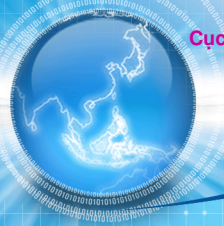
Công tác phòng ngừa phát hiện tố giác tội phạm công nghệ cao của các cơ quan báo chí



Cục Quản lý phát thanh, truyền hình và thông tin điện tử

Báo điện tử tại Việt Nam

- Theo Nghị định 51/2002/NĐ-CP ngày 26/4/2002 quy định chi tiết thi hành Luật Báo chí, Luật sửa đổi, bổ sung một số điều của Luật Báo chí, Báo điện tử là tên gọi loại hình báo chí thực hiện trên mạng thông tin máy tính "internet, intranet".
- **Đặc điểm của Báo điện tử**
- + Không bị giới hạn bởi không gian, thời gian, địa điểm, khoảng cách địa lý.
- + Tính nhanh chóng,
- + Tính tương tác cao
- + Tính tìm kiếm
- Hiện nay, tại Việt Nam có khoảng 53 cơ quan báo chí điện tử (46 báo điện tử, 7 tạp chí điện tử); khoảng 250 cơ quan báo chí (báo, tạp chí, đài) có giấy phép thiết lập trang thông tin điện tử tổng hợp trên internet.

Các vụ tấn công vào báo điện tử và trang thông tin điện tử của Việt nam

- *Cơ quan báo chí*
- 1. Tối 26-10/2003, website của báo điện tử Thể Thao Việt Nam đã bị các hacker xâm nhập vào hệ thống bảo mật và tấn công, thay đổi một loạt nội dung của trang web này...
- 2. Ngày 27/3/2011, Báo Người đưa tin - Báo điện tử của Báo Đời sống & Pháp luật - đã bị tin tặc tấn công từ chối dịch vụ. Cuộc tấn công kéo dài gần 2 giờ đồng hồ, bắt đầu từ 10 giờ 30 (27/3). Trước đó, chiều 26/03/2011 trong khoảng thời gian 16 giờ 10- 16 giờ 30, hệ thống của báo cũng đã bị tấn công DDoS.
- 3. Ngày 9/6/2011, Tờ báo điện tử Petrotimes.vn vào lúc hơn 20h (9/6), một lượng truy cập khoảng trên 600 ngàn kết nối đồng thời đã dồn vào websie petrotimes.vn khiến website bị ngừng hoạt động vì quá tải. Không chỉ bị tấn công từ chối dịch vụ, toàn bộ dữ liệu của website Petrotimes đã bị hacker xóa sạch.

Các vụ tấn công vào báo điện tử và trang thông tin điện tử của Việt nam

- 4. Tháng 11 năm 2010, một tờ báo điện tử lớn của Việt Nam bị tấn công khi độc giả không thể truy cập được trong gần 1 tháng.
- - Ngày đến tháng 8 năm 2011, tờ báo điện tử này tiếp tục bị tấn công trong suốt gần 1 tháng không truy cập được mặc dù huy động năng lực ứng cứu, nhà cung cấp dịch vụ internet mở rộng đến tận 20 Gbps (hiện nay, hầu hết các báo điện tử đáp ứng được khoảng 2-5 Gbps).

Các vụ tấn công vào báo điện tử và trang thông tin điện tử của Việt nam

- *Cơ quan nhà nước, doanh nghiệp:*
- 1. Tháng 6/2011, trang web một cơ quan của Bộ ngoại giao cũng đã bị tin tặc xâm nhập và treo cờ nước ngoài, đồng thời thay đổi nội dung các đường link bên trái website
- 2. Ngày 26/10/2011, VozForums.com và Diadiem.com, là 2 trang web có nhiều thành viên đã bị tấn công và mất quyền kiểm soát tên miền.
- 3. Trong vòng chưa đầy 15 ngày đầu tháng 6/2011, đã có 249 website của Việt Nam bị hacker tấn công, phần lớn là nhằm thay đổi giao diện. Đây là một đợt tấn công mạng diện rộng, mà mục tiêu hacker nhắm vào là các website quan trọng, chính thống của các cơ quan nhà nước (hơn 50 website tên miền gov.vn).

Hiện tượng tấn công đáng chú ý nhất trong thời gian qua

- Đây là hình thức tấn công được chuẩn bị từ trước. Hacker đã cài các phần mềm backdoor (tạo cổng sau để xâm nhập lại) và các phần mềm gián điệp dạng keylogger, từ đó lấy trộm được các mật khẩu quản trị hệ thống, lên kế hoạch phá hoại hàng loạt bằng chương trình hẹn giờ xóa sạch ổ cứng.
- Cài đặt lại toàn bộ hệ thống máy chủ mới và triển khai các biện pháp bảo mật hệ thống chặt chẽ, hacker tiếp tục tìm cách lấy trộm tài khoản email nội bộ và tài khoản xuất bản của hệ thống quản trị nội dung (CMS) của báo. Tài khoản xuất bản nội dung được hacker sử dụng để xuất bản nội dung xấu lên các chuyên mục của báo.

Hiện tượng tấn công đáng chú ý nhất trong thời gian qua

- Sau khi đội ngũ kỹ thuật đưa toàn bộ hệ thống xuất bản nội dung (CMS) vào trong mạng nội bộ (không cho phép nhập nội dung và xuất bản từ xa), hacker chuyển hướng sang tấn công các chuyên trang (sử dụng mã nguồn mở), thay đổi nội dung tiêu đề các tin bài.
- Sau khi toàn bộ các hệ thống xuất bản nội dung và chuyên trang được đưa vào mạng nội bộ, không thể xâm nhập qua Internet, hacker chuyển hướng sang tấn công từ chối dịch vụ phân tán DDOS với quy mô lớn chưa từng có tại Việt Nam.

Khả năng ứng phó của báo chí điện tử

- ** Khả năng ứng phó của các cơ quan báo chí khi bị tấn công còn hạn chế.*
- - Ý thức người sử dụng không cao:
- + máy tính không có phần mềm diệt vi rút.
- + Sử dụng USB không diệt vi rút.
- + Gửi và nhận mail không kiểm soát.
- - Hạ tầng công nghệ kém, trình độ kỹ thuật chưa được đào tạo chuyên sâu, chưa có quản trí nội dung chuyên biệt.
- - Phần mềm quản trị không phải viết riêng, hầu hết là sử dụng những phần mềm có sẵn cùng 1 mã nguồn mở cũ và vẫn còn lỗi.

Khả năng ứng phó của báo chí điện tử

- ** Vấn đề cần phải quan tâm hiện nay.*
- *- Con người*
- + Nâng cao ý thức người sử dụng để không bị khai thác trái phép các tài khoản.
- + Ý thức đội ngũ quản trị, vận hành.
- + Đào tạo thường xuyên về công nghệ cho các đối tượng sử dụng máy tính
- + Xây dựng các Quy trình, Quy định về đảm bảo an ninh, an toàn thông tin. Thường xuyên kiểm tra, giám sát việc tuân thủ thực hiện.

Khả năng ứng phó của báo chí điện tử

- *- Công nghệ*
- +Hệ thống phần mềm quản lý nội dung (tự xây dựng hoặc đi thuê đơn vị bền ngoài cần phải đảm bảo yếu tố bảo mật, không để được hiện tượng khai thác trái phép
- + Trang bị mở rộng tài nguyên cho đúng với quy mô hoạt động, nâng cao tính sẵn sàng.
- + Đầu tư các trang thiết bị cần thiết để có thể đối phó với các hình thức tấn công cũ và mới.
- + Trang bị các hệ thống phần mềm bản quyền bao gồm từ máy chủ tới máy trạm, từ Hệ điều hành tới các phần mềm ứng dụng phục vụ để đảm bảo các máy tính không bị virus hoặc bi khai thác
- + Thuê các dịch vụ về an ninh, an toàn thông tin của bên thứ 3 để có sự kiểm tra chéo về công tác bảo mật, an toàn thông tin.

Khả năng ứng phó của báo chí điện tử

- *- Cơ quản Quản lý*
- + Thành lập đường dây nóng, điều phối chung giữa các đơn vị: các nhà cung cấp dịch vụ, Trung tâm ứng cứu khẩn cấp, Cục phòng chống tội phạm công nghệ cao, các đơn vị, doanh nghiệp chuyên môn về bảo mật, an toàn thông tin để ứng cứu, ngăn chặn và tìm nguồn gốc tấn công, phá hoại.

XIN CHÂN THÀNH CÁM ƠN SỰ CHÚ Ý LẮNG NGHE CỦA QUÝ VỊ