# Hack thuê

## Điều tra thị trường chợ đen của dịch vụ hack tài khoản email bán lẻ

### Ariana Mirian

Một địa chỉ email duy nhất thường tiết lộ toàn bộ danh tính trực tuyến của một người, từ ngân hàng, đến kinh doanh, profile mạng xã hội và nhiều thứ khác. Nhận dạng này không chỉ được sử dụng khi đăng ký vô số dịch vụ này mà còn được sử dụng để đặt lại mật khẩu cho các dịch vụ này khi cần đến. Do đó, kẻ tấn công giành quyền truy cập vào tài khoản email cũng có nguy cơ xâm phạm tất cả các dịch vụ khác được liên kết với tài khoản đó. Các chính trị gia, nhà báo và những người tham gia tiền tệ mã hóa đều là nạn nhân của các cuộc tấn công nhắm mục tiêu ban đầu là tài khoản email của họ sau đó tàn phá các tài khoản trực tuyến khác gắn với các tài khoản email đó.

Vì tài khoản email có thể cung cấp nhiều thông tin, nhiều loại tấn công nhắm vào chúng: đoán mật khẩu, đánh cắp mã thông báo truy cập, gian lận đặt lại mật khẩu và lừa đảo, là một vài kiểu tấn công có thể kể đến. Các nhà cung cấp email đã thêm các cơ chế như câu hỏi bảo mật, lọc thư rác và xác thực hai yếu tố để hạn chế tỷ lệ thành công của các cuộc tấn công này. Các biện pháp phòng vệ này ngăn chặn nhiều trường hợp, do đó làm tăng độ tinh vi và thời gian cần thiết để truy cập tài khoản. Tuy nhiên, những kẻ tấn công có mục tiêu cụ thể, sẵn sàng bỏ thêm công sức để truy cập vào một tài khoản khi đối mặt với các phòng thủ kín kẽ này.

Mặc dù các cuộc tấn công nhắm mục tiêu thường bị cho là tấn công khả năng cấp quốc gia, thì có một thị trường chợ đen mới nổi cho các dịch vụ "hack thuê", tấn công nhắm mục tiêu cho bất kỳ ai sẵn sàng trả một khoản chi phí nào đó. Mục đích của các dịch vụ này là xâm nhập vào tài khoản của nhiều nhà cung cấp email khác nhau, như ví dụ trong hình 1. Vì các dịch vụ này chỉ mới xuất hiện, ít ai biết được cách chúng tấn công nạn nhân của chúng và mức độ rủi ro mà chúng gây ra.

(hình 1)

Để hiểu rủi ro này, ACM đã điều tra thị trường chợ đen hack thuê, nhận diện 27 dịch vụ hack tài khoản email bán lẻ và thử dùng các dịch vụ này. Sử dụng danh tính bí mật, ACM đã tham gia với các dịch vụ này để đột nhập vào "nạn nhân" mà thực sự là tài khoản Google mà ACM kiểm soát. Làm việc với Google, ACM đã ghi lại cả những tương tác giữa ACM với tin tặc và cách tin tặc cố gắng tấn công nạn nhân.

### Để bắt một tin tặc

Nhìn chung, thị trường chợ đen nhắm mục tiêu toàn lừa đảo, nhưng một số dịch vụ cũng đã thực hiện tấn công tinh vi, mà phương thức tấn công chính vẫn là các chiêu lừa đảo. Các cuộc tấn công này là liên tục, được cá nhân hóa và có thể vượt mặt bảo mật SMS 2FA (xác thực hai yếu tố). Sử dụng các thông tin thu được từ các cuộc tấn công này để xác định các nạn nhân khác, ACM ước tính cứ một trong một triệu tài khoản Google là bị tấn công. Với sự tinh vi của các cuộc tấn công lừa đảo, ACM cho tin rằng biện pháp phòng vệ tốt nhất cho người dùng là bảo vệ tài khoản bằng các khóa bảo mật U2F (Universal 2nd Factor) dưới dạng cơ chế 2FA. Khóa bảo mật U2F bảo vệ chống lại các cuộc tấn công lừa đảo tinh vi vì giao thức U2F xác thực tên miền trước khi gửi mã 2FA, ngăn người dùng khỏi bị lừa đảo. Mặc dù trọng tâm của cuộc điều tra này là về các tài khoản Google, nhưng những bài học rút ra được khái quát hóa tương đối tốt cho các nhà cung cấp email khác.

#### Khám phá dịch vụ

Việc điều tra các dịch vụ hack thuê bắt đầu bằng cách tìm kiếm các diễn đàn chợ đen tiếng Anh, Trung Quốc và Nga để tìm các quảng cáo liên quan đến việc chiếm đoạt tài khoản mục tiêu. ACM cũng đã tìm trên Google các từ khóa dành riêng cho việc chiếm quyền điều khiển để xác định các dịch vụ có mặt tiền cửa hàng công khai và ACM đã liên hệ với các nhóm lạm quyền trong các công ty Internet lớn để tìm kiếm khách hàng tiềm năng như vậy mà họ đang theo dõi. Trong tất cả, 27 dịch vụ hack thuê tiềm năng đã được xác định. Phần lớn các dịch vụ này được quảng cáo bằng tiếng Nga và có giá dao động từ $23 đến $500 mỗi hợp đồng.

#### Đóng giả người mua

Đối với 27 dịch vụ hack thuê, ACM đã liên lạc qua một "người mua giả” (persona) duy nhất để bảo vệ danh tính và để tránh liên kết các tương tác của ACM giữa các dịch vụ này. Mỗi persona được đặt một tên dựa theo ngôn ngữ bản địa của dịch vụ hack. Ví dụ: nếu dịch vụ được quảng cáo bằng tiếng Nga, thì ACM chọn tên chung và họ bằng tiếng Nga cho persona đó. ACM cũng tạo một tài khoản Google cho mỗi persona để sử dụng cho tất cả các giao tiếp qua email. Đối với các dịch vụ không phải tiếng Anh, một người bản ngữ dịch khi giao tiếp.

#### Chọn một nạn nhân

Khi ký hợp đồng dịch vụ hack thuê, ACM tạo ra nhân vật nạn nhân persona để làm mục tiêu. Các nạn nhân persona cũng được tạo các footprint trực tuyến lớn nhằm giống điều kiện thực tế. Điều này có nghĩa là tạo tên và tài khoản Google cho nạn nhân theo cách tương tự như tính cách người mua thông thường. Hộp thư đến của nạn nhân persona cũng gồm tập hợp các tin nhắn từ kho thư điện tử Enron để tạo ấn tượng rằng tài khoản Google ấy đang được sử dụng. ACM đã thay thế tên và thông tin nhận dạng khác từ tin nhắn của Enron bằng thông tin của nạn nhân. Hơn nữa, địa chỉ Gmail của nạn nhân được thiết lập bảo vệ SMS 2FA, hình thức 2FA được sử dụng rộng rãi nhất hiện nay. Điều này được sử dụng để xác định xem các dịch vụ hack thuê có thể qua mặt loại bảo vệ này hay không.

Ngoài ra, ACM tạo một trang web quảng cáo một doanh nghiệp nhỏ mà nạn nhân sở hữu hoặc làm việc tại đó. ACM đã mua tên miền của các trang web từ đấu giá để đảm bảo mỗi tên miền có lịch sử trước đó. ACM cũng mua bảo vệ quyền riêng tư cho từng tên miền để bảo vệ thông tin đăng ký (một nghiên cứu gần đây cho thấy 20% tên miền được bảo vệ theo cách này, vì vậy ACM không mong đợi sự bảo vệ quyền riêng tư sẽ bị đánh dấu red flag). Trang web này được liên kết với địa chỉ email của nạn nhân, cũng như địa chỉ email của một cộng tác viên hư cấu. Bằng cách này, ACM có thể xác định liệu các dịch vụ hack thuê có tấn công cộng sự để làm đòn bẩy có quyền truy cập vào tài khoản nạn nhân hay không. ACM cũng đã tạo một trang Facebook cho nạn nhân để xem liệu các dịch vụ hack thuê có sử dụng nó trong các cuộc tấn công của họ hay không. Tất cả các mục trên trang Facebook là riêng tư (người dùng công cộng sẽ không thể xem các mục này) ngoại trừ phần About Me, nơi trang web của nạn nhân được liệt kê (dưới dạng quảng cáo cá nhân cho doanh nghiệp của nạn nhân).

#### Giám sát các cuộc tấn công

Do không chắc chắn về phương thức tấn công mà các dịch vụ hack thuê này sẽ sử dụng, ACM đã tạo ra một cơ sở hạ tầng giám sát rộng rãi, sẽ báo ngay khi người dùng trái phép nhập và sửa đổi tài khoản Google. ACM cũng theo dõi các trang web để ghi lại tất cả khách truy cập. Cơ sở hạ tầng giám sát này bao gồm: (1) tập lệnh ứng dụng Google cho Gmail trong mọi tài khoản; (2) Nhật ký Google; và (3) một mạng lưới bắt tất cả lưu lượng truy cập đến các trang web hư cấu.

Tập mã lệnh ứng dụng Google được tải vào Gmail cho mỗi tài khoản là đoạn script được chỉnh lại dựa trên một nghiên cứu được sử dụng trong nghiên cứu trước đó.Tập mã lệnh ứng dụng Google sẽ gửi thông tin đến máy chủ được kiểm soát qua proxy cho biết liệu tập lệnh có được kết nối với tài khoản hay không và liệu có mọi thay đổi đối với tài khoản. Ví dụ: tập lệnh ứng dụng Google sẽ cho biết liệu một tin nhắn mới đã xuất hiện trong hộp thư đến hay thư mục spam, nếu một tin nhắn được chuyển vào thùng rác hoặc nếu bất kỳ tin nhắn nào được đánh dấu là “chưa đọc” của người dùng. Việc ghi nhật ký này nhằm ghi lại hành động của những kẻ tấn công khi chúng thâm nhập được vào tài khoản.

ACM cũng có thể phân tích bất kỳ hoạt động đăng nhập nào vào tài khoản Google của nạn nhân. Các bản log này được các đồng nghiệp Google của ACM nắm bắt và phân tích, ghi lại các lần thử đăng nhập vào tài khoản và nguồn gốc của chúng, các kỹ thuật tấn công đăng nhập brute-force và liệu 2FA có được kích hoạt trên tài khoản để thử đăng nhập đáng ngờ hay không.

Cuối cùng, ACM ghi lại mọi lưu lượng truy cập mạng đến trang web của mỗi nạn nhân. Như đã đề cập, địa chỉ trang web đã được liên kết trên phần About Me trên trang Facebook của nạn nhân. Nếu kẻ tấn công có thể tìm thấy trang web thông qua trang Facebook, điều này sẽ rõ ràng khi theo dõi bản lưu capture mạng. Việc capture mạng cũng sẽ hiển thị nếu có bất kỳ kiểu hack nào đến tài khoản Google là từ cùng một địa chỉ IP đang truy cập các trang web.

#### Cân nhắc về pháp lý và đạo đức

Vì nghiên cứu này liên quan đến việc thực hiện các hoạt động bất hợp pháp nên có những câu hỏi về đạo đức và pháp lý cần xem xét.

Về mặt pháp lý, có hai mối lo ngại: truy cập trái phép vào tài khoản Google và vi phạm các điều khoản dịch vụ của Google. Tại Hoa Kỳ cũng như ở nhiều quốc gia khác, việc truy cập trái phép vào tài khoản điện tử là bất hợp pháp. Thuê dịch vụ để thực hiện hành động này có thể được coi là hỗ trợ và tiếp tay; tuy nhiên, vì các tài khoản email nằm dưới sự kiểm soát của ACM và tổ chức đã hợp tác với nhà cung cấp dịch vụ (Google), nên ACM đã ủy quyền rõ ràng cho các thực thể truy cập vào tài khoản. Hơn nữa, việc tạo tài khoản Google giả mạo vi phạm các điều khoản dịch vụ của Google, nhưng nghiên cứu này đã được cả Google và cố vấn chung cho UC San Diego chấp thuận, trước khi tiến hành khảo sát.

Mặc dù nghiên cứu này không được xem xét về mặt nhân quyền thông qua hội đồng đánh giá của ACM bởi vì ACM đã cân nhắc đây là hành vi của doanh nghiệp, không phải hành vi của cá nhân. Ngoài ra cũng có những cân nhắc đạo đức khác. Bằng cách tạo ra nạn nhân hư cấu và người mua giả (persona), ACM đã loại bỏ khả năng bất kỳ cá nhân nào bị hại trong nghiên cứu này. Hơn nữa, ACM đã tương tác với các dịch vụ này trong phạm vi các điều khoản của họ và trả tiền cho họ nếu họ thành công. ACM cho rằng những bài học rút ra từ nghiên cứu này lớn hơn chi phí thanh toán cho các dịch vụ hack.

### Playbook hack thuê

Thí nghiệm được quản lý và hệ thống ghi log nhật ký cho phép kiểm tra playbook mà kẻ tấn công sử dụng để chiếm đoạt tài khoản nạn nhân. Chỉ năm trong số 27 dịch vụ mà ACM liên hệ thực sự đã cố xâm nhập vào tài khoản Google của nạn nhân. Cần lưu ý hack thuê được xem là "thành công" còn tùy thuộc vào hành động của ACM: trong một số trường hợp, ACM đã cung cấp mật khẩu hoặc mã 2FA khi được nhắc nhở bởi một trang lừa đảo, trong khi trong các trường hợp khác, ACM không phản hồi các email lừa đảo.

Nhìn chung, ACM không nhận thấy có kiểu tấn công brute-force đăng nhập nào, cũng như liên lạc với tài khoản Facebook của nạn nhân hoặc liên lạc với email của cộng sự nạn nhân. Trong số năm dịch vụ cố gắng truy cập vào tài khoản, một dịch vụ đã gửi phần mềm độc hại nạn nhân thực thi thông qua email. Mặc dù ACM không thể chạy tệp thực thi trong sandbox máy ảo, VirusTotal đã báo cáo rằng phần mềm thực thi phần mềm độc hại là trojan truy cập từ xa. Bốn dịch vụ khác sử dụng phương thức lừa đảo làm công cụ tấn công chính. ACM chia sẻ những phát hiện chính ở đây, chi tiết cụ thể hơn được đề cập trong báo cáo đầy đủ khác.

#### Mồi email và lừa đảo

Tất cả các cuộc tấn công bắt đầu với một email lừa tài khoản nạn nhân. Những mồi lừa đảo thường là mạo danh một số nhân vật đáng tin cậy hoặc có thẩm quyền, có lẽ để thúc đẩy nạn nhân nhấp vào liên kết. Có năm loại mồi trên tất cả các tin nhắn lừa đảo: mạo danh nhân viên liên kết, ngân hàng, người lạ, một cơ quan chính phủ hoặc Google. Hình 2 hiển thị cụ thể chi tiết này. Giả làm nhân viên lừa đảo để dụ dỗ nạn nhân nhấp vào "hình ảnh" (dẫn đến trang lừa đảo), trong khi những kẻ lạ mặt bao gồm một người không xác định gửi email cho người dùng bằng "hình ảnh" hoặc liên kết. Tuy nhiên, giả danh chính phủ, ngân hàng và Google để truyền đạt cảm giác cấp bách trong các email lừa đảo. Hình 3 cho thấy các ví dụ về một mồi nhử của chính phủ (được dịch sang tiếng Anh) và một mồi nhử Google.

(hình 2-3)

Trung bình, những kẻ tấn công đã gửi 10 tin nhắn trong suốt 25 ngày và sử dụng các mồi khác nhau trong các cuộc tấn công dai dẳng của chúng. Hình 2 minh họa hành vi này, cho thấy thời gian kể từ khi những kẻ tấn công gửi tin nhắn email đầu tiên của chúng, loại mồi nhử cho mỗi tin nhắn và khi chúng ta nhấp vào mồi nhử (có khả năng tạm dừng mọi tấn công tiếp theo). Dấu X cho biết khi ACM nhấp vào liên kết trong tin nhắn được gửi cho nạn nhân. Mỗi hàng tương ứng với một nạn nhân và các số ở bên phải biểu thị tổng số email được gửi bởi một dịch vụ. Con mồi phổ biến nhất là bắt chước giao diện Google, tiếp theo là giả cộng sự, sau đó là email từ người lạ.

Trong số các dịch vụ đã gửi mồi cá nhân, tất cả trừ một người hỏi người mua để biết thêm chi tiết trước thời hạn (chẳng hạn như tên và địa chỉ email của một nhân viên đã biết). Một dịch vụ có thể xây dựng mồi nhử được cá nhân hóa mà không cần thêm thông tin từ người mua, chỉ ra rằng dịch vụ này đã tìm kiếm và tìm thấy trang web trực tuyến được xây dựng cho nạn nhân. Tuy nhiên, ACM cũng đã mua hai hợp đồng khác từ dịch vụ này và trong cả hai trường hợp, bên dịch vụ đã hỏi người mua để biết chi tiết về nạn nhân. Những khác biệt trong hành vi cho thấy các dịch vụ này có nhiều người làm việc đằng sau.

Như đã đề cập trước đây, tất cả trừ một trong các dịch vụ đều dựa vào lừa đảo là công cụ tấn công chính. Nhấp vào liên kết lừa đảo đã đưa ACM đến một trang đích trông giống như trang đăng nhập Google. Sau khi nhập mật khẩu, ACM đã được đưa đến một trang nhắc về mã 2FA. Tất cả các dịch vụ có thể truy cập vào tài khoản đã làm như vậy bằng cách lừa đảo mã SMS 2FA, vượt mặt bảo vệ bảo mật này.

#### Thích ứng trực tiếp

Trong khi hầu hết các dịch vụ đều xác định có bảo mật 2FA trong luồng lừa đảo thì có hai dịch vụ tấn công lừa đảo cho thấy chúng có thể vượt được cơ chế bảo mật này. Ban đầu, hai dịch vụ này không xác định mã 2FA. Luồng lừa đảo của chúng ban đầu đã thu thập mật khẩu và sau đó cố gắng đăng nhập vào tài khoản Google, nhưng đã bị 2FA chặn thành công. Sau khi nhận ra điều này, cả hai dịch vụ đều gửi cho nạn nhân các email bổ sung với cấu trúc khác với các email đã gửi trước đó. Một trong hai dịch vụ này đã gửi một tin nhắn mới, khi được nhấp, sẽ yêu cầu cả mật khẩu và mã 2FA. Dịch vụ còn lại cũng thay đổi chiến lược và tính đến cách vượt mã 2FA, bằng cách gửi các tin nhắn lừa đảo trông giống như các tin nhắn được gửi từ dịch vụ thứ ba. Những điểm tương đồng này gợi ý việc sử dụng các công cụ phổ biến giữa các dịch vụ.

Lưu ý rằng các dịch vụ này có thể vượt mặt 2FA được vì chúng lừa lấy mã SMS 2FA từ người dùng. Như đã đề cập trước đây, SMS 2FA là hình thức 2FA được sử dụng rộng rãi nhất và ACM muốn xem liệu người sử dụng có dễ bị tấn công hack thuê giả định hay không. Để ngăn các dịch vụ hack thuê có được quyền truy cập vào tài khoản, người dùng nên thiết lập khóa bảo mật 2FA, vì mã đó không thể lừa đảo được.

#### Sau khi tấn công được

Khi có quyền truy cập vào tài khoản của nạn nhân, các dịch vụ hack thuê bắt đầu xóa mọi chứng cứ và đảm bảo khả năng lấy lại quyền truy cập nếu cần. Các dịch vụ này có được quyền truy cập vào tài khoản nạn nhân, sau đó đã xóa tất cả các thông báo email của Google liên quan đến đăng nhập thiết bị mới từ cả hộp Inbox và Trash. Không có dịch vụ nào thay đổi mật khẩu, nhưng ACM đã quan sát thấy ba dịch vụ nhanh chóng xóa số xác thực và số khôi phục 2FA khỏi tài khoản nạn nhân sau khi chúng vào được. ACM cho rằng chúng đã thực hiện bước này để đảm bảo người mua có thể truy cập vào tài khoản và để dịch vụ có thể lấy lại quyền truy cập vào tài khoản, nhưng ACM không thấy bất kỳ dịch vụ nào đăng nhập lại vào tài khoản sau lần đăng nhập đầu tiên. Về bản chất, các dịch vụ đã thực hiện các biện pháp phòng ngừa để loại bỏ footprint trực tuyến của chúng khỏi tài khoản Google mà chúng xâm nhập được.

Khi tài khoản email bị truy cập trái phép, ngoại trừ một dịch vụ duy nhất đã khởi tạo tính năng trong Google có tên là Takeout, cho phép chúng tải xuống nội dung email của tài khoản nạn nhân và cung cấp gói thông tin cho người mua ảo. Chỉ có một dịch vụ tránh đăng nhập vào tài khoản nạn nhân và cung cấp mật khẩu cho người mua mà không sử dụng trước. Những phát hiện này nêu bật một rủi ro mới về dữ liệu và các quy định xung quanh việc hợp lý hóa quyền truy cập vào dữ liệu người dùng. Mặc dù có ý định cải thiện khả năng sử dụng cho người dùng, các khả năng như Takeout cũng làm tăng mức độ dễ dàng mà một vụ cướp có thể làm lộ tất cả dữ liệu người dùng cho một dịch vụ. Kể từ nghiên cứu này, Google đã bổ sung thêm xác minh tăng cường cho các hành động tài khoản nhạy cảm.

### Nạn nhân thực sự và hoạt động thị trường

Dựa trên những phát hiện này, ACM đã phân tích diễn đàn của các dịch vụ thành công nhất để hiểu mức giá của chúng cho các dịch vụ khác. Hơn nữa, ACM trình bày ước tính số nạn nhân thực sự bị ảnh hưởng bởi các dịch vụ này dựa trên dấu vết đăng nhập từ Google. Phát hiện của ACM cho thấy thị trường này là khá hẹp.

#### Dịch vụ thay thế và giá cả

Mặc dù cuộc điều tra của ACM tập trung chủ yếu vào Google vì những ràng buộc pháp lý, nhiều dịch vụ hack thuê mà ACM liên hệ cũng có khả năng xâm nhập vào các loại tài khoản khác. Hình 4 cho thấy giá của các dịch vụ hack thuê từ ngày 10 tháng 10 năm 2018. Tất cả giá đều tính bằng đô la Mỹ, được chuyển đổi từ đồng rúp của Nga. Dấu \* cho biết giá quảng cáo của dịch vụ thấp hơn giá xuất chi cuối cùng được dịch vụ yêu cầu.

(hình 4)

Trong năm dịch vụ này, tấn công nhà cung cấp dịch vụ email của Nga là ít tốn kém nhất, trong khi tài khoản Google hoặc Yahoo là tốn kém nhất. Tấn công vào tài khoản mạng xã hội ở mức giá trung bình. Các quảng cáo cho một trong các dịch vụ thể hiện giá thay đổi theo thời gian, được hiển thị trong Hình 5. Giá hack tài khoản Google đã tăng nhiều nhất từ 123 đô la lên 384 đô la cho mỗi tài khoản trong hai năm qua trong khi chi phí hack nhà cung cấp dịch vụ email của Nga vẫn không thay đổi. Những khác biệt và thay đổi giá này có lẽ là kết quả của vô số yếu tố như nhu cầu, thay đổi về bảo mật và cạnh tranh từ các dịch vụ khác.

(hình 1)

#### Nạn nhân theo thời gian

Trong số 27 dịch vụ mà ACM ký hợp đồng, chỉ có ba dịch vụ có thể đăng nhập vào tài khoản email nạn nhân thành công. Google đã phân tích metadata liên quan với các lần thử đăng nhập thành công và thấy rằng cả ba dịch vụ đều dựa trên quy trình tự động hóa giống hệt nhau để kiểm tra tính hợp lệ của mật khẩu, vượt mặt bảo mật như 2FA và tải xuống toàn bộ nội dung email của nạn nhân. Mặc dù địa chỉ người gửi và địa chỉ email gửi khác nhau cho các hợp đồng khác nhau, quy trình tự động hóa đăng nhập là như nhau trong suốt tám tháng mà các dịch vụ này được ký hợp đồng. Google đã có thể tạo được dấu vết đặc trưng về cách thức đăng nhập tự động này và phân tích hồi tố có bao nhiêu tài khoản Gmail có nỗ lực đăng nhập đáng ngờ.

Google đã xác định 372 tài khoản được nhắm mục tiêu theo khung đăng nhập tự động này từ ngày 16 tháng 3 năm 2018 đến ngày 15 tháng 10 năm 2018 hoặc khoảng một trong số 1 triệu người dùng Google. Hình 6 cho thấy bảng phân tích hàng tuần về số lượng tài khoản Google được nhắm mục tiêu. Xin lưu ý rằng những con số này là giới hạn tối thiểu, vì ACM không thể suy ra có bao nhiêu người dùng được nhắm mục tiêu bởi các dịch vụ này nhưng không nhấp vào liên kết (hoặc cung cấp thông tin của họ để cấp quyền truy cập), chỉ có bao nhiêu người dùng có tài khoản được truy cập bởi những dịch vụ này. Mặc dù có những hạn chế nhưng khối lượng hoạt động của các dịch vụ hack thuê là khá nhỏ khi so sánh với các dịch vụ khác như bộ công cụ lừa đảo, ảnh hưởng đến hơn 12 triệu người dùng mỗi năm. ACM cho rằng hack thuê vào tài khoản email cá nhân là thị trường hẹp so với các thị trường khác, chẳng hạn như phân phối phần mềm độc hại.

(hình 6)

### Thảo luận

Nhìn chung, các dịch vụ hack thuê tính phí $100- $400 mỗi hợp đồng được xem là đã tạo ra các cuộc tấn công tinh vi, liên tục và được cá nhân hóa có thể vượt qua 2FA thông qua lừa đảo. Tuy nhiên, nhu cầu về các dịch vụ này dường như chỉ giới hạn ở thị trường hẹp, bằng chứng là số lượng dịch vụ nhỏ có thể khám phá, số lượng dịch vụ thành công thậm chí còn nhỏ hơn và thực tế là những kẻ tấn công này chỉ nhắm mục tiêu vào khoảng một triệu người dùng Google . Hơn nữa, thị trường này bị cho là có dịch vụ khách hàng kém, vì nhiều dịch vụ chậm hoặc không nhất quán trong phản hồi của họ đối với người mua ảo của ACM.

Không xét đến hành vi của thị trường, nghiên cứu này làm sáng tỏ tầm quan trọng của khóa bảo mật đối với người dùng cho rằng tài khoản email của mình đang có nguy cơ, vì chỉ có khóa bảo mật mới có thể bảo vệ người dùng khỏi các cuộc tấn công được xét đến trong nghiên cứu này. Tuy nhiên, khi thị trường phát triển và cơ chế bảo mật thay đổi, các cuộc tấn công cũng có thể thay đổi và chuyển từ lừa đảo sang các mối đe dọa dai dẳng hơn như phần mềm độc hại.

Kết hợp với nghiên cứu này, Google đã giới thiệu hai biện pháp phòng vệ mới để giúp bảo vệ chống lại lừa đảo MITM, để bảo vệ tốt hơn chống lại các dịch vụ này. Google hiện chạy các heuristic bổ sung khi bạn đăng nhập và cũng ngăn một số dạng framework đăng nhập tự động. Ngoài ra, hai trong số các dịch vụ đã tăng gần gấp đôi giá hack tài khoản Google kể từ khi Google triển khai các biện pháp bảo vệ mới cho người dùng, mặc dù không biết liệu việc tăng giá này có phải là ngẫu nhiên hay là do Google tăng cường cơ chế bảo mật.

#### Nhìn nhận

Tác giả cảm ơn các đồng tác giả của ấn phẩm nghiên cứu ban đầu vì sự giúp đỡ và phản hồi của họ khi viết bài viết này: Kurt Thomas, Geoffrey M. Voelker, Joe DeBlasio, and Stefan Savage. We would also like to thank Mikhail Kolomogorov for his significant assistance with translating email messages, as well as translation help from Kirill Levchenko, Vector Guo Li, and Ivan Mikhailin. Our thanks to Shawn Loveland for providing additional leads on underground hack-for-hire services. We thank Elie Bursztein, Angelika Moscicki, Tadek Pietraszek, and Kashyap Puranik for their feedback on the original research study. We are also thankful to the editors for their feedback. This work was supported in part by NSF grants CNS-1629973 and CNS-1705050, and DHS grant AFRL-FA8750-18-2-0087.