

Chân dung tin tặc Việt vừa bị trục xuất sau 7 năm ngòai tù Mỹ

Đứng sau một trong những hệ thống bán danh tính khách hàng lớn nhất từng tồn tại, tin tặc (hacker) Ngô Minh Hiếu kiếm được hơn 3 triệu USD trước khi bị mật vụ Mỹ bắt tại đảo Guam năm 2013.

Ngô Minh Hiếu sinh năm 1989 ở Gia Lai và có biệt danh Hieupc. Vừa được thả và trục xuất về Việt Nam sau 7 năm ngòai tù tại Mỹ, Hiếu đã liên hệ với trang KrebsOnSecurity từ nơi cậu ta đang phải cách ly bắt buộc do dịch Covid-19, để chia sẻ câu chuyện của bản thân. Hiếu hy vọng sẽ thuyết phục những người giỏi về máy tính đừng đi theo vết xe đổ của mình.

Ở thời đỉnh cao trong “sự nghiệp tội phạm mạng”, Hiếu kiếm tới 125.000 USD/tháng nhờ điếu hành dịch vụ bán thông tin cá nhân chi tiết lấy được từ những công ty môi giới dữ liệu hàng đầu thế giới. Và chính lòng tham đã khiến Hiếu rơi vào bẫy của Mật vụ Mỹ.

Trong vài năm bắt đầu từ khoảng 2010, chỉ có một thiêu niên duy nhất ở Việt Nam, tên là Ngô Minh Hiếu, điếu hành một trong những dịch vụ nổi tiếng và sinh lời nhiều nhất trên mạng Internet, chuyên bán “fullz” – bộ dữ liệu cá nhân đánh cắp được bao gồm tên, ngày sinh, số thẻ an sinh xã hội, email và địa chỉ thực tế của một khách hàng.

Lúc bị bắt vào năm 2013, Hiếu đã kiếm được trên 3 triệu USD nhờ bán dữ liệu cho những kẻ ăn trộm danh tính và các đường dây tội phạm có tổ chức hoạt động trên đất Mỹ.

Tháng 2/2013, đặc vụ Mỹ Matt O’Neill đã thực hiện thành công kế hoạch dụ Hiếu rời Việt Nam đến Guam, để bắt giữ và đưa ra tòa án tại Mỹ. O’Neill hiện là Giám đốc Trung tâm chiến dịch

điều tra toàn cầu của Mật vụ Mỹ, chuyên hỗ trợ điều tra các tổ chức tội phạm xuyên quốc gia.

O'Neill cho biết đã tiến hành điều tra dịch vụ bán danh tính do Ngô Minh Hiếu điều hành, sau khi đọc về dịch vụ này trong một câu chuyện có tựa đề "Danh tính của bạn trị giá bao nhiêu?" trên trang KrebsOnSecurity năm 2011. Theo ông, hoạt động của Hiếu đã tiếp tay cho cả một hệ thống tội phạm mạng đánh cắp các tài khoản và gian lận tín dụng lên tới hơn 1 tỷ USD.

"Tôi không rõ có tên tội phạm mạng nào gây tổn thất tài chính cho người Mỹ nhiều hơn Hiếu hay không. Cậu ta đã bán thông tin cá nhân của hơn 200 triệu người Mỹ, cho phép mọi đối tượng mua chúng chỉ với giá vài xu", O'Neill nói.

Khi còn nhỏ, Hiếu được gia đình mua cho một chiếc máy tính và cậu ta đam mê máy tính từ đó. Lớn lên, Hiếu sang New Zealand học đại học và lúc đó, Hiếu đã là admin của nhiều diễn đàn hacker trên web đen. Trong lúc học, nam sinh viên đã phát hiện một lỗ hổng trong mạng lưới máy tính của trường làm lộ dữ liệu thanh toán. Báo cho quản trị viên IT nhưng không ai quan tâm, Hiếu bèn hack luôn cả hệ thống rồi dùng lỗ hổng đó tấn công các trang web khác và ăn trộm được rất nhiều thông tin.

Sau khi bị nhà trường phát hiện và báo cảnh sát, Hiếu phải về nước khi hết học kỳ 1 vì không được gia hạn thị thực. Để trả thù, Hiếu tấn công trang web của trường, khiến nó tê liệt ít nhất 2 ngày.

Về Việt Nam, Hiếu đi học lại nhưng vẫn dành nhiều thời gian lên mạng trên các diễn đàn tội phạm mạng. Cậu chuyên thủ hack cho vui sang hack vì tiền, khi thấy dễ dàng kiếm tiền từ đánh cắp dữ liệu khách hàng. Cậu cũng giao du với một số bạn bè từ các diễn đàn ngầm và bắt đầu nghĩ đến đánh cắp dữ liệu cá nhân để bán.

"Tiền kiếm được quá nhanh đã khiến tôi mê mẩn", Hiếu tâm sự.

Số tiền phí pháp 3 triệu USD

Một trong những trang web của Ngô Minh Hiếu chuyên cung cấp dịch vụ đánh cắp danh tính.

Mục tiêu lớn đầu tiên của Hiếu là công ty báo cáo tín dụng MicroBilt ở New Jersey.

“Tôi hack nên tổng của họ, đánh cắp cơ sở dữ liệu người dùng để có thể dùng đăng nhập khách hàng nhằm tiếp cận dữ liệu [người dùng] của họ. Tôi đã ở trong hệ thống của họ khoảng gần một năm mà họ không hay hay biết”, Hiếu nhớ lại.



Tiếp đó, Hiếu lập trang Superget[.]info, chuyên bán hồ sơ người dùng cá nhân. Ban đầu, dịch vụ của Hiếu được thực hiện thủ công nhưng sau đó, hacker này tìm ra cách sử dụng các máy chủ mạnh ở Mỹ để tự động thu thập lượng lớn dữ liệu người dùng từ các hệ thống của MicroBilt và các hãng dữ liệu khác. MicroBilt đã phát hiện và đẩy Hiếu ra khỏi hệ thống, nhưng Hiếu trở lại được nhờ một lỗ hổng khác.

Sau này, Hiếu tìm thấy một mục tiêu hấp dẫn hơn, đó là công ty Mỹ Court Ventures chuyên lập hồ sơ công cộng từ tài liệu tòa án. Thứ Hiếu quan tâm thực chất là thỏa thuận chia sẻ dữ liệu của Court Ventures với US Info Search, vì hãng môi giới dữ liệu này có khả năng tiếp cận nhiều hồ sơ người dùng nhạy cảm

hơn. Bằng một vài thủ thuật, Hiếu thuyết phục được Court Ventures tin mình là một nhà điếu tra tư nhân ở Mỹ.

Năm 2012, Court Ventures được mua lại bởi Experian – một trong những tổ chức tín dụng khách hàng lớn của Mỹ. Hiếu trả cho Experian hàng nghìn đôla mỗi tháng để mua dữ liệu khách hàng, thông qua các tài khoản mới lập và đa số ở Trung cộng, Malaysia và Singapore.

Đặc vụ O'Neill cho biết, trang web của Hiếu thực hiện hàng chục nghìn lệnh truy vấn mỗi tháng và kiếm bộn tiền nhờ ăn chênh lệch. Trong khi Court Ventures thu của Hiếu 0,14USD, thì cậu ta thu của khách hàng 1USD.

Hiếu bị Mật vụ Mỹ bắt tới và họ phát hiện một số email Hiếu gửi cho các đồng phạm, hướng dẫn cách thanh toán tiền cho Experian bằng cách chuyển khoản từ các ngân hàng châu Á. Các đặc vụ bắt đầu tìm cách đưa Hiếu vào bẫy.

Tính đến năm 2012, Hiếu đã kiếm được hơn 3 triệu USD từ các hoạt động trên mạng. Cậu nói với cha mẹ rằng mình kiếm tiền nhờ phát triển website cho các công ty.

Sa bẫy và hối hận

Cuối cùng, Hiếu đã “cắn câu” của mật vụ Mỹ khi tới Guam để gặp một hacker người Anh nhằm dàn xếp một số vụ việc và thiết lập hợp tác. Hiếu không hay biết người này đã bị kết án và chính là “mồi nhử”, khiến cậu ta sa bẫy ngay khi bước chân xuống máy bay.

Sau khi bị tạm giam 2 tháng ở Guam, Hiếu bị đưa tới New Jersey, nơi hacker thừa nhận đã thâm nhập vào MicroBilt cùng nhiều hệ thống khác. Hiếu kể rằng, trong quá trình xét xử, tòa án liên bang đã nhận khoảng 13.000 thư khiếu nại từ các nạn nhân. Họ trình bày mình bị mất nhà, mất việc và không còn khả năng mua nhà hay duy trì nguồn tài chính. Điếu đó khiến Hiếu nhận ra mình là kẻ tội tề và cảm thấy rất ân hận.



“Nhà tù là một nơi khốc liệt, nhưng nó cho tôi thời gian nghĩ về cuộc đời và các lựa chọn của mình. Tôi đang cố gắng làm điều tốt và trở nên tốt đẹp hơn mỗi ngày. Giờ đây, tôi hiểu ra rằng tiền chi là một phần của cuộc sống, chứ không phải tốt đẹp và cũng không mang lại hạnh phúc thực sự”.

“Tôi hy vọng những tội phạm mạng rút kinh nghiệm từ những gì tôi đã trải qua và dừng tay, thay vào đó hãy sử dụng các kỹ năng của mình góp phần làm cho thế giới tốt đẹp hơn”.

[Theo Internet](#)