CUỘC TẤN CÔNG CỦA SÂU IM TỰ ĐỘNG LÀ ĐIỀU KHÓ TRÁNH

Việc xuất hiện đầy bất ngờ của một rootkit trong con sâu máy tính tấn công thông qua mạng tin nhắn tức thời (IM) đã làm bùng lên sự lo sợ về việc tin tặc đã đủ khả năng tổ chức các cuộc tấn công bằng sâu máy tính hoàn toàn tự động tr&eci

Việc xuất hiện đầy bất ngờ của một rootkit trong con sâu máy tính tấn công thông qua mạng tin nhắn tức thời (IM) đã làm bùng lên sự lo sợ về việc tin tặc đã đủ khả năng tổ chức các cuộc tấn công bằng sâu máy tính hoàn toàn tự động trên mạng IM. Trong vụ tấn công thông qua mạng IM gần đây nhất - đối với mạng AIM của American o-nline, rootkit lockx.exe đã được "nhúng" kèm với con trojan W32/Sdbot có nhiệm vụ tải về và cài đặt rất nhiều phần mềm nguy hiểm giấu mặt. Đây là lần đầu tiên SDBot bị phát hiện là được sử dụng trong việc tấn công qua mạng IM. "Tình hình cho chúng ta thấy một điều là thời cuộc hiện nay đã đủ chín muồi cho các cuộc tấn công bằng sâu máy tính tự động trên mạng IM. Mà thông thường những cuộc tấn công kiểu này sẽ gây ra rất nhiều thiệt hại nghiêm trọng," Jose Nazario, kỹ sư phần mềm cao cấp của Arbor Networks Inc - một hãng chuyên về bảo mật – cho biết. Nazario - đồng thời còn là một nhà nghiên cứu sâu máy tính – cho biết sự xuất hiện của SDBot trong cuộc tấn công mạng IM vừa qua đã chỉ ra xu hướng phát triển hiện nay của các phần mềm nguy hiểm - Một khi đã lây nhiễm lên máy tính của người sử dụng thì sẽ tải về một loại các công cụ khác trong đó có cả rootkit và phần mềm gián điệp sau đó sử dụng một mạng IRC để kiểm soát các botnet và tiếp tục phát tán. Theo Nazario thì hiện nay những người lập trình sâu máy tính tấn công qua mạng IM đã trở thành các chuyên gia trong việc điều khiển máy tính cũng như danh sách bạn bè trên ứng dụng tin nhắn tức thời của người sử dụng để phát tan các loại virus hay phần mềm nguy hiểm. Chris Boyd, chuyên gia của FaceTime Communications đồng thời là người đã phát hiện ra rootkit và SDBot trong sâu máy tính tấn công mạng AIM vừa qua cũng có đồng quan điểm với Narario. Boyd tin tưởng rằng việc nhúng rootkit vào trong "bộ ứng dụng gián điệp virus" là một phương thức tấn công mới - một phương thức phát tán các con trojan cửa sau nhằm chiếm quyền điều khiển máy tính của người sử dụng. Ví như rootkit "lockx.exe" được lập trình để kết nối kến máy chủ IRC nhằm thực hiện các mệnh lệnh của kẻ tấn công muốn giấu mặt. Hồi đầu năm nay Microsoft cũng thực sự lo ngại về việc mạng MSN Messenger của hãng này cũng sẽ bị sử dụng cho các cuộc tấn công bằng sâu tự động. Hãng này ngay lập tức phải sửa chữa mọi lỗi bảo mật trong ứng dụng IM người sử dụng. Vào thời điểm đó, những đoạn mã khai thác lỗi trong ứng dụng MSN Messenger đã được phát tán rộng rãi trước khi Microsoft cho vá lỗ hổng bảo mật 24 giờ đồng hồ. Tyler Wells, giám đốc kĩ thuật cao cấp tại FaceTime Communications, cho rằng những lỗi tràn bộ nhớ đệm trong các ứng dụng IM chính là công thức dẫn đến thảm hoạ tấn công. "Chúng tôi đã được xem các tài liệu mô tả việc khai thác các lỗi bảo mật cho phép thực thi các đoạn mã nguy hiểm từ xa trong các ứng dụng IM. Nếu xếp chung lại thì đây cũng không khác mấy các cuộc tấn công bằng sâu tự động. Hơn thế tấn công kiểu này tin tặc không phải lừa một ai phai nhắp chuột vào một đường liên kết siêu văn bản nào cả." "Những kẻ tấn công trước tiên sẽ nhắm đến việc khai thác các lỗi vốn có trong các ứng dụng IM. Lấy ví dụ AIM ngày này đã có thêm chức năng cập nhật ảnh avatar trước mỗi ID trên danh sách bạn bè của người sử dụng hay phát một bài nhạc mà không cần phải nhắp chuột. Tất cả các ứng dụng tin nhắc tức thời ngày nay đều là một sự kết hợp các ứng dụng như VOIP, truyền tải tệp tin, chia sẻ ảnh hay nghe radio trên Internet. Những bổ sung kiểu này luôn là mối quan tâm về bảo mật. Mỗi khi ứng dụng IM được bổ sung thêm một tính năng của hãng thứ 3 thì có điều tốt là bạn có thêm chức năng mới còn điều hại là bạn phải "kế thừa" mọi vấn đề bảo mật của ứng dụng

đó." Nazario cho biết thêm là thông qua các nghiên cứu chi tiết đã được thực hiện thì các cuộc tấn công bằng sâu tự động trên mạng IM sẽ có mức độ phát tán rất nhanh. "Tình trạng tồi tệ nhất mà các nghiên cứu này phát hiện ra là mọi ứng dụng IM đang kết nối trực tuyến tại thời điểm vụ tấn công đều sẽ bị lây nhiễm và vấn đề chỉ là thời gian." "Các cuộc tấn công bằng sâu IM tự động là không thể tránh khỏi và có thể xảy ra bất cứ lúc nào. Tôi lấy làm ngạc nhiên là cho đến tận bây giờ chưa có vụ tấn công nào như vậy xảy ra. Đây là một phương thức phát tán virus phần mềm nguy hiểm rất nhiệu quả và nhanh chóng. Người sử dụng cần cảnh giác hơn nữa" Nazario nói.
HVD - (eWeek)