HACKER NGÀY CÀNG MA MÃNH TRONG VIỆC ẨN MÌNH

Bọn tộ

Bọn tội phạm mạng liên tục nâng "trình" trong việc che giấu và ngụy trang cho các đoạn mã tấn công hiểm độc của chúng, hãng bảo mật Arbor Networks cảnh báo.

Ngày càng xuất hiện nhiều những đoạn mã độc (thường viết bằng ngôn ngữ JavaScript) dùng để tấn công PC được giấu bên trong hình họa Flash, khiến cho việc kiểm tra nguồn gốc của trang web cũng khó lòng mà phát hiện được chúng.

"Những công cụ gây rối này tuy đơn giản nhưng lại rất hiệu quả", chuyên gia Jose Nazario tuyên bố. "Các phương pháp bảo mật vốn dựa trên dấu hiệu đặc trưng để nhận dạng mã độc cũng bị che mắt".

Còn theo website StopBadware.org, hình thức tấn công trực tuyến đã trở nên quá phổ biến. Hàng chục ngàn Website rình rập để cài đặt mã độc vào những máy tính hớ hênh thông qua lỗ hổng bảo mật của trình duyệt Web.

Rất nhiều vụ tấn công đã sử dụng JavaScript. Ban đầu, bọn chúng chỉ sử dụng JavaScript "trơn", nhưng đến nay thì tình hình đã thay đổi.

Trò "mèo đuổi chuột"

Nguồn: Infotech

Chuyên gia Nazario đã phát hiện được một đoạn Flash có tên "Makemelaugh" mà sau khi người dùng kích hoạt sẽ ngấm ngầm download Trojan về máy. Nhiệm vụ của Trojan này là tìm mọi cách đánh cắp thông tin ngân hàng và tài chính của nạn nhân. Ngoài ra, còn có một hình hoạt Flash

của cô nàng lắm scandal Paris Hilton - với nhiệm vụ biến PC thành zombie và tham gia vào mạng botnet.

Một toolkit mới đang được truyền tay trong giới hacker dưới tên gọi NeoSploit sẽ nhận dạng trình duyệt Web và chực chỉ các lỗ hổng bên trong trình duyệt này để triển khai tấn công.

Tất nhiên, các chuyên gia bảo mật vẫn có cách chống trả. "Bọn chúng bị giới hạn bởi quy định rằng JavaScript bắt buộc phải được giải mã thì trình duyệt mới hiểu được. Nếu như bạn có thể phân tích nó bên ngoài trình duyệt, bạn sẽ đoán được mục đích cuối cùng của đoạn mã".

Các công cụ hiệu quả để điều tra mã script, theo khuyến cáo của Nozario là NJS, SpiderMonkey và Rhino. Còn các file Flash có thể phân tích được thông qua một chương trình có tên Flasm.

Mặc dù vậy, hacker vẫn có thể nhúng trực tiếp mã JavaSript bên trong trang Web và khởi động chúng mà không hề thông báo gì, bất kể là bạn đang lướt Net bằng trình duyệt nào.

Để bảo vệ mình, người dùng nên vô hiệu hóa tính năng JavaScript trong trình duyệt, nhưng như thế thì lại ảnh hưởng đến chức năng bình thường của nhiều Website. Một giải pháp khác là sử dụng các phần mềm bảo mật như SiteAdvisor của McAfee hay Google Toolbar, vốn đã được trang bị "sổ đen" về những website nguy hiểm.

Trọng Cầm