VIRUS CÓ KHẢ NĂNG PHÁ HỆ THỐNG NHÀ MÁY ĐIỆN, LỌC DẦU

Được hãng bảo mật Symantec đặt tên là Duqu, virus này có khả năng phá vỡ hệ thống kiểm soát của các nhà máy điện, nhà máy lọc dầu và mạng lưới cơ sở hạ tầng quan trọng khác. Duqu được phát hiện trong một vài hệ thống máy tính

Phần mềm này được viết bởi cha đẻ của Stuxnet, hoặc ít nhất cũng là người đã tiếp cận trực tiếp với nó.

Các nhà nghiên cứu tại Symantec cho biết, cũng như giống như người anh em Stuxnet, Duqu được thiết kế nhằm xâm nhập vào hệ thống kiếm soát công nghiệp bằng cách thao túng SCADA (hệ thống điều khiển và giám sát thu thập dữ liệu), chi phối quá trình vận hành của các thiết bị. Song cách tiếp cận của Duqu với hệ thống lại khác Stuxnet.

Duqu có khả năng phá vỡ hệ thống kiểm soát của các nhà máy điện

Thay vì trực tiếp tấn công SCADA, Duqu thu thập dữ liệu từ các nhà sản xuất hệ thống điều khiển công nghiệp, để xâm nhập vào bên thứ ba một cách dễ dàng hơn. Người sử dụng Duqu có thể ghi lại thao tác trên bàn phím và những thông tin hệ thống, rồi chuyển các thông tin đó cùng các dữ liệu thu thập được vào một máy chủ kiểm soát và điều khiển.

Duqu tự ngụy trang bằng một mã hợp pháp, có chứng nhận số tại một tập đoàn Đài Loan. Theo F-Secure (hãng bảo mật của Phần Lan), tập đoàn này là C-Media Electronics. Chứng nhận có hạn tới 2/8/2012, nhưng đã bị hủy bỏ vào ngày 14/10 vừa qua.

Duqu được cài đặt để chạy 36 ngày, sau đó, nó tự động tách mình khỏi hệ thống đã bị nhiễm virus. Theo Liam O Murchu, chuyên gia hàng đầu về Stuxnet, phầm mềm này cố gắng ngụy trang bằng cách đính kèm một tập tin đuôi jpeg cỡ 100 x 100 pixel. Đại diện Symantec cho biết, phần mềm này đã được sử dụng từ tháng 12/2010. Tuy nhiên, vẫn chưa xác định được cách chúng xâm nhập được vào hệ thống.

Duqu không có khả năng tự sao chép, nhưng theo các nhà nghiên cứu, “Duqu là tiền thân của những vụ xâm nhập kiểu Stuxnet trong tương lai”.

Loại virus mới của họ nhà Stuxnet ra đời ngay sau khi Cơ quan An ninh nội địa Mỹ (DHS) cảnh báo rằng nhóm tin tặc Anonymous sẽ nhanh chóng bắt đầu phá hoại hoặc làm tê liệt các cơ sở kiểm soát trong công nghiệp. Song họ cũng cho rằng “có ít khả năng Anonymous chịu trách nhiệm về các vụ tấn công này".