VIRUS NỘI LÂY LAN NHANH NHẤT TỪ TRƯỚC ĐẾN NAY

Từ thờ

Từ thời điểm cuối tuần trước đến nay, cư dân mạng sử dụng công cụ chat yahoo (IM) xôn xao trước sự xuất hiện của một virus có tốc độ lây nhiễm được đánh giá là nhanh nhất từ trước đến nay và tỏ ra hết sức nguy hại.

Nguy hiểm hơn, virus này còn lây lan sang cả các ĐTDĐ qua đường bluetooth và những ĐTDĐ có chức năng duyệt web, e-mail qua Wi - Fi. Trong khi đó, các chuyên gia an ninh mạng vẫn chưa xác định được loại virus này cũng như chưa có biện pháp ngăn chặn sự lây lan quá nhanh của nó.

Với những máy tính bị nhiễm virus, cửa sổ IM ngay cả khi đang để ở chế độ ẩn danh (invisible) cũng tự động chuyển sang chế độ hiển hiện (available) rồi bôi đen tất cả các nick có trong IM. Đồng thời, cửa sổ một folder cũng tự động hiện lên để add (đưa vào) file dữ liệu chứa virus từ đường dẫn C\WINDOW\hinhem.scr gửi cho tất cả các nick được bôi đen.

Nếu chủ nhân của nick nào vô ý bấm vào đường link nguy hiểm này, máy tính sẽ lập tức bị nhiễm virus và sẽ tự động thực hiện các thao tác spam (phát tán) virus như mô tả ở trên.

Một đặc điểm đáng chú ý nữa là tất cả các IM trên máy tính bị nhiễm virus đều được tự động thêm vào rất nhiều status message (thông điệp) của các bài hát rất "sến" cùng với đường link chứa virus, chẳng hạn:

"Loi em noi cho tinh chung ta, nhu doan cuoi trong cuon phim buon. Nguoi da den nhu la giac mo roi ra di cho anh bat ngo... http://nhatquanglan6.t35.com", hay "Tha nguoi dung noi se yeu minh toi mai thoi thi gio day toi se vui hon. Gio nguoi lac loi buoc chan ve noi xa xoi, cay dang chi tieng minh toi… http://gaigoibaucat.xlphp.net".

Virus trên còn lây lan qua mạng LAN, khiến các mạng LAN có thể bị trục trặc bất cứ lúc nào.

Ngoài ra, nếu máy tính bị nhiễm loại virus này, khi xử lý văn bản bằng phần mềm Word, hoặc trình bày trên phần mềm QuarkExpress, Corel Draw…, nhiều đoạn C\WINDOW\hinhem.scr liên tục tự động chèn vào văn bản. Cũng có những thời điểm, văn bản đang được xử lý bị bôi đen toàn bộ, chữ thường chuyển sang chữ in hoa.

Theo phản ánh của nhiều bạn đọc qua đường dây nóng của báo Tiền phong, nhiều máy ĐTDĐ đã bị nhiễm virus với những đường link tương tự khi bật chế độ bluetooth hoặc lướt web, nhận gửi mail.

Ông Hoàng Tuấn Anh, chuyên gia tin học, Giám đốc Cty Cavinet cho rằng những phân tích ban đầu cho thấy đây là virus do các hacker Việt Nam viết và phát tán lên mạng. "Những gì virus đang phát tán cho thấy nó hết sức nguy hiểm. Người dùng máy tính phải đặc biệt cảnh giác với loại virus này" - Ông Hoàng Tuấn Anh cảnh báo.

Chuyên gia tin học này nhận định đây là virus có tốc độ lây nhiễm nhanh nhất từ trước đến nay. "Trong khoảng thời gian từ 60 – 80 giây, IM bị nhiễm virus lại spam virus một lần. Khi chat có biểu hiện này, người dùng nên tắt máy, tạm thời không sử dụng và nhờ nhân viên kỹ thuật can thiệp. Không nên sử dụng chat trong thời điểm này" - Ông Tuấn Anh đưa ra lời khuyên.

Liên lạc với ông Nguyễn Tử Quảng - Giám đốc Trung tâm An ninh mạng ĐHBK Hà Nội (BKIS), chúng tôi được đề nghị chuyển mẫu virus để phân tích và ông khẳng định sẽ xác định virus để cập nhật phiên bản diệt virus trong thời gian sớm nhất.

Chuyên gia phân tích virus Lê Tiến Thịnh thuộc BKIS cho biết đây là biến thể mới của virus nội, tương tự như virus Catch IM và Dakrong xuất hiện hồi đầu năm nay. BKIS vẫn đang tiếp tục phân tích virus này.

Virus trên đang làm đau đầu các chuyên gia tin học trong suốt mấy ngày qua. Tại nhiều công sở, nhân viên kỹ thuật đã sử dụng những phần mềm diệt virus phiên bản cập nhật mới nhất của Symantec, BKAV của Trung tâm An ninh mạng ĐHBK Hà Nội… nhưng không thể phát hiện ra virus này.

Do đó, cách ngăn chặn duy nhất hiện nay đối với virus trên là diệt bằng phương pháp thủ công, loại bỏ hệ điều hành trên máy đã bị nhiễm virus và cài đặt lại. Tuy nhiên, không nhiều người sử dụng máy vi tính có đủ kỹ năng để có thể áp dụng được phương pháp này.