KEYLOGGER ĐỘC HẠI LAN TRÀN TRÊN INTERNET

Các chương trình keylogger độc hại hiện đã trở thành một vấn đề nổi cộm trên Internet và là một ví dụ điển hình về tình trạng ăn cắp trực tuyến. Có thể nói chính những tên trộm ăn cắp tài sản trí tuệ hay thông tin người sử dụng l&agra

Các chương trình keylogger độc hại hiện đã trở thành một vấn đề nổi cộm trên Internet và là một ví dụ điển hình về tình trạng ăn cắp trực tuyến. Có thể nói chính những tên trộm ăn cắp tài sản trí tuệ hay thông tin người sử dụng là những kẻ đã đổ thêm dầu vào ngọn lửa keylogger đang bùng lên mạnh mẽ. Theo một báo cáo gần đây nhất của iDefense thì số lượng các chương trình keylogger đã tăng lên mạnh mẽ trong năm nay. Đây cũng là một phần của làn sóng các phần mềm độc hại đa chức năng được tích hợp tính năng ghi nhận mọi hoạt động của bàn phím (keylogger). Hơn thế nữa những phần mềm như thế này ngày nay lại còn có thêm khả năng qua mặt các công cụ diệt virus-phần mềm nguy hiểm khiến cho việc phát hiện ra chúng trở nên rất khó khăn. Tính đến cuối năm nay sẽ có ít nhất là 6.000 chương trình keylogger độc hại được phát tán. Con số này đã tăng hơn 2.000% so với 5 năm trước đây. Trên thực tế keylogger đã có mặt từ nhiều năm trước đây và cũng được phân phối như một ứng dụng hoàn toàn hợp pháp với vai trò như một công cụ giám sát cho những đối tượng như bậc cha mẹ muốn giám sát sự truy cập Internet của con cái mình … Và đôi khi các công ty bảo mật lại phải rất nhiều trực trặc với các nhà phát triển phần mềm keylogger thương mại. Gần đây nhất là hãng sản xuất phần mềm chống spyware Sunbelt Software đã suýt bị hãng RetroCoder của Anh kiện vì đã liệt kê phần mềm SpyMon keylogger của hãng này vào trong danh sách phần mềm nguy hiểm của Sunbelt. Điều khoản người sử dụng cuối cùng của SpyMon ngăn cấm mọi công ty phát triển phần mềm chống virus và chống phần mềm gián điệp không được phép sử dụng hay phân tích phần mềm keylogger của RetroCoder. Trong khi đó các hãng bảo mật đã phát triển thành công kí hiệu (signatures) giúp cho việc ngăn chặn các phần mềm keylogger độc hại trước khi những phần mềm như thế này cài đặt lên máy tính của người sử dụng. Tuy nhiên vẫn có những chương trình mới với những kí hiệu đặc biệt lấy từ những trang web cho phép tải những đoạn mã nguy hiểm. Trong một số trường hợp, các đoạn mã nguy hiểm này còn được giao bán giúp cho người khác có thể tạo ra rất nhiều biến thể phần mềm nguy hiểm khác nhau. Keylogger đặc biệt phổ biến ở những nước mà tình trạng lừa đảo ngân hàng trực tuyến thực sự là một vấn đề lớn như ở Brazil. Keylogger hơn thế lại còn được tích hợp đi kèm với một số con trojan như Banker hay PWSteal - những con trojan được lập trình với mục đích giúp phát tán keylogger thông qua việc người sử dụng nhấp chuột vào một đường liên kết trên web nào đó. Nói chung, keylogger đã gần như trở thành một vấn nạn trên Internet ngày nay