TIN TẶC SÁNG TẠO RA "MÃ ĐỘC DÙNG MỘT LẦN"

Các ch

Các chuyên gia nghiên cứu và hãng bảo mật đang phải điên đầu trước sự xuất hiện của một thủ đoạn tấn công người dùng mới có thể dễ dàng lọt qua con mắt giám sát của họ.

Theo đó, tin tặc sẽ bắt cóc một website và cấy vào đó những mã độc. Nếu người dùng vô tình truy cập vào website này PC của họ sẽ bị lây nhiễm mã độc nếu chưa được cài đặt đầy đủ các bản vá lỗi. Nhiệm vụ chính của những mã độc đó là bắt cóc hệ thống phục vụ cho mục tiêu khác của tin tặc hoặc ăn cắp thông tin cá nhân bí mật của người dùng.

Hãng bảo mật Finjan cho biết điểm đặc biệt trong phương thức tấn công này là tin tặc sử dụng mã JavaScript để bảo đảm mỗi người dùng khi truy cập vào website đó chỉ bị nhiễm mã độc một lần.

"Phương thức tấn công này là minh chứng rõ nhất cho một bước nhảy vọt trong độ phức tạp của các vụ tấn công. Phương thức mới đã hạn chế tới mức tối đa sự lộ diện của mã độc trước những nghiên cứu bảo mật hay phân tích chi tiết. Mỗi người chỉ có thể nhìn thấy mã độc một lần duy nhất".

Khi người dung truy cập vào website tin tặc sẽ ghi lại địa chỉ IP của họ vào cơ sở dữ liệu. Nếu người dùng lại truy cập vào website một lần nữa mã lập trình sẽ xác nhận IP và không tuồn mã độc vào PC của họ nữa. Ngoài ra tin tặc còn có thể chặn không cho mã độc lây nhiễm vào PC của người dùng ở một quốc gia nhất định nào đó.

Phương pháp này đã giúp tin tặc che giấu được mã độc của chúng trước con mắt của các chuyên gia nghiên cứu bảo mật. Giờ đây chúng có thể muốn mã độc của chúng tồn tại đến chừng nào mà chúng muốn. Nhưng các hãng bảo mật cũng đã kịp phát hiện được hiểm hoạ từ hình thức tấn công này.

Hiện vẫn chưa thống kê được có bao nhiêu website sử dụng hình thức tấn công như thế này. Tuy nhiên Finjan cảnh báo phương thức này đang rất được ưa chuộng trong giới tin tặc.

Hoàng Dũng