ADWARE, SPYWARE NAY ĐÃ LÀ … ROOTKIT

Theo hãng bảo mật F-Secure thì số lượng các rootkit tấn công các hệ thống chạy hệ điều hành Windows được phát hiện trong năm nay đã tăng lên nhanh chóng. Đây là chính là kết quả của việc các hãng kinh doanh phần mềm quảng cáo v&agrave

Theo hãng bảo mật F-Secure thì số lượng các rootkit tấn công các hệ thống chạy hệ điều hành Windows được phát hiện trong năm nay đã tăng lên nhanh chóng. Đây là chính là kết quả của việc các hãng kinh doanh phần mềm quảng cáo và gián điệp đã sử dụng những kĩ thuật phức tạp hơn nhằm che dấu và ngăn cản việc gỡ bỏ cài đặt các ứng dụng của họ. Để chứng minh cho quan điểm của mình F-Secure đưa ra ví dụ cụ thể: ContextPlus – nhà phát triển phần mềm quảng cáo Apropos and PeopleOnPage adware – là hãng phải chịu trách nhiệm cho một số lượng khá lớn các vụ lấy nhiễm rootkit. Công nghệ BlackLight của F-Secure đã giúp cho hãng này phát hiện ra được những “công nghệ rootkit tiên tiến” trong phần mềm Apropos - một phần mềm gián điệp chuyên thu thập thói quen truy cập web và thông tin hệ thống trên máy tính của người sử dụng để gửi về cho ContextPlus. Không giống với các sâu máy tính hay bot thông thường sử dụng công nghệ rootkit để tránh bị phát hiện và tiêu diệt, Apropos sử dụng công nghệ rootkit nhằm mục đích che dấu sự hoạt động của nó dưới nền hệ điều hành. Mikko Hypponen, chuyên gia cao cấp của F-Secure, cho biết số liệu thống kê về rootkit của Microsoft là khá giống với với số liệu của F-Secure. “Trong 9 tháng kể từ khi chúng tôi cho ra mắt công nghệ BlackLight, chúng tôi đã phát hiện ra những điều tương tự như Microsoft đã thấy.” Trong khi đó, Microsoft thông báo cho biết có tới 20% trong số các phần mềm nguy hiểm tấn công hệ điều hành Windows XP Service Pack 2 trong năm qua là những “rootkit giấu mặt”.