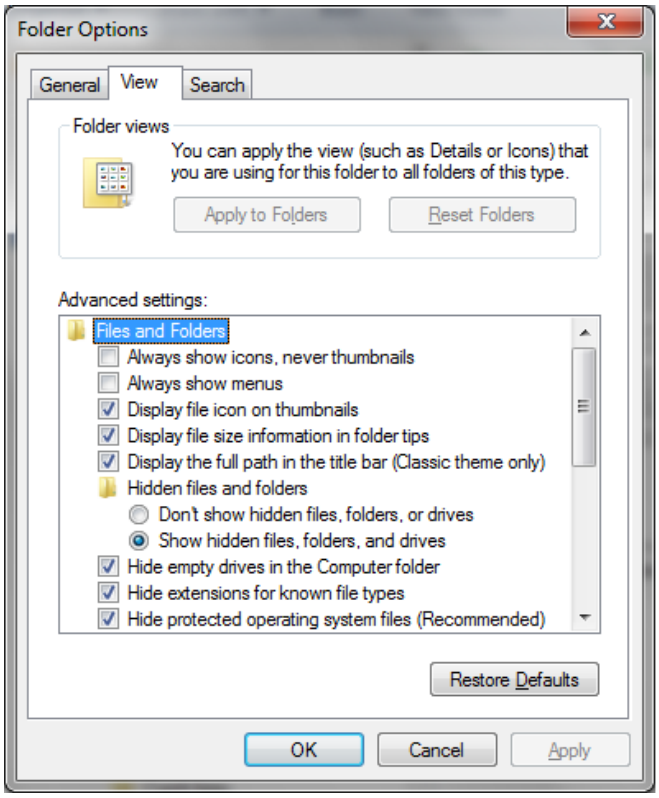
THÔNG TIN VỀ MÃ ĐỘC GIẢ MẠO THUMBNAIL TRÊN WINDOWS

Bên cạnh hình thức giả mạo các tệp tin tài liệu làm thành phần trung gian để cài mã độc vào máy người dùng thì việc giả mạo các biểu tượng thông thường (Icon) của tệp tin tài liệu nhằm che dấu kiểu tệp tin thực thi (.exe, .com, .dll…) đã được tin tặc sử dụng và đã bị ghi nhận trước đây. Do nhận thức người dùng đã tốt hơn nên việc giả mạo theo cách này bắt đầu giảm hiệu quả, tin tặc đã bắt đầu sử dụng một cách thức mới là giả mạo lược ảnh (Thumbnail) của tệp tin để lừa người dùng chạy các tệp tin mã độc. Tất cả các hệ điều hành từ Windows Vista trở về sau có thể là mục tiêu tấn công của loại mã độc giả mạo Thumnail này.

1. Thumbnail Previews là gì

Thumbnail Preview là một tùy chọn của Window Explorer trên các hệ điều hành từ Window Vista trở về sau, khi ta đặt chế độ hiển thị tệp tin từ cửa sổ Windows Explorer ở mức biểu tượng trung bình trở lên thì Thumbnail sẽ hiện ra chứ không phải là biểu tượng thông thường về loại ứng dụng (Icon) nữa.



Các tùy chọn liên quan tới Thumnails Preview gồm:

1. Always show icons, never thumbnails (luôn hiển thị biểu tượng - Icon, không hiển thị Thumnails).
2. Display file icon on thumbnails (hiển thị Icon trên Thumnails).
3. Hide extensions for known file types (ẩn phần mở rộng của tập tin).

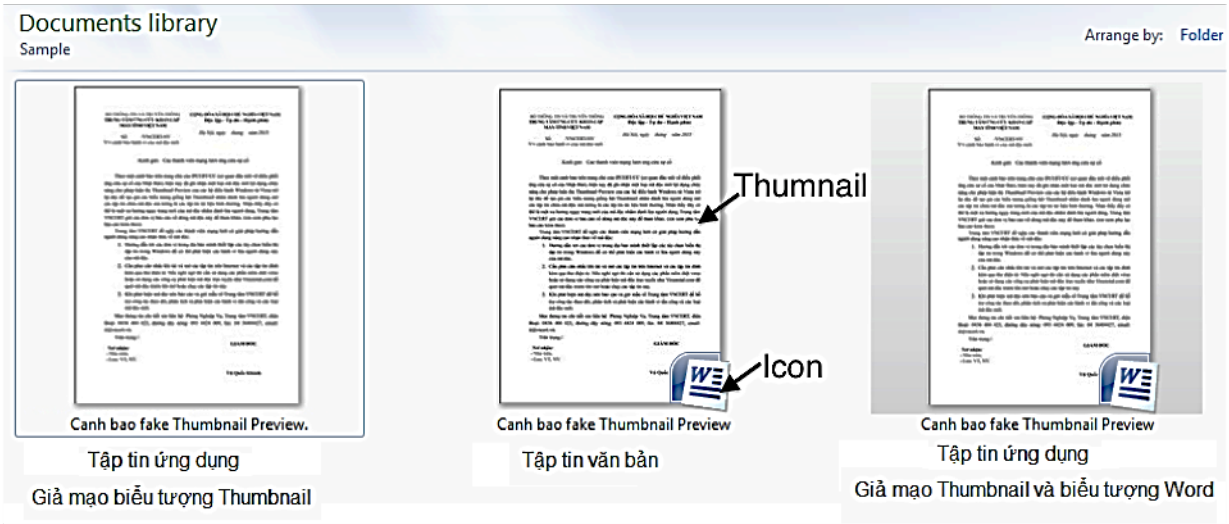
2. Cách thức giả mạo của mã độc che dấu qua Thumbnail Previews

Để minh họa việc giả mạo Thumbnail Previews, chúng ta xem xét trường hợp có hai tệp tin thực thi với Thumbnail giả mạo không có Icon và với Thumbnail giả mạo kèm theo Icon của phần mềm soạn thảo văn bản Microsoft Word.

Trong hình 1 và hình 2 bên dưới, ta thấy ba tệp tin trong đó có hai tệp tin là ứng dụng (.exe) và một tệp tin văn bản được xem ở chế độ bật và chế độ tắt hiển

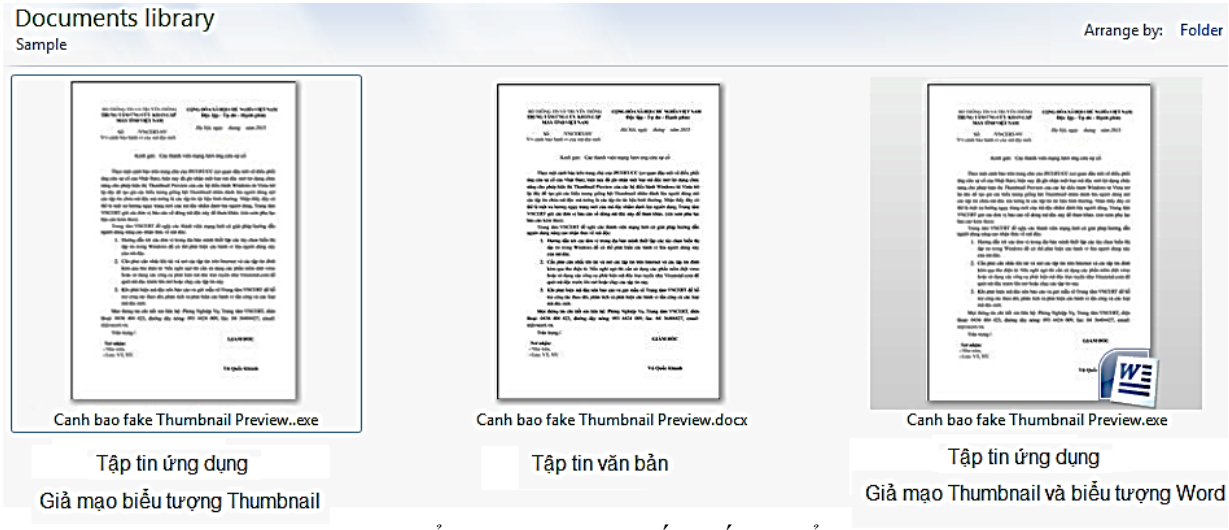
thị Icon trên Thumnails (*Display file icon on thumbnails)*. Rõ ràng ta không thể phân biệt được đâu là tệp tin văn bản và đâu là tệp tin ứng dụng (thực thi).

- Khi bật chế độ hiển thị Icon



Hình 1. Hiển thị tập tin khi bật chế độ hiển thị Icon

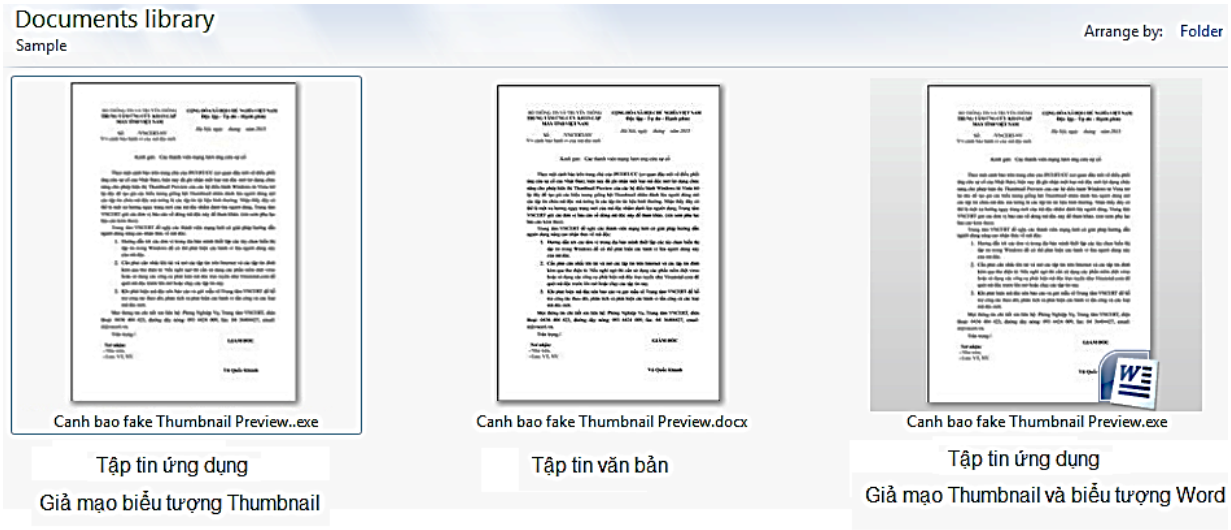
- Khi tắt chế độ hiển thị Icon



Hình 2. Hiển thị tập tin khi tắt chế độ hiển thị Icon

Nếu chỉ nhìn vào các biểu tượng tệp tin thì có thể thấy rằng việc phân biệt đâu là tệp tin thực thi (.exe) và đâu là tệp tin văn bản là không dễ. Để quan sát được các tệp tin này, ta cần tắt chức năng *Hide extensions for known file types*.

Trong hình 3 bên dưới sau khi tắt chức năng ẩn phần mở rộng của tệp tin thì ta sẽ quan sát thấy tệp tin ở giữa là tệp tin văn bản, trong khi tệp tin hai bên là các tệp tin ứng dụng (.exe). Như vậy phải quan sát phần đuôi mở rộng của cả ba tệp tin trên thì mới có thể quan sát được đâu là tệp tin ứng dụng, đâu là tệp tin văn bản.



Hình 3: Hiển thị tệp tin ứng dụng giả mạo biểu tượng tệp tin văn bản và tệp tin văn bản ở chế độ hiện thị phần mở rộng của tệp tin

Theo chế độ mặc định, hệ điều hành luôn chọn sẵn các chế độ hiển thị biểu tượng tệp tin đi kèm và ẩn phần đuôi mở động của tệp tin được sử dụng, do đó sẽ có một biểu tượng Icon ở trên Thumbnail và không có phần mở rộng của tệp tin. Chính vì vậy, người sử dụng thông thường sẽ căn cứ vào biểu tượng Icon ở trên Thumbnail để nhận biết loại tệp tin. Đây chính là kẽ hở mà tin tặc lợi dụng để giả mạo lừa người sử dụng. Trung tâm Điều phối ứng cứu sự cố khẩn cấp máy tính Nhật bản đã ghi nhận được một số mẫu mã độc dạng này (thông tin tham khảo xem tại website của Trung tâm VNCERT: http://vncert.gov.vn).

3. Khuyến nghị

Nhận thấy đây có thể là một xu hướng mới để ngụy trang cho các tệp tin độc hại của tin tặc, Trung tâm VNCERT khuyến cáo tới các thành viên mạng lưới thực hiện hướng dẫn tới người dùng máy tính trong địa bàn mình về loại mã độc này để cảnh giác. Cụ thể là:

1. Chú ý và cảnh giác khi tải và mở các tệp tin trên Internet đặc biệt là các tệp tin đính kèm qua thư điện tử.
2. Nên bật tùy chọn hiện thị phần đuôi tệp tin để dễ dàng quan sát các tệp tin mình sẽ mở.
3. Khi mở tệp tin theo kiểu chạy tự động hay chạy trực tiếp (kích đúp chuột, nhấn phím enter…), cần đặc biệt quan tâm đến loại tệp tin, nếu phát hiện các tệp tin bất thường loại này (ví dụ như tệp tin ứng dụng thực thi nhưng lại có biểu tượng của Word, PDF…) thì nhanh chóng báo về cho các cơ quan chức năng để phối hợp xử lý.