# MÃ ĐỘC CẤP ĐỘ NHÂN SẼ NGÀY MỘT PHỔ BIẾN

Theo c

Theo các chuyên gia nghiên cứu bảo mật của F-Secure, xu hướng sử dụng phần mềm độc cấp độ nhân sẽ ngày càng trở nên phổ biến hơn trong giới tội phạm mạng.

Kimmo Kasslin - một chuyên gia nghiên cứu bảo mật của F-Secure - nhận định đây sẽ là một hiểm hoạ khôn lường.

Khác với các dạng phần mềm độc hại truyền thống chỉ có chức năng vận hành như một phần mềm ứng dụng thông thường, phần mềm độc hại cấp độ nhân tồn tại và hoạt động sâu trong nhân lõi hệ điều hành - bộ phận chịu trách nhiệm liên kết giữa phần mềm và phần cứng.

"Dạng phần mềm độc hại này vận hành ở cấp độ ưu tiên và chia sẻ các nguồn tài nguyên tương tự như một hệ điều hành độc lập. Mục tiêu của chúng là hạ gục mọi giải pháp bảo vệ hệ thống," ông Kasslin cho biết.

Các chuyên gia nghiên cứu của F-Secure nhận định xu hướng này chắc chắc sẽ dẫn đến một cuộc "chạy đua vũ trang" mới giữa một bên là phần mềm bảo mật và một bên là phần mềm độc hại cấp độ nhân.

Mục tiêu của cuộc đua là những mã nguồn có thể vận hành ở cấp độ sâu nhất trong hệ điều. Càng gần gũi với các chức năng cơ bản nhất của hệ điều hành thì càng hiệu quả.

"Đây là điều mà hiện vẫn chưa có bất kỳ một hãng bảo mật nào làm được. Trong khi đó, trên mạng Internet đã xuất hiện hàng loạt mã nguồn có đầy đủ chức năng và khả năng như một mã độc cấp độ nhân".

Kể từ năm 2005 số lượng phần mềm độc hại cấp độ nhân không ngừng gia tăng. Bình quân mỗi tháng trong năm 2006 có 2,63 phần mềm độc hại cấp độ nhân mới xuất hiện.

Hầu hết các phần mềm độc hại cấp độ nhân hiện có đều vận hành nhờ vào các rootkit. Đây là công cụ cho phép giấu kín các phần mềm độc hại truyền thống để tránh "con mắt giám sát" của các phần mềm bảo mật.

"Trong khi đó những thông tin về việc xây dựng phần mềm độc hại cấp độ nhân, cách thức ứng

dụng rootkit, cách thức vượt qua tường lửa cá nhân, cách thức tạo ra backdoor ... xuất hiện đầy rẫy trên mạng Internet".

Phần mềm độc hại cấp độ nhân bắt đầu thu hút được sự chú ý của cộng đồng sau khi Microsoft công bố giải pháp bảo vệ PatchGuard sẽ được tích hợp trong hệ điều hành Vista. Đây là giải pháp giúp khoá cứng hoàn toàn nhân hệ điều hành.

Các chuyên gia bảo mật tin rằng chỉ không lâu nữa thôi giải pháp bảo vệ nói trên sẽ bị tin tặc bẻ gẫy và các hãng bảo mật sẽ lại vào cuộc để bảo vệ người dùng.