thông tin.

"Trước đây mình thường theo dõi bản đồ lây nhiễm virus corona của Vũ Hán nhưng muốn xem kỹ từng nước vẫn rất khó. Sau đó tìm thấy trang thông tin này, giao diện trực quan hơn hẳn, rất dễ theo dõi số lượng ca nhiễm bệnh, số người tử vong hoặc hồi phục của cả thế giới lẫn Việt Nam", Trần Anh, nhân viên văn phòng ở TP HCM chia sẻ.

Dự án của nhóm cũng nhận được nhiều đánh giá tốt từ giới công nghệ trong nước. Hùng Trần, Founder của Got It, đánh giá cao phần tổng hợp thông tin chính thống của trang web. "Trong hoàn cảnh này, việc có được nguồn tin tốt là vô cùng quan trọng, để mọi người bình tĩnh đánh giá tình hình và có những kế hoạch tốt thay vì hoang mang. Giải pháp của dân công nghệ nhiều khi rất đơn giản nhưng hiệu quả thiết thực", anh viết trên trang cá nhân.

Khuyến nghị: Người dùng chỉ nên lấy thông tin về dịch bệnh từ các trang web chính thống đã được kiểm duyệt, tránh đưa tin giả dẫn đến việc có thể xử lý về pháp lý trong tình hình dịch bệnh đang có diễn biến phức tạp.

Link tham khảo: https://vnexpress.net/so-hoa/nguoi-viet-lam-web-ve-virus-corona-trong-12-tieng-4050805.html

2. Google mạnh tay ngăn bên thứ ba theo dõi người dùng Chrome

Google cho biết, trong hai năm tới, họ sẽ loại bỏ việc sử dụng cookie của bên thứ ba - một loại dấu vết kỹ thuật số mà nhiều công ty sử dụng để theo dõi hoạt động của người dùng web cho mục đích quảng cáo trực tuyến.

Hành động này đã được Google tuyên bố trong một bài đăng trên blog vào tháng 8/2019, nhưng đây là lần đầu tiên gã khổng lồ tìm kiếm đưa ra mốc thời gian cụ thể cho sáng kiến của mình.

Mặc dù bước đi này giúp bảo vệ quyền riêng tư của người dùng đối với các công ty bên thứ ba. Tuy nhiên, động thái này sẽ gây ảnh hưởng không nhỏ đến các bên liên quan. Bởi theo CNET, Chrome hiện chiếm 64% thị phần trình duyệt được sử dụng.

Trong một bài đăng trên blog gần đây, Google tin tưởng rằng với việc lặp lại và phản hồi liên tục, các cơ chế bảo mật và bảo mật mở như Privacy Sandbox có thể duy trì một trang web lành mạnh, hỗ trợ quảng cáo theo cách sẽ khiến cookie của bên thứ ba trở nên lỗi thời. Khi các phương pháp này đã giải quyết được nhu cầu của người dùng, nhà xuất bản và nhà quảng cáo đã phát triển các công cụ để giảm thiểu cách giải quyết.

Tuy nhiên, điều đó không làm thay đổi tỷ lệ của Google trong việc làm giảm sử dụng dữ liệu web để tạo lợi nhuận của chính họ. Google không đưa ra dấu hiệu nào cho thấy nó sẽ thay đổi đáng kể chính sách của chính mình.

Mặc dù việc chặn cookie đã trở thành một phương pháp ngày càng phổ biến để lấy lại quyền riêng tư của một số người dùng và đã trở thành một điểm bán hàng cho các đối thủ của Chrome như Mozilla Firefox, nhưng nó cũng đã tạo ra các phương pháp theo dõi web khác như "lấy dấu vân tay".

Phương pháp giám sát web này sử dụng nhiều thông tin bí mật hơn để theo dõi thói quen của người dùng, bao gồm thiết bị theo dõi, phông chữ và các điểm dữ liệu khác để tạo một định danh duy nhất.

Ngoài việc giúp bảo vệ quyền riêng tư của người dùng, Google cũng sẽ xác định rõ hơn tầm quan trọng và sức mạnh của chính mình trong thị trường quảng cáo hướng đối tượng.

Link tham khảo: http://antoanthongtin.vn/cong-nghe-thong-tin/google-manh-tay-ngan-ben-thu-ba-theo-doi-nguoi-dung-chrome-105803

3. Cisco vá lỗ hổng DoS, lỗ hổng tiết lộ thông tin trong các thiết bị chuyển mạch doanh nghiệp nhỏ

Mới đây, Cisco đã thông báo cho khách hàng về việc một số thiết bị chuyển mạch doanh nghiệp nhỏ bị ảnh hưởng bởi các lỗ hổng có mức độ nghiêm trọng cao và có thể bị khai thác nhằm lấy thông tin nhạy cảm và thực hiện các cuộc tấn công từ chối dịch vụ (DoS).

Lỗ hổng CVE-2019-15993 và CVE-2020-3147 được báo cáo cho Cisco bởi Ken Pyle của DFDR Consulting. Hai lỗ hổng này đều có thể bị khai thác từ xa và không cần xác thực, và cả 2 đều ảnh hưởng đến giao diện người dùng dựa trên web của thiết bị chuyển mạch.

Lỗ hổng tiết lộ thông tin là do thiếu các điều khiển xác thực phù hợp. Lỗ hổng có thể bị khai thác bằng cách gửi các yêu cầu HTTP đến giao diện người dùng của một thiết bị bị ảnh hưởng. Kẻ tấn công có thể tận dụng điểm yếu này để giành quyền truy cập vào các tệp cấu hình.

Lỗ hổng DoS là do xác thực không đúng các yêu cầu được gửi đến giao diện web, có thể bị khai thác để khiến thiết bị thực hiện thao tác tải lại, từ đó tạo ra điều kiện để tấn công DoS bằng cách gửi yêu cầu độc hại.

Cisco đã tung bản vá cho cả hai lỗ hổng và cho biết chưa nhận thấy các cuộc tấn công khai thác trên thực tế.

Khuyến nghị: Người quản trị và người dùng cần cập nhật các bản vá mới nhất của thiết bị để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cisco-va-lo-hong-dos-lo-hong-tiet-lo-thong-tin-trong-cac-thiet-bi-chuyen-mach-doanh-nghiep-nho.13181/

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	Wordpress	CVE 2020 7109 CVE 2012 4919 CVE 2020 7104 …	Nhóm 10 lỗ hổng trên một số thành phần của phần mềm Wordpress (The Elementor Page Builder,...) cho phép đối tượng tấn công tấn công XSS.	Đã có thông tin xác nhận và bản vá.
2	Qualcomm	CVE 2019 10558 CVE 2019 14005 CVE 2019 14013 …	Nhóm 28 lỗ hổng trên thiết bị Qualcomm (QCS605, QM215, SDA660, MSM8953,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý. 10 lỗ hổng có điểm CVSS: 10,0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
3	Intel	CVE 2019 14601 CVE 2019 14596 CVE 2019 14629	Nhóm 03 lỗ hổng trên thiết bị Intel (Intel(R) Chipset Device Software INF Utility,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Codesys	CVE 2020 7052	01 lỗ hổng trên sản phẩm của Codesys (Control V3, Gateway V3, HMI V3,...) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
5	Apache	CVE 2019 17570	01 lỗ hổng trên phần mềm Apache cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
6	Citrix	CVE 2012 4606	01 lỗ hổng trên sản phẩm của Citrix (Citrix XenServer 4.1, 6.0, 5.6 SP2, 5.6 Feature Pack 1,…) cho phép đối tượng tấn công truy cập hệ thống trái phép.	Chưa có thông tin xác nhận và bản vá
7	Microsoft	CVE 2019 1352 CVE 2019 1460 CVE 2018 8654	Nhóm 10 lỗ hổng trên hệ điều hành Microsoft (Git for Visual Studio,…) cho phép đối tượng	Chưa có thông tin

		…	tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.	xác nhận và bản vá
8	Facebook	CVE 2019 18426	01 lỗ hổng trên ứng dụng Facebook (Whatsapp Desktop phiên bản trước 0.3.9309, Whatsapp for iPhone phiên bản trước 2.20.10,…) cho phép đối tượng tấn công tấn công XSS.	Chưa có thông tin xác nhận và bản vá

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

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	xjpakmdcfuqe.biz
5	xjpakmdcfuqe.com
6	and30.blabladomdom.com
7	xjpakmdcfuqe.in
8	amnsreiuojy.ru
9	ovrz52z140.ru
10	hzmksreiuojy.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.