NĂM LÝ DO ĐỂ CẦN CÓ MỘT PHƯƠNG PHÁP MỚI CHỐNG VIRUS

Như chúng ta thấy, các chương trình diệt virus thường không bắt kịp với các mối đe dọa, do vậy thỉnh thoảng bạn lại bắt gặp máy tính của bạn có các malware nhưng phần mềm diệt virus trên máy tính của bạn vẫn không làm gì được. Tồi tệ hơn nữa, đ&oci

Như chúng ta thấy, các chương trình diệt virus thường không bắt kịp với các mối đe dọa, do vậy thỉnh thoảng bạn lại bắt gặp máy tính của bạn có các malware nhưng phần mềm diệt virus trên máy tính của bạn vẫn không làm gì được. Tồi tệ hơn nữa, đôi khi bạn còn phát hiện thấy các rootkit trên các server mạng đã download vài GB các hình ảnh khiêu dâm thông qua sự thay đổi luồng dữ liệu (ADS). Các phiên bản của Norton đã được cài đặt sẵn trên mỗi máy chủ đó, nhưng nó không thể phát hiện rootkit bởi vì chúng boot trên zero-ring trước khi các ứng dụng antivirus tải và cho hệ điều hành thấy rằng mọi thứ đều bình thường. Không có cái gì có thể quan sát được ADS vậy nên các chương trình diệt virus không thể bắt được việc download tại đây. Vấn đề ở đây là malware thay đổi một cách rất êm ả và âm thầm trong vòng nhiều năm gần đấy. Người ta đã liệt kê được 5 đặc điểm quan trọng trong các mối đe dọa hiện nay để giúp cho các chương trình antivirus/antispyware có thể theo kịp: 1. Tiêu điểm tấn công của malwareĐã qua rồi thời kỳ tấn công gây phiền hà kiểu cũ. Thay vào đó, ngày nay malware thường tập trung vào các người dùng với các mô hình hoạt động riêng biệt. Nó thường phụ thuộc vào người dùng làm cái gì, site nào anh ấy truy cập online, dù anh ta download từ các site đầy rủi do hay anh ta cẩn thận trong việc download các file được gắn với các e-mail, các vấn đề tương tự như vậy. 2. Malware thay đổi code liên tụcChúng thay đổi ký hiệu của chúng hàng ngày, chính vì vậy mà các chương trình antivirus không thể theo kịp. 3. Vì lợi íchCác malware bây giờ chủ yếu là các tội phạm kinh doanh, mục đích của chúng là tiền hoặc các đối thủ cạnh tranh nhau. Thủ phạm gây ra là cả những kỹ sư có kiến thức về phần mềm, thường là những người làm việc tốt trong các công ty antispyware. 4. Một vài antispyware là malwareĐây là một cái bẫy rất nguy hiểm cho người dùng. Ví dụ, các trang web khiêu dâm thường thỏa thuận với những người cung cấp malware, khi một ai đó truy cập vào site này, nó sẽ download một chương trình giả mạo chống virus cùng với tranh ảnh khiêu dâm. Thoạt đầu người dùng hiểu nó như là một "dịch vụ" khi các pop-up quảng cáo xuất hiện trên trang, sau đó trang này sẽ quét ổ cứng của nạn nhân và "tìm được" một vài virus. Để loại trừ chúng, tất cả công việc mà người dùng phải làm sau đó là mua chương trình này với giá khoảng 10$. Trên thực tế không có chương trình virus nào được phát hiện và đã được xóa bỏ nhưng bạn vẫn phải trả tiền cho những công việc đó, tất cả những gì có được chỉ là sự cam đoan giả mạo rằng máy tính của bạn đã hoàn toàn sạch. Trên thực tế, sau khi việc này xảy ra hậu quả tốt nhất mà bạn gặp phải là đã "sở hữu" một chương trình diệt virus "dởm", còn tồi tệ hơn thì có thể có cái gì đó âm thầm nằm sau firewall máy bạn. Và như vậy, 10$ nhân với hàng nghìn nạn nhân sẽ cho kẻ lừa đảo này một số lượng tiền đáng kể. 5. Các chương trình antivirus chuẩn thường không có hiệu quả Những kẻ thiết kế ra malware luôn luôn test tác phẩm của chúng với các sản phẩm chống virus của các hãng như: Norton, McAfee và các hệ thống antivirus và antispyware thông thường khác để chúng làm cho các chương trình này không phát hiện được malware khi nó xâm nhập tới. Sau một thời gian, những hãng diệt virus nào tốt thì bắt kịp và các lỗ hổng lại được vá còn các hãng kém thì thay đổi mã của họ để các chương trình này không bị lặp lại lỗi đó nữa. Jason Bradley, người chịu trách nhiệm cho các giải pháp máy tính của CCE tại Oxford, người đã quản lý khoảng 400 máy tính, sau một thời gian nghiên cứu đã cho ra một phần mềm bằng một phương pháp mới đó là phần mềm Prevx. Bạn đọc có thể tham khảo và download về dùng thử tại địa chỉ

http://www.prevx.com. Trong phương pháp mới này Jason Bradley có nói: "Tôi luôn luôn tìm các vấn đề mới và Prevx là một phương pháp hoàn toàn khác. Nó không biên dịch các chương trình và kiểm tra các ký hiệu mà nó quan sát các hoạt động chính". Prevx cài đặt một tác nhân trên máy tính của người dùng và tải xuống trước trong chu kỳ boot sau đó kiểm tra các hoạt động của các đoạn mã chạy trên máy tính. Nó gửi dữ liệu quay trở lại Prevx server tại Anh, nơi mà nó được so sánh với tất cả các người dùng Prevx khác đang chạy phần mềm đó. Nếu tìm thấy sự khác nhau ở đây, nó sẽ gửi một bản tin quay trở lại đến các máy tính của người dùng đang đợi chúng. Sau đó người dùng có thể quyết định xem có tháo bỏ đoạn mã đó hay không.