

DỊCH VỤ WEB NGÀY CÀNG ... NGUY HIỂM

Với việc ngày càng đông người dùng chuyển sang check mail, thanh toán và làm việc bằng ứng dụng Web, giới tội phạm mạng bắt đầu bám riết họ hòng khai thác thông tin tài khoản và những dữ liệu có giá khác.

Với việc ngày càng đông người dùng chuyển sang check mail, thanh toán và làm việc bằng ứng dụng Web, giới tội phạm mạng bắt đầu bám riết họ hòng khai thác thông tin tài khoản và những dữ liệu có giá khác.

Nguồn: Security Labs

Trong vài tuần trở lại đây, lần lượt dịch vụ email của Yahoo, mạng diễn đàn ảo Orkut của Google rồi hệ thống thanh toán trực tuyến PayPal của eBay lần lượt biến thành mục tiêu của các vụ tấn công. Cả ba hãng đều đã thừa nhận có lỗ hổng bảo mật trong dịch vụ của mình và nhanh chóng khắc phục. Các vụ tấn công diễn ra vào thời điểm Microsoft - hãng có hệ điều hành chạy trên 90% số máy tính của toàn thế giới - vừa mới vá hàng chục lỗ hổng trong các ứng dụng email, trình duyệt, phần mềm văn phòng v...v..., một số lượng lỗ hổng có thể coi là kỷ lục. Đây cũng đang là thời điểm thịnh vượng của những diễn đàn xã hội ảo như MySpace.com và các dịch vụ lịch, tin nhắn Web do Google, Yahoo cùng nhiều hãng khác cung cấp. "Cái khó ló cái khôn" lẽ dĩ nhiên, với việc người dùng đổ xô vào dùng những dịch vụ trên nền Web, giới hacker không thể làm ngơ. Trong mắt chúng, đây đúng là một mảnh đất màu mỡ chưa được khai phá. "Chúng bắt đầu nhận ra rằng có hàng tấn scripts sơ hở, yếu ớt và rất dễ hack", Eric Sites, phó chủ tịch nghiên cứu và phát triển của Sunbelt Software cho biết. Một trong những phát hiện gần đây nhất là loại sâu tấn công vào Orkut, diễn đàn xã hội ảo trực thuộc Google. Con sâu này lừa các thành viên click vào một đường link ảnh, nhưng lại ngấm ngầm tải về máy một phần mềm độc hại. Những dữ liệu như tên và mật khẩu, cùng với các file Windows thường lưu thông tin về tài khoản ngân hàng của người dùng sẽ bị malware này theo dõi và tự động gửi về cho chủ nhân sâu. "Kẻ xấu đang tiến thêm một bậc và ngày càng trở nên hiểm độc hơn. Thật đáng buồn vì đây quả là một ý tưởng xuất chúng. Chắc chắn trong thời gian tới, chúng ta sẽ còn chứng kiến nhiều trường hợp như thế này nữa", Chris Boyd, chuyên gia bảo mật phát hiện ra loại sâu trên nhận định. Mục tiêu tất yếu Trước đó, vào tháng 10 năm ngoái, MySpace.com, diễn đàn có tới 88 triệu thành viên đăng ký, đã bị một malware tấn công: Mỗi thành viên đột nhiên bổ sung thêm hàng triệu người khác vào danh sách bạn bè của mình. Vụ việc khiến cho MySpace trở nên quá tải và trực trặc mất một thời gian,

nhưng nguy hiểm hơn, nó giống lên hồi chuông cảnh báo về nguy cơ các ứng dụng/dịch vụ Web sẽ bị tấn công. Giới phân tích cho rằng việc hacker loay hoay tìm hướng đi mới là tất yếu, do người dùng máy tính ngày càng cảnh giác hơn. Họ chịu khó cài đặt và chạy các phần mềm bảo mật cũng như miến vá cập nhật hơn hẳn ngày trước. "Có thể nói, chúng ta đã buộc chúng "Cái khó ló cái khôn". Hacker đang cố lườn lách xuống dưới tầm quét của radar bằng cách đột nhập vào những khu vực mới, nơi cảnh vệ lơ lửng", giám đốc trung tâm Phản ứng bảo mật của Symantec cho biết. Phản ứng nhanh Một động cơ nữa thúc đẩy hacker nhòm ngó các dịch vụ Web là sức mạnh và tính cơ động cao của những ngôn ngữ lập trình Web, cho phép trình duyệt vận hành hết như ứng dụng Word, Excel v.v... Gần đây, một loại sâu Yahoo đã tấn công vào đoạn script bị lỗi trong Ajax, báo động sự ra đời của thế hệ malware kiểu mới. Với loại sâu này, người dùng không cần click vào file đính kèm cũng vẫn bị dính chương, chỉ cần họ mở file ra đọc. Sau đó, sâu sẽ tự gửi mail đến tất cả cái tên có trong sổ địa chỉ của nạn nhân và gửi chúng về một máy chủ từ xa, có lẽ là để phục vụ việc phát tán thư rác. Tuy nhiên, khác với các ứng dụng chạy trên desktop, những hãng như Yahoo, Google và PayPal có thể nhanh chóng bịt lại các lỗ hổng này. PayPal đã tiến hành khắc phục sự cố gần như ngay lập tức bằng cách chỉnh sửa lại vài dòng mã trên máy chủ, chặn đứng khả năng lỗ hổng nói trên bị khai thác. Trong khi đó, những hãng như Microsoft khi muốn vá lỗi trong máy tính cá nhân phải upload miến vá lên mạng. Người dùng sẽ tải các miến vá này về và cài đặt vào máy - một chu trình tốn nhiều thời gian hơn. Thiên Ý