Tội phạm mạng ngày càng tinh vi

Tại một cuộc hội thảo do công ty NetEvents tổ chức gần đây ở San Jose, California, Mỹ, các quan chức an ninh của nước này đã cảnh báo về sự tinh vi của tội phạm mạng hiện nay. Trong nhiều trường hợp, sự sơ suất của con người đã tiếp tay cho các hành động tấn công của tin tặc.

Chiến Thắng

Các diễn giả, từ trái sang, MK Palmore, Ronald Layton và Michael Levin.

Vào mùa xuân năm ngoái, một hôm ông David Mifflin ở San Antonio xem bản báo cáo tín dụng của mình trên mạng. Ông nhận thấy có điều gì đó không ổn. Ngân hàng Chase Bank đề nghị ông cung cấp một số thông tin liên quan đến yêu cầu xin mở thẻ tín dụng, trong khi ông không hề làm điều này. Để kiểm tra tình hình, Mifflin đã gọi điện thoại cho ngân hàng và được biết, tin tặc *(hacker)* đã đánh cắp thông tin về danh tính, số an ninh xã hội của ông. "Đừng phát hành thẻ, đó là kẻ giả mạo", Mifflin nói với ngân hàng.

Kể lại với đài NPR, Mifflin cho biết nhiều ngày, nhiều tuần sau đó, kẻ gian vẫn tiếp tục nỗ lực dùng tên ông để yêu cầu mở thẻ tín dụng. Điều đó khiến ông thấy rất phiền toái và bất an, đến nỗi nhiều đêm ông giật mình tỉnh giấc vì bị ám ảnh.

Mifflin cho hay, sau khi phát hiện ra những điều này, ông đã phải đăng ký sử dụng dịch vụ của công ty báo cáo tín dụng Experian, với mức phí 26 đô la một tháng. "Tôi phải trả 300 đô la một năm chỉ để xem thông tin của chính mình", Mifflin bực bội nói. "Đó là thông tin của tôi, lẽ ra tôi phải có quyền xem bất cứ lúc nào, và miễn phí".

Nạn nhân Equifax

Vụ tấn công của tin tặc nhằm vào hãng thông tin tín dụng Equifax của Mỹ bị phát giác (ngày 29-7) gây ảnh hưởng tới khoảng một nửa dân số Mỹ, tương đương 143 triệu người. Tin tặc đã tiếp cận được các thông tin nhạy cảm như tên, ngày sinh, địa chỉ, số an sinh xã hội, thậm chí số giấy phép lái xe. Nguy hiểm hơn, theo Equifax, số thẻ tín dụng của khoảng 209.000 người Mỹ đã bị lộ, trong đó có cả những công dân Mỹ sống ở nước ngoài như Anh và Canada.

Equifax là một công ty báo cáo tín dụng có chức năng theo dõi và đánh giá tài chính của người tiêu dùng Mỹ. Công ty này được cung cấp hầu hết các thông tin như khoản vay nợ, thẻ tín dụng, tiền thuê nhà, địa chỉ và thông tin nơi làm việc... để thực hiện công tác đánh giá.

Vụ tấn công nhằm vào Equifax được cho là vụ trộm số an sinh xã hội lớn nhất trong lịch sử nước Mỹ. Nó khiến cho các nhà lập pháp, các công tố viên và những nạn nhân bị đánh cắp thông tin, kiểu như trường hợp của ông Mifflin, rất tức giận.

Đã hơn hai tháng trôi qua, hậu quả của vụ tin tặc nói trên được dự báo sẽ còn kéo dài. Vậy những kẻ tin tặc này là ai? Chúng muốn gì? Làm sao để ngăn chặn? Đó là những câu hỏi được nêu ra tại cuộc hội thảo Global Press Summit 2017 (tạm dịch là Gặp gỡ báo chí toàn cầu), do NetEvents tổ chức ở California. Khách mời là các ông MK Palmore từ Cơ quan Điều tra Liên bang Mỹ (FBI) tại San Francisco; Ron Layton, Phó trợ lý Giám đốc Cơ quan Đặc vụ Mỹ (USSS); Michael Levin, cựu quan chức của Bộ An ninh nội địa Mỹ.

Tin tặc không còn độc lập

Ông MK Palmore (FBI) chia tội phạm mạng ra làm bốn dạng: những kẻ xâm phạm vì động cơ tài chính, những kẻ thực hiện các vụ đe dọa, những kẻ tấn công vì mục tiêu xã hội hay mang tính chất chính trị, và cuối cùng là những kẻ nhắm đến các quốc gia. Phổ biến nhất trong số đó, theo ông, là tội phạm có động cơ tài chính.

"Tin tặc đa phần là nam giới, trong độ tuổi từ 14-32", Palmore nói và nhấn mạnh có những đối tượng chỉ mới 14 tuổi.

Quan chức FBI này cho hay, ông chứng kiến nhiều trường hợp, những kẻ tin tặc không học bất cứ trường nào mà tự tìm hiểu thông tin trên mạng, sau đó dùng kiến thức tự học để thực hiện các vụ tấn công và gian lận. Tội phạm mạng đa số là ẩn danh, vì vậy rất khó cho lực lượng thực thi pháp luật trong việc truy tìm và bắt giữ.

Vì sao những kẻ tấn công vì động cơ tài chính lại chiếm số đông? Ông Ron Layton (USSS) nhớ lại câu chuyện về một tên cướp ngân hàng nổi tiếng ở Mỹ cách đây vài thập niên, có tên là Willie Sutton. Khi được cảnh sát hỏi, tại sao lại đi cướp ngân hàng, Sutton thản nhiên trả lời: "đơn giản đó là nơi cất giữ tiền".

Layton cho biết, Cơ quan Đặc vụ Mỹ được quốc hội Mỹ thành lập từ năm 1865, chủ yếu để ngăn chặn nạn tiền giả. Trải qua nhiều năm, nhiệm vụ của cơ quan này đã chuyển từ xử lý tiền giấy sang "tiền nhựa" (thẻ tín dụng) và tội phạm kỹ thuật số.

"Chúng tôi hiện đang đối phó chủ yếu với "tội phạm điện tử" trong lĩnh vực ngân hàng", ông nói. Là người có 25 năm kinh nghiệm, Layton cho hay, trước đây lực lượng của ông thường gặp các nhóm tin tặc hoạt động độc lập, làm việc theo phong cách riêng. Song vài năm trở lại đây, họ đã có những thay đổi đáng kể. "Chúng biết nhau, hợp tác với nhau. Đó là sự thách thức đối với tất cả chúng ta", ông nói.

Michael Levin, cựu quan chức Bộ An ninh Nội địa, người đã chuyển sang khu vực tư nhân, lại có quan điểm khác. Ông cho biết, chỉ có lực lượng thực thi pháp luật mới quan tâm tới tin tặc là ai, bởi họ muốn bắt giữ kẻ xấu. Còn lại, người ta không quan tâm những đối tượng này. Họ chỉ cần làm sao bảo vệ được thông tin, hoặc khôi phục được trang mạng trở lại mỗi khi bị tấn công, xảy ra sự cố, hay mất dữ liệu. "Vì vậy, những gì chúng tôi đang cố gắng tập trung vào khu vực tư nhân là làm thế nào để giúp các doanh nghiệp bảo vệ được mình khỏi trở thành mục tiêu tấn công", ông nói.

Lỗi của con người

Ông Levin so sánh, vụ tấn công mạng nhiều khi cũng giống như đột vụ nhập vào xe hơi. Đối tượng đầu tiên sẽ thử giật cánh cửa, nếu không được mới phá vỡ cửa sổ. Nhiều chiếc xe bị mất chỉ vì chủ... quên khóa cửa. "70 - 80% các vụ tấn công mạng là do lỗi của con người", ông nói.

Vụ tấn công nhằm vào hãng Equifax đang gây chấn động thế giới là một ví dụ điển hình về việc mắc phải những lỗi sơ đẳng. Theo ông Levin, công ty này đã mắc một lỗi rất đơn giản là không tạo ra các chế độ bảo mật tương xứng cho máy chủ.

"Lỗi này từng xảy ra cách đây 20 năm và giờ vẫn được lặp lại", ông nhấn mạnh.

Ông Ron Layton dẫn chứng: "Hầu hết các vụ đột nhập thành công đều là do an ninh được cài đặt ở mức độ thấp, chẳng hạn như sử dụng mật khẩu *(password)* kiểu 1234...". Vị quan chức USSS cho rằng yếu tố con người là rất quan trọng trong việc bảo đảm an ninh mạng. Theo ông, tin tặc hiểu rất rõ tâm lý của người sử dụng. Chúng nắm được một thứ gây nghiện mới, đó là sự tò mò. Chính sự tò mò khiến bạn vừa lái xe vừa nhắn tin, luôn muốn đọc những thông tin mới xuất hiện trên mạng.

Bằng chứng của sự tò mò về thông tin mới có ở nhiều nơi tại Mỹ, trong đó có các quán cà phê. Hãy thử vào bất kỳ quán cà phê nào ở Mỹ mà xem, mọi người đều cắm mặt vào thiết bị di động thay vì nói chuyện với nhau, và người ta nhấp con trỏ chuột (click) vào mọi thứ. Điều đó khiến cho bọn lừa đảo trực tuyến thường thành công, vì người ta quá tò mò. Họ luôn muốn xem đường dẫn *(link)* đó dẫn đến đâu, nếu nhấp con trỏ vào thì điều gì sẽ diễn ra... "Một tỷ lệ lớn các virus độc hại xâm nhập vào hệ thống là do con người *click* vào tập tin giả đính kèm e-mail", ông Layton khẳng định.

Đông tình với quan điểm này, ông Levin cho hay, dù công ty có công nghệ tốt nhất nhưng nếu các nhân viên của họ không được giáo dục và nhấp vào mọi e-mail họ nhận được và nhấp vào tất cả những liên kết hay tệp đính kèm, thì công nghệ cũng bó tay. Ông Levin kể: "Từ khi tôi không còn làm cho chính phủ và chuyển ra khu vực tư nhân, tôi đã phát hiện thấy một lỗ hổng lớn trong cách mà các doanh nghiệp đang xử lý bảo mật. Họ quên mất một điều rất quan trọng là đào tạo con người để tự vệ. Các công ty thuê người mới, đặt họ vào những vị trí, vai trò quan trọng, cung cấp cho họ máy tính nhưng lại không nói cho họ biết là có thể và không thể làm gì". Một trong những điều lớn nhất mà ông Levin phát hiện ra là, trên thực tế có nhiều tổ chức không muốn dành thời gian để giáo dục nhân viên về những gì họ có thể và không thể làm. Lần đầu tiên trên thế giới, chúng ta có một thế hệ như hiện nay, đó là một người sống suốt đời với chiếc máy tính. Vì vậy, đã đến lúc mọi công dân, mọi quốc gia, mọi tổ chức phải tìm cách để giáo dục con người cách tự bảo vệ mình.

"Nếu công ty của tôi có 10 đô la để chi tiêu, thì tôi sẽ chi tất cả 10 đô la ấy vào việc giáo dục", ông Layton nói.

NetEvents là một công ty của Anh, được thành lập năm 1996. Trong hơn 20 năm qua, công ty này luôn thúc đẩy các mối quan hệ giữa báo chí, các chuyên gia, các nhà sản xuất thiết bị, các công ty phần mềm, các nhà khai thác viễn thông, các công ty dữ liệu/lưu trữ, các nhà tích hợp hệ thống, các nhà kinh doanh và các hiệp hội...

NetEvents tổ chức các cuộc gặp giữa các nhà lãnh đạo về công nghệ bao gồm chủ tịch, giám đốc điều hành, các quan chức cao cấp từ các công ty công nghệ hàng đầu với các nhà báo và nhà phân tích cao cấp đến từ mọi khu vực trên thế giới để giao lưu, tìm hiểu, cung cấp thông tin mới nhất về những sự sáng tạo, hoạt động kinh doanh... trong lĩnh vực công nghệ thông tin.

Chủ đề của cuộc gặp năm nay là những phát minh sáng tạo trong lĩnh vực trí tuệ nhân tạo, an ninh mạng, Internet vạn vật và dữ liệu đám mây.