

THEO CHÂN HACKER LÀM "ĐẠO CHÍCH" ONLINE

"Anh thích Laptop IBM hay Ipad nano 60 GB?" - Dak nói, giọng không có vẻ gì là đang đùa - "Em đang có hơn ngàn con "CC chùa" (mã thẻ tín dụng trực tuyến bị ăn cắp) còn ngon, chưa xài, ship thẳng hàng về Việt Nam đơn giản.

"Anh thích Laptop IBM hay Ipad nano 60 GB?" - Dak nói, giọng không có vẻ gì là đang đùa - "Em đang có hơn ngàn con "CC chùa" (mã thẻ tín dụng trực tuyến bị ăn cắp) còn ngon, chưa xài, ship thẳng hàng về Việt Nam đơn giản. Anh chỉ phải ra hải quan làm thủ tục nhận hàng. Tỷ lệ thành công khoảng 60%, có gan thì em làm liền!" Tập làm "Newbie" Sự thực là Dak (nickname của một chàng thanh niên Việt Nam sinh năm 1984) không hề đùa, trước đó chỉ vài phút, Dak hướng dẫn tôi bằng một vài từ khóa search trên Google để lần đến một shop bán hàng online nước ngoài bị lỗi lập trình Jet Database - Một dạng của lỗi SQL Injection.. Bằng một vài câu lệnh khác, anh ta bắt đầu thay đổi các số từ nhỏ cho đến lớn để tìm ra cột có chứa giá trị username và password của admin. "Theo kinh nghiệm thì cột 262 thường tương ứng với số 46" - Dak đã chiến thắng.

"CC chùa" được rao bán trên nhiều diễn đàn...

"Việc tiếp theo là tìm ra link Cpanel", cũng bằng kinh nghiệm. Dak nói: "Các shop thông thường hay có các link Cpanel kiểu mặc định ban đầu của mã nguồn, (như <http://www.tênshop.com/shopadmin.asp> hoặc [tênshop.com/shopadmin1.asp](http://www.tênshop.com/shopadmin1.asp)) thường thì các shop đã thay đổi link, nhưng thực tế là không phải ai cũng mẫn mà với những công việc rắc rối của quy trình bảo mật. Sai lầm chết người thường đến từ những lỗ hổng đơn giản nhất". Dak giảng giải và bắt đầu lấy từ database của shop này các mã tài khoản tín dụng (CC - Credit Card) có thể dùng để thanh toán trực tuyến. Cho đến trước khi những chủ tài khoản này kịp phát hiện ra vấn đề và đổi mật khẩu, Dak có toàn quyền sử dụng chúng để order bất cứ mặt hàng nào có giá thấp hơn tổng số tiền của tài khoản. Và thường thì anh ta ship hàng từ một vài shop lớn khác, thông qua các dịch vụ chuyển phát trung gian để gửi nó về Việt Nam dưới dạng gift (quà tặng). Mọi việc chỉ diễn ra chưa đầy 30 phút. Nhưng thực ra, kinh nghiệm và may mắn đã giúp Dak lần này, thường thì những lần khác phải khá vất vả, trình độ bảo mật ngày càng cao khiến việc hack shop không phải lúc nào cũng thành công, có khi hacker phải ngồi lì vài ngày, việc thay các giá trị từ thấp đến cao vào câu lệnh tìm ra bảng chứa giá trị cột pass admins có khi từ 1 đến vài trăm, mất rất nhiều thời gian. "Không có bất cứ shop nào dám tuyên bố là mình bảo mật bất khả xâm phạm, và những lỗi phổ biến nhất thường là Jet database và SQL Injection". Dak nhận định. Dak

mới 22 tuổi, cậu ta biết chat lần đầu tiên cách đây 4 năm, khi đang học lớp 11, sau đó, mày mò học làm web tặng bạn gái trên một số diễn đàn, Dak bắt đầu có nhu cầu sử dụng các tên miền dài hạn và được host tương đối tốt. Cậu được một số đàn anh trong "thế giới ngầm" chỉ dạy việc sử dụng các "CC chùa" để mua tên miền và host. "Đó là những tài sản vô hình (tên miền, dung lượng hosting - NV), em gần như không cảm thấy áy náy và có lỗi vì em không trục lợi gì về vật chất khi muốn có những thứ để xây dựng forum và web âm nhạc miễn phí cho bạn bè" - Dak tâm sự. Nâng cao trình độ Quá trình đi lên từ "newbie" (lính mới) của Dak diễn ra bằng con đường tự học hỏi và mò mẫm trên các diễn đàn là chính. Đôi khi cũng có những bậc đàn anh có trình độ và nhiều kinh nghiệm chỉ dạy tận tình. Song để ship được thành công, đòi hỏi nhiều kinh nghiệm tự mày mò hơn là kiến thức. Dak nói: "Nguyên việc fake IP (dùng địa chỉ IP ảo trên Internet) khi mua hàng trực tuyến bằng tài khoản "chùa" đã là một yêu cầu sơ đẳng, phải làm sao để IP không phải là IP ở Việt Nam, quan trọng hơn, State (địa chỉ) của IP sử dụng phải trùng với state của CC sử dụng mới đạt đến độ tin cậy cao nhất, song đó vẫn chưa phải là tất cả, lần ship hàng nào cũng cần thêm yếu tố may rủi". Trước đây, Dak và cư dân thế giới ngầm CC "chùa" thường dùng một số tool như Findnot, nhưng hiện tại, chủ yếu họ dùng các dạng "private sock", tức là dùng sock riêng bằng cách remote qua một Host trung gian do shipper tự mua. Dữ liệu sẽ được chuyển qua host trung gian này đến shop. Như thế khi shop trực tuyến check IP sẽ chỉ thấy được IP của host, còn Shipper sau khi xóa log từ Host sẽ bảo mật được IP mà không ai biết, và các IP luôn có "độ sạch" cao! "CC chùa" được phát tán đầy trên mạng, phần lớn trong số đó không còn xài được nữa, song có những người chuyên hack shop để bán CCV (mã thẻ tín dụng đã được chứng thực) và những thứ này thường là đáng tin cậy." - Dak nói tiếp và khẳng định: "Những người có đủ trình độ hack shop ngày càng ít đi, phần lớn dân shipper thường xài CC có sẵn do người khác share hoặc bán cho, điều đó làm cho cư dân thế giới ngầm ngày càng hỗn loạn. Những tay chuyên nghiệp bắt đầu giữ miếng để làm riêng và việc này vì thế ngày càng khó phát hiện". Sau vài năm nghiên cứu về lập trình và hacking, Dak - vốn rất có năng khiếu bắt đầu tự hack được những shop hàng đầu tiên để có CC của riêng mình. Dần dần, trình độ của Dak để sử dụng chúng sao cho hiệu quả cũng bắt đầu nâng lên. Tất nhiên, nó cũng đồng nghĩa với việc cậu ta ngày càng lún sâu vào vòng xoáy của ma lực và tội lỗi. Tất nhiên không phải bất kỳ thông số nào của "CC chùa" cũng dùng được ngay. Trước khi sử dụng nó vào mục đích mong muốn. Các shipper cần có một công đoạn quan trọng và cũng hết sức sơ đẳng là... đọc CC. Dak nói: "CC chia làm nhiều loại như Visa, Amex (American Express), Master Card,... Mỗi loại thẻ có con số đầu tiên khác nhau. Do vậy cần chú ý khi chọn loại mã thẻ tín dụng phù hợp. Sau đó là đến công đoạn kiểm tra xem CC live or died (Thông số còn chính xác hay đã bị thay đổi)." Thông thường Dak check CC ở một dịch vụ của Yahoo. Nếu các thông số là chính xác, dịch vụ đó sẽ accept CC của cậu ta - nghĩa là CC đó hoàn toàn có thể mang ra sử dụng. Một thủ thuật khác để biết số tiền hiện có trong tài khoản là so sánh giá cả: "Anh hãy thử tiến hành những bước đầu mua hàng bằng CC hack được ở một shop online" Dak giải thích - và chọn món hàng bất kỳ, nếu shop chấp nhận việc mua hàng, nghĩa là số tiền trong tài khoản lớn hơn hoặc bằng giá tiền món hàng trong shop đó. Khi đó, anh có thể hoàn tất việc mua bán hoặc cancel để chọn món hàng khác ở bất kỳ shop nào. Luật lệ của "Thế giới ngầm"

...và được các shipper share cho nhau vô tội vạ qua email!

Tất cả việc trao đổi của tôi và Dak đều được diễn ra qua chat YahooMessenger. Đó là một trong những luật lệ quy ước của "thế giới ngầm". Nếu không thực sự cần thiết thì tốt nhất không cần biết thông tin thật về nhau, không webcam, gọi nhau bằng nick và tất nhiên, rất khó để hai shipper gặp nhau ngoài đời. Tôi và Dak quen nhau qua một diễn đàn về hacking, Dak bắt đầu liên lạc thường xuyên với tôi khi tôi ngỏ ý muốn được cậu ta hướng dẫn thử ship hàng "chùa", thực ra thì chúng tôi chỉ thực sự thân nhau sau khi tôi giúp cậu ta không bị block nick trên một diễn đàn do một người bạn của tôi lập ra. Ngay cả như vậy, Dak vẫn giấu tên thật và cho rằng việc gặp nhau là phiền hà. Nhưng việc chia sẻ thì luôn là một phần không thể thiếu trong "thế giới ngầm", cho dù tôi mới chỉ thuyết phục được Dak coi tôi là newbie (người mới vào nghề). "Tất cả mọi người mới đều phải học cách chia sẻ. Không ai ăn hết được cả ngàn CC trong một cái shop cả. Nên chia chác nó cho những người khác, ai nhanh chân người đó hưởng. Như thế bất cứ khi nào anh cần anh cũng có thể có "hàng" để xài từ những sự chia sẻ trở lại." Dak bắt đầu nhồi nhét vào đầu tôi. Luật bất thành văn thứ hai: tinh thần màu cờ sắc áo! Có một điều mỉa mai là tất cả những tài khoản do người Việt Nam mở ở nước ngoài là những tài khoản "ngon" nhất. Sẽ chẳng ai nghi ngờ một chủ tài khoản người Việt mua hàng gửi về cho đồng hương nước nhà! Nhưng shipper "thế giới ngầm" quy ước với nhau là không bao giờ xài tài khoản của người Việt. Thậm chí, kẻ nào xài mà bị phát hiện, chắc chắn sẽ nhận được thái độ ghét bỏ và kỳ thị từ đa số những shipper khác. Dak cho biết cậu ta là một thành viên của diễn đàn hiện đang qui tụ những shipper giỏi nhất ở Việt Nam. "Nhưng những luật lệ ở đó rất nghiêm khắc, anh phải có nhiều người giới thiệu, mình tôi không đưa anh vào được! Ở đó có rất nhiều kinh nghiệm của các bậc đàn anh, nhiều tài nguyên và "CC chùa". Quyền truy cập vào các box kín trong diễn đàn này phụ thuộc vào chất lượng các bài viết của anh và số lượng các bài cảm ơn sau mỗi bài viết đó". Cuộc thử nghiệm đầu tiên Trong lúc chat và trao đổi với tôi, Dak đưa ra một quyết định bất ngờ, cậu ta muốn thử ship món hàng đầu tiên về Việt Nam. "Các bậc đàn anh trong thế giới ngầm từng nhiều lần hướng dẫn em, bài học đã thuộc lòng, nhưng chưa thử lần nào" - Dak bắt đầu bài học mới cho tôi. Sau khi có đầy đủ thông số chính xác của một CC còn expire date (hạn sử dụng), shipper tiến hành giao dịch trên các website bán hàng trực tuyến, (Apple.com, eBay.com, iPod.com...) và các dịch vụ chuyển hàng (như Fedex...) nếu suôn sẻ, sau khoảng 3 ngày thông tin sẽ được xử lý và hàng "lên đường". Một tuần hoặc sớm hơn, nó sẽ có mặt ở Việt Nam, chờ được lấy về. Giờ mới là khâu quyết định! Sau khi nhận được giấy báo nhận hàng, shipper sẽ đến cơ quan hải quan, kỳ kèo thuế má (thường là nói mình là sinh viên, hàng gửi về có giá trị thấp để xin miễn thuế), thực ra chính đòn tâm lý này sẽ khiến các cán bộ hải quan tin món hàng có giá trị thấp và hoàn toàn trong sạch... Để chắc ăn, giới shipper chuyên nghiệp thường có một khâu kỳ công nữa: kiếm một cái chứng minh nhân dân giả, thay ảnh họ vào đó để đánh lừa hải quan, điều này sẽ giúp shipper ngăn ngừa

những hậu quả có thể gặp phải sau này với cơ quan pháp luật! Dak khẳng định, đa số giới shipper còn hoạt động hiện nay đều giống như cậu ta: rất trẻ và mạnh mẽ, thường thì dưới 25, và am hiểu nhiều thứ, từ kỹ năng IT đến các công đoạn giao dịch hàng hóa trực tuyến. Dak bảo: "Phần lớn các bậc đàn anh có tuổi mà em biết đều đã giải nghệ, họ buộc phải nghĩ cách làm ăn chân chính, hơn là ngày càng mạo hiểm với trò chơi phù phiếm nhưng đầy ma lực của thế giới ngầm". "Anh thích iPod Nano 60 GB hay ĐTDĐ?" Dak hỏi. "Cậu đã check xong CC rồi à?" "CC của em luôn live bất cứ lúc nào, iPod hay điện thoại?" "Em định ship với số hàng có giá trị bao nhiêu?" "Khoảng 2000 USD, em sẽ nhận hàng bằng địa chỉ nhà trọ của em. Địa chỉ của anh là gì, em gửi tặng anh một con iPod làm quà, có gì em chịu, anh vô can". "Uhm...3h đêm rồi. Anh phải đi ngủ", tôi signout và biến. Bốn ngày sau, Dak cho biết chuyến hàng 5 con iPod mua từ châu Âu của cậu ta đã bị trả lại nơi xuất sau khi đến Mỹ mà không rõ lý do. "Chỉ có thể nói là em thiếu may mắn, có lẽ shop này đã quá cảnh giác với những địa chỉ nhận hàng ở Việt Nam". Trên thực tế, việc ship hàng trực tiếp về Việt Nam đã trở nên quá nguy hiểm, và gần như không còn shipper có kinh nghiệm nào còn dám liều lĩnh. Dak đã tìm ra lời giải cho thất bại lần đầu tiên của mình, vài ngày sau cậu ta bắt đầu tìm kiếm những nhịp cầu móc nối xuyên quốc gia. Dak giảng giải với tôi về Drop (danh từ dành cho những người nhận "hàng" thuê ở nước ngoài. Và hứa sẽ giới thiệu tôi với một "cao thủ" dày dạn trong thế giới ngầm! Thế Phong