KEVIN MITNICK

WILLIAM L. SIMON

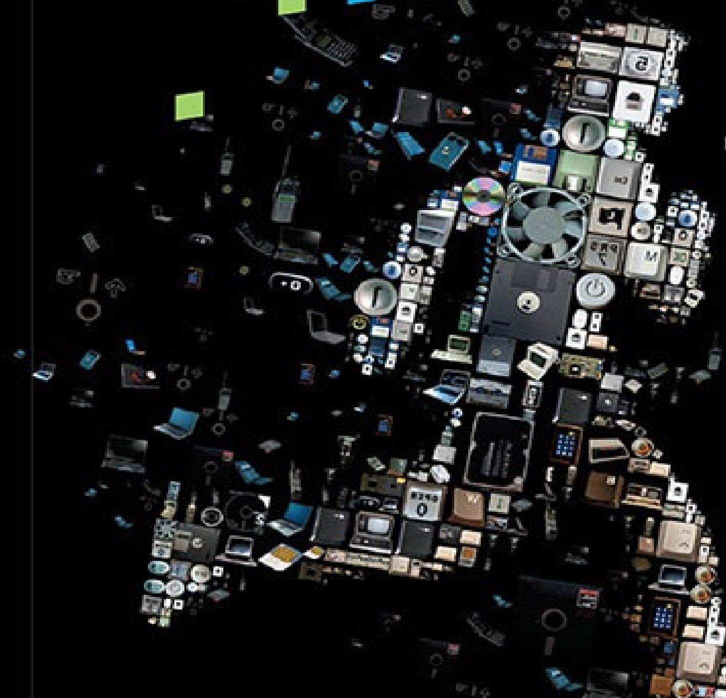
Trần Thanh Hương và LeVN dịch

GHOST IN THE WIRES

AN TOÀN THÔNG TIN TRONG KỶ NGUYÊN SỐ

BÓNG MA TRÊN MẠNG

CUỘC PHIÊU LƯU CỦA HACKER BỊ TRUY NÃ GẮT GAO NHẤT THẾ GIỚI



alphabooks
NHÀ XUẤT BẢN CÔNG THƯƠNG

BÓNG MA TRÊN MẠNG

Tác giả: **William L. Simon, Kevin Mitnick**

Nguyên tác: **Ghost in the Wires**

Nhà xuất bản: **NXB Công Thương**

An Toàn Thông Tin Trong Kỷ Nguyên Số

Trong kỷ nguyên số, vấn đề bảo mật và an toàn trên không gian mạng ngày càng trở nên quan trọng, không chỉ đối với các doanh nghiệp, tổ chức, chính phủ, mà còn đối với từng cá nhân. Việt Nam có 58 triệu tài khoản Facebook (tính đến hết quý 1/2018); 127 triệu thẻ ngân hàng với 66,6 triệu tài khoản thanh toán cá nhân; cùng hàng tỷ các giao dịch mua bán, trao đổi trên mạng diễn ra mỗi ngày. Chính vì vậy, an ninh mạng trong kỷ nguyên số đang trở thành một chủ đề ngày càng nóng.

Chỉ rất gần đây, nhiều tài khoản Facebook cũng như email cá nhân đã bị hacker tấn công và chiếm đoạt. Thủ đoạn của hacker khá đơn giản khi tận dụng các sơ hở của người dùng cũng như các lỗi bảo mật của hệ thống, nhưng chúng đã gây ra những thiệt hại rất lớn cả về vật chất và tinh thần cho người dùng – rất nhiều thông tin cá nhân bị lộ và bị mất, và điều đó cũng đang xảy ra với rất nhiều tổ chức, công ty, cả tư nhân lẫn nhà nước.

Ngay đầu tháng 11/2018, một số nguồn tin lan truyền trên mạng cho rằng hệ thống công nghệ của Thế giới Di động bị hacker tấn công và thông tin của khách hàng bị tiết lộ. Các tài khoản thẻ ngân hàng cũng như email và số điện thoại cá nhân bị kẻ xấu công khai trên mạng dù cho nghi vấn lộ dữ liệu khách hàng vẫn đang tiếp tụcđược điều tra, xác minh.

Ngược về quá khứ, tháng 4/2018, website của ngân hàng Vietcombank bị tấn công. Sự cố xảy ra với trang con của website Vietcombank khi người dùng đăng ký email liên kết với tài khoản ngân hàng. Khi được chia sẻ qua Facebook, ảnh bìa của trang con này hiển thị dòng chữ “Đại học Quốc gia Hà Nội”. Hacker còn để lại hai câu thơ “Trăm năm Kiều vẫn là Kiều/ Sinh viên thi lại là điều tất nhiên”.

Năm 2016, hệ thống các sân bay lớn tại Việt Nam như Sân bay Quốc tế Tân Sơn Nhất, Sân bay Quốc tế Nội Bài, Sân bay Quốc tế Đà Nẵng, Sân bay

Phú Quốc đều bị hacker tấn công và để lại nhiều nội dung xúc phạm, xuyên tạc.

Cuối năm 2014, hệ thống các website của VCCorp cũng bị tấn công, làm tê liệt hoạt động truy cập vào toàn bộ hệ thống website báo chí đối tác của VCCorp và gây thiệt hại trực tiếp tới hoạt động của các trang này, đồng thời ảnh hưởng tới hàng triệu độc giả và người tiêu dùng sử dụng các dịch vụ trực tuyến của họ. Theo VCCorp, ước tính sơ bộ sau hai ngày bị tấn công, số tiền VCCorp bị thiệt hại vào khoảng 5 tỷ đồng, bao gồm tất cả các loại doanh thu như quảng cáo, thương mại điện tử…

Trên thực tế, không ít những vụ tấn công mạng đã xảy ra liên tiếp tại Việt Nam trong thời gian gần đây và để lại những hậu quả không hề nhỏ. Những vụ việc như thế này đang gióng lên một hồi chuông cảnh báo đối với các cá nhân cũng như doanh nghiệp trong thời đại số. Với xu thế phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0 trên toàn thế giới, trong đó có Việt Nam, sự bùng nổ của các thiết bị IoT sẽ mang lại nhiều nguy cơ tiềm ẩn về các cuộc tấn công trên không gian mạng hoặc bị kẻ xấu lợi dụng để tấn công vào các hạ tầng.

Chuyên gia an toàn thông tin, vấn đề bảo mật không có tính tuyệt đối. Ngay cả các cường quốc trong ngành công nghệ thông tin-bảo mật như Anh, Pháp, Đức, Mỹ, Trung Quốc... cũng đều bị hacker tấn công. Vậy các doanh nghiệp và người dùng Việt Nam phải làm gì để vừa có thể tận dụng được những lợi thế của nền công nghiệp IoT mà vẫn đảm bảo an toàn thông tin trên mạng?

Nhằm mang tới cho độc giả và các doanh nghiệp, tổ chức những kiến thức cơ bản về bảo mật dữ liệu, cảnh báo người đọc về vấn đề quyền riêng tư và nâng cao ý thức bảo mật thông tin, Apha Books trân trọng giới thiệu bộ sách “An toàn thông tin trong kỷ nguyên số” gồm 4 cuốn: The Cuckoo’s Egg (Gián điệp mạng), Ghost in the Wires (Bóng ma trên mạng), The Art of Invisibility (Nghệ thuật ẩn mình) và Hackers lược sử. Thông qua các câu chuyện ly kỳ hấp dẫn về những cuộc truy bắt hacker, những chiến công của các hacker mũ trắng – những kẻ mê máy tính thông minh và lập dị, dám mạo hiểm, bẻ cong các quy tắc và đẩy thế giới vào một hướng đi hoàn toàn mới, độc giả sẽ có được cái nhìn toàn diện về hacker, về đạo đức nghề nghiệp cũng như tương lai của ngành công nghệ để có được cái nhìn rõ ràng hơn về an ninh mạng, chủ đề chưa bao giờ hết nóng hổi của các tín đồ mạng.

Bộ trưởng TT&TT Nguyễn Mạnh Hùng đã nhấn mạnh: "An toàn, an ninh mạng được coi là điều kiện để thúc đẩy chính phủ điện tử, chính phủ số và nền công nghiệp nội dung số. Vì vậy, Việt Nam phải trở thành cường quốc về an ninh mạng". Đồng hành với những vấn đề thời sự nhức nhối hiện nay, với bộ sách này, Apha Books và các đối tác – những nhà cung cấp các giải pháp bảo mật & an ninh mạng như CMC, Netnam, Securitybox, CyRadar... mong muốn đóng góp một phần tri thức cho xã hội, giúp nền kinh tế số Việt Nam phát triển lành mạnh, bền vững.

Trân trọng giới thiệu!

Tháng 11/2018

Công ty Cổ phần Sách Alpha

Lời Giới Thiệu

Hôm nay, khi tôi đang suy nghĩ về lời giới thiệu cho cuốn sách tuyệt vời này, hệ thống thu thập thông tin của SecurityBox thông báo cho tôi hai tin tức rất quan trọng. Một là hệ thống thương mại điện tử của một tập đoàn trong nước bị tấn công, hacker đã lấy cắp và công bố số lượng lớn dữ liệu người dùng. Hai là 59 học viên của trường Học viện Kỹ thuật Mật mã sắp tổ chức lễ tốt nghiệp và trở thành những chuyên gia an ninh mạng được đào tạo bài bản. Những sự kiện đối lập giữa "tấn công" và "phòng thủ" như thế này vô tình lại rất liên quan đến nội dung của cuốn sách, hồi ký về cuộc đời và sự nghiệp kỳ lạ của Kevin Mitnick, người từng được coi là hacker bị truy nã gắt gao nhất thế giới.

Kevin Mitnick luôn có tên trong mọi bảng xếp hạng những hacker nguy hiểm nhất mọi thời đại. Ông nổi tiếng với khả năng tấn công mọi hệ thống phức tạp bằng phương pháp tấn công phi kỹ thuật (social engineering). Phương pháp này nhắm thẳng đến người dùng đang tham gia vào hệ thống, Kevin sẽ giao tiếp trực tiếp hoặc gián tiếp với những người này, đặt họ vào tình huống khiến họ vô tình cung cấp thông tin quan trọng cho phép ông có thể dễ dàng chiếm quyền điều khiển hệ thống.

Ngày nay, kỹ thuật tấn công này vẫn rất phổ biến, điển hình là trên mạng xã hội Facebook, khi hacker giả danh người thân, người nổi tiếng hoặc công ty nổi tiếng để lừa đảo các nạn nhân, khiến họ tin tưởng và tự động thực hiện những hành vi do hacker đề xuất. Tuy nhiên, khi đọc cuốn sách này, tôi nhận ra Kevin Mitnick còn là một kỹ sư công nghệ xuất chúng, chính sự kết hợp hoàn hảo giữa tấn công bằng kỹ thuật và phi kỹ thuật mới là điều làm nên tên tuổi của ông.

Chi tiết quan trọng nhất trong cuộc đời của Kevin chính là việc ông bị bắt giam vì tấn công vào hệ thống tối mật của chính phủ Mỹ. Việc không bao giờ thực hiện các hành vi phá hoại là điều đáng ngưỡng mộ của hacker này. Điều này lý giải vì sao sau khi ra tù, các công ty từng bị Kevin tấn công đã thuê ông tư vấn về giải pháp đảm bảo an ninh mạng.

Ngay tại SecurityBox, chúng tôi cũng có các chuyên gia và công nghệ cho phép tìm ra những điểm yếu có thể bị tấn công trong hệ thống mạng của khách hàng. Chúng tôi hiểu rằng việc có trong tay công cụ để kiểm soát một hệ thống lớn, cũng giống như khi nhìn thấy một lượng tiền lớn còn bỏ ngỏ, chúng ta sẽ khó tránh khỏi lòng tham. Vấn đề nằm ở khái niệm “đạo đức”, chúng tôi phải giữ được đạo đức làm nghề và đào tạo kỹ sư của mình cũng phải như vậy.

Bóng ma trên mạng thể hiện ham muốn kiểm soát, tấn công mọi hệ thống mạng, sự ám ảnh đối đầu với chính quyền và bản lĩnh của một hacker tài năng. Việc Kevin từng trải qua cuộc cách mạng máy tính và Internet với tư cách là một hacker kiêm chuyên gia an ninh mạng đã góp phần khiến cuốn sách này trở thành tư liệu quý báu dành cho các chuyên giao bảo mật, kỹ sư an ninh mạng hoặc thậm chí là các hacker. Tôi tin rằng, cuốn sách này sẽ rất thú vị không chỉ đối với những người trong nghề mà còn hữu ích cho bất kỳ ai đang sống trong kỷ nguyên số hiện nay nhằm nâng cao hiểu biết và ý thức bảo vệ các “tài sản số” của chính mình.

Bùi Quang Minh

CEO SecurityBox

Bùi Quang Minh đã có 15 năm kinh nghiệm làm việc trong lĩnh vực bảo mật với tư cách là hacker mũ trắng kiêm chuyên gia về an ninh mạng. Năm 2010, ông đã phát hiện và công bố lỗ hổng phần mềm của các hãng công nghệ nổi tiếng thế giới như Google, Microsoft. Năm 2011, ông công bố lỗ hổng nghiêm trọng trong mạng 3G của ba nhà mạng Mobifone, Vinaphone và Viettel. Ngoài ra, ông cũng là đồng tác giả của một số phát hiện bảo mật nghiêm trọng từng được công bố trong và ngoài nước.

Lời Tựa

Tôi gặp Kevin Mitnick lần đầu tiên vào năm 2001 trong đợt quay bộ phim tài liệu *The History of Hacking* (tạm dịch: *Lịch sử hacking*) của kênh Discovery Channel và chúng tôi giữ liên lạc từ đó. Hai năm sau, tôi bay tới Pittsburgh để gặp anh trong buổi diễn thuyết của anh ở Đại học Carnegie Mellon. Tại đây, tôi đã chết lặng khi nghe anh nói về lịch sử hacking của mình. Anh đã đột nhập vào hệ thống máy tính của các công ty nhưng không hủy dữ liệu, cũng không hề dùng hay bán các thông tin thẻ tín dụng mà mình có trong tay. Anh lấy trộm phần mềm nhưng chưa từng bán chúng. Anh hack cho vui, và vì tính thử thách trong đó.

Trong buổi diễn thuyết, Kevin kể chi tiết câu chuyện khó tin về việc anh đã quấy phá cuộc truy lùng của Cục Điều tra Liên bang (FBI) đối với mình ra sao. Kevin đã thâm nhập vào toàn bộ quá trình điều tra, phát hiện ra một "người bạn" hacker mới hóa ra lại là kẻ chỉ điểm của FBI, biết tên và địa chỉ của toàn bộ tổ FBI phụ trách vụ này, thậm chí còn nghe lỏm được các cuộc gọi và tin nhắn thoại của những người đang cố thu thập bằng chứng chống lại mình. Anh còn thiết lập cả một hệ thống cảnh báo riêng để biết được khi nào FBI chuẩn bị chiến dịch vây bắt.

Khi các nhà sản xuất của chương trình truyền hình Screen Savers (tạm dịch: Bảo vệ màn hình) mời Kevin và tôi cùng dẫn một tập, họ đề nghị tôi nói về một thiết bị điện tử mới xuất hiện trên thị trường tiêu dùng dạo đó: Hệ thống định vị toàn cầu (GPS). Tôi được yêu cầu lái xe lòng vòng trong khi họ theo dõi xe tôi qua thiết bị định vị. Khi chương trình lên sóng, các nhà sản xuất yêu cầu tôi lái theo lộ trình tưởng chừng như rất ngẫu nhiên. Thế rồi, một thông điệp hiện ra:

FREE KEVIN

(tạm dịch: Hãy trả tự do cho Kevin)

Chúng tôi lại cùng xuất hiện trong một chương trình khác vào năm 2006, khi Kevin là người dẫn chương trình tạm thời cho buổi trò chuyện Coast to Coast AM (tạm dịch: Từ bờ đông sang bờ tây) của Art Bell và mời tôi cùng tham gia với tư cách khách mời. Trước đó, tôi thường ở vị trí là người lắng nghe các câu chuyện về anh; còn buổi tối hôm đó, anh là người phỏng vấn tôi và chúng tôi đã vô cùng vui vẻ, hệt như mỗi lần gặp gỡ trước đó.

Kevin đã làm thay đổi cuộc sống của tôi. Một ngày nọ, tôi phát hiện ra anh thường gọi cho tôi từ những nơi rất xa: Anh ở Nga để diễn thuyết, ở Tây Ban Nha để giúp một công ty giải quyết các vấn đề an ninh, ở Chile để tư vấn cho một ngân hàng đã bị xâm nhập máy tính. Nghe thật tuyệt! Tôi đã không đụng tới hộ chiếu của mình suốt 10 năm cho tới khi những cuộc gọi này khiến tôi ngứa ngáy. Kevin giới thiệu tôi với một đại diện chuyên đặt lịch cho các buổi diễn thuyết của anh. Cô ấy nói với tôi: “Tôi có thể đặt các buổi nói chuyện cho anh luôn.” Vậy là nhờ Kevin, tôi đã trở thành kẻ dịch chuyển khắp năm châu như anh.

Kevin trở thành một trong những người bạn tốt nhất của tôi. Tôi thích ở gần anh để được nghe về các trải nghiệm khai phá và mạo hiểm. Anh đã sống một cuộc đời đầy say mê và hấp dẫn hệt như những bộ phim về tội phạm hay nhất.

Giờ đây, bạn cũng có thể biết đến tất cả những câu chuyện mà tôi đã lần lượt được nghe trong suốt những năm qua. Ở khía cạnh nào đó, tôi thấy ghen tị với những trải nghiệm trong hành trình mà bạn sắp bắt đầu. Bạn sẽ thấy say mê câu chuyện khó tin, gần như là không tưởng về cuộc đời và những kỳ tích mà Kevin Mitnick đã tạo ra.

— Steve Wozniak, đồng sáng lập công ty Apple

Lời Nói Đầu

"Cuộc đột nhập thực tế": lẻn vào tòa nhà của công ty mục tiêu. Tôi không bao giờ thích làm việc này. Quá nguy hiểm. Chỉ viết về nó thôi cũng khiến tôi vã mồ hôi rồi.

Nhưng tôi đã ở đó, núp trong bãi đỗ xe tối đen của một công ty trị giá hàng tỷ đô-la trong buổi tối mùa xuân ấm áp để tìm cơ hội. Một tuần trước, tôi đã ghé thăm tòa nhà này vào ban ngày, lấy cớ chuyển một bức thư cho nhân viên tại đây. Lý do thực sự là để tôi có thể nhìn kỹ thẻ ID của họ. Công ty này đặt ảnh nhân viên ở góc trái phía trên, tên ngay bên dưới, họ ở trước, in hoa. Tên công ty ở phía dưới thẻ, màu đỏ, cũng in hoa.

Tôi từng đến Kinko's và xem qua trang web của công ty, do đó, tôi có thể tải về và sao chép hình ảnh logo công ty. Có ảnh này và bản scan ảnh của chính mình, tôi chỉ mất chừng 20 phút dùng Photoshop để thiết kế và in ra một tấm thẻ nhân viên công ty khá chuẩn, rồi nhét nó vào một dây đeo thẻ rẻ tiền mua ở một cửa tiệm bách hóa. Tôi chế thêm một thẻ ID giả nữa cho bạn mình, người đã đồng ý đi cùng trong trường hợp tôi cần giúp đỡ.

Bất ngờ thay, những tấm thẻ này thậm chí còn không cần phải trông giống hàng thật. 99% là người ta sẽ chỉ liếc mắt nhìn nó lấy lệ. Miễn sao những chi tiết chính yếu ở đúng vị trí và trông có vẻ giống thẻ thật, bạn sẽ dễ dàng vượt qua cửa kiểm soát… đương nhiên là trừ khi có một gã bảo vệ quá hăng hái hoặc một nhân viên nào đó khoái trò kiểm tra an ninh khăng khăng muốn nhìn thật kỹ. Đây là mối nguy hiểm bạn buộc phải chấp nhận nếu sống một cuộc đời như tôi.

Trong bãi đỗ xe, tôi nấp vào chỗ kín đáo, theo dõi từng đốm sáng lóe lên từ những điếu thuốc của dòng người bước ra ngoài nghỉ giải lao. Cuối cùng, tôi phát hiện ra một nhóm nhỏ chừng 5-6 người chuẩn bị quay trở lại tòa nhà. Cửa hậu là một trong những cánh cửa chỉ mở khóa khi nhân viên đặt thẻ ra vào của mình lên máy đọc thẻ. Khi cả tốp xếp thành hàng đi qua cửa, tôi nhảy ngay vào cuối hàng. Gã ở phía trước với tay lên cửa và để ý thấy còn ai đó đứng ngay sau, đưa mắt để đảm bảo tôi có đeo thẻ nhân viên của công ty, rồi giữ cửa giúp. Tôi gật nhẹ cảm ơn.

Kỹ thật này gọi là "tailgating" – theo đuôi.

Vào tới trong, thứ đầu tiên đập vào mắt tôi là tấm áp phích chình ình trước mắt. Nó là một tấm áp phích an ninh, cảnh báo bạn không được giữ cửa cho người khác và yêu cầu mỗi người đều phải qua cửa bằng cách đặt thẻ của mình vào máy đọc thẻ. Có điều, thói lịch thiệp xã giao, phép lịch sự đối với "đồng nghiệp" đồng nghĩa với việc lời cảnh báo trên tấm áp phích an ninh này thường xuyên bị tảng lờ.

Khi đã yên vị ở trong tòa nhà, tôi bắt đầu bước qua từng dãy hành lang đầy những người đang rảo bước trên đường thực hiện nhiệm vụ quan trọng nào đó. Trên thực tế, tôi đang trong hành trình khám phá, cố tìm cho ra Phòng Công nghệ Thông tin (IT). Sau khoảng 10 phút, tôi tìm thấy nó ở khu phía tây của tòa nhà. Tôi đã chuẩn bị kỹ càng trước đó và biết tên của một trong những kỹ sư mạng ở đây; tôi đoán là anh ta có toàn quyền quản trị hệ thống máy tính của cả công ty.

Chết tiệt! Nơi anh ta ngồi không phải là một ô làm việc dễ dàng thâm nhập, mà là một văn phòng riêng … đằng sau cánh cửa đã bị khóa kín. Nhưng tôi đã có cách. Trần nhà được làm từ những tấm vật liệu vuông, trắng, cách âm vẫn thường được dùng để tạo ra lớp trần thấp có khoảng trống ở giữa có thể bò qua, nơi chứa các đường ống, đường dây điện, thông khí…

Tôi gọi điện cho chiến hữu để yêu cầu trợ giúp và quay trở lại cửa hậu để mở cửa cho anh vào. Với dáng người cao lêu nghêu và gầy, hy vọng anh ấy có thể làm được việc mà tôi không thể. Quay trở lại phòng IT, anh ấy trèo lên một chiếc bàn. Tôi ôm chặt hai chân anh, đẩy anh lên cao đủ để có thể nâng một tấm trần vuông lên và trượt nó sang một bên. Trong lúc tôi căng sức để nâng cao hơn nữa, thì anh ấy cũng cũng xoay xở để có thể túm chặt lấy một đường ống và đu lên. Vài phút sau, tôi nghe thấy tiếng anh nhảy vào văn phòng khóa kín. Nắm cửa xoay mở và anh đứng đó, người đầy bụi, miệng cười nhăn nhở.

Tôi bước vào phòng và nhẹ nhàng đóng cửa. Chúng tôi đã an toàn, ít có khả năng bị phát hiện. Căn phòng tối đen. Bật đèn có thể gây nguy hiểm mà cũng không cần thiết – ánh sáng phát ra từ chiếc máy tính của gã kỹ sư đủ để tôi nhìn thấy mọi thứ mình cần, giảm thiểu được khối rủi ro. Tôi nhìn lướt trên bàn, kiểm tra ngăn kéo trên cùng và dưới bàn phím xem liệu gã có ghi lại mật khẩu máy tính ở đâu đó không. Tiếc là không. Nhưng đó không phải là vấn đề.

Từ túi đeo hông, tôi rút ra một chiếc đĩa CD với phiên bản có thể khởi động máy tính của hệ điều hành Linux, chứa bộ công cụ dành cho hacker và thả vào ổ CD của gã, sau đó khởi động lại máy. Một trong những công cụ này cho phép tôi thay đổi mật khẩu quản trị trên máy tính; sau khi đổi xong, tôi có thể đăng nhập bình thường. Tôi bỏ chiếc đĩa CD ra khỏi ổ và khởi động lại máy tính một lần nữa, lần này là để đăng nhập vào tài khoản quản trị.

Thao tác nhanh nhất có thể, tôi cài đặt một phần mềm gián điệp cho phép truy cập từ xa (remote access Trojan), phần mềm mã độc giúp tôi có toàn quyền đăng nhập vào hệ thống, nhờ vậy tôi có thể ghi lại thao tác bàn phím, lấy được chuỗi mã băm[*] mật khẩu và thậm chí, điều khiển webcam chụp hình người đang sử dụng máy tính. Loại Trojan mà tôi cài đặt sẽ khởi động kết nối mạng Internet tới một hệ thống khác dưới quyền kiểm soát của tôi sau mỗi vài phút, cho phép tôi toàn quyền kiểm soát máy tính của nạn nhân.

Mã băm (hash): Chuỗi ký tự có độ dài cố định do các thuật toán mã hóa thông tin tạo ra, được dùng phổ biến trong việc kiểm tra chữ ký điện tử, tập tin… (BTV)

Gần xong việc, ở bước cuối cùng, tôi vào phần lưu thông tin cấu hình hoạt động của máy tính và đặt mục “tài khoản đăng nhập lần cuối” (last logged-in user) sang tài khoản của gã kia, như vậy tôi sẽ không để lại bất kỳ dấu vết nào cho lần đăng nhập này bằng tài khoản quản trị. Sáng hôm sau, gã kỹ sư có thể phát hiện ra mình đã thoát khỏi máy. Không thành vấn đề: miễn sao khi đăng nhập, mọi thứ trông vẫn hệt như cũ là được.

Tôi đã sẵn sàng rời đi. Lúc này, chiến hữu của tôi đã đặt tấm lát trần vào chỗ cũ. Trên đường ra, tôi khóa phòng lại như cũ.

Sáng hôm sau, gã kỹ sư bật máy vào khoảng 8 giờ 30 phút, và phần mềm gián điệp đã khởi động kết nối tới máy tính xách tay của tôi. Bởi Trojan đang chạy trên tài khoản của gã còn tôi nắm toàn quyền quản trị miền, nên chỉ mất vài giây để xác định được bộ điều khiển miền[*] chứa toàn bộ mật khẩu tài khoản của cả công ty. Một công cụ hacker có tên “fgdump” cho phép tôi trích xuất các chuỗi mã băm mật khẩu của tất cả người dùng.

Bộ điều khiển miền (domain controller): Máy chủ có chức năng phản hồi các yêu cầu xác nhận an ninh (như đăng nhập, kiểm tra quyền, v.v…). (BTV)

Chỉ sau vài giờ, tôi đã quét toàn bộ chuỗi mã băm này qua một “bảng danh sách cầu vồng” (rainbow table) – một cơ sở dữ liệu khổng lồ chứa các chuỗi mã băm mật khẩu có sẵn – nhằm khôi phục mật khẩu của hầu hết nhân viên trong công ty. Tôi còn tìm được một trong những máy chủ back-end[*] xử lý các giao dịch khách hàng, nhưng mã số thẻ tín dụng đều bị mã hóa. Không thành vấn đề: Tôi phát hiện ra chìa khóa để mã hóa số thẻ được giấu trong một đoạn mã chương trình lưu bên trong cơ sở dữ liệu của máy tính được gọi là “máy chủ SQL”, có khả năng tiếp cận bất kỳ quản trị cơ sở dữ liệu nào.

Back-end: Thuật ngữ chỉ giai đoạn kết thúc của một quá trình xử lý, khái niệm này thường được sử dụng trong lĩnh vực phát triển phần mềm, ám chỉ việc tương tác với hệ quản trị dữ liệu. (BTV)

Hàng triệu triệu số thẻ tín dụng. Tôi có thể mua sắm cả ngày bằng cách mỗi lần sử dụng một thẻ khác nhau mà không bao giờ cạn thẻ.

Nhưng tôi không làm vậy. Câu chuyện thực này không phải tái hiện cảnh hacking đã đẩy tôi vào bước đường cùng. Ngược lại, đó là công việc tôi được thuê làm.

Đây là thứ chúng tôi gọi là “pen test” (đánh giá bảo mật), viết tắt của cụm từ “penentration test” (phép thử đột nhập) và nó chiếm phần lớn những gì đang diễn ra trong cuộc sống của tôi. Tôi đã tấn công vào những công ty lớn nhất trên hành tinh và đột nhập vào những hệ thống máy tính tốt nhất từng có – chính các công ty đã thuê tôi để giúp họ hàn gắn các kẽ hở và phát triển hệ thống an ninh, nhờ đó họ không trở thành nạn nhân kế tiếp của trò hack. Phần lớn kiến thức tôi có được là nhờ tự học với nhiều năm nghiên cứu phương pháp, chiến thuật, chiến lược để phá vỡ an ninh máy tính, và để học hỏi thêm nhiều điều về cơ chế hoạt động của các hệ thống máy tính cùng hệ thống viễn thông.

Đam mê của tôi dành cho công nghệ và sự mê hoặc của nó đã đẩy tôi vào một hành trình gập ghềnh. Hành vi hack liều lĩnh đã khiến tôi phải trả giá bằng 5 năm bóc lịch trong tù và khiến những người tôi yêu thương tổn thương.

Đây là câu chuyện của tôi, từng chi tiết đều chính xác theo những gì tôi nhớ, các ghi chép cá nhân, biên bản phiên tòa công khai, các tài liệu có được thông qua Luật Tự do Thông tin, bản ghi âm các cuộc nghe lén FBI, nhiều giờ phỏng vấn và cả các cuộc thảo luận cùng hai kẻ chỉ điểm của chính phủ.

Đây là câu chuyện kể về hành trình trở thành hacker máy tính bị truy nã gắt gao nhất thế giới của tôi.

PHẦN MỘT

Sự ra đời của một hacker

KHỞI ĐẦU CHÔNG GAI

Bản năng tìm cách tránh né rào cản và chốt chặn của tôi bắt đầu từ rất sớm. Hồi một tuổi rưỡi, tôi đã tìm ra cách để trèo khỏi cũi, bò tới thanh chắn an toàn ở cửa và tìm được cách mở nó. Đối với mẹ tôi, đây là dấu hiệu cảnh báo đầu tiên cho những gì sau này.

Yjcv ku vjg pcog qh vjg uauvgo wugf da jco qrgtcvqtu vq ocmg htgg rjqpg ecnnu?

Tôi là con một trong nhà. Sau khi cha bỏ đi lúc tôi lên ba, mẹ tôi, tên là Shelly, và tôi đã sống trong những căn hộ đẹp với mức giá trung bình thuộc các khu dân cư an toàn ở Thung lũng San Fernando, chỉ cách thành phố Los Angeles một ngọn đồi. Chúng tôi sống nhờ công việc chạy bàn của mẹ tại một trong những nhà hàng nằm trên Đại lộ Ventura, chạy theo hướng đông-tây suốt chiều dài thung lũng. Cha tôi sống ở một bang khác và dù có quan tâm đến tôi, nhưng nhìn chung, ông chỉ tới thăm tôi vài lần cho tới khi ông chuyển đến Los Angeles năm tôi 13 tuổi.

Mẹ con tôi chuyển nhà nhiều đến mức tôi không có cơ hội kết bạn như những đứa trẻ khác. Tôi dành thời thơ ấu cho các thú vui đơn độc, phần lớn là những hoạt động không phải di chuyển. Khi tôi còn đi học, các thầy cô thường nói với mẹ rằng tôi thuộc nhóm 1% đứng đầu về toán và đánh vần, vượt xa so với các bạn cùng tuổi. Nhưng do bản tính hiếu động, nên thật khó để tôi có thể ngồi yên một chỗ.

Trong suốt quá trình trưởng thành của tôi, mẹ đã lấy thêm ba người chồng và có vài người bạn trai. Một kẻ hành hung tôi, một gã khác – tay này làm trong lực lượng chấp pháp – đã quấy rối tôi. Không giống như các bà mẹ mà tôi từng biết, mẹ chưa bao giờ làm ngơ. Ngay khi bà phát hiện ra tôi bị đối xử tệ hại – hoặc thậm chí chỉ là bị nặng lời – gã đàn ông đó sẽ phải ra khỏi nhà ngay lập tức. Tôi không định kiếm cớ bao biện, nhưng tôi thường tự hỏi không biết những gã đàn ông ưa bạo lực kia có góp phần làm nên tư tưởng chống đối lực lượng chức năng của tôi hay không.

Mùa hè là khoảng thời gian tuyệt vời nhất, đặc biệt là khi mẹ làm theo ca và được nghỉ vào giữa ngày. Tôi sung sướng được mẹ cho đi bơi ở bãi biển Santa Monica tuyệt vời. Mẹ nằm trên cát, tắm nắng và thư giãn, nhìn tôi chơi đùa cùng những con sóng, bị sóng đánh ngã rồi lại nhổm lên cười. Ngoài ra, tôi còn tập luyện mấy kiểu bơi được học ở trại hè YMCA mà tôi đã tham gia được vài kỳ (tôi luôn ghét chúng trừ những lúc được dẫn ra biển).

Khi còn bé, tôi khá giỏi thể thao và cảm thấy thích thú khi được chơi tại Giải Bóng chày Thiếu niên (Little League). Tôi nghiêm túc với việc này tới mức dành hết thời gian rảnh rỗi để tập đánh bóng. Nhưng niềm đam mê dẫn tới hành trình trọn đời của tôi bắt đầu từ năm tôi lên 10. Người hàng xóm sống trong căn hộ đối diện có cô con gái trạc tuổi mà tôi rất có cảm tình. Ở tuổi đó, điều tôi thấy hứng thú hơn cả lại là thứ mà cha cô bé mang tới: ảo thuật.

Ông là một nhà ảo thuật có tài với những màn ảo thuật bằng lá bài, đồng xu và những hiệu ứng hoành tráng đầy mê hoặc. Nhưng quan trọng hơn, tôi nhìn thấy niềm hân hoan trên gương mặt các khán giả của ông khi bị qua mặt, dù đó là một người, ba người, hay cả căn phòng. Dù chưa từng thực sự suy ngẫm về điều này, nhưng việc phát hiện ra rằng con người thích bị lừa đã ảnh hưởng rất lớn đến đường đời của tôi.

Cửa hàng bán đồ ảo thuật chỉ cách nhà một cuốc xe đạp ngắn trở thành chốn bí mật yêu thích của tôi trong thời gian rảnh rỗi. Ảo thuật là cánh cửa đầu tiên đưa tôi đến với nghệ thuật qua mặt con người.

Đôi khi thay vì đạp xe, tôi sẽ nhảy lên xe buýt. Vào một ngày nọ, vài năm sau, Bob Arkow, một tài xế xe buýt, người để ý thấy tôi mặc chiếc áo phông có ghi "CBers Do It on the Air" (tạm dịch: Dân chơi mạng làm việc như trên mây), đã nói rằng anh ta vừa kiếm được một thiết bị cầm tay Motorola vốn là chiếc bộ đàm của cảnh sát. Tôi nghĩ có thể gã đã bắt được tần số của cảnh sát, nếu thế thì thật tuyệt. Hóa ra, gã bịp tôi chuyện đó, nhưng Bob là một gã cuồng chơi vô tuyến điện nghiệp dư[*] (ham radio), và sự nhiệt tình của gã với thú vui đó đã khơi lên mối quan tâm trong tôi. Gã cho tôi thấy cách thực hiện một cuộc gọi miễn phí thông qua sóng vô tuyến điện, nhờ một tính năng có tên là miếng vá tự động[*] trên một số vô tuyến điện nghiệp dư. Gọi điện thoại miễn phí! Điều này khiến tôi ấn tượng không tài nào kể xiết. Tôi nghiện trò này luôn.

Vô tuyến điện nghiệp dư (ham radio hay còn gọi là amatuer radio): Thiết bị sử dụng các dải tần số vô tuyến cho mục đích phi thương mại như giải trí, trao đổi tin nhắn… (ND)

Miếng vá tự động (auto patch): Một tính năng của ham radio, được dùng để thực hiện cuộc gọi đi trên điện thoại. Người dùng có bộ thu phát có thể tạo ra tín hiệu điện thoại quay ở trạng thái âm kép đa tần để thực hiện các cuộc gọi bị giới hạn trong mô-đun của miếng vá tự động đến các số điện thoại cố định, như cuộc gọi nội hạt hoặc các số điện thoại không mất phí. (BTV)

Sau vài tuần tham dự lớp học buổi tối, tôi đã nắm được mạch liên lạc vô tuyến và các quy định về ham radio để qua bài thi viết, và cũng đã đủ thành thạo về mã Morse để lấy được chứng chỉ. Chẳng bao lâu sau, tôi nhận được một phong bì từ Ủy ban Truyền thông Liên bang (FCC) đựng giấy phép ham radio của tôi, mà không nhiều đứa trẻ mười mấy tuổi có được. Tôi tự hào ghê gớm.

Lừa gạt mọi người bằng ảo thuật cũng thú vị. Nhưng học cách vận hành hệ thống điện thoại mới mê hoặc. Tôi muốn biết mọi thứ liên quan tới công ty điện thoại. Tôi muốn thông thạo cách thức vận hành bên trong đó. Tôi luôn đạt điểm cao hồi cấp 1 và cấp 2, nhưng đến năm lớp 8 hay lớp 9, tôi bắt đầu trốn học và lảng vảng ở Henry Radio, một cửa hàng ham radio phía Tây Los Angeles, để đọc sách về lý thuyết vô tuyến điện hàng giờ liền. Đối với tôi, điều đó tuyệt như một chuyến đi đến Disneyland vậy. Ham radio cũng đem đến một số cơ hội để tôi có thể giúp đỡ cộng đồng. Có dạo tôi hoạt động tình nguyện vào các dịp cuối tuần nhằm cung cấp dịch vụ hỗ trợ thông tin liên lạc cho hội Chữ thập Đỏ địa phương. Có mùa hè tôi cũng làm việc tương tự cả tuần cho kỳ Thế vận hội dành cho người khuyết tật.

Đối với tôi, những chuyến xe buýt hệt như một kỳ nghỉ – tận hưởng khung cảnh thành phố, ngay cả ở những nơi quen thuộc. Thời tiết ở Nam California luôn hoàn hảo, trừ những lúc có sương mù. Vé xe tốn 25 xu, thêm 10 xu để đổi chuyến. Vào kỳ nghỉ hè khi mẹ đi làm, có khi tôi ngồi xe buýt cả ngày. Đến năm 12 tuổi, đầu óc tôi đã nảy ra những ý tưởng khác người. Một ngày tôi phát hiện ra, nếu có thể tự bấm vé chuyển chuyến, mình sẽ chẳng tốn xu nào.

Cha và chú bác tôi đều là những người bán hàng khéo miệng. Tôi đoán mình thừa hưởng gen đó nên ngay từ nhỏ, tôi đã có tài thuyết phục mọi người làm điều gì đó cho mình. Tôi lên xe buýt qua cửa trước và ngồi gần ghế lái. Khi tài xế dừng đèn đỏ, tôi nói: “Cháu đang thực hiện một bài tập ở trường và cần bấm lỗ tạo hình thù hay ho lên mấy miếng bìa các-tông. Cháu thấy cái máy bác dùng để bấm lỗ lượt chuyển chuyến tuyệt quá. Cháu có thể mua nó ở đâu ạ?”

Tôi không nghĩ người tài xế sẽ tin tôi vì điều này nghe thật ngu ngốc. Hẳn ông ấy không ngờ một thằng nhóc ở độ tuổi tôi lại đang cố lợi dụng mình. Ông ấy cho tôi biết tên cửa hiệu, và khi tôi gọi đến đó, họ nói chiếc máy bấm lỗ có giá 15 đô-la. Khi bạn 12 tuổi, bạn có thể nghĩ kế để xin mẹ 15 đô-la không? Tôi làm chuyện đó ngon ơ. Ngay ngày hôm sau, tôi đã có mặt ở cửa hàng để mua máy bấm lỗ. Nhưng đó mới chỉ là Bước 1. Làm thế nào để có được cả một xấp vé chuyển chuyến còn trống?

Hừm, người ta rửa xe buýt ở đâu nhỉ? Tôi đi bộ đến một trạm xe gần đó, thấy một thùng rác lớn ở trạm nơi các xe được dọn rửa, đu lên trên đó và nhìn ngó.

Trúng lớn rồi!

Tôi nhét đầy túi những tập vé chưa dùng hết – lần đầu tiên trong vô vàn lần "Lục-thùng-rác" sau này.

Tôi có trí nhớ khá tốt và đã cố gắng nhớ lịch xe buýt của gần như toàn bộ Thung lũng San Fernando. Tôi bắt đầu đi khắp nơi có hệ thống xe buýt – Quận Los Angeles, Quận Riverside, Quận San Bernandino. Tôi vui sướng nhìn ngắm tất cả các địa danh khác nhau đó và thu nhận thế giới xung quanh.

Trong quá trình rong ruổi, tôi kết bạn với Richard Williams, người cũng làm trò tương tự nhưng có chút khác biệt. Thứ nhất, Richard là con trai của một tài xế xe buýt, nên việc cậu ta được đi lại miễn phí bằng xe buýt là điều đương nhiên. Thứ hai (ít nhất lúc đầu là vậy) là cân nặng: Richard mập ú và thường dừng ở Jack in the Box[*] để gọi một phần bánh Taco cỡ lớn 5-6 lần một ngày. Tôi học theo lối ăn uống của cậu ta gần như ngay lập tức và bắt đầu phát tướng phần bụng.

Jack in the Box: Thương hiệu đồ ăn nhanh ở Mỹ. (ND)

Chẳng bao lâu sau, một cô bé với mái tóc vàng tết đuôi sam đi cùng chuyến xe buýt đến trường bảo tôi: "Trông cậu cũng dễ thương đấy, nhưng hơi béo. Cậu phải giảm cân đi."

Liệu tôi có tiếp nhận lời khuyên tuy khó nghe nhưng đúng đắn đó không? Không.

Liệu tôi có gặp rắc rối vì đã lục-thùng-rác để có vé chuyển chuyến và đi xe miễn phí không? Cũng không. Mẹ nghĩ tôi thật thông minh, còn cha nghĩ tôi thật sáng tạo, và những tài xế biết tôi tự bấm vé chuyển chuyến nghĩ đó là một trò vui lớn. Cứ như thể, tất cả những người biết tôi đều đang khuyến khích tôi làm vậy.

Trên thực tế, tôi không cần lời khen ngợi từ mọi người để những trò quỷ đẩy tôi vào rắc rối. Ai ngờ rằng một lần mua sắm nhỏ lại có thể dạy cho tôi một bài học sẽ làm thay đổi cuộc đời tôi sau này… theo một hướng không may?