GOOGLE: 10% WEBSITE CHỨA MÃ ĐỘC

Cứ tro

Cứ trong 10 trang web được Google "nhòm đến" lại có một trang web chứa mã độc có thể tấn công PC của bất kỳ người dùng nào. Đây là kết luận mới nhất từ một cuộc khảo sát và phân tích kỹ lưỡng 4,5 triệu website của hãng.

Trong số đó khoảng 450.000 trang web có thể thực hiện tấn công "drive-by download" lên PC người dùng. Tức là dạng trang web có khả năng bí mật cài đặt mã độc lên PC của người dùng mà họ không hề biết một chút nào.

Ngoài ra còn có 700.000 trang web khác được cho rằng chứa chấp mã độc có khả năng bắt cóc PC biến nó thành công cụ phục vụ các mục tiêu đen tối khác của tin tặc như gửi thư rác chẳng hạn.

Để giải quyết được vấn đề này các chuyên gia nghiên cứu đề xuất nhà cung cấp dịch vụ tìm kiếm hàng đầu trên Internet nên bắt đầu tiến hành phân tích kỹ lưỡng để lọc ra những trang web được cho là độc hại.

Website ma

"Drive-by download" hiện đã trở thành hình thức tấn công PC phổ biến hiện nay. Mục tiêu của hình thức tấn công này tuồn mã độc vào trong PC người dùng để ăn cắp thông tin cá nhân khi họ bị lừa truy cập vào một trang web độc hại.

"Để lừa người dùng truy cập và cài đặt mã độc kẻ tấn công thường giả mạo cung cấp thông tin về một sự kiện nổi bật thu hút được nhiều sự chú ý của người dùng. Kỹ thuật này được gọi là social engineering." Đây là khẳng định của chuyên gia nghiên cứu Google Niels Provos cùng các đồng nghiệp đưa ra trong bản báo cáo "Ma trong trình duyệt" (The ghost in the browser).

Người dùng thường nhận được một đường liên kết đến một trang web hứa hẹn sẽ cung cấp cho họ những dạng nội dung như thông tin, phần mềm có bản quyền...

Phần lớn các lỗ hổng bảo mật bị lợi dụng để tấn công người dùng web là lỗi bảo mật trong trình duyệt Internet Explorer. Đây là một điều hoàn toàn dễ thấy bởi đây chính là loại trình duyệt được sử dụng nhiều nhất.

Một số mã độc sau khi lây nhiễm vào PC còn gây rất nhiều khó chịu cho người dùng như cài đặt thêm những thanh công cụ trình duyệt linh tinh, thay đổi trang chủ trình duyệt, thay đổi bookmarks ...

Nhưng loại mã độc được sử dụng phổ biến nhất trong các vụ tấn công "drive-by download" là keylogger có khả năng ghi nhận các thao tác thực hiện trên bàn phím để ăn cắp thông tin dữ liệu cá nhân của người dùng.

Một loại mã độc khác cũng thường được dùng là mã độc có khả năng bắt cóc và biến PC người dùng thành một "BOT" - một dạng PC có thể bị điều khiển từ xa.

"Drive-by download" là minh chứng rõ ràng nhất cho sự chuyển đổi hình thức tấn công của tin tặc. Trước đây chúng chủ yếu sử dụng hình thức phát tán mã độc truyền thống bằng cách đính kèm theo email.

Không phải website nào cũng an toàn

Song song bên cạnh đó Google cũng phân tích phương pháp chèn mã độc vào các trang web được dùng phổ biến nhất hiện nay.

Kết quả cho thấy phần lớn mã độc thường không được thiết kế hoặc kiểm soát bởi chính người chủ website mà chúng thường được chèn vào thông qua các quảng cáo hoặc widget (một dạng ứng dụng web nhỏ gọn).

Sự phát triển của nền tảng Web 2.0 và nội dung người dùng tự tạo đã mang đến cho tin tặc một kênh "phân phối" mã độc khác. Ví dụ tin tặc có thể đưa lên blog hoặc diễn đàn những đường liên kết hoặc một hình ảnh độc hại chứa sẵn mã độc sẵn sàng tấn công bất kỳ ai vô tình nhấp chuột vào đó.

Cuộc khảo sát của Google cũng phát hiện được rằng giờ đây những nhóm tội phạm còn có khả năng bắt cóc cả một máy chủ web và cài đặt mã độc lên mọi trang web lưu trữ trên máy chủ đó.

Máy tính được dùng làm thử nghiệm của các chuyên gia nghiên cứu Google đã bị nhiễm cùng một lúc 50 loại mã độc khác nhau khi truy cập vào một trang web được lưu trữ trên một máy chủ bị bắt cóc.

Google - hiện đang là một thành viên của liên minh StopBadware - lên tiếng cảnh báo người dùng không nên truy cập vào các trang web đã được cảnh báo là độc hại. Nếu đường liên kết đến trang web đó xuất hiện trên trang kết quả tìm kiếm của Google nó sẽ đi kèm thêm dòng cảnh báo "This site may harm your computer" (Trang web này có thể gây hại cho PC của bạn).

Hoàng Dũng