TÌM HIỂU SIÊU VIRUS ĐANG ĐE DỌA CÔNG NGHIỆP TOÀN CẦU

Nhiều chuyên gia an ninh và nhân viên chính phủ đồng loạt cảnh báo cao độ rằng những hacker cao thủ hoàn toàn có thể sử dụng những thông tin công khai về đoạn mã được biết đến dưới cái tên siêu virus Stuxnet để phát triển ra các biến thể

Stuxnet là một dạng sâu (worm) trên hệ điều hành Windows. Nó được phát hiện lần đầu tiên vào tháng 6/2010 bởi một công ty bảo mật Belarus có tên là VirusBlokAda.
Stuxnet là mẫu sâu máy tính đầu tiên được phát hiện có khả năng thâm nhập và tái cấu trúc các hệ thống công nghiệp, cũng là sâu máy tính đầu tiên chứa rootkit điều khiển logic khả lập (PLC rootkit). Stuxnet được viết ra để tấn công trực tiếp vào các hệ thống giám sát điều khiển và thu thập dữ liệu(SCADA) sử dụng trong điều khiển các quy trình công nghiệp.
Stuxnet có thể tự động xâm nhập vào một hệ thống, đánh cắp công thức pha trộn sản phẩm, xáo trộn thành phần nguyên liệu; đánh lừa hệ điều hành và phần mềm diệt virus rằng mọi thứ vẫn đang hoạt động bình thường.

Stuxnet được viết ra để tấn công trực tiếp vào các hệ thống giám sát điều khiển và thu thập dữ liệu (SCADA) sử dụng trong điều khiển các quy trình công nghiệp.
Thiệt hại đầu tiên mà Stuxnet gây ra cho đến nay được báo cáo là vụ tấn công vào hệ thống điều khiển chương trình hạt nhân của Iran. Iran sử dụng hệ thống điều khiển của Siemens. Và, mặc dù Siemens phủ nhận mọi tác hại của sâu này, Iran đã thừa nhận việc họ chậm trễ trong kế hoạch triển khai hạt nhân tại Natanz là do sự phá hoại của Stuxnet vào ngày 29/11 vừa qua.

Trong bản báo cáo với Ủy ban Thượng viện về An ninh Lãnh thổ và Nội vụ Chính phủ Hoa Kỳ, ông Sean McGurk, quyền giám đốc của trung tâm an ninh mạng quốc gia trực thuộc Uỷ ban này khẳng định: Hệ thống điều khiển của một số ngành công nghiệp đặc biệt sử dụng các phần mềm "dính dáng" tới Windows và có thể bị đoạn mã độc này tấn công. Nhiều mảng công nghiệp trọng yếu sẽ bị ảnh hưởng, từ công nghiệp xe hơi cho đến hoá chất hay hoá thực phẩm.

Dean Turner, Giám đốc Mạng lưới Thông minh Toàn cầu của tập đoàn Symantec xác nhận rằng con virus này hoàn toàn có khả năng tung đòn tấn công như trên đã nêu, và cho rằng "tác động của Stuxnet tới thế giới thực cao hơn rất nhiều so với bất cứ mối nguy nào chúng ta từng gặp trong quá khứ".

Công ty an ninh mạng của Nga Kaspersky Labs đã mô tả Stuxnet như “một dạng vũ khí thông minh linh động và đáng sợ”.
Mặc dù đoạn mã của Stuxnet cực kì tinh vi và phức tạp, nhưng điều đó không đồng nghĩa rằng các hacker sừng sỏ không thể sử dụng nó cho các mục đích tấn công khác nhau. Nhất là khi nó được rao bán trên các chợ đen của giới hacker.
Ngoại trừ Iran, một thống kê không đầy đủ cho thấy Stuxnet đang đe dọa tới an ninh thông tin toàn cầu.
Tại Việt Nam, bản tin An ninh mạng tháng 9/2010 của Bkav cho biết, Stuxnet đứng thứ tư trong danh sách 10 virus lây nhiều nhất trong tháng 9/2010. Bản tin không nêu rõ đối tượng tấn công của Stuxnet.

Sau đây là một số nước đã chịu ảnh hưởng bởi Stuxnet:

Nước
Số máy tính nhiễm

Trung Quốc
6,000,000 (chưa kiểmchứng) (01 tháng 11)

Iran
62,867

Indonesia
13,336

ẤnĐộ
6,552

HoaKỳ
2,913

Úc
2,436

Anh
1,038

Malaysia
1,013

Pakistan
993

Phần Lan
7

Đức
5 (Tháng 9)