NẾU HACKER TRẺ CÓ SÂN CHƠI LÀNH MẠNH

Sân ch

Sân chơi đó, có thể là câu lạc bộ về bảo mật do các chuyên viên dẫn dắt, sẽ giúp hacker trẻ nâng cao ý thức và kiến thức pháp luật...

Theo nghĩa ban đầu, hacker là những chuyên viên tin học cực kỳ giỏi về lập trình, an ninh mạng. Những chuyên viên này phát hiện các lỗ hổng an ninh và đưa ra biện pháp vá lại. Công việc của họ đặt nền tảng cho ngành bảo mật máy tính phát triển, một số công ty bảo mật đã ra đời với sự tham gia các các hacker như thế. Có thể gọi đây là hacker thế hệ đầu tiên.

Các vụ phá phách của "lính mới" tăng nhanh

Nguyên tắc đạo đức chung của cộng đồng hacker thuộc thế hệ đầu tiên là sự chia sẻ thông tin kỹ thuật. Mọi hành động gây ra thiệt hại đều bị xem là không đúng chuẩn mực của hacker chân chính.

Tuy nhiên, dần dần giới hacker phân hóa, có người tiến hành những hành động phá hoại, tống tiền, đánh cắp dữ liệu, tiền bạc... Từ đó hình thành ra khái niệm chia hacker làm ba nhóm: mũ trắng, mũ đen và mũ xám.

Hacker mũ trắng dò tìm lỗ hổng bảo mật với mục đích "vá" những lỗ hổng đó. Khi phát hiện lỗ hổng, họ cung cấp thông tin về lỗi bảo mật cho người có trách nhiệm quản lý website với mục đích giúp đỡ. Họ cũng có thể được các công ty thuê xâm nhập vào hệ thống mạng nội bộ hay website để kiểm tra mức độ bảo mật.

Hacker mũ xám cũng hành động có thể không vì tiền khi phát hiện lỗ hổng. Tuy nhiên, họ muốn tìm kiếm danh tiếng nên thường đưa công khai lên mạng hay báo chí những lỗi bảo mật do họ phát hiện.

Hacker mũ đen xâm nhập vào một hệ thống với chủ ý phá hoại hệ thống mạng hay kiếm tiền bất chính.

Những hacker thứ thiệt là các chuyên viên siêu giỏi trong lĩnh vực bảo mật. Hầu như không có website nào có thể dám bảo đảm 100% là chống lại các vụ tấn công của họ. Giới hacker này thường tự viết ra những công cụ riêng để vượt qua các hàng rào bảo mật. Họ có khả năng làm

điên đảo mọi hệ thống dù được bảo vệ cẩn thận đến đâu. Thực tế tại Mỹ cho thấy, website của Bộ Quốc phòng Mỹ, Cục Điều tra Liên bang (FBI) hay của người khổng lồ phần mềm Microsoft đều có thể bị xâm nhập.

Để được giới hacker quốc tế công nhận rất khó khăn. Hầu hết các vụ phá hoại gần đây ở VN thường do những người mà giới hacker gọi là "newbie" hay "script kiddies" hoặc "packet monkeys", nói nôm na là "lính mới". Khác với hacker, "lính mới" không đủ trình độ viết công cụ riêng. Họ dùng các tiện ích được người khác viết và có sẵn trên mạng để dò tìm lỗ hổng của website và tấn công. Kỹ năng của họ chỉ ở mức bình thường nhưng vì công cụ có sẵn rất nhiều nên số lượng "lính mới" ngày càng tăng và mức độ phá phách của họ khá nguy hiểm.

Với tình trạng an ninh lỏng lẻo như hiện nay, nếu các hacker thứ thiệt (và là hacker ở nước ngoài) ra tay thì mức độ thiệt hại sẽ khó lường hết được.

Cần vá "lỗ hổng" trong đầu

Sự việc website Bộ GD-ĐT bị tấn công cho thấy tình trạng an ninh còn khá lỏng lẻo của nhiều website ở VN nói chung và trong hệ thống cơ quan Nhà nước nói riêng. Nguyên nhân không chỉ có lỗ hổng nằm trên website mà còn cả trong đầu, tức nhận thức của những người có liên quan.

Không phải bây giờ tình trạng phá hoại và tội phạm trên mạng mới rộ lên. Ngay từ năm 2000-2001, Báo Người Lao Động đã vài lần lên tiếng cảnh báo về tình trạng an ninh lỏng lẻo khiến hacker đánh cắp mật khẩu Internet tung lên mạng tràn lan.

Năm 2002, tại Ngày hội Hacker VN, một số hacker mũ trắng cho biết họ đã phát hiện và liên hệ với các đơn vị quản lý website nhưng hầu hết cảnh báo của họ rơi vào im lặng.

Khoảng năm 2004, rộ lên tình trạng ăn cắp mã thẻ tín dụng (thường gọi là CC chùa). Việc dùng CC chùa phổ biến đến mức VN gần như bị cô lập khỏi nền thương mại điện tử thế giới vì các giao dịch bằng thẻ tín dụng từ VN đều bị từ chối.

Từ năm 2005, nhiều vụ tấn công website nghiêm trọng xảy ra, trong đó có cả một số vụ do các nhóm hacker Thổ Nhĩ Kỳ là thủ phạm.

Các trung tâm an ninh mạng như: VSEC, BKIS, VNCERT ... liên tục đưa ra cảnh báo về tình trạng thiếu an ninh trong hệ thống website Nhà nước lẫn doanh nghiệp, nhưng các lỗ hổng vẫn chậm được khắc phục.

Nguyên nhân sâu xa khiến còn quá nhiều lỗ hổng trên website bắt nguồn từ chính sự chủ quan của những người có trách nhiệm quản lý. Có quan chức ngành giáo dục phát biểu rằng ông nghĩ "website của Bộ GD-ĐT, ai nỡ phá". Có thể nói, đó là những lỗ hổng an ninh bắt nguồn từ nhận thức của người quản lý website.

Với công cụ hack được cung cấp tràn lan, giới trẻ cũng dễ tò mò muốn dùng thử, nhất là khi lỗi

bảo mật cứ phơi bày sờ sờ ra đó. Giá như giới trẻ có được các sân chơi lành mạnh thì các vụ phá phách sẽ giảm đi, chẳng hạn các câu lạc bộ về bảo mật do các chuyên viên dẫn dắt. Như vậy, vừa hướng các em đến công nghệ bảo mật để giúp ích cho xã hội, vừa giúp các em nâng cao ý thức, tránh những lỗ hổng về kiến thức pháp luật.

Đồng Phước Vinh