NHIỀU HACKER LÊN TIẾNG PHÊ PHÁN TỆ NẠN DDOS

Ngay sau bài Bảo kê trực tuyến, nhiều website lại bị tấn công dồn dập với quy mô lớn hơn. Trong khi các doanh nghiệp không dám lên tiếng thì DDoS, hành động được cho là hủy hoại tài nguyên mạng, cũng rất được giới hacker quan tâm và họ đã l&ecir

Ngay sau bài Bảo kê trực tuyến, nhiều website lại bị tấn công dồn dập với quy mô lớn hơn. Trong khi các doanh nghiệp không dám lên tiếng thì DDoS, hành động được cho là hủy hoại tài nguyên mạng, cũng rất được giới hacker quan tâm và họ đã lên tiếng. Ông Hoàng Ngọc Diêu, chuyên viên giải pháp công nghệ thông tin của một công ty bảo hiểm tại Australia và là thành viên Ban quan trị một diễn dàn hacker lớn ở Việt Nam, cho rằng tấn công từ chối dịch vụ (DDoS) là một trong những kết quả của sự tìm tòi và thử nghiệm trong thế giới bảo mật. Nó cũng giống như con dao bén. Nếu người dùng có thiện chí, họ sẽ cảnh báo sự nguy hại khi sử dụng con dao này không đúng chỗ, không đúng mức. Còn ngược lại, công cụ này sẽ được dùng trong bất kỳ hoàn cảnh, mục đích nào. "DDoS trở thành vấn nạn như hiện nay bởi nó rơi vào tay của quá nhiều kẻ thiếu thiện chí và bất cứ người làm công tác bảo mật nào cũng chán ghét", ông Diêu khẳng định. "Chúng tôi chỉ nhắm vào các website công nghệ thông tin, diễn đàn và những địa chỉ khiêu dâm (xxx), mà không đụng chạm đến doanh nghiệp nếu không bị admin thách thức", một hacker có nickname hero_zero tiết lộ. "DDoS là cách dễ thành công, đơn giản và ít mất thời gian, chỉ cần 'bắt' được thật nhiều website. Phần đông người chọn tấn công DDoS là các thành viên trẻ tuổi, không có khả năng xâm nhập vào website của người khác". Có ý kiến cho rằng đây là giải pháp cuối cùng và bất đắc dĩ nhất của hacker, khi không thể khai thác lỗi hay tấn công mục tiêu. Mục đích chính của DDoS là ngăn người dùng truy cập vào website. Lợi dụng đặc điểm này, một số hacker đã tiến hành DDoS thuê kiếm tiền. "Tôi được thuê phá một website Việt Nam với giá 2.000 USD, nếu tôi không DDoS thì cũng có kẻ khác nhận làm việc này. Hơn nữa, tôi cũng muốn thử trình độ bảo mật và đột nhập vào nguồn cơ sở dữ liệu rất lớn của họ", một hacker nước ngoài thổ lộ. Giới hacker Việt Nam đang truyền tai về một nhóm chuyên DDoS thuê kiếm tiền với khách hàng là giới kinh doanh, bảo mật... Tấn Quang, một hacker ở TP HCM, cho biết: "Khá nhiều tay thuê 'xã hội đen' trên mạng khử đối thủ cạnh tranh, tấn công DDoS qua lại, cuối cùng cả hai đều thiệt hại và chẳng giải quyết được vấn đề gì. An ninh mạng lại trở nên tồi tệ hơn và giới công nghệ thông tin cùng hacker chân chính lại cảm thấy bất an". Cộng đồng công nghệ thông tin từng chứng kiến những đợt tấn công DDoS có quy mô mà ngay cả giới hacker cũng e ngại sức mạnh của việc "mượn gió bẻ măng" này. Bởi người dùng mạng bình thường không thể phân biệt được những banner trên website đã bị cài các đoạn mã tấn công DDoS, hay khi họ vào một website nghe nhạc, click vào một bài hát là cùng lúc đã thực hiện 2 chương trình, trong đó có lệnh tấn công một site khác. Đối mặt trực tiếp với DDoS không ai khác ngoài các chuyên viên và nhóm nghiên cứu bảo mật. Với họ, đây là hành động chứng tỏ sự yếu kém về kiến thức và đáng bị xem thường, cần lên án nhất. Cũng vì thế, ông Diêu cho rằng ở nước ngoài không mấy ai chính thức công bố chủ quyền của một dạng DDoS nào đó, ngoại trừ mục đích nghiên cứu và khắc phục. "Ở các nước, tấn công DDoS cũng rất đa dạng nhằm thử nghiệm, gây áp lực hoặc chứng minh quan điểm... Tuy nhiên, nó xuất hiện và chấm dứt một cách khá ngắn ngủi", hacker kỳ cựu này nhận định. DDoS - con dao hai lưỡi Cũng vì những tác hại không lường này mà nhu cầu tìm hiểu về DDoS và lượng người đến các lớp bảo mật ngày một tăng. Ông Võ Đỗ Thắng, Trưởng phòng dự án và đào tạo của Trung tâm đào tạo quản trị mạng Athena (TP HCM), cho biết: "Việc giảng dạy bảo mật là một vấn đề khá nhạy cảm trước tình hình hiện nay. Để bảo vệ hệ thống của mình, học

viên phải được trang bị những kiến thức về cơ chế tấn công và giải pháp chống đỡ". Học công nghệ thông tin nói chung hay bảo mật nói riêng không thể dựa vào lý thuyết, mà phải trình diễn trên hệ thống. Với DDoS cũng vậy, toàn bộ quá trình tấn công được các giảng viên thực hiện ngay trên mạng nội bộ. "Chúng tôi cung cấp các công cụ DDoS cho học viên chỉ nhằm vào mục đích học tập và luôn định hướng học viên đi đúng đường, trở thành chuyên gia bảo mật. Bài học đầu tiên chúng tôi giảng dạy bao giờ cũng là đạo đức", ông Thắng nói thêm. "Nhưng thực tế, trung tâm cũng không thể kiểm soát và chịu trách nhiệm nếu học viên vận dụng những kiến thức đã học để phá phách". Hiện tượng DDoS các website ở Việt Nam đang phát triển rất mạnh, gần như là phong trào. Phần lớn do sinh viên sử dụng các công cụ sẵn có tấn công DDoS (script kiddies). Để tiếp cận với những kẻ tổ chức tấn công (DDoSer) dạng này, một hacker bày cách: "Tạo cái nick thật pro, tìm một code DDoS và thử nghiệm vài website, khi đó sẽ có nhiều người liên hệ với bạn. Để biết ai là kẻ tấn công từ chối dịch vụ, trước hết bạn phải là DDoSer". Lượng DDoSer tại Việt Nam ngày một tăng lên, nhưng điều này không có nghĩa là phần lớn hacker tán thành nó. Tấn Quang, tâm sự: "Đó thực sự là thảm họa và những người hiểu biết, có 'nghề' và có ý thức sẽ không gây hại các website hay thể hiện quyền lực bằng cách này. Đừng tấn công vì những mục đích không chính đáng. Hãy nói không cùng DDoS.". Đại diện cho một nhóm hacker vừa tuyên bố "đoạn tuyệt" với kiểu DDoS bộc bạch: "Chúng tôi thấy mình đã sai lầm khi xuất bản công cụ DDoS x-flash. DDoS khiến bản thân kẻ tấn công cũng bị thiệt hại do tốn băng thông mạng của máy tính cá nhân để phát động, chưa kể đến khả năng bị tấn công DDoS lại. Sửa chữa những sai lầm trong quá khứ, chúng tôi sẽ ngưng xuất bản những công cụ tấn công đồng thời vô hiệu hóa những gì phát tán trước đó vì chúng có một số đặc điểm dễ nhận ra và phòng chống". Hạn chế DDoS phải có sự phối hợp giữa kỹ thuật và pháp lý Theo chuyên gia bảo mật Hoàng Ngọc Diêu, để giảm thiểu thiệt hại ở mức thấp nhất, webmaster có thể dùng một số firewall mềm như HCe'firewall hay các script firewall khác, đồng thời kiểm tra website mỗi ngày và log script không tiếp tay cho kẻ tấn công. Mặt khác, ISP cũng cần có trách nhiệm giám sát lượng zombie (máy tính đã bị khống chế) đang bị lợi dụng để tấn công, thông báo cho người sử dụng biết về tình trạng vô tình tiếp tay và lọc những website bắt nguồn DDoS. Bên cạnh đó, Luật về tội phạm công nghệ cao cũng là giải pháp đánh vào tâm lý những người tấn công DDoS. Ông Diêu nói thêm: "Các cơ quan chức năng cũng phải quan tâm đúng mức những vấn đề ảnh hưởng đến thương mại điện tử, bởi chúng trực tiếp tác động đến nền kinh tế quốc gia. Luật hiện hành cần sửa đổi kịp thời và nghiêm khắc xử lý những hành động mang tính phá hoại trên môi trường liên mạng". "Để truy tìm thủ phạm, nhất thiết phải có sự phối hợp và quyết tâm cao của doanh nghiệp, ISP, chuyên gia công nghệ thông tin và Luật dành cho tội phạm Internet", ông Nguyễn Anh Hào, giảng viên chuyên về bảo mật của Trung tâm đào tạo quản trị mạng Athena, nhận xét. "Nếu luật pháp quy định chặt chẽ các hình phạt và xử nghiêm những tội phạm tin học này thì sẽ hạn chế phần nào những DDoSer đùa nghịch đồng thời có tác dụng răn đe rất tốt đối với những kẻ vì tiền, đang được xem là ngòi nổ cho loại hình kiếm lợi bất chính trên mạng". "Dù rằng một số thành viên đam mê tin học và muốn chứng tỏ mình đã có những hành động không đúng, nhưng không hẳn tất cả hacker đều là người xấu hay những kẻ phá hoại", một hacker bày tỏ. "Trước khi buộc tội DDoS, doanh nghiệp thương mại điện tử cần xem xét lại thực lực, vật chất và trình độ kỹ thuật của mình. Bởi lẽ kỹ thuật bảo mật còn yếu thì dù không bị DDoS hay hack, cũng không sống được". Còn ông Hoàng Ngọc Diêu thì khẳng định: "Việc các chuyên viên kỹ thuật phó mặc cho những nhà cung cấp phần mềm, phần cứng, router, firewall là thái độ tiêu cực trước hiểm hoạ DDoS và sẽ không đưa đến kết quả tích cực".
Văn Hồng - Nguyễn Hằng