CẢNH BÁO VIRUS MỚI LÂY QUA YAHOO MESSENGER TẠI VN

Trong ngày 10/4/2006 nhiều người sử dụng Yahoo Messenger tại Việt Nam cho biết có một số virus mới giả dạng một đường link “anhdep.jpg” và tự phát tán rất mạnh.

Khi Click vào đường link của virus giả dạng file ảnh, s

Trong ngày 10/4/2006 nhiều người sử dụng Yahoo Messenger tại Việt Nam cho biết có một số virus mới giả dạng một đường link “anhdep.jpg” và tự phát tán rất mạnh.

Khi Click vào đường link của virus giả dạng file ảnh, sẽ hiện ra giao diện như trên ảnh. Bạn đừng dại mà ấn vào "run" hay "save"!

Virus không rõ xuất xứ nói trên truyền đi một tin nhắn vào tất cả các nickname có trong YM friend list, nguyên văn như sau: “Gái đẹp! ...hãy xem cái này đi...” và đường link đi kèm: /Giift/?file=Anhdep.jpg hoặc /Gift/?file=e-card.htm... được hosting từ tên miền xrobots.net. Tuy trên đường link hiển thị đuôi jpg (định dạng ảnh), nhưng khi người dùng click vào link trên, sẽ có một software hiện ra và có đuôi dạng exe. Giao diện bắt bạn chọn “Run” (chạy) hoặc “save” (ghi vào máy). Nhìn qua đường link này, có thể thấy ngay tác giả đường link đã cố tình lừa người sử dụng với tên file Anhdep.jpg, thông qua cú pháp ?file=. Thực chất, khi bấm vào link, máy tính sẽ hỏi người dùng có muốn download 1 file anhdep.jpg.exe (anhdep.jpg là tên file) về máy hay không. Ngay sau khi người dùng dại dột để virus xâm nhập vào máy nếu chạy các software hiện ra, phần mềm của Virus sẽ tự động send cho tất cả các địa chỉ Yahoo Messenger trong list yahoo của bạn nếu bạn mở nick chat. Chính người bị dính virus cũng không biết mình đang phát tán các link nguy hiểm này. Hiện chưa có thống kê cụ thể về các tác hại của virus nói trên, xong với tốc độ phát tán kinh khủng bằng cấp số nhân, rõ ràng nó đang đặt cộng đồng mạng Việt Nam trước nguy cơ bảo mật rất lớn. Tất cả các link phát tán virus "gaidep"; "anhdep"... đều đến từ địa chỉ website www.xrobots.net. Đây là một trang web đen có chứa nhiều virus và spyware. Một số nguồn tin đáng tin cậy cho hay, domain này mới chỉ được lập ra hai ngày trước, song các virus, spyware từ đây đang phát tán một cách kinh khủng trong cộng đồng mạng Việt Nam chủ yếu qua

Yahoo Messenger. Theo nguồn tin riêng của VietNamNet, rất có thể tác giả của đường link này là người Việt Nam (vì người dùng Yahoo Messenger bị nhiễm hầu hết là người Việt Nam). Đây là một loại BOT virus, khi xâm nhập vào máy tính sẽ khống chế quyền điều khiển (còn gọi là máy tính zombie), tạo thành một mạng máy tính Botnet để tác giả virus điều khiển. Một số hacker VN chưa có trình độ còn tìm cách phát tán các loại virus BOT này bằng cách... thuê trẻ nhỏ ra cài ngoài hàng Internet với giá 1.000đ/máy. Ở cấp độ phản ứng bảo mật quốc gia, khi có sự việc tương tự, nhà cung cấp dịch vụ Internet nắm đường truyền Internet ra quốc tế (ở Việt Nam là VDC) cần có biện pháp can thiệp sớm để chặn hoạt động truy cập từ Việt Nam vào tên miền www.xrobots.net. Việc làm này trước mắt sẽ giảm thiểu khả năng phát tán của virus lây qua Yahoo Messenger do người dùng thiếu hiểu biết click vào. Lời khuyên tốt nhất là khi có các tin nhắn offline hoặc các message lạ của bất kỳ người nào trong Yahoo Messenger list của bạn gửi đến có chứa các link liên quan đến địa chỉ xrobots.net hoặc các link không rõ mục đích, hãy tắt ngay cửa sổ chat đó và không click vào link hay chạy (run) software nào hiện lên màn hình. Với các máy đã bị nhiễm, các bạn có thể xóa file virus một cách thủ trong ổ C:\Windows, delete file messenger.exe. Nếu không xóa được thì chạy Safe Mode và xóa trong đó. Cách cuối cùng là xóa file C:\Windows\messenger.exe từ MSDOS. Thế Phong