TẤT TẦN TẬT VỀ REVERSE ENGINEERING Ở MỸ:

- Mảng chuyên môn trong cybersecurity với lương khởi điểm trên 100,000 USD cho người mới ra trường! Trong cybersecurity, malware reverse engineering là chuyên môn phân tích cơ chế hoạt động của mã độc dựa vào cấu trúc và chức năng của chúng. Vì mã độc thường ở trong dạng compiled binaries (e.g. file exe trên Windows), việc phân tích cần chúng ta phải đọc hợp ngữ (assembly) và decompiled code chứ không phân tích source code như thông thường.

Chính vì vậy, reverse engineering được coi là một trong những chuyên môn khó nhất trong cybersecurity. Công việc của reverse engineer thì sẽ thường tập trung vào 3 mảng chính:

PHÂN TÍCH VÀ PHỤC HỒI:

Reverse engineer sẽ phân tích mã độc để hiểu được sự ảnh hưởng của chúng sau những cuộc tấn công an ninh mạng. Sau đó, họ sẽ trợ giúp loại bỏ malware và phục hồi hệ thống cho những công ty khách hàng. Một ví dụ mà mình làm gần đây là vụ Change Healthcare ở Mỹ khi team mình phải phân tích mã độc tống tiền để giúp các bệnh viện phục hồi hệ thống mạng của họ một cách an toàn.

THEO DÕI HOẠT ĐỘNG CỦA TỘI PHẠM AN NINH MẠNG:

Dữ liệu phân tích từ mã độc còn giúp theo dõi hoạt động của các nhóm tội phạm an ninh mạng lớn hoặc những tổ chức được tài trợ bởi chính phủ các nước. Thông thường, các tổ chức này sẽ được tracked thông qua sự tương đồng giữa những mã độc mà họ sử dụng, và nhiệm vụ của reverse engineers là phân tích để confirm những sự tương đồng đó.

NHẬN DIỆN MÃ ĐỘC:

Sau khi phân tích, reverse engineer sẽ giúp viết detection signatures (mã nhận diện) dựa trên những đặc tính của mã độc. Với signatures từ một mã độc, chúng ta có thể dễ dàng tìm kiếm những mã độc khác trong cùng một chủng nếu chúng cùng chia sẻ những đặc tính này. Những signatures này cũng chính là thứ giúp các chương trình anti-virus như Windows Defender, Avast, và Crowdstrike quét và nhận diện mã độc trên hệ thống của chúng ta.

Thị trường công việc cho reverse engineer tại Mỹ:

Vì mảng này là một chuyên môn của cybersecurity nên sẽ ít có job openings hơn so với các nghề khác trong field. Nhưng mà cũng vì thế nên job security rất ổn định và có rất ít layoffs. Vì là specialized field nên lương khởi điểm cho reverse engineer ở Mỹ cũng khá cao, dao động từ 120k đến 200k USD tuỳ theo công ty.

Điều đặc biệt và cũng là điều mình thích nhất của mảng này là không nhất thiết phải có bằng cấp hoặc chứng chỉ nhất định trong ngành. Đây là một file mà chỉ cần có kỹ năng và biết cách trình bày những kỹ năng này cho các nhà tuyển dụng là có thể có job! Nếu các bạn hứng thú, mình sẽ làm một post chia sẻ cách mình đã nhập field này ntn!