Để duyệt Web thực sự an toàn

Trong quá trình duyệt Web, dù vô tình hay hữu ý chắc hẳn bạn đã truy cập tới những Website chứa nhiều nguy cơ mất an toàn. Thậm chí, nếu chỉ thường xuyên ghé thăm các trang Web chính thống, bạn vẫn có khả năng bị tấn công bởi chính các Website được cho là an toàn đang ngày càng trở thành mục tiêu của giới tin tặc. Để duyệt Web thực sự an toàn, bạn cần hiểu rõ các nguy cơ có thể xảy đến mỗi khi vào mạng, đồng thời áp dụng nhiều cấp độ bảo mật nhằm bảo vệ hệ thống và cô lập các mối đe doạ trong trường hợp bị tấn công.

NẮM RÕ CÁC NGUY CƠ

Các phương thức tấn công trình duyệt Web có thể được phân thành hai nhóm chính. Nhóm thứ nhất tấn công trực tiếp vào trình duyệt. Nhóm này bao gồm:

Tấn công XSS (Cross-site scripting): kẻ tấn công chèn các mã độc hại một cách trái phép vào Website chính thống, các mã lệnh này sau đó sẽ được trình duyệt của bạn tự động thực thi mỗi khi truy cập Website bị nhiễm độc.

Tấn công CSRF (Cross-site request forgery): kẻ tấn công chèn mã lệnh vào một trang Web cho phép chúng gửi đi các yêu cầu dưới vai trò của bạn, thông qua trình duyệt của bạn, tới một địa chỉ khác (chẳng hạn trang Web của ngân hàng).

Tấn công Click-jacking: kẻ tấn công hiển thị đè một nút nhấn ẩn lên trên một Website, và bạn có thể vô tình ấn vào đó.

Tấn công trình duyệt sử dụng các trang Web hay liên kết lừa đảo để tái định hướng bạn tới những địa chỉ không trông đợi, từ đó chiếm dụng phiên trình duyệt (session hijacking), tải phần mềm vào máy người dùng, hay thực hiện các giao dịch xấu (chẳng hạn chuyển tiếp thư điện tử của bạn tới hòm thư của

kẻ tấn công).

Nhóm các phương thức tấn công Web thứ hai nhắm mục tiêu tới toàn bộ hệ thống. Các cuộc tấn công hệ thống kiểu này thường khai thác các lỗ hổng bảo mật của trình duyệt hoặc các trình gắn thêm (plug-in) như QuickTime hay Flash để kiểm soát máy tính. Phương thức tấn công này tận dụng các lỗi tràn bộ đệm hay các điểm yếu để cài đặt virút, sâu máy tính và thực hiện các cuộc tấn công từ xa.

Để bảo vệ hệ thống khỏi cả hai dạng thức tấn công này đồng thời cô lập các mối đe doạ trong trường hợp bị tấn công, bạn cần áp dụng nhiều cấp độ bảo vệ khác nhau. Có thể khởi đầu bằng việc lưu trữ các mật khẩu bằng trình quản lý mật khẩu "1Password" (http://agilewebsolutions.com/products/1Password). Ở mức độ cao hơn, bạn cần sử dụng đa trình duyệt hay thậm chí triển khai đa hệ điều hành để đảm bảo an toàn ở mức tối đa. Dù hàng ngày ghé thăm những Website dạng nào, bạn cũng nên cân nhắc các chỉ dẫn dưới đây bởi chắc chắn chúng sẽ hữu ích với bạn.

ĐA TRÌNH DUYỆT

Phương án phòng vệ đầu tiên là sử dụng các trình duyệt Web khác nhau cho các hoạt động khác nhau. Như vậy, ngay cả khi tin tặc kiểm soát

được một diễn đàn trên mạng mà bạn đang đăng nhập, chúng cũng không thể lợi dụng điều đó để tấn công tài khoản ngân hàng trực tuyến của bạn nếu bạn sử dụng một trình duyệt riêng cho các giao dịch với ngân hàng. Hoặc chẳng hạn nếu bạn sử dụng một trình duyệt riêng để truy cập vào mạng xã hội Facebook, vụ lây nhiễm sâu máy tính theo phương thức XSS trên Facebook thời gian gần đây cũng không thể "vươn" sang trình duyệt khác để truy xuất vào các tài khoản thương mại điện tử hay Web mail của bạn.

Bạn nên sử dụng trình duyệt chính là Firefox 3.5 (http://www.mozilla.com/firefox/) có cài đặt các plug-in NoScript (http://noscript.net/) và Adblock Plus (http://adblockplus.org/).

Với plug-in NoScript cho Firefox, bạn có thể kiểm soát và tuỳ chỉnh việc thực thi các đoạn mã lệnh (script) trên trang Web. Theo mặc định, NoScript sẽ vô hiệu hoá Java, JavaScript, Flash và những nội dung động khác thường hay bị các cuộc tấn công lợi dụng. NoScript cho phép tuỳ chỉnh việc kiểm soát nên bạn có thể phê chuẩn cho các script trên một trang Web cụ thể được phép thi hành tạm thời hay vĩnh viễn. Bởi việc tấn công một trình duyệt mà

không thực thi các script hay plug-in gần như là bất khả thi, việc cài đặt và sử dụng NoScript sẽ rất hiệu quả trừ khi bạn vô tình phê chuẩn cho một trang Web có chứa mã độc.

Adblock Plus sử dụng danh sách đen bao gồm các Website chứa quảng cáo hoặc phần mềm độc hại, để từ đó tự động chặn nội dung từ các Website này. Có thể sử dụng Adblock Plus như một giải pháp dự phòng cho NoScript trong trường hợp bạn nhầm lẫn và cho phép các script nguy hiểm thi hành. Những kẻ xấu đang gia tăng sử dụng các quảng cáo dạng banner để phân phối mã độc, và Adblock Plus cung cấp khả năng bảo vệ tăng cường.

Ngoài hai plug-in này, hãy thiết lập để Firefox không lưu mật khẩu của bạn (tại Preferences / Security) và sử dụng trình quản lý mật khẩu 1Password (http://agilewebsolutions.com/products/1Password) thay thế.

Bạn nên sử dụng Firefox để duyệt các trang Web thông thường hay các Website thương mại điện tử chẳng hạn như Amazon. Đối với các Website đòi hỏi bạn nhập nhiều thông tin cá nhân quan trọng (chẳng hạn về tài khoản ngân hàng) hay các Website ẩn chứa nhiều nguy cơ, hãy áp dụng các biện pháp nghiêm ngặt hơn được giới thiệu dưới đây.

Do Safari hoạt động ít bị treo hơn Firefox, bạn cũng có thể sử dụng trình duyệt này cho các Website có nguy cơ cao hoặc chứa nhiều thông tin quan trọng. Để an toàn hơn, tại Preferences -> General, bạn vô hiệu hoá tính năng "Open Safe Files After Downloading", và tại Preferences -> Autofill, vô hiệu hoá "User Names And Passwords".

Theo mặc định, cả Firefox và Safari sẽ tìm cách nhận diện các Website lừa đảo đã biết, bằng cách sử dụng các danh sách đen công cộng (trong Firefox vào Preferences -> Security -> Block Reported Attack Sites; trong Safari vào Preferences -> Security -> Warn When Visiting A Fraudulent Website). Hãy đừng thay đổi các thiết lập này và giữ cho chúng ở trạng thái kích hoạt.

Ngoài ra nếu bạn có sử dụng các phần mềm đọc tin RSS, hãy vô hiệu hoá tất cả các plug-in để ngăn mã độc hại, chẳng hạn một tệp tin video gây tràn bộ đệm, được gửi qua RSS feed.

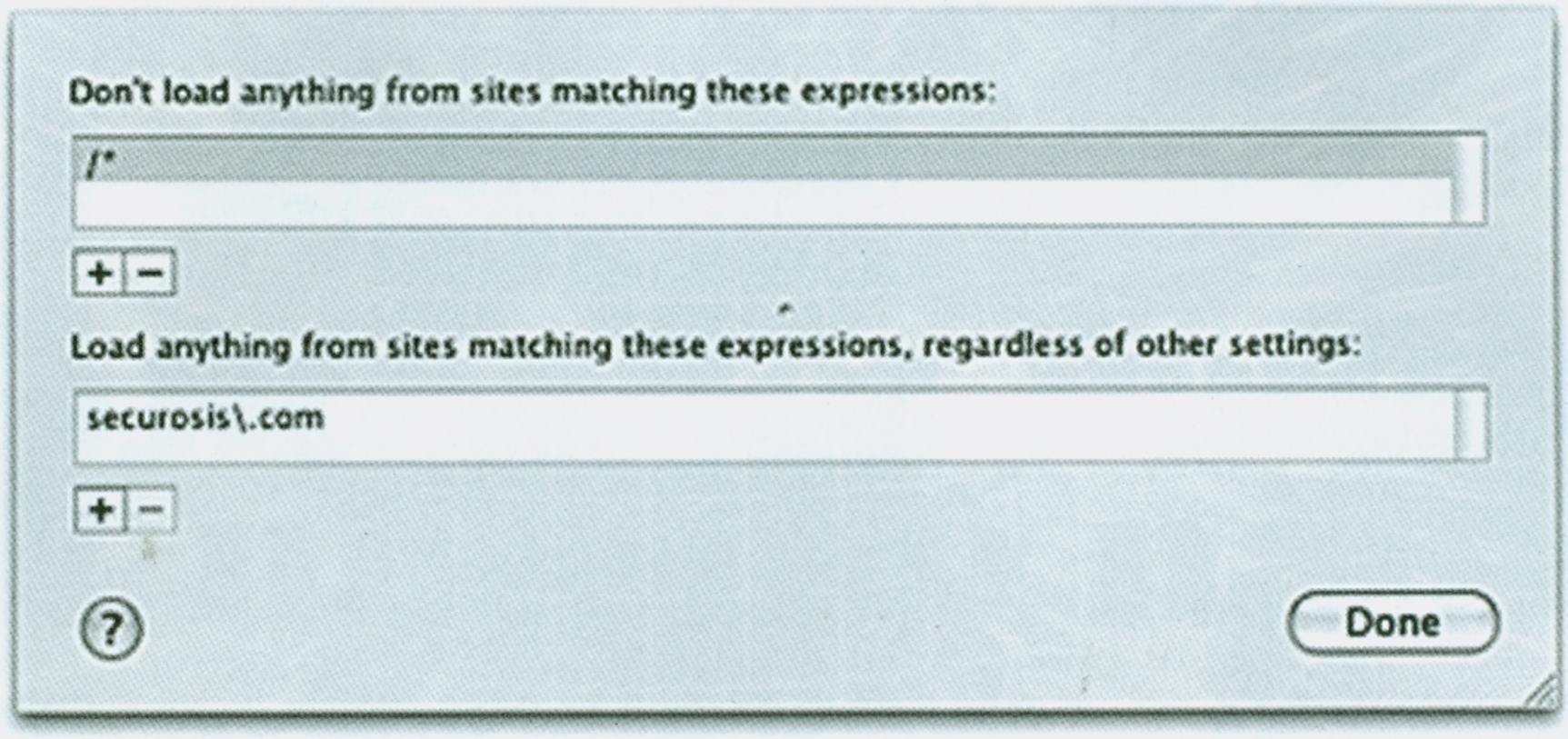
CÁC TRÌNH DUYỆT CHUYÊN DỤNG

Mặc dù Firefox và Safari là khá tốt cho việc duyệt Web nói chung, tuy nhiên khi cần mức độ bảo vệ cao hơn, bạn có thể sử dụng các trình duyệt chuyên dụng hoặc trình duyệt dành riêng cho Website (Site specific browser – SSB).

Cụm từ "trình duyệt chuyên dụng" ở đây để chỉ các trình duyệt thông thường nhưng chỉ sử dụng khi truy cập một Website nhất định. Chẳng hạn một người sử dụng máy Mac có thể chỉ dùng trình duyệt OmniWeb (http://www.omnigroup.com/applications/omniweb/) khi quản trị thông tin trên Website công ty.

OmniWeb cho phép tạo các quy tắc phức tạp quy định những Website nào mà trình duyệt có thể mở và không được phép mở. Trong trường hợp người sử dụng OmniWeb được nhắc tới trên đây, họ sẽ chặn mọi Website nằm ngoài tên miền công ty. Để thực hiện điều này, bạn vào Preferences -> Ad Blocking, nhấn vào "Edit The Blocked URLs List". Tại hộp thoại này, danh sách phía trên chứa các Website bị chặn, hãy bổ sung quy tắc "/*" để chặn tất cả các Website. Danh sách phía dưới chứa các Website được tin cậy (danh sách này có mức ưu tiên cao hơn danh sách Website bị chặn), hãy bổ sung tên miền của công ty (chẳng hạn "congty.com.vn") để chỉ cho phép mở các địa chỉ từ tên miền này. Cả hai danh sách này đều cho phép sử dụng các biểu thức chính quy phức tạp, vì thế bạn có thể tạo ra những quy tắc lọc rất chi tiết.

Đối với các Website không hoàn toàn tin cậy, bạn nên sử dụng trình duyệt dành riêng cho Website – SSB. Chẳng hạn như trường hợp đã nhắc tới trên



đây, nếu thận trọng với Facebook, bạn hãy truy xuất nó thông qua SSB.

SSB về căn bản là bản rút gọn của trình duyệt mà bạn có thể tự tạo chỉ bằng vài cú nhấp chuột. SSB có thể được tạo bằng trình bổ sung (add-on) Prism trên Firefox (https://addons.mozilla.org/en-US/firefox/addon/6665). Sau khi đã cài đặt Prism, hãy mở Website mong muốn và chọn Tools -> Convert Web Site To Application.

Không giống như đối với trình duyệt chuyên dụng, bạn có thể sử dụng SSB cho nhiều Website khác nhau. Tuy nhiên, do mỗi SSB sử dụng một tiến trình hệ thống hoàn toàn riêng biệt, bạn có thể cấu hình để phần mềm tường lửa giới hạn phạm vi truy cập Web cho từng SSB. Ngoài ra, nếu tin tặc tấn công được SSB, chúng cũng không xâm phạm được tới các trình duyệt khác cũng như không đánh cắp được thông tin lịch sử duyệt Web của người dùng – ngoại trừ dữ liệu của chính SSB đó.

ĐA HỆ ĐIỀU HÀNH

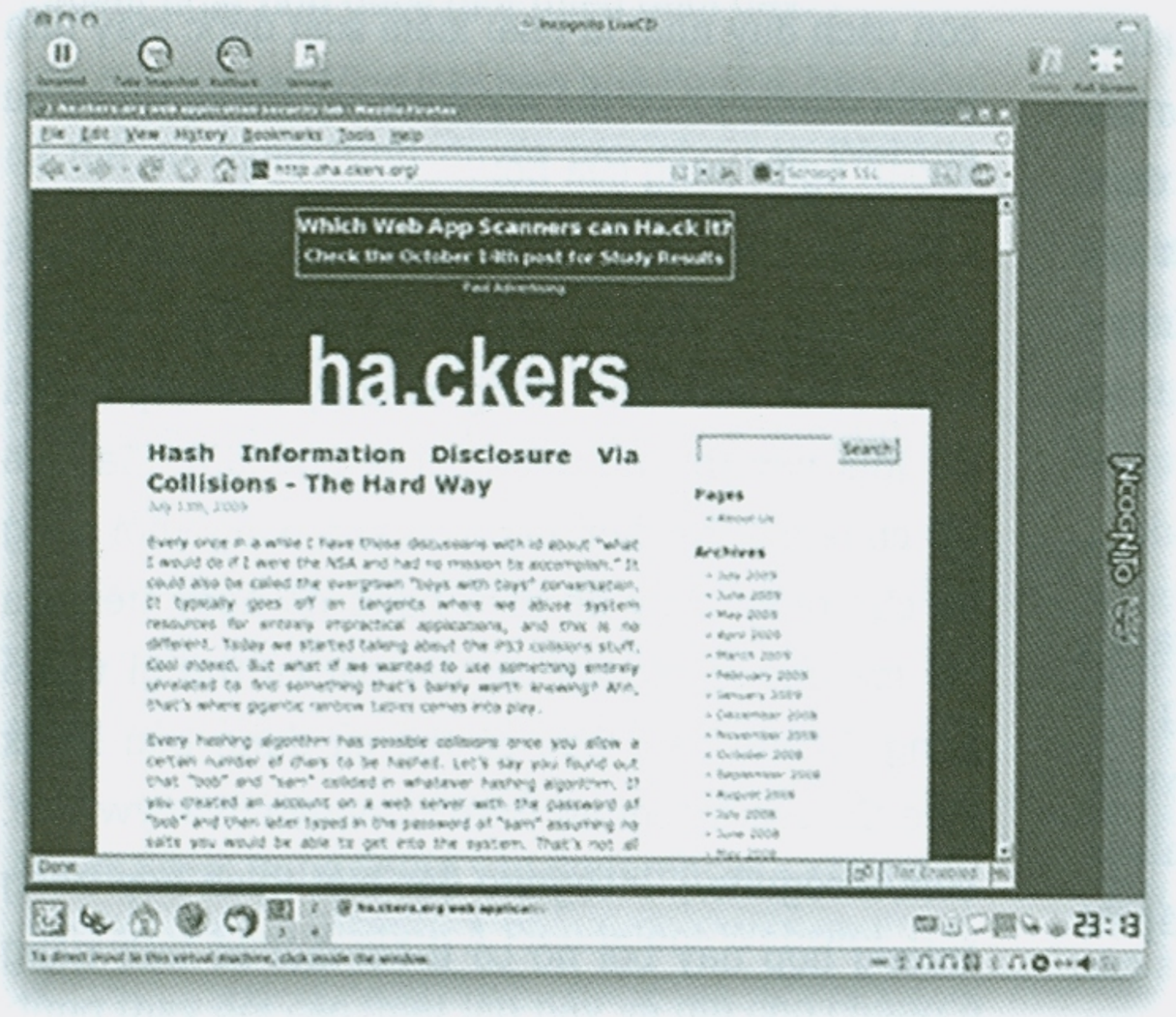
Đối với các Website có nguy cơ cao hay chứa các thông tin đặc biệt quan trọng, hãy sử dụng các phần mềm tạo máy ảo như VMware (http://www.vmware.com/) hoặc Parallels (http://www.parallels.com/) để cách ly các hoạt động duyệt Web ở cấp độ cao hơn.

Chẳng hạn, bạn có thể thực hiện tất cả các giao dịch với ngân hàng trên một máy ảo riêng, sử dụng Microsoft Internet Explorer 8 chạy trên bản thử nghiệm ứng viên (Release Candidate) mới nhất của hệ điều hành Windows 7. IE8 hoạt động trên Windows 7 rất an toàn, đặc biệt là khi bạn không sử dụng nó để vào bất kỳ trang Web nào ngoại trừ Website của ngân hàng, cũng như không sử dụng máy ảo cho thư điện tử hay bất kỳ hoạt động Internet nào khác. Tuân thủ điều này sẽ giúp loại trừ mọi khả năng các cuộc tấn công trình duyệt có thể xảy ra (trừ khi chính Website của ngân hàng đã bị tin tặc kiểm soát), và những kẻ tấn công chỉ còn cách duy nhất là phải kiểm soát được máy tính người dùng mới có thể lấy được các thông tin về tài khoản ngân hàng của họ.

Để đạt được mức độ an toàn cực cao khi duyệt Web, hãy sử dụng trình duyệt trên một hệ điều hành khác được khởi động và chạy trực tiếp từ đĩa CD (đĩa này thường được gọi là Live CD). Đĩa Live CD chứa một hệ điều hành có khả năng khởi động và cho phép chạy hệ điều hành đó ngay trên đĩa CD mà không đòi hỏi cài đặt bất cứ thứ gì vào ổ cứng. Chẳng hạn, bạn có thể sử dụng bản Linux Live CD của Incognito (http://anonymityanywhere.com/incognito/). Incognito đặc biệt thích hợp trong trường hợp này bởi nó có thêm một số tính năng

giúp nâng cao tính riêng tư. Tuy nhiên, bất kỳ bản Live CD nào có kèm theo trình duyệt Web đều phù hợp.

Do các đĩa CD đều chỉ cho phép đọc mà không thể ghi dữ liệu nên máy ảo sẽ chạy hoàn toàn trong bộ nhớ RAM mà không tác động gì đến hệ thống tệp tin trên ổ cứng, ngoại trừ phần dành cho bộ nhớ ảo. Tin tặc có thể chiếm giữ và dành toàn quyền kiểm soát máy ảo này nhưng không thể thay đổi bất cứ dữ liệu gì trong hệ thống. Do trạng thái của máy ảo không bao giờ được ghi lại vào đĩa cứng, nên tất cả những gì người sử dụng cần làm là tắt hệ điều hành và khởi động lại để đưa máy ảo trở lại trạng thái nguyên gốc.



Các kỹ thuật trên đây nhằm đem lại mức độ an toàn rất cao khi duyệt Web, dành cho những người thường xuyên phải truy cập những Website có nguy cơ cao hoặc chứa nhiều thông tin quan trọng. Tuy nhiên, những phương pháp này cũng thích hợp và dễ áp dụng đối với bất kỳ ai quan tâm đến vấn đề bảo mật. Ở mức độ thấp nhất, bạn cũng nên sử dụng một trình quản lý mật khẩu độc lập, một trình duyệt chuyên dụng hoặc SSB cho các giao dịch tài chính trực tuyến, và có thể kèm theo một máy ảo để đôi lúc truy cập những Website có nguy cơ cao.

Minh Đức