ÁC MỘNG MANG TÊN VIRUS

Đã xa rồi cái thời tác giả của những con virus làm điêu đứng hàng triệu máy tính chỉ là dân hacker tuổi teen "ngựa non háu đá", muốn chứng tỏ bản lĩnh nam nhi. Bây giờ ngoái đầu nhìn lại, dù sao đấy vẫn còn là "d

Đã xa rồi cái thời tác giả của những con virus làm điêu đứng hàng triệu máy tính chỉ là dân hacker tuổi teen "ngựa non háu đá", muốn chứng tỏ bản lĩnh nam nhi. Bây giờ ngoái đầu nhìn lại, dù sao đấy vẫn còn là "dĩ vãng tốt đẹp". Bạn nghĩ kết luận này có vẻ ngược đời và kỳ cục? Trên thực tế, tình hình bảo mật hiện nay so với ngày ấy thực sự đã là "một trời một vực". Những cuộc tấn công hôm nay có quy mô hẹp hơn, nhưng tấn công rất trúng mục tiêu - xuyên thủng cả những hệ điều hành được gia cố mạnh nhất. Thay thế cho "lũ ngựa non háu đá" ngày xưa, viết ra một chương trình virus nào đó chỉ để lừng danh thiên hạ thì nay, các cuộc tấn công hầu như đều được tài trợ bởi các băng nhóm tội phạm. Mục đích của chúng rất rõ ràng: đánh cắp thông tin (cả dữ liệu tập đoàn lẫn tài khoản cá nhân) để sử dụng trong các phi vụ lừa đảo tinh vi. Thế nên không có gì quá ngạc nhiên, khi chính những phần mềm được thiết kế để bảo mật hệ thống lại tự mình biến thành mục tiêu của dân hacker. Bên cạnh làn sóng tấn công nhằm vào hệ điều hành Windows, một xu hướng khác đang mạnh dần lên là tấn công vào những chương trình ứng dụng được nhiều người cài đặt. Từ phần mềm cơ sở dữ liệu, phần mềm chống virus, phần mềm backup dữ liệu hay thậm chí cả phần mềm nghe nhạc - tất cả những hớ hênh của các chương trình này đều bị khai thác triệt để. Thông tin tập đoàn và thậm chí quốc gia đều bị đặt trước nguy cơ xâm nhập. "Các vụ tấn công đều nhằm vào việc đánh cắp thông tin", giám đốc quản lý sản phẩm của Symantec, nhận định. Nguy cơ mới Thật nguy hiểm khi đa số người dùng luôn chủ quan rằng họ đã được an toàn vì luôn cài đặt miếng vá bảo mật mới nhất. Bạn phải luôn đảm bảo rằng ngoài hệ điều hành, các chương trình ứng dụng khác cài đặt trong máy cũng luôn được cập nhật. Một điều may mắn là ngày càng nhiều chương trình, chẳng hạn như Adobe Acrobat Reader và Mozilla Firefox, chịu trang bị hệ thống tự động cập nhật (Xin lưu ý là cả AAR lẫn Firefox đều từng bị tấn công trong năm 2005). Và bởi vì các ứng dụng này chạy được trên đủ loại hệ thống khác nhau, nên người dùng hệ điều hành Mac OS X hay Linux cũng không thể tự ru ngủ rằng chẳng hacker nào thèm động đến mình. Nhìn lại bản báo cáo Top 20 lỗ hổng bảo mật nghiêm trọng nhất 2005 của SANS, ta sẽ thấy có tới 9 trường hợp được thiết kế để tấn công vào nhiều nền điều hành khác nhau. Các chương trình chia sẻ file như eDonkey, Kazaa và BitTorrent là các mục tiêu bị bắn phá nhiều nhất. Vấn đề chính ở đây là tất cả các file được phát tán qua những mạng P2P này đều có thể là tác nhân gây truyền nhiễm virus mà người dùng chẳng hay biết gì. Tội lỗi của media Từ Windows Media Player, RealPlayer cho đến iTunes và CD của Sony BMG, đa số các phần mềm nghe nhạc phổ cập đều dính lỗ hổng bảo mật, cho phép kẻ tấn công tự động cài đặt những chương trình hiểm độc như theo dõi bàn phím, đánh cắp mật khẩu và các thông tin tài khoản khác. Chính vì thế, kết luận rằng download trái phép là phạm pháp và có nguy cơ bị kiện cáo cao vẫn còn chưa đủ. Nguy cơ bảo mật là một lý do thuyết phục khác để bạn phải cân nhắc tới việc tránh xa các chương trình chia sẻ file. Một xu hướng khác cũng rất đáng lo ngại là bọn hacker ngày càng bắn phá máy chủ web nhiều hơn. Trong trường hợp xấu nhất, bọn chúng có thể tạo ra các site giả, hoặc thậm chí giật quyền kiểm soát site thật - để tiến hành các vụ tấn công nhằm vào tất cả những ai ghé thăm file, thông qua các lỗ hổng có trong trình duyệt. (Nhiều website sử dụng ngôn ngữ scripting PHP đã bị đặt trong tầm ngắm năm nay). Một vài viên thuốc an thần Xem ra, cơn ác mộng mang tên virus này còn khiến bạn đau đầu và mất ngủ triền miên. Trong khi chờ đợi

một phương thuốc hiệu nghiệm, hãy tự an ủi cho mình bằng vài viên thuốc an thần. Một kinh nghiệm rút ra là tất cả các hãng cung cấp phần cứng và phần mềm máy tính đều phải học theo Microsoft cùng Apple trong việc cung cấp cơ chế bảo mật và cập nhật cho hệ thống một cách tự động. Bọn tội phạm tấn công vào các sơ hở với tốc độ ngày càng nhanh và tất nhiên, chúng ta chẳng bao giờ có thể nói :"Này, đợi tôi cài xong hệ thống bảo mật đã" với chúng. Có thể nói, tư duy bảo mật của cả người tiêu dùng lẫn các hãng công nghệ đều đã bị lạc hậu tới... 6 năm. 6 năm trước, những kẻ tấn công chỉ nhắm đến hệ điều hành - khi đó chẳng được một doanh nghiệp hệ điều hành nào tiến hành cập nhật tự động. Giờ đây, những kẻ tấn công lại chuyển sang nhòm ngó các ứng dụng phổ biến - và tất nhiên, tất cả các ứng dụng này cũng chẳng được cập nhật tự động nốt. Các doanh nghiệp phần mềm đang loay hoay xây dựng cơ chế cho phép cập nhật ứng dụng tự động, còn người dùng thì hãy biết tự quý mình bằng việc cài đặt bảo mật bằng tay trước cái đã. Thiên Ý