SPAM, VIRUS VÀ MALWARE: NHỮNG XU HƯỚNG NỔI BẬT TRONG NĂM 2007

Ngày 1

Ngày 14/12/2007, IronPort Systems, một đơn vị kinh doanh của Cisco và là hãng hoạt động trong lĩnh vực bảo vệ trước spam, virus và spyware cho doanh nghiệp, đã công bố bản báo cáo về tình hình bảo mật năm 2007 và những xu hướng bảo mật Internet. Bản báo cáo của IronPort đã nêu bật những trào lưu bảo mật chủ đạo hiện nay và đưa ra những gợi ý về những phương thức bảo vệ chống lại thế hệ mới tinh vi hơn của những mối đe dọa Internet dự kiến sẽ nổi lên trong tương lai.

Thông tin là tiền tệ của thế giới mới

Những cuộc tấn công của spam, virus và malware gây ra rất nhiều tốn kém. Trung bình một người sử dụng phải dành 5-10 phút một ngày để "chiến đấu" với spam. Chi phí "dọn dẹp vệ sinh" ước tính đạt 500 USD cho mỗi máy tính để bàn. Nhưng tốn kém nhiều hơn nữa là mất dữ liệu. Dù đó là do một cuộc tấn công nguy hiểm, hay là một sai lầm vô ý, việc mất dữ liệu có thể làm cho một công ty bị giảm sức mạnh nhãn hiệu, giảm giá trị của cổ đông và gây tổn hại danh tiếng và độ tin cậy của khách hàng. Truyền thông liên lạc điện tử và dữ liệu đang được luân chuyển là những mối nguy hiểm nhất đối với khả năng mất dữ liệu trong doanh nghiệp hiện nay. Những giải pháp tường lửa cùng những giải pháp bảo mật mạng khác hiện nay không bao gồm những khả năng chống mất dữ liệu để bảo mật cho những dữ liệu đang được luân chuyển. Những biện pháp quản lý quan trọng, ví dụ như quét nội dung, chặn những liên lạc chứa những dữ liệu nhạy cảm và mã hóa, đang bị thiếu. Ước tính khoảng 60 triệu người có dữ liệu về bản thân được phơi bày trong vòng 13 tháng qua, và ước tính khoảng 20 tỷ USD được dành cho những chi phí để "dọn dẹp vệ sinh" và khắc phục việc giảm hiệu suất làm việc trên toàn cầu. Có tới 60% dữ liệu của doanh nghiệp được lưu trữ trên các máy tính để bàn và máy tính xách tay không được bảo vệ. Ngoài ra, 48% các tổ chức không có một chính sách thông báo cho các khách hàng khi những dữ liệu cá nhân của họ bị đe dọa.

Nhìn về phía trước: Malware xã hội

Malware hiện đại mượn những đặc tính từ các trang cộng tác và nối mạng xã hội gắn liền với Web 2.0. Malware hiện nay là một loại malware có khả năng cộng tác, thích nghi và rất thông minh. Nó ẩn mình trước các chương trình chống malware – nằm trong các máy tính tại doanh nghiệp hoặc gia đình hàng tháng hoặc hàng năm, mà không bị phát hiện. Những biến thể mới

của các Trojan và malware ngày càng có mục tiêu tấn công xác định và có vòng đời ngắn. Điều này khiến chúng trở nên khó bị phát hiện hơn. Quan điểm cũ cho rằng: "những gì tôi không nhìn thấy thì sẽ không làm hại tôi" đã không còn giá trị. Các tổ chức đang ngày càng phải chịu nhiều áp lực để đảm bảo tính toàn vẹn của những thông tin nhạy cảm của mình – đó có thể là những số thẻ tín dụng, thông tin về thu nhập của doanh nghiệp hay các kế hoạch cho các các sản phẩm mới. Những kẻ viết malware đang xây dựng các mạng tinh vi được thiết kế để thu thập những dữ liệu này, và ngày càng khó khăn hơn trong việc phát hiện và ngăn chặn. Các đội ngũ bảo mật CNTT cần tiến hành các bước để đánh giá luồng luân chuyển của malware trong mạng của mình và triển khai một hệ thống bảo mật toàn diện vốn bao gồm những kỹ thuật tiên tiến như phát hiện đe dọa ngay trên hệ thống mạng và kiểm soát truy cập mạng.

Những thống kê và phát hiện khác

Những xu hướng tổng quát về spam và malware có thể được phân loại theo đặc tính bởi một số lượng lớn hơn những cuộc tấn công tinh vi, lén lút và có nhiều mục tiêu hơn. Dung lượng spam đã tăng 100%, tới hơn 120 tỷ thông điệp spam một ngày. Tức là có khoảng 20 thông điệp spam một ngày được gửi tới mỗi con người trên trái đất này.

Spam đã trở nên ít tập trung vào việc bán sản phẩm hơn và tập trung hơn vào việc phát triển các hệ thống mạng spam. Những phiên bản trước của các cuộc tấn công spam chủ yếu là bán một số loại sản phẩm nào đó (dược phẩm, thế chấp lãi suất thấp…). Tuy nhiên, spam hiện nay bao gồm một số lượng đường link ngày càng lớn, chỉ tới các website phát tán malware. Malware này thường được thiết kế để mở rộng hơn nữa kích cỡ và quy mô của mạng, vốn là nơi khởi nguồn đầu tiên của spam này.

Những virus khó nhìn thấy hơn nhưng lại đang tăng lên về số lượng. Những người viết virus đã phát triển hơn so với những cuộc tấn công phát tán hàng loạt trước đây như "Netsky" và "Bagel". Trong năm 2007, các virus đã phát triển với nhiều hình thái và biến thể hơn nhiều và chủ yếu đi kèm với sự tăng trưởng rất nhanh của các mạng cực kỳ tinh vi.

Thời gian hiệu lực của một kỹ thuật tấn công cụ thể đã giảm đáng kể. Trong các năm trước, những người phát tán spam sẽ triển khai một kỹ thuật chủ yếu, như sử dụng các hình ảnh được nhúng trong hàng tháng. Những kỹ thuật gần đây hơn, như spam MP3, chỉ kéo dài trong vỏn vẹn 3 ngày. Nhưng các cuộc tấn công quy mô nhỏ hơn này lại nhiều hơn. Trong khi kỹ thuật spam bằng hình ảnh trong năm 2006 là kỹ thuật mới chủ đạo thì năm 2007 đã có hơn 20 loại file đính kèm được sử dụng trong một loạt các kỹ thuật tấn công có vòng đời ngắn.

Lê Quang