Cách thức hoạt động của Hacker

Nhờ các phương tiện truyền thông, từ hacker đã được biết đến với tiếng xấu. Khi nói tới từ này, mọi người đều nghĩ đến những kẻ xấu có kiến thức về máy tính luôn tìm cách để hại mọi người, lừa gạt các tập đoàn, ăn cắp thông tin và thậm chí là phá hoại nền kinh tế hoặc gây ra chiến tranh bằng cách thâm nhập vào hệ thống máy tính quân đội. Mặc dù chúng ta không thể phủ nhận vẫn còn một số hacker không có mục đích xấu, họ vẫn chỉ chiếm phần nhỏ trong cộng đồng hacker.

Thuật ngữ hacker máy tính lần đầu tiên được sử dụng vào giữa những năm 1960. Một hacker vốn là một lập trình viên – kẻ đã hack code máy tính. Hacker có khả năng tìm kiếm nhiều cách khác nhau để sử dụng máy tính, tạo các chương trình mà không ai có thể hiểu được. Chúng là những người tiên phong đi đầu trong ngành công nghiệp máy tính khi xây dựng mọi thứ từ những ứng dụng nhỏ dành cho hệ điều hành. Trong lĩnh vực này, những người như Bill Gates, Steve Jobs và Steve Wozniak đều là hacker khi họ có thể nhận biết được khả năng máy tính có thể làm được gì và tạo ra các cách khác nhau để đạt được những khả năng đó.

Một cách gọi thống nhất dành cho những hacker trên là sự ham hiểu biết, ham học hỏi. Những hacker này tự hào không chỉ về khả năng tạo chương trình mới, mà còn về khả năng biết cách những chương trình khác cùng với hệ thống hoạt động như thế nào. Mỗi khi một chương trình có một bug – lỗi kỹ thuật khiến chương trình khó có thể hoạt động – hacker thường tạo ra một bản patch – bản vá để chữa lỗi. Một số người đã chọn nghề có thể nâng cao kỹ năng của họ, nhận tiền từ những phần mềm họ tạo ra.

Cùng với sự phát triển của máy tính, các nhà lập trình viên máy tính bắt đầu kết nối với nhau thành một hệ thống. Không lâu sau đó, thuật ngữ hacker đã

có nghĩa mới – những kẻ sử dụng máy tính để đột nhập vào một mạng lưới mà họ không phải là thành viên. Thông thường, hacker không có ý đồ xấu. Họ chỉ muốn biết được máy tính trong một mạng làm việc như thế nào và liệu có một rào cản nào đó giữa chúng.

Thực tế, điều này vẫn xảy ra ngày nay. Trong khi có rất nhiều câu chuyện về các hacker xấu phá hoại hệ thống máy tính, xâm nhập vào mạng và phát tán virus. Hầu hết các hacker rất tò mò, họ muốn biết tất cả những sự phức tạp của thế giới máy tính. Một số sử dụng kiến thức của mình để giúp các tổ chức và chính phủ xây dựng một hệ thống bảo mật an toàn hơn. Một số khác có thể sử dụng kỹ năng của mình vào mục đích xấu.

Trong bài báo này, chúng ta sẽ tìm hiểu những kỹ năng thông thường hacker hay sử dụng để thâm nhập hệ thống máy tính, khám phá về văn hóa hacker cùng với các loại hacker khác nhau. Ngoài ra, bài báo còn nói về những hacker nổi tiếng.

Hệ thống cấp bậc hacker

Theo nhà tâm lý học Marc Rogers, có một số nhóm nhỏ của hacker như newbies, cyberpunks, coders và cyber terrorists. Newbies là những kẻ truy cập trái phép mà không nhận thức được máy tính và các chương trình hoạt động như thế nào. Cyberpunk là những kẻ có hiểu biết và khó bị phát hiện và bị bắt hơn so với newbie khi xâm nhập hệ thống bởi chúng có xu hướng khoe khoang về sự hiểu biết. Coder viết các chương trình để các hacker khác sử dụng vào việc xâm nhập hệ thống và điều khiển hệ thống máy tính. Một cyber terrorist là hacker chuyện nghiệp chuyên xâm nhập hệ thống để kiếm lợi nhuận. Chúng có thể phá hoại cơ sở dữ liệu của một công ty hay một tập đoàn để sở hữu những thông tin quan trọng.

Đối với những hacker trên, ngoài tài năng và sự hiểu biết là code. Trong khi có một cộng đồng hacker lớn trên mạng Internet, chỉ có một số nhỏ trong chúng thực sự có khả năng code chương trình. Rất nhiều hacker tìm kiếm và tải code được viết bởi người khác. Có rất nhiều chương trình khác nhau mà hacker sử dụng để thâm nhập vào máy tính và mạng. Những chương trình

này giúp hacker rất nhiều, một khi chúng biết cách hoạt động của một hệ thống, hắn có thể tạo ra các chương trình để khai thác hệ thống đó.

Những hacker nguy hiểm thường sử dụng các chương trình để

• **Khóa bàn phím:** Một số chương trình giúp các hacker nhận tất cả những gì người dùng máy tính gõ vào bàn phím. Sau khi đã được cài đặt trên máy của nạn nhân, chương trình sẽ ghi lại toàn bộ các phím trên bàn mà người dùng gõ, cung cấp mọi thông tin để hacker có thể xâm nhập vào hệ thống, thậm chí là ăn cắp thông tin cá nhân quan trọng của ai đó.

• **Hack mật khẩu**: Có rất nhiều cách để ăn trộm mật khẩu của ai đó, từ việc đoán mật khẩu cho tới việc tạo ra các thuật toán để kết hợp các kí tự, con số và biểu tượng. Họ cũng có thể sử dụng cách tấn công brute force, có nghĩa là hacker sử dụng tất cả các kiểu kết hợp khác nhau để có thể truy cập. Một cách khác là phá mật khẩu bằng cách sử dụng kiểu tấn công dictionary attack, một chương trình có khả năng điền những từ thông thường vào mật khẩu.

• **Lây nhiễm một máy tính hoặc một hệ thống với virus:** Virus máy tính là những chương trình được thiết kế để tự sao chép và gây các lỗi như xâm nhập vào máy tính để xóa sạch mọi thứ trong ổ đĩa hệ thống. Hacker có thể tạo ra một virus để xâm nhập hệ thống, nhưng nhiều hacker khác thường tạo một virus rồi gửi chúng tới những nạn nhân tiềm năng thông qua email, tin nhắn nhanh hay các website với nội dung có thể tải được hoặc qua các mạng đồng đẳng.

• **Gain backdoor access:** Giống với hack mật khẩu, một số hacker tạo các chương trình để tìm kiếm những đường dẫn không được bảo vệ để thâm nhập vào máy tính và hệ thống mạng. Trong thời gian đầu của Internet, rất nhiều hệ thống máy tính không có nhiều biện pháp bảo vệ, tạo điều kiện cho hacker tìm kiếm đường dẫn vào hệ thống mà không cần tới tài khoản và mật khẩu. Một cách khác hacker hay sử dụng để lây nhiễm một máy tính hoặc một mạng là sử dụng Trojan horse. Không giống như virus, trojan không có chức năng tự sao chép nhưng lại có chức năng hủy hoại tương tự virus. Một trong

những thứ giăng bẫy của Trojan horse là nó tự nhận là giúp cho máy của thân chủ chống lại virus nhưng thay vì làm vậy nó quay ra đem virus vào máy.

• **Tạo một máy tính ảo:** Một máy tính ảo là máy tính hacker dùng để gửi spam hoặc thực hiện kiểu tấn công Distributed Denial of Service (DDoS – tấn công từ chối dịch vụ). Sau khi nạn nhân chạy một đoạn code, kết nối được mở ra giữa máy tính của nạn nhân với hệ thống của hacker. Hacker có thể bí mật kiểm soát máy tính của nạn nhân, sử dụng nó để thực hiện mục đích xấu hoặc phát tán spam.

• **Gián điệp trên email:** Hacker đã tạo code để giúp chúng chặn và đọc email, một cách gần giống như nghe trộm. Ngày nay, hầu hết các email đều được mã hóa phức tạp để phòng trừ trường hợp nếu emai này bị hacker chặn, hắn cũng không thể đọc được nội dung bên trong.

Văn hóa Hacker

Phreak siêu đẳng

Trước khi có hacker máy tính, những kẻ thông minh nhưng rất hay tò mò đã tìm các cách khác nhau để thâm nhập vào hệ thống điện thoại, được gọi là phreaking. Bằng cách phreaking, những người này có thể thực hiện một cuộc gọi dài miễn phí hoặc thậm chí là thực hiện cuộc gọi trên máy của người khác.

Rất nhiều hacker là những kẻ khó gần gũi. Sở thích mãnh liệt nhất của chúng là máy tính và lập trình có thể trở thành rào cản giao tiếp. Để chúng với các thiết bị riêng, một hacker có thể bỏ ra hàng giờ làm việc trên máy tính và quên đi mọi thứ xung quanh.

Mạng Internet đã tạo cơ hội cho hacker có thể gặp những người cùng sở thích. Trước khi Internet trở nên dễ dàng tiếp cận, hacker đã có thể thiết lập và truy cập bulletin board systems (BBS - Hệ thống bảng tin trên nền máy tính). Một hacker có thể "đăng cai" một BBS trên máy tính của họ rồi cho phép mọi người truy cập vào hệ thống để gửi tin nhắn, chia sẻ thông tin, chơi game và tải các chương trình. Hacker này chia sẻ thông tin cho hacker khác, thông tin được chia sẻ một cách nhanh chóng.

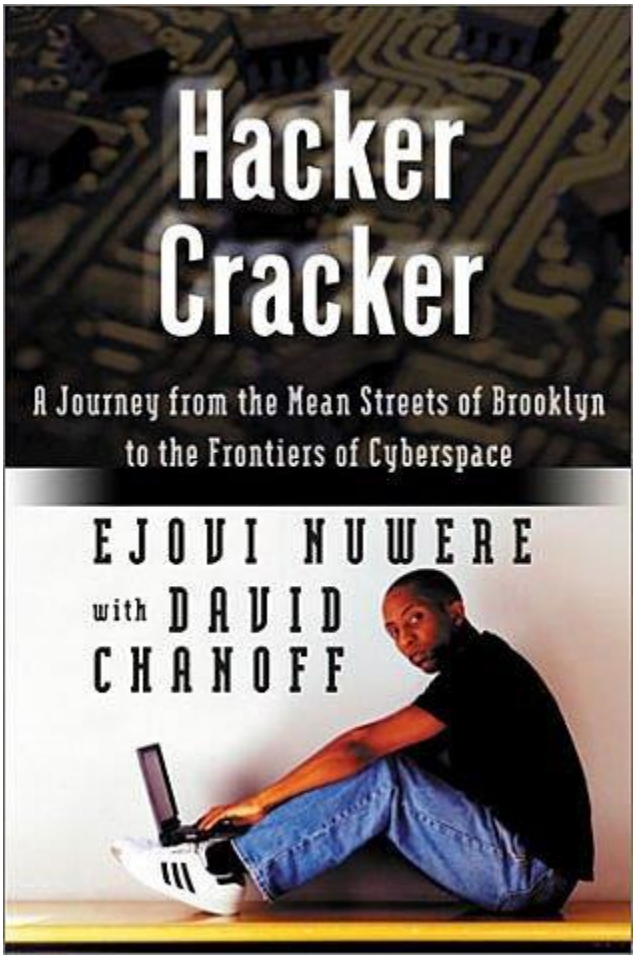
Một số hacker còn đăng tải thành tích của mình trên BBS, khoe khoang về việc đã thâm nhập một hệ thống bảo mật. Thông thường, chúng sẽ đăng tải một tài liệu nào đó từ cơ sở dữ liệu của nạn nhân để chứng minh. Vào đầu những năm 1990, cơ quan hành pháp chính thức coi các hacker là mối đe dọa lớn đối với hệ thống bảo mật. Có hàng trăm người có thể hack hệ thống bảo mật nhất trên thế giới.

Ngoài ra, có rất nhiều trang Web được tạo ra dành cho hack. Thời báo "*2600: The Hacker Quarterly*" đã dành riêng các chuyện mục dành cho hacker. Các bản được in ra vẫn có trên các quầy báo. Các trang khác như Hacker.org còn tích cực ủng hộ việc học, trả lời các câu đố hay tổ chức các cuộc thi dành cho hacker để kiểm tra kỹ năng của chúng.

Khi bị bắt bởi cơ quan hành pháp hoặc các tập đoàn, một số hacker thừa nhận rằng họ có thể gây ra vấn đề lớn. Hầu hết các hacker đều không muốn gặp rắc rối, thay vào đó, họ hack hệ thống chỉ bởi muốn biết hệ thống đó hoạt động như thế nào. Đối với một hacker, hệ thống bảo mật như Mt. Everest, chúng xâm nhập chỉ vì thử thách tuyệt đối. Tại Mỹ, một hacker có thể gặp rắc rối khi chỉ đơn giản là đi vào một hệ thống. Điều luật về lạm dụng và gian lận máy tính không cho phép truy cập hệ thống máy tính.

Hacker và Cracker

Rất nhiều lập trình viên khăng khăng cho rằng từ hacker được áp dụng cho những người tôn trọng luật pháp, những người tạo ra các chương trình và ứng dung hoặc tăng khả năng bảo mật cho máy tính. Còn đối với bất kì ai sử dụng kỹ năng với ý đồ xấu đều không phải là hacker mà là cracker.



Cracker xâm nhập hệ thống và gây thiệt hại hoặc tệ hơn thế. Không may rằng, hầu hết mọi người không thuộc cộng đồng hacker đều sử dụng từ hacker như một nghĩa xấu bởi họ không biết cách phân biệt giữa hacker và cracker.

Không phải tất cả hacker đều muốn truy cập những hệ thống máy tính. Một số người sử dụng kiến thức và sự thông minh của mình để tạo ra những phần mềm tốt, các biện pháp bảo mật an toàn. Thực tế, rất nhiều hacker đã từng đột nhập vào hệ thống, sau đó đã sử dụng sự hiểu biết, sự khéo léo của mình để tạo ra những phương pháp bảo mật an toàn hơn. Nói theo cách khác,

Internet là sân chơi giữa những kiểu hacker khác nhau – những kẻ xấu, hoặc mũ đen, những người luôn tìm mọi cách để xâm nhập trái phép hệ thống hoặc phát tán virut và những người tốt, hoặc mũ trắng, những người luôn tăng cường cho hệ thống bảo mật và phát triển những phần mềm diệt virut "khủng".

Tuy vậy, hacker, theo cả 2 bên đều hỗ trợ các phần mềm mã nguồn mở, chương trình mà nguồn code có sẵn cho mọi người học, sao chép, chỉnh sửa. Với các phần mềm mã nguồn mở, hacker có thể học từ kinh nghiệm của các hacker khác và và giúp tạo ra các chương trình hoạt động tốt hơn trước đây. Các chương trình có thể là những ứng dụng đơn giản tới hệ điều hành phức tạp như Linux.

Có một số sự kiện về hacker hàng năm, hầu hết là ủng hộ các hành động chịu trách nhiệm. Một hội nghị được tổ chức hàng năm ở Las Vegas có tên DEFCON thu hút được hàng ngàn người tham gia để trao đổi các phần mềm, tham dự các cuộc tranh luận, hội thảo về hack và phát triển máy tính cũng như thỏa mãn sự tò mò của mình. Một sự kiện tương tự có tên Chaos Communication Camp để chia sẻ phần mềm, ý tưởng và thảo luận.

Hackers và luật pháp

Nhìn chung, hầu hết các chính phủ rất lo ngại hacker. Khả năng xâm nhập vào những máy tính không được bảo vệ, ăn trộm thông tin quan trọng nếu chúng thích, là đủ để các cơ quan chính phủ coi đây là ác mộng. Những thông tin bí mật hoặc tin tình báo là cực kì quan trọng. Rất nhiều cơ quan chính phủ không mất thời gian vào việc phân biệt những hacker tò mò muốn thử kỹ năng của mình với hệ thống an ninh bảo mật cao cấp và một gián điệp.

Các điều luận đã thể hiện điều này. Tại Mỹ, có một số luật cấm các hành động hack như 18 U.S.C. § 1029 tập trung vào việc tạo, cung cấp và sử dụng code và các thiết bị giúp hacker truy cập trái phép một hệ thống máy tính. Điều luật này chỉ ghi sử dụng hoặc tạo ra các thiết bị với mục đích lừa gạt, vì

vậy, những hacker bị bắt có thể cãi rằng anh ta chỉ sử dụng thiết bị để tìm hiểu cách hoạt động của một hệ thống bảo mật.

Một luật quan trọng khác là 18 U.S.C. § 1030, nghiêm cấm việc truy cập trái phép hệ thống máy tính của chính phủ. Thậm chí, nếu một hacker chỉ muốn vào thử một hệ thống, người này vẫn phạm luật và bị phạt bởi đã truy cập không công khai máy tính chính phủ.

Việc xử phạt tùy theo mức độ, từ phạt tiền cho tới bỏ tù. Tội nhẹ cũng khiến hacker có thể bị bỏ tù 6 tháng, tội nặng có thể khiến hacker mất 20 năm trong tù. Một công thức từ trang Web của bộ tư pháp Hoa Kỳ dựa trên thiệt hại hoại kinh tế do một hacker gây nên, cùng với số nạn nhân mà người đó gây ra sẽ quyết định án phạt cho hacker này.

Đời sống hacker

Những hacker nào tuân thủ tốt luật pháp sẽ có được cuộc sống tốt. Một số công ty đã thuê hacker để tìm lỗi trong hệ thống bảo mật của họ. Hacker cũng có thể kiếm lợi bằng cách tạo ra các chương trình và ứng dụng tiện ích, giống như 2 sinh viên của trường đại học Stanford, Larry Page và Sergey Brin. Page và Brin đã làm việc cùng nhau để tạo ra một công cụ tìm kiếm với tên gọi Google. Năm 2008, họ đã được xếp thứ 26 trong danh sách của tạp chí Forbe những người giàu có nhất thế giới.

Những nước khác cũng có các luật tương tự. Đức mới đây đã ra một luật cấm sở hữu "các công cụ hack". Các nhà phê bình cho rằng luật này là quá rộng và có rất nhiều ứng dụng hợp pháp sẽ bị cấm bởi sự không rõ ràng trong điều luật này. Một số khác thì cho rằng, chiểu theo điều luật, các công ty có thể vi phạm luật nếu họ thuê hacker để tìm kiếm lỗi trong hệ thống bảo mật.

Hacker có thể thực hiện hành động phạm pháp ở một nước khi đang thoải mái ngồi ở một nước khác. Vì vậy, lần theo dấu vết của một hacker là cả một quá trình phức tạp. Các cơ quan hành pháp sẽ phải liên hệ với các nước để tìm kiếm kẻ tình nghi, quá trình này có thể mất hàng năm. Một vụ nổi tiếng là trường hợp chính phủ Mỹ đã kiện hacker Gary McKinnon. McKinnon, một

tay hacker người Anh đã đột nhập thành công vào nhiều máy tính quân sự của quân đội Mỹ và NASA, cho biết các hệ thống này được bảo mật khá yếu.

Hackers nổi tiếng

Steve Jobs và Steve Wozniak, người sáng lập của Apple, đều là hacker. Một số hành động ban đầu của họ thậm chí còn tương tự với các hành động của hacker nguy hiểm. Tuy nhiên, cả Jobs và Wozniak đã từ bỏ những hành động xấu và tập trung vào việc tạo ra phần mềm và phần cứng máy tính. Nỗ lực của họ đã dẫn đường cho kỷ nguyên máy tính cá nhân – trước Apple, hệ thống máy tính được cho là tài sản của các tập đoàn lớn, rất đắt và cồng kềnh đối với những người thu nhập trung bình.

Linus Torvalds, cha đẻ của Linux, cũng là một hacker nổi tiếng. Hệ điều hành mã nguồn mở của anh ta rất phổ biến với những hacker khác. Anh đã giúp khái niệm phần mềm mã nguồn mở được biết đến nhiều hơn, cho thấy khi bạn mở thông tin đối với mọi người, bạn có thể thu hoạch được rất nhiều lợi ích.

Richard Stallman, thường được viết tắt là RMS, người sáng lập ra dự án GNU, một hệ điều hành miễn phí. Ông là nhà sáng lập ra tổ chức phần mềm tự do FSF và chống lại các điều luật như quản lý quyền kỹ thuật số (Digital Rights Management).

Một trong những hacker mũ đen khác là Jonathan James. Ở tuổi 16, cậu đã trở thành hacker tuổi vị thành niên đầu tiên bị tống vào tù vì tội rình mò bên trong máy chủ của Cơ quan giảm thiểu các mối đe dọa quốc phòng của Mỹ (DTRA). Jonathan đã cố tình cài đặt một cửa hậu vào trong máy chủ để cho phép mình truy cập vào những email nhạy cảm cũng như tên người dùng, mật khẩu của các nhân viên cơ quan này. Ngoài ra, Jonathan còn tấn công vào Cơ quan Hàng không Vũ trụ Mỹ (NASA) và đánh cắp phần mềm trị giá 1,7 triệu USD. Trên mạng, cậu ta dùng nickname là “c0mrade”.

Kevin Mitnick gây được sự chú ý từ những năm 1980 đã đột nhập vào Bộ tư lệnh an ninh phòng không Bắc Mỹ (NORAD) khi mới 17 tuổi. Danh tiếng

của Mitnick đã nổi lên cùng với những vụ đột nhập của anh, thậm chí có tin đồn rằng Mitnick đã liệt kê FBI vào danh sách muốn tấn công nhất. Trong đời thường, Mitnick đã bị bắt một vài lần vì tội đột nhập vào hệ thống bảo mật để truy cập các phần mềm máy tính.

Kevin Poulsen, hay Dark Dante, là chuyên gia hack hệ thống điện thoại. Kevin nổi tiếng với vụ hack hệ thống máy chủ điện thoại KIIS-FM. Hành động tin tặc của Poulsen cũng "chẳng giống ai", tấn công vào hầu hết các đường dây điện thoại của Mỹ, làm đảo lộn các số liệu điện thoại ghi trong Yellow Page, hậu quả làm cho nội dung cuộc điện thoại trở nên lộn xộn. Đặc biệt, Poulsen còn can thiệp bằng cách chuyển mạch để chiếm số 102 - số đoạt giải thưởng một chiếc ôtô Porsche 944-S2 trong khuôn khổ chương trình khuyến mại tại khu vực này. Năm 1991, Poulsen bị bắt, bị phạt tù giam 5 năm. Khi mãn hạn tù, Poulsen chuyển sang làm nhà báo và hiện là Tổng biên tập tờ Wired News.

Adrian Lamo hack hệ thống máy tính bằng cách sử dụng các máy tính ở thư viện và các quán café Internet. Anh ta có thể hack những hệ thống lớn để tìm những lỗ hổng bảo mật rồi lợi dụng nó để truy cập vào hệ thống. Sau đó, anh ta lại gửi thông báo tới công ty chủ quản để cho họ biết về lỗ hổng này. Không may cho Lamo, anh ta hoạt động vì sở thích chứ không phải là một chuyên gia được thuê và hành động này là phạm pháp. Ngoài ra, anh ta cũng đã rình mò quá nhiều, đọc nhiều tài liệu mật và truy cập những tài liệu mật. Anh ta bị bắt sau khi đột nhập vào hệ thống máy tính thuộc thời báo nổi tiếng New York Times.

Chúng ta có thể ước chừng có đến hàng ngàn hacker hoạt động trực tuyến, nhưng một con số cụ thể là điều không thể. Rất nhiều hacker không nhận thức rõ điều họ đang làm – họ chỉ đang sử dụng các công cụ nguy hiểm mà bản chất họ cũng hoàn toàn không biết. Số khác biết rõ những gì họ đang làm khi có thể ra, vào một hệ thống mà có thể không ai biết.