HACKER DEFENDER NGỪNG HOẠT ĐỘNG

Tác giả của Hacker Defender - trang web chuyên kinh doanh thu lời từ các công cụ rootkit - đã quyết định ngừng mọi hoạt động kinh doanh. Hacker Defender - một Windows rootkit mã nguồn mở - đã trở nên rất nổi tiếng trong giới nghiên cứu bảo mật trên toàn thế giới và được

Tác giả của Hacker Defender - trang web chuyên kinh doanh thu lời từ các công cụ rootkit - đã quyết định ngừng mọi hoạt động kinh doanh. Hacker Defender - một Windows rootkit mã nguồn mở - đã trở nên rất nổi tiếng trong giới nghiên cứu bảo mật trên toàn thế giới và được biết đến như là rootkits được phát tán rộng rãi nhất trên Internet. Một cách khái quát nhất, rootkit chính là những công cụ giúp tin tặc che dấu mọi hoạt động trước con mắt của người sử dụng cũng như các nhà quản trị. Hacker Defender có khả năng sửa đổi một số hàm của Windows và hàm Native API cho phép tin tặc có thể giấu các tệp tin, luồng hay các loại thông tin khác trước con mắt của ứng dụng bảo mật. Hãng bảo mật F-Secure cho biết rootkit này còn mở một cổng sau và cài đặt một bộ chuyển cổng (port redirector) khiến cho việc phát hiện cổng sau bằng các phương pháp truyền thống như quét cổng từ xa trở nên rất khó khăn. Từ hơn một năm nay, trang web Hacker Defender đã kinh doanh dựa trên phiên bản công cụ rootkit này cũng như cung cấp các phiên bản công cụ mã nguồn mở miễn phí. Tuy nhiên, cuối tuần trước tác giả của trang web này đã quyết định chấm dứt mọi hoạt động của trang web. Tác giả của công cụ Hacker Defender cho biết việc phát triển rootkit này là nhằm khuyến khích lôi kéo ngành công nghiệp vào cuộc giúp tăng cường khả năng bảo vệ cho người dùng. "Chúng tôi đã chứng minh được một điều là các biện pháp phát hiện rootkit ngày nay là không tốt và mới được triển khai nửa vời." Còn hãng bảo mật F-Secure cho rằng việc trang web Hacker Defender ngừng hoạt động là một tin tốt cho người sử dụng. Nhưng việc trang web ngừng hoạt động không thể đồng nghĩa với việc rootkit Hacker Defender sẽ biến mất. Người sử dụng vẫn cần phải cẩn thận. "Backdoor.Win32.Hacdef là một rootkit mã nguồn mở vì thế chắc rằng chúng ta sẽ còn phát hiện thêm nhiều biến thể mới của công cụ này." Gần đây các chuyên gia cũng đã phát hiện ra một chương trình kinh doanh dựa trên các công cụ nguy hiểm tấn công người dùng máy tính kiểu như Hacker Defender. HVD - (Techworld)