Những cách Hacker sử dụng để ẩn danh

Tin tặc sử dụng nhiều cách khác nhau để ẩn danh trong khi hack, tuy nhiên phải nói rằng ẩn danh hoàn toàn là chuyện không tưởng nhưng các hacker có thể an toàn và ẩn danh ở mức độ nào đó và đảm bảo việc thoi dõi ngược lại là rất khó. Dưới đây là một số phương pháp giúp hacker ẩn danh trong khi đang xâm nhập vào hệ thống nào đó.

1. Không sử dụng Windows

Windows đầy những lỗ hổng có thể bị khai thác. Hàng tháng Microsoft phát hành bản vá bảo mật với các bản sửa lỗi mới nhất. Những lỗ hổng này có thể cho phép phần mềm gián điệp xâm nhập, hoàn toàn vượt qua tất cả các nỗ lực giấu tên của bạn. Bất kỳ hacker nào muốn ẩn danh đều tránh Windows như bệnh dịch. Thay vào đó, họ sử dụng hệ điều hành nguồn mở mã nguồn mở an toàn, chẳng hạn như Tails và Whonix.

2. Không kết nối trực tiếp với mạng Internet

Tránh mọi người theo dõi địa chỉ IP thực của bạn thông qua việc sử dụng các dịch vụ VPN và TOR.

VPN cho phép người dùng tạo ra một đường hầm riêng. Bất cứ ai cố gắng theo dõi từ phía mạng Internet chỉ có thể xem địa chỉ của máy chủ VPN, có thể là một máy chủ nằm ở bất kỳ quốc gia nào trên thế giới mà bạn chọn.

TOR là một mạng lưới toàn bộ các node định tuyến lưu lượng truy cập của bạn. Mỗi node trong đường truyền chỉ nắm được IP của node trước đó. Cuối cùng, các lưu lượng truy cập đi qua mạng Internet thông thường từ một trong những node này, gọi là exit point. Cách tiếp cận hoàn hảo nhất là kết hợp cả hai và sử dụng VPN trước khi đi vào TOR.

Ngoài ra, hacker còn sử dụng các proxy chain, nó cho phép hacker có thể định tuyến lưu lượng truy cập của họ thông qua một loạt các máy chủ proxy và ẩn danh bằng cách ẩn nấp sau chúng. Thực tế, nó làm cho các máy chủ proxy (proxy server) chuyển tiếp yêu cầu của hacker sao cho có vẻ như yêu cầu đó đến từ máy chủ proxy không phải từ các máy chủ hacker. Hacker thực sự khiến lưu lượng truy cập đi qua các proxy và do đó IP của họ được thay đổi nhiều lần và IP gốc không được hiển thị.

3. Không sử dụng địa chỉ email thực

Thay vào đó, hãy sử dụng các dịch vụ email ẩn danh hoặc remailer. Các dịch vụ email nặc danh cho phép bạn gửi email cho ai đó mà không để lại bất cứ dấu vết nào, đặc biệt nếu kết hợp với truy cập VPN hoặc TOR. Remailer là dịch vụ bạn có thể sử dụng tài khoản email thật để gửi email và nó sẽ chuyển tiếp thư đó ở chế độ nặc danh. Một vài remailer còn có thể gửi lại mail nhưng việc này có thể là hành động "gậy ông đập lưng ông". Nó có thể ghi lại địa chỉ thực của bạn, tuy nhiên remailer có thể thêm các lớp ẩn danh bổ sung để đảm bảo an toàn.

4. Không sử dụng Google

Google theo dõi mọi thứ bạn làm để phục vụ cho các quảng cáo của họ mà người dùng có thể click vào. Có nhiều cách để khai thác công cụ tìm kiếm hữu ích này mà không để lại danh tính như dịch vụ StartPage cho các kết quả google mà không lưu trữ địa chỉ IP, cookie hoặc kết quả tìm kiếm. DuckDuckGo cũng là dịch vụ tương tự như vậy.

Ngoài ra, trình duyệt Tor Browser cũng là một sự lựa chọn thông minh. Khi sử dụng trình duyệt này, lưu lượng truy cập hoặc các gói dữ liệu có nguồn gốc từ máy tính được thực hiện để đi qua một điểm nhất định gọi là node. Trong toàn bộ quá trình yêu cầu đến trang web cụ thể, địa chỉ IP sẽ được thay

đổi nhiều lần và không thể xác định được địa chỉ IP của bạn do trình duyệt đã tạo những lớp mã hóa. Do đó các hacker có thể duyệt Internet nặc danh. Ngoài ra, trình duyệt Tor còn cho phép bạn truy cập vào Dark Web hoặc web ẩn.

5. Không sử dụng Wifi công cộng

Có hai vấn đề ở đây, một là địa chỉ MAC duy nhất sẽ được router ở nơi công cộng nghi lại, mặc dù bạn có thể tránh điều này bằng cách sử dụng MAC spoofing. Nếu bạn bị từng truy ngược lại địa chỉ MAC thật thì có thể tìm ra máy tính gốc, cộng thêm với việc CCTV của quán có thể ghi lại hình ảnh và danh tính của bạn sẽ bị truy ra. Thứ hai tấn công Wifi rất phổ biến, kỹ thuật tấn công man-in-the-middle qua Wifi sẽ làm lộ tẩy tất cả nỗ lực giấu tên của bạn. Tuy nhiên các hacker khác sẽ cần phải trên cùng một mạng Wifi vật lý để biết danh tính của bạn.

6. Sử dụng Macchanger

MAC là viết tắt của Media Access Control. Thay đổi Mac là một trong những việc cần làm của các hacker để ẩn danh. Mỗi thiết bị có một địa chỉ MAC duy nhất được cung cấp bởi các nhà sản xuất tương ứng. Các gói dữ liệu được chuyển giao có một địa chỉ MAC nguồn và địa chỉ MAC đích. Bây giờ, nếu gói dữ liệu bị chặn hoặc theo dõi, địa chỉ MAC có thể được xác định và dễ dàng truy tìm hacker. Vì vậy, hacker thường thay đổi địa chỉ MAC của họ trước khi thực hiện các cuộc tấn công.

Các tin tặc thực có thể thêm vào nhiều lớp bảo mật để ẩn danh các hoạt động của họ. Tuy nhiên, sáu cách ở trên là những cách hữu ích nhất.