Saturday, 24 February 2024

Google Tracking Assumption

In this test , we do not spoof fingerprint on web view.
So, on the same version of iOS (as same webkit version also) have same webview fingerprint

---

Test case :

Real Device	**iPhone 6s ,14.0.1 (web view fingerprint A)**	**iPhone 6s ,14.0.1 (webbrowser fingerprint A)**	
Spoof Device	**Random Device, Spoof random iOS version**	**Random Device, Spoof to 14.0.1**	
Result	**Register Gmail -> disable after 10-20 account**	**All Good Until Now**	

Kết luận:

Google dựa trên webview fingerprint, sau đó đối chiếu iOS version (hoặc có thể fingerprint khác, có tác dụng như mỏ neo) từ App hoặc UserAgent.
Xem tỉ lệ match giữa 2 bên là bao nhiêu để đưa ra unsual activity hay ko.

Trong database của Google tồn tại rất nhiều device với webview fingerprint khác nhau. Nhưng ở iOS nếu cùng version thì sẽ dùng chung 1 webview fingerprint.

Vậy nên, khi mình spoof ở real device tới một iOS version khác. Nhưng vẫn giữ nguyên data webview fingerprint như vậy. Thì dẫn đến việc Google detect rằng thiết bị này lạ so với bt => dissable.

Trong một test khác, mình đổi fingerprint webgl. Thì lại register ra gmail Unver. Nhưng lại bị ver liền sau đó 30'-1hour. Nghĩa là Google vẫn đang chấp nhận new webview fingerprint vào kho data của nó. Nhưng nó sẽ đòi ver lại để xem có đúng là fingerprint đó chuẩn hay k.

Một test khác, mình tạo profile trắng với test case như case đầu tiên + spoof webgl fingerprint , sau đó mình cho nó đi lướt web trên nhiều trang khác nhau và save lại session đó 3 ngày sau mở ra. Mình vẫn reg được Unver và vẫn sống tới giờ. Test case này hiện tại mình ngâm được 5 ngày. Từ chủ nhật tuần trước.

Như vậy, suy ra trên browser mình có ưu điểm nhược điểm khi build lại fingerprint hoặc dùng profile của người ta ntn:

Trên browser, có nhiều hardware khác nhau, để tạo một atlas device webview fingerprint chỉnh rồi fake theo nó gần như là điều không thể.

Chưa kể cách check fingerprint là khác nhau.

Xài Gologin, MultiLogin …

Ưu điểm : Ở giải pháp này ưu điểm là profile được phân bố cho rất nhiều người. Mình xài lại thì tỉ lệ profile đó match với db của Google rất là lớn

Nhược Điểm: Khi scale lớn trên một nền tảng, tỉ lệ bị trùng rất cao. Vì lượng profile chắc chắn sẽ bị limit của tụi nó

Xài riêng:

Ưu điểm: Scale vô tư vì mình có thể gen device ra bn cũng được.
Nhược điểm: Tỉ lệ match với db google gần như bằng 0. Vì mình tự tạo fingerprint riêng. Muốn để google db chấp nhận fingerprint data của mình thì phải nuôi profile đó một thời gian. (Chưa biết là bao lâu). Và phải spam fingerprint data đó rất nhiều để tăng tỷ lệ match fingerprint.

Giải pháp. hiện tại cho web browser: **KO CÓ**