NHỮNG ĐE DOẠ BẢO MẬT LỚN NHẤT NĂM 2007

Thế gi

Thế giới mạng ngày càng trở nên mất an toàn hơn, hàng chục, thậm chí là hàng trăm các loạt virus, phần mềm độc hại (malware) được tạo ra mỗi ngày, gây thiệt hại rất lớn cho người dùng. Trong hoàn cảnh đó, việc kiểm soát các hành vi của bạn trên mạng cũng như nắm được quy luật và phương thức hoạt động của malware sẽ giúp bạn giảm được thiệt hại không đáng có.

Đe doạ số 1: IE

Dẫn đầu trong danh sách các mục tiêu "bắn phá" về bảo mật trong hầu hết các báo cáo gần đây của FBI và Viện SANS là trình duyệt Internet Explorer của Microsoft. Lý do: là trình duyệt được sử dụng rộng rãi hiện nay, IE mang lại cho giới tin tặc nhiều khoản thu khổng lồ nếu chúng khai thác các lỗ hổng của ứng dụng này.

Cội nguồn những trục trặc bảo mật trong IE chính là công nghệ ActiveX (của Microsoft), cho phép các website có thể chạy những chương trình thực thi trên PC thông qua trình duyệt người dùng. Các bản vá lỗi (patch) và nâng cấp, gồm cả Windows XP SP2 và gần đây nhất là IE7, đã làm cho ActiveX an toàn hơn nhưng thật không may là ngày càng có nhiều các lỗ hổng cho phép phần mềm độc hại có thể qua mặt những tính năng bảo mật, cộng với thực tế quá tò mò của người dùng máy tính nên sự cải thiện của ActiveX chẳng đáng là bao. Thật đáng mừng là ngoại trừ một số hạn chế (chẳng hạn như không vào được trang Windows Update của Microsoft) thì bạn vẫn có thể sử dụng IE để duyệt Web hiệu quả mà không cần có tính năng ActiveX.

Để vô hiệu hoá ActiveX trong IE6 và 7, bạn vào Tools > Internet Options > Security > Custom Level > Run ActiveX controls and plug-ins > chọn Disable (xem hình 1). Nhấn OK > Yes > OK để đóng hộp thoại. Để kích hoạt ActiveX trên một trang web đã biết và được đánh giá là an toàn, bạn vào Tools > Internet Options > Security > chọn Trusted Sites > nhấn Sites, và nhập địa chỉ site vào hộp thoại rồi nhấn Add. Bỏ lựa chọn Require server verification (https:) for all sites in this zone, rồi nhấn Close và OK.

Hình 1

Nếu bạn để ActiveX ở chế độ "enable", bạn sẽ nhanh chóng gặp các trường hợp site nguy hiểm (cài phần mềm độc hại) và phần đính kèm e-mail yêu cầu cài đặt trình điều khiển ActiveX trên hệ thống. Trừ khi bạn chắc 100% những trình điều khiển này là an toàn và hợp pháp thì mới cho phép cài đặt, còn nếu không hãy huỷ bỏ chúng.

Bạn phải thường xuyên cập nhật Windows và trình duyệt để giảm thiểu nguy cơ bảo mật bất kể trình duyệt mặc định đó có thể là IE, Firefox, hay Opera đi chăng nữa. Để nâng cấp Windows XP, bạn hãy truy cập vào trang update.microsoft.com (phải sử dụng trình duyệt IE mới có thể vào trang này – một dạng độc quyền thường thấy của Microsoft chăng?) và cài đặt bản Service Pack (SP) 2 nếu máy tính của bạn chưa có bản nâng cấp này. Tiếp theo chọn Start > Control Panel > System > và nhấn và tab Automactic Updates. Chọn chế độ "Automatic (recommended)" nếu bạn hoàn toàn tin tưởng Microsoft. Chọn chế độ "Download updates for me, but let me choose when to install them" nếu bạn chỉ hơi tin tưởng Microsoft. Và chọn chế độ "Notify me but don't automatically download or install them" để bạn có thể tự quyết định nên cài hay không cài bản nâng cấp.

Nếu bạn cảm thấy IE6 đã quá nhàn chán thì hãy nâng cấp lên phiên bản mới – IE7 (khả năng bảo mật ActiveX đã được cải thiện). Ngoài ra, vẫn còn một cách khác tốt hơn để giảm nguy cơ bảo mật từ ActiveX là download và cài đặt một trình duyệt khác, rồi cấu hình chúng thành trình duyệt mặc định trên hệ thống. Trong trường hợp này, Firefox của Mozilla được coi là sự thay thế tốt nhất cho IE. Tuy nhiên, việc Firefox dần trở nên phổ biến đã thu hút sự chú ý của giới tin tặc và các lỗ hổng của trình duyệt này dần dần bị phơi bày. Mặc dù không có phần mềm nào là an toàn tuyệt đối, nhưng rất nhiều chuyên gia tin rằng Opera vẫn là trình duyệt tốt nhất với chỉ số an toàn cao hơn IE và Firefox.

Đe doạ số 2: Lừa đảo trực tuyến và đánh cắp danh tính

Trên thực tế, rất có thể bạn đã từng là nạn nhân của trò lừa đảo trực tuyến (phishing). Loại hình tấn công này không phải là mới nhưng vẫn là phương thức lừa đảo rất thành công, bằng chứng là trong thời gian qua số nạn nhân phishing ngày càng gia tăng. Khởi đầu cho hình thức lừa đảo này là bạn sẽ nhận được một thông báo giả mạo từ ngân hàng, PayPal, eBay, hoặc các tài khoản trực tuyến khác. Theo đó, thông báo này yêu cầu bạn cần xác nhận lại thông tin bằng cách cung cấp tên và mật khẩu truy cập, thông tin về số thẻ tín dụng, tài khoản ngân hàng. Bạn thường được yêu cầu nhấn vào đường link để truy cập vào trang web của ngân hàng (thực chất là giả mạo) để khai báo thông tin.

Khi con mồi đã cắn câu, những kẻ lừa đảo (phisher) sẽ thu thập dữ liệu của nạn nhân, rồi bán chúng cho kẻ cần mua hoặc sử dụng chúng để rút tiền trong tài khoản người dùng. Tin tặc thường tạo ra một website nguy hiểm, chỉ khác chút so với website thực (chẳng hạn như www.amazom.com thay cho www.amazon.com với hy vọng người dùng không để ý khi truy cập vào.

Rất có thể bạn đã từng biết tới quy định của ngân hàng là không bao giờ gửi cho khách hàng e-mail yêu cầu họ log-in vào tài khoản, mà hầu hết các thông điệp có vẻ như được gửi đi từ các tổ chức tài chính đều thuộc dạng "phishing". Do vậy tốt hơn hết là bạn không mở chúng ra và cũng không nhấn vào bất cứ đường link nào trong thông điệp này. Nếu bạn lo lắng rằng ngân hàng đang cố liên hệ với bạn để thông báo một vấn đề nào đó thì hãy mở website (tự nhập địa chỉ) của ngân hàng đó ra và đăng nhập trực tiếp vào tài khoản của mình; hoặc tốt hơn hết là hãy nhấc điện thoại gọi cho nhân viên chăm sóc khách hàng để hỏi thông tin.

Nếu phát hiện những dấu hiệu khả nghi từ e-mail gửi tới cho bạn, hoặc các trang web truy cập vào (để khai báo thông tin cá nhân), bạn nên báo cho nhà chức trách hoặc ngân hàng để ngăn chặn. Thường các trang phishing có tuổi đời không lâu, nó chỉ xuất hiện trong ít hôm rồi biến mất sau khi thực hiện xong nhiệm vụ mà chủ nhân của nó tạo ra.

Cả IE7 và Firefox 2 đều được trang bị tính năng chống phishing mới, có thể so sánh đường link với cơ sở dữ liệu các trang phishing đã được biết tới trước khi hiển thị trang web. Riêng IE7, thời gian cài đặt trình duyệt này sẽ kéo dài thêm chút ít nếu người dùng lựa chọn tính năng lọc (filter) phishing trong quá trình setup. Để kích hoạt tính năng này, bạn vào Tools > Phishing Filter > Turn on Automatic Website Checking > và nhấn OK.

Trong khi đó, tính năng lọc phishing của Firefox 2 được kích hoạt mặc định nhưng nó lại download một danh sách tĩnh các site phishing xuống máy để phân tích và đối chiếu. Để sử dụng dịch vụ Phishing Protection thay thế của Google, bạn vào Tools > Options > Security > và chọn "Check by asking Google about each site I visit" (hình 2). Chú ý là bạn sẽ phải chấp nhận thoả thuận giấy phép của nhà cung cấp dịch vụ (ở đây là Google).

Hình 2
Rất nhiều chương trình bảo mật và tường lửa đều dược trang bị tính năng bảo vệ chống đánh cắp danh tính. Chức năng này sẽ kiểm soát dòng dữ liệu nhạy cảm (mật khẩu, số thẻ tín dụng, số ID…) được chuyển khỏi máy tính và sẽ tiến hành khoá những hành vi trái phép.

Đe doạ số 3: Phần mềm độc hại

Những kẻ tạo ra virus, chương trình gián điệp (spyware), và chương trình quảng cáo (adware) luôn đổi mới cách thức "tiếp thị" và xâm nhập vào máy tính của bạn với mục đích đánh cắp thông tin, phá huỷ dữ liệu hoặc lợi dụng PC của bạn làm bàn đạp tấn công sang máy tính khác. Những bước sau đây sẽ giúp bạn giữ mình được an toàn trước những nguy cơ này:

Nghĩ kỹ trước khi nhấn chuột: Các file đính kèm có đuôi .exe, .com, .bat, và .scr cũng như một số tệp tin tài liệu được đính kèm đoạn mã script như: .doc, .xls… có thể xâm nhập thẳng vào máy tính của bạn chỉ với một động tác nhấp chuột đơn. Tuy nhiên, hiện nay có rất nhiều các chương trình e-mail ngăn không cho người dùng truy xuất vào các file đính kèm có đuôi dạng thực thi (.exe, .com…).

Sử dụng tính năng lọc thư rác: Mặc dù có một số phần mềm độc hại tìm cách đột nhập vào máy tính thông qua trình duyệt, nhưng e-mail vẫn được xem là tài nguyên chính và là mục tiêu lớn nhất của loại phần mềm này. Việc cài đặt một chương trình lọc spam sẽ giúp bạn giảm nguy cơ kích hoạt các đoạn script độc hại gắn kèm trong thông điệp nhận về.

Nâng cấp phần mềm diệt virus: Vẫn để chương trình diệt virus chạy trên máy sau khi chúng đã hết thời gian sử dụng còn tệ hơn việc bạn không dùng phần mềm diệt virus nào. Bởi khi đó, bạn không chỉ không cập nhập được bản nâng cấp mới (cơ sở dữ liệu nhận dạng virus) mà còn tạo cơ

hội cho các phần mềm độc hại khai thác lỗ hổng đã được biết tới trong chương trình diệt virus. Nếu máy tính của bạn buộc phải chạy các chương trình có bản quyền thì bạn nên sử dụng chương trình diệt virus miễn phí AVG Anti-Virus (www.grisoft.com).

Sử dụng nhiều lựa chọn hơn: Bạn chỉ có thể cài đặt và sử dụng một chương trình diệt virus tại một thời điểm trên máy tính bởi các động cơ quét thời gian thực của chúng sẽ xung đột với nhau. Nếu bạn nghi ngờ tính hiệu quả của phần mềm diệt virus trên máy tính, thì nên sử dụng chương trình quét virus trực tuyến miễn phí, chẳng hạn như ActiveScan (xem hình 3) của Panda Software (http://www.pandasoftware.com/products/ActiveScan.htm) hoặc HouseCall của Trend Micro (http://housecall.trendmicro.com/).

Hình 3
Thận trong khi download: Bất cứ chương trình nào mà bạn download và chạy trên hệ thống đều có thể gây nguy hại cho máy tính, nó có thể tạo một cơ chế phục vụ cho việc xâm nhập hoặc làm bàn đạp để tấn công sang máy tính khác. Bạn chỉ download những phần mềm từ các nguồn đã được chứng thực tính an toàn. Những nguồn này khi đưa phần mềm lên trang họ đã tiến hành quét để phát hiện các phần mềm nguy hiểm từ trước.

Sử dụng tường lửa nhiều hướng: Windows XP và Vista đều được trang bị tường lửa khoá các cuộc tấn công từ bên ngoài. Trong các bản Windows XP SP2 hoặc sau này, tính năng tường lửa được kích hoạt mặc định. Tuy nhiên, để tăng mức độ an toàn bạn nên khoá cả những kết nối không mong muốn gửi đi từ máy tính của chính mình (Windows XP không có khả năng này, bạn phải cài đặt phần mềm tường lửa riêng), đề phòng trường hợp malware phát tán spam hoặc cố kết nối với máy chủ từ xa.

Trong khi đó, Windows Vista có thể ngăn được cả kết nối từ bên trong ra, nhưng việc cấu hình nó không dễ dàng đối với đa số người dùng Windows. Thay vào đó, bạn có thể sử dụng một trong số nhiều chương trình tường lửa đa hướng miễn phí như ZoneAlarm Free (Zone Labs - http://www.zonealarm.com) hoặc Outpost Firewall Free (Agnitum - http://www.agnitum.com). Phần lớn các gói phần mềm bảo mật thương mại đều tích hợp chương trình tường lửa.

Sử dụng chương trình diệt phần mềm gián điệp: Spyware, adware và một số cookies trình duyệt có thể làm chậm hệ thống của hạn, gây nhiều phiền nhiễu và liên tục theo dõi các hoạt động trực tuyến của bạn. Các ứng dụng antispyware có cách thức làm việc tương tự như những phần mềm diệt virus, giúp phát hiện và loại bỏ những chương trình không mong muốn trên PC.

PCWORLD đánh giá Spy Sweeper 5 (http://www.webroot.com – 30USD/năm) là ứng cử viên sáng giá cho việc ngăn chặn các phần mềm gián điệp.

Nâng cấp Windows XP: Bản SP2 sẽ làm Windows XP an toàn hơn rất nhiều, nhưng hệ điều hành cũng tồn tại nhiều lỗ hổng bảo mật đang bị tin tặc khai thác. Trong khi đó, chức năng kiểm soát truy cập người dùng mới của Windows Vista sẽ hỏi ý kiến của bạn trước khi kích hoạt bất cứ chương trình nào, giúp giảm thiểu nguy cơ tấn công tự động của malware (từ web) vào máy tính của bạn, mặc dù người ta đã phát hiện ra một số lỗ hổng trong hệ điều hành này. Còn Mac OS và

Linux thì lại có cơ chế bảo vệ việc kích hoạt chương trình rất chặt chẽ. Chính vì thế hai hệ điều hành này ít khi là mục tiêu tấn công của tin tặc.

Văn Hân