# KEYLOGGER... "KẺ THÙ" GIẤU MẶT!

Các chương trình ghi nhận hoạt động bàn phím (keylogger) dạng thương mại có thể nói là hiểm họa bảo mật thuộc dạng "kinh hoàng" nhất hiện nay. Khác xa với các chương trình dạng "mã độc" như virus, trojan, spyware..., đa số các chương t

Các chương trình ghi nhận hoạt động bàn phím (keylogger) dạng thương mại có thể nói là hiểm họa bảo mật thuộc dạng "kinh hoàng" nhất hiện nay. Khác xa với các chương trình dạng "mã độc" như virus, trojan, spyware..., đa số các chương trình keylogger thương mại đều được Windows và các chương trình bảo mật xem như một ứng dụng "hợp pháp" khi được cài đặt vào máy tính. Chính vì vậy mà bất kỳ một tay hacker "tay mơ" nào cũng có thể sưu tầm được một chương trình keylogger tinh vi nào đó để tìm hiểu những bí mật riêng tư hoặc làm hại người khác... Thủ phạm ăn cắp các tài khoản chat, email, game o-nline... hiện nay đa số đều xuất phát từ các chương trình keylogger thương mại tinh vi đã được ai đó bí mật cài đặt vào các máy tính dạng công cộng như các máy tính văn phòng, tiệm Internet..., thậm chí các máy tính tại gia đình. Việc phát hiện dấu vết hoạt động của các keylogger thương mại vô cùng khó khăn, ngay cả với những người chuyên dùng keylogger để "do thám" người khác, vì hầu như mỗi chương trình keylogger đều có những kỹ năng "ngụy trang" khác nhau và hết sức tinh vi. Một số keylogger thuộc dạng "quang minh chính đại" sẽ thể hiện chính bản thân nó ngay trong nơi lưu trữ danh mục các chương trình ứng dụng "Program Files", và bạn cũng có thể phát hiện sự hoạt động của nó trong thẻ "Applications" của "Windows Task Manager".

Đa số các keylogger "mã độc" chỉ có thể ghi nhận lại một số thao tác hạn hẹp như các ký tự được gõ vào ô "Username", "Password"... chẳng hạn. Trong khi đó, các keylogger thương mại có thể ghi nhận gần như 100% mọi thao tác diễn ra trên bàn phím đúng theo thứ tự mà người dùng đã gõ vào. Ngoài ra, khả năng được xem là độc đáo nhất của keylogger thương mại chính là tính năng "chụp hình" lại mọi diễn biến xảy ra trên màn hình và xuất ra dưới dạng ảnh số vô cùng trực quan. Chính khả năng này đã vô hiệu hóa luôn kiểu bảo mật bằng cách sử dụng "bàn phím ảo" mà nhiều người dùng "kỹ tính" thường sử dụng hiện nay.

Nhưng đa số các keylogger thuộc hạng thứ dữ hiện nay hầu như không để lại bất kỳ dấu vết gì có thể phát hiện sự hoạt động của nó. Sau khi cài đặt thành công, các keylogger dạng này sẽ cung cấp cho chủ nhân của nó password hoặc một tổ hợp phím nóng khá phức tạp, thường đến những bốn phím, để chỉ riêng chủ nhân của nó mới có thể kích hoạt chương trình. Phương pháp mà các "cao thủ" sử dụng keylogger thường làm là cài đặt ứng dụng keylogger vào một thư mục con "hóc bò tó" ẩn sâu bên trong các ứng dụng khác, xóa đi tên hiển thị trong nơi lưu trữ danh mục các chương trình ứng dụng "Program Files", thậm chí đổi luôn tên của file thực thi... Tuy nhiên vẫn có một số phương pháp cơ bản để phát hiện một keylogger nằm vùng nào đó. Về nguyên tắc, bạn chỉ có thể tìm ra được một keylogger đang ẩn mình trong máy tính khi biết được một số đặc điểm

riêng của nó như: tên của thư mục cài đặt, tên file thực thi, định dạng file chứa thông tin ăn cắp được do nó xuất ra, tên của file chứa "mã độc"... Đa số các keylogger thương mại hiện nay đều tự động tạo ra một kiểu file dạng văn bản (thường là TXT hoặc HTM) để ghi nhận mọi hoạt động từ bàn phím,cũng như tạo ra các file ảnh (thườnglà JPG hoặc BMP) thể hiện mọi nội dung mà nó chụp lại từ màn hình. Keylogger sẽ tự động lưu lại các file này vào một thư mục "kín" nào đó sau một khoảng thời gian nhất định. Chính vì vậy, bạn có thể dễ dàng xác định được máy tính của mình có bị keylogger "đột kích" hay không bằng cách "săn" các file TXT hoặc JPG lạ theo kiểu tìm "hú họa" theo thời gian để liệt kê hàng loạt file TXT và JPG được tạo ra đồng loạt trong một khoảng thời gian nào đó. Tuy nhiên, các chương trình keylogger cao cấp "đặc dị" không đặt tên file lưu theo dạng dễ bị phát hiện như TXT hoặc JPG. Nó sẽ có định dạng file với phần đuôi lạ hoắc mà bạn chưa biết đến bao giờ, thậm chí có những loại file mà chỉ có thể mở ra xem được bằng chính ứng dụng keylogger sinh ra nó. Với keylogger "cao thủ" này, dường như chỉ có cách duy nhất để phát hiện là bạn phải biết chính những đặc điểm riêng của nó. Tối thiểu cũng phải nằm lòng được định dạng file do thám đặc thù của nó hoặc tên file thực thi.