185.000 MÁY TÍNH BỊ NHIỄM VIRUS RONTOKBRO TRONG THÁNG 7

Trong tháng 7, tiếp tục đứng đầu danh sách những virus lây lan nhiều nhất trong tháng, "Rontokbro" đã trở thành một cái tên phải lưu ý "bất đắc dĩ" của người sử dụng ở Việt Nam. Theo hệ thống giám sát virus của Trung tâm An ninh mạng, đã

Trong tháng 7, tiếp tục đứng đầu danh sách những virus lây lan nhiều nhất trong tháng, "Rontokbro" đã trở thành một cái tên phải lưu ý "bất đắc dĩ" của người sử dụng ở Việt Nam. Theo hệ thống giám sát virus của Trung tâm An ninh mạng, đã có khoảng 185.000 máy tính ở Việt Nam bị nhiễm loại Virus này trong tháng 7. Ngoài việc ảnh hưởng trực tiếp đến công việc của những người sử dụng do máy tính khi bị nhiễm Virus này sẽ chạy rất chậm và thỉnh thoảng tự khởi động lại, sự lây lan của Rontokbro còn ảnh hưởng nặng nề đến tài nguyên của cả hệ thống mạng, gây tốn băng thông, tắc nghẽn đường truyền... Để sớm chấm dứt trình trạng lây lan mạnh mẽ của Rontokbro, khuyến cáo các quản trị mạng nên rà soát lại toàn bộ hệ thống của mình, tắt hết các thư mục, ổ đĩa chia sẻ không cần thiết, cài đặt phần mềm diệt virus và cập nhật phiên bản mới nhất cho tất cả các máy trong mạng. Các quản trị mạng cũng nên cài đặt phần mềm diệt virus tại cửa ngõ ra vào Internet của hệ thống mạng nội bộ (Gateway Scan), đây chính là nơi chặn virus hiệu quả nhất vì có thể diệt virus trước khi chúng kịp xâm nhập vào các máy tính bên trong mạng. Trong tháng 7 đã có 49 loại virus máy tính cả "nội" lẫn "ngoại" lây lan tại Việt Nam, gần gấp đôi con số của tháng 6. Trong số đó phải kể đến 2 virus nội lây lan qua Yahoo! Messenger làm náo loạn cộng đồng xử dụng phần mềm này. Mặc dù người sử dụng tại Việt Nam không còn quá xa lạ với những loại virus lây qua Yahoo! Messenger, nhất là sau khi virus Gaixinh mới "bùng nổ" cách đây không lâu (tháng 4/2006), nhưng số máy tính máy tính bị nhiễm 2 virus lây qua Yahoo! Messenger trong tháng 7 tính đến nay vẫn lên tới vài chục nghìn. Do đó, người sử dụng cần lưu ý trong lúc đang hội thoại (chatting) mà nhận được đường link từ người bên kia thì hãy cẩn thận. Đây có thể do virus tự sinh ra để đánh lừa, phải chắc chắn là người đang hội thoại gửi cho mình thì mới bấm vào link đó. Đã xuất hiện hiện tượng một số kẻ phát tán Adware (phần mềm quảng cáo bất hợp pháp) với mục đích quảng cáo, hiện tượng này trên thế giới đã rất phổ biến, tuy nhiên ở Việt Nam thì đang có dấu hiệu gia tăng. Những Adware xuất xứ từ Việt Nam như KeepmeScript hay ExploitJS đang trở thành một vấn đề đau đầu đối với rất nhiều người sử dụng máy tính tại Việt Nam. Theo hệ thống giám sát BKIS số lượng máy tính bị nhiễm các loại Adware này cũng nhiều không kém số lượng máy tính bị nhiễm các loại Virus khác. Hiện nay, các Adware này của Việt Nam chủ yếu lợi dụng lỗi của trình duyệt Internet Explorer (IE) khi xử lý XML để xâm nhập trái phép vào máy tính của người sử dụng. Nếu trình duyệt IE của bạn chưa được cập nhật bản vá lỗi, chỉ cần bạn vô tình vào một trong những trang web có cài đặt ngầm mã độc thì máy tính của bạn có thể bị nhiễm Adware ngay mà bạn không hề hay biết. Để phòng chống các Adware này, bạn cần nhanh chóng cập nhật bản vá lỗi cho IE. Việc có khá nhiều máy tính tại Việt Nam bị nhiễm Adware "nội" cũng phản ánh một xu hướng hoạt động hiện nay của một số tin tặc tại Việt Nam: lập ra các diễn đàn âm nhạc, tin tức online…, tìm cách thu hút thật nhiều thành viên, sau đó âm thầm cài đặt các đoạn mã độc lên máy tính của họ. Nhờ đó, tin tặc có thể chiếm quyền điều khiển máy tính của nạn nhân, quảng cáo, lấy cắp thông tin, hay thậm chí tạo dựng mạng Botnet (mạng máy tính ma) để phục vụ cho các cuộc tấn công DDos. Để tự bảo vệ mình cũng như cộng đồng, người sử dụng không nên vào những diễn đàn âm nhạc, tin tức online… khi chưa rõ nguồn gốc. Đó có thể là những cái "bẫy" đang được giăng sẵn và chỉ chờ để xâm nhập lên máy tính của bạn. Trong tháng qua, 5 virus lây lan nhiều nhất là: W32.Rontokbro.Worm,

W32.RontokbroE.Worm, W32.RontokbroK.Worm, W32.RunDllUSBB.Worm, W32.YmHeart.Worm. Theo đánh giá của các chuyên gia, tháng 7 đã xảy ra nhiều sự kiện an ninh mạng có ảnh hưởng lớn tới tình hình an ninh mạng ở Việt Nam. Trước tiên là việc kẽ hở trong hai phần mềm nguồn mở Webmin/Usermin bị khai thác. Sự việc dẫn đến hậu quả nghiêm trọng khi ở Việt Nam, một số nhà cung cấp dịch vụ hosting lớn có sử dụng phiên bản bị lỗi của hai phần mềm này, khiến tin tặc có thể đột nhập dễ dàng vào hệ thống, đặt 400 website vào tình trạng nguy hiểm, trong đó có các ngân hàng, các cơ quan nhà nước. Sự kiện nổi bật thứ hai trong tháng, đó là việc thủ phạm tấn công từ chối dịch vụ (DDoS) vào hệ thống của công ty Nhân Hoà bị bắt giữ. Đây là lần thứ hai, tin tặc tấn công DDoS bị sa lưới kể từ sau vụ Nguyễn Thành Công (DantruongX) tấn công vào công ty Việt Cơ. Với sự kiện này, có lẽ loại tội phạm tấn công DDos các website thương mại diễn ra trong vài năm gần đây sẽ bị đẩy lùi. Trong tháng 7 này, hơn 30 trang web đặt tại hai máy chủ của một nhà cung cấp dịch vụ hosting đã bị tin tặc tấn công, và để lại dòng chữ "kuwait hacker", rất may đây chỉ là các cuộc tấn công mang tính chất "chứng minh khả năng", của một nhóm tin tặc nước ngoài. Cũng trong tháng này, một tin tặc Việt Nam, với nickname là GuanYu, đã xâm nhập vào trang chủ của một nhà cung cấp dịch vụ lớn khác ở Việt Nam, tên này có lẽ đã kịp thu thập thông tin của 16 trang web khác cùng đặt trên hệ thống máy chủ của công ty này. Dưới đây là thông tin về các lỗ hổng bảo mật quan trọng trong tháng 7 có thể ảnh hưởng tới các hệ thống mạng tại Việt Nam: Các lỗ hổng trong bản cập nhật của Microsoft tháng 07, Lỗ hổng của Webmin/Usermin, Lỗ hổng trên MS PowerPoint, Lỗi tràn bộ đệm của MS IIS, Lỗi SQL Injection của Invision PowerBoard. L.Quang