# Tấn công DDoS, "hung thần" của các trang web

**DDoS là kiểu tấn công làm cho mục tiêu, là các trang web, dịch vụ trực tuyến, trở nên quá tải. Người dùng gặp khó khăn, hay thậm chí không thể truy cập vào các trang web, dịch vụ này.**

Hiện chưa có giải pháp ngăn chặn triệt để kiểu tấn công từ chối dịch vụ phân tán DDoS (Distributed denial of service), chỉ có thể hạn chế phần nào thiệt hại hay giảm bớt cường độ tấn công.

Đầu tháng 3/2011, trang blog WordPress là nạn nhân tiếp theo của tấn công DDoS. Tại Việt Nam, thời gian qua một số trang web truyền thông, cung cấp dịch vụ cũng trở thành nạn nhân của các cuộc tấn công DDoS.

Động cơ tấn công DDoS trong suốt thập kỷ qua có thể do mục tiêu chính trị, tống tiền, cạnh tranh không lành mạnh… Việc tìm ra thủ phạm tấn công DDoS thường rất khó khăn, phức tạp và mất rất nhiều thời gian, khi mà những hình thức tấn công ngày càng tinh vi phức tạp.

***Sau đây là một số cuộc tấn công DDoS đáng chú ý trên thế giới trong những năm qua:***

## Máy tính chạy hệ điều hành Windows trở thành công cụ cho các cuộc tấn công từ chối dịch vụ

Năm 2000, các cuộc tấn công DDoS vào Yahoo, eBay, eTrade, Amazon.com và CNN xuất phát từ các máy tính chạy Unix của các doanh nghiệp và các trường đại học, nhưng sau đó vài tuần, malware chỉ đạo cuộc tấn công, có tên gọi là Trinoo, chuyển sang các máy tính chạy Windows để khởi phát các cuộc tấn công.

## DDos tấn công các máy chủ Internet quan trọng

13 máy chủ Internet cấp cao nhất (Internet root servers) bị tấn công DDos vào năm 2002, tuy nhiên các nhà quản trị hệ thống đã kịp thời phát hiện, kiểm soát và ngăn chặn cuộc tấn công DDOs gây "sập" hệ thống mạng Internet. Sau cuộc tấn công, các máy chủ này đã được thiết lập giới hạn Internet Control Message Protocol (ICMP - các thông điệp được dùng để xác định khi nào một hệ thống mạng có thể phân phối các gói tin) nhằm tránh tái diễn các kiểu tấn công tương tự trong tương lai. 13 máy chủ Internet này chứa các thư mục gốc (master directory) phân giải tên miền và địa chỉ IP.

## Tấn công DDoS qui mô lớn vào Estonia

Các trang web của chính phủ, ngân hàng, trường học tại Estonia bị tê liệt do tấn công DDos vào tháng 5/2007. Tuy nhiên, các trang web bị tấn công này đã khôi phục nhanh chóng sau đó. Các nhà phân tích bảo mật nghi ngờ cuộc tấn công xuất phát từ Nga, nhưng họ chưa thể lần ra dấu vết, vì các cuộc tấn công DDOs thường không khởi phát từ một nơi.

## Sâu Storm

Năm 2007, sâu Storm xuất hiện và lây lan nhanh chóng. Một khi đã lây nhiễm vào máy tính người dùng, sâu sẽ gửi đi hàng triệu thư rác. Trong suốt đợt tấn công của sâu Storm, một số nhà nghiên cứu bảo mật nhận định rằng,

người đứng sau hoặc tự bản thân sâu Storm đang phát động cuộc tấn công DDoS nhắm vào các nhà nghiên cứu, đang tìm cách khống chế nó. Sâu Storm có thể phát hiện những ai đang thực hiện truy tìm các máy chủ phát lệnh tấn công, và tiến hành trả đũa bằng cách phát động tấn công DDos nhắm vào người đó, nhằm đánh sập kết nối Internet của họ.

**DDoS tấn công Georgia**

Tấn công DDoS vào các trang web chính phủ, ngân hàng tại Georgia năm 2007 do các tổ chức tội phạm ở Nga thực hiện (tổng cộng có 54 trang web là mục tiêu của cuộc tấn công này, trong đó hầu hết là các trang web truyền thông, chính phủ, ngân hàng). Tại thời điểm đó, nhiều nhà phân tích, cho rằng đây là cuộc tấn công "mềm" trước khi Nga thực hiện cuộc tấn công quân sự vào Georgia. Tuy nhiên, sau đó, các cuộc điều tra cho thấy cuộc tấn công DDoS này do các băng nhóm tội phạm ở Nga thực hiện. Các tin tặc dùng các công cụ tấn công dựa trên HTTP, thay cho ICMP.

**Twitter bị tấn công DDoS**

Tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial Of Service) là kiểu tấn công làm cho hệ thống máy tính hay hệ thống mạng quá tải, không thể cung cấp dịch vụ hoặc phải dừng hoạt động.

Trong các cuộc tấn công DDoS, máy chủ dịch vụ sẽ bị "ngập" bởi hàng loạt các lệnh truy cập từ lượng kết nối khổng lồ. Khi số lệnh truy cập quá lớn, máy chủ sẽ quá tải và

Tháng 8/2009, tấn công DDoS vào các trang mạng xã hội như Twitter, Facebbok, LiveJournal và một số trang của Google, chỉ nhằm "đánh phá" các trang blog, bài viết của blogger Cyxymu ở Georgia.

không còn khả năng xử lý các yêu cầu. Hậu quả là người dùng không thể truy cập vào các dịch vụ trên các trang web bị tấn công DDoS.

**DDos tấn công Amazon trước lễ giáng sinh**

Nhà cung cấp dịch vụ phân giải tên miền (DNS) cho Amazon bị tấn công DDoS, khiến người dùng không thể truy cập vào máy chủ Amazon.com và Amazon Web Services vào ngày 23/12/2009, đây là thời điểm mua sắm sôi động nhất trong năm tại các nước khu vực Bắc Mỹ.

**Nhóm tin tặc Anonymous tấn công DDoS trang Visa.com**

Ngày 7/12/2010, trang Visa.com bị nhóm tin tặc Anonymous tấn công DDoS. Theo nhóm tin tặc, họ thực hiện cuộc tấn công này nhằm phản đối việc các hãng tài chính khóa tài khoản của WikiLeaks, sau khi trang này dự kiến công bố các tài liệu mật của Bộ ngoại giao Mỹ. Trước đó nhóm tin tặc này đã thực hiện các cuộc tấn công các trang web Mastercard và PayPal.

**Trang web chính phủ Hàn Quốc bị tấn công**

Ngày 4/3/2011, 40 trang web thuộc chính phủ Hàn Quốc tê liệt vì tấn công DDoS.

Bộ luật Hình sự Việt Nam, sửa đổi bổ sung 37/2009/QH12 ngày 19/6/2009, tại các điều 224, 225, 226, 226a, 226b có các qui định về tội phát tán vi rút, chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số. Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet. Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác. Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản.