**Vụ tấn công doanh nghiệp TMĐT Viet Co Ltd**

Đây là lần đầu tiên một Hacker bị bắt vì hành vi tấn công DDos tại Việt Nam. Hành động tấn công từ chối dịch vụ DDos đã làm ảnh hưởng nghiêm trọng tới nền thương mại điện tử còn đang trong những bước phát triển đầu tiên ở Việt Nam.

Sự việc tìm ra và bắt được thủ phạm tấn công DDos lần đầu tiên như thế này sẽ giúp cho các doanh nghiệp thương mại điện tử yên tâm kinh doanh.

Diễn biến:

-Chủ nhật ngày 12/3/2006 website thương mại điện tử VietCo.com bị tấn công từ chối dịch vụ DDos, làm cho không thể hoạt động được, nhân viên công ty phải nghỉ việc.

-Buổi tối cùng ngày anh Phùng Minh Bảo - giám đốc công ty Việt Cơ liên lạc tới Trung tâm An ninh mạng BKIS nhờ trợ giúp.

-8 giờ tối thứ hai ngày 13/3/2006 Trung tâm An ninh mạng BKIS lấy được file Log (nhật ký trên máy chủ) từ website của VietCo do anh Bảo cung cấp. Sau khi phân tích logfile thấy rằng đây không phải là tấn công Xflash như đã từng xảy ra ở Việt Nam trước đây.

-Sau 4 ngày điều tra họ đã tìm ra cơ chế của cuộc tấn công, tìm ra thủ phạm và các thông tin liên quan. Kẻ tấn công tên là Nguyễn Thành C, tức DantruongX thuộc nhóm Haker Bé yêu, một Hacker "nổi đình nổi đám" từ nhiều năm nay. Trước đây bọn này chuyên đi tấn công các website của các Hacker khác, nhưng có dấu hiệu cho thấy chúng đang rút vào hoạt động bí mật và có động cơ kiếm tiền bất chính.

-Các thông tin trên được cung cấp cho đơn vị chống tội phạm công nghệ cao thuộc Cục cảnh sát điều tra tội phạm kinh tế và chức vụ Bộ Công An (C15). Sau hơn 1 tháng điều tra tiếp theo, Cơ quan an ninh đã khẳng định chính xác Nguyễn Thành C là thủ phạm, tên này còn dính líu tới 1 vụ việc vi phạm khác liên quan tới đường dây làm giả thẻ ATM. Nguyễn Thành C đã bị bắt vào sáng 28/4/2006, đến chiều cùng ngày hắn đã khai nhận tội.

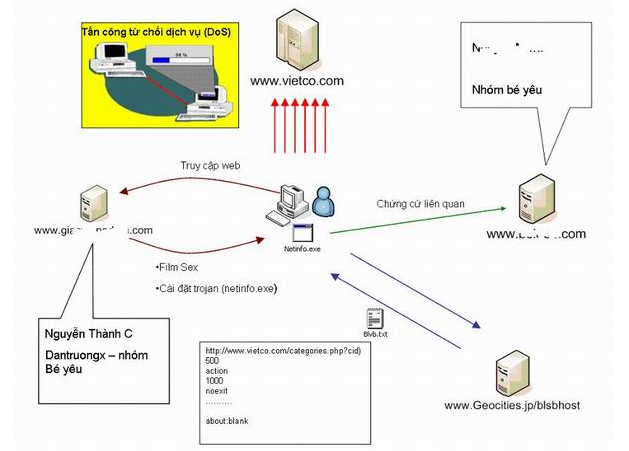
-Nguyễn Thành C và đồng bọn đã xây dựng được 1 hệ thống mạng máy tính ma (BOTNET), tức là đã chiếm được quyền điều khiển của rất nhiều máy tính nối mạng ở Việt Nam mà chủ nhân cũng không hay biết. Những máy tính này sẽ được chúng điều khiển từ xa để tấn công vào bất kỳ website nào chúng muốn. Trong hơn 1 tháng qua, theo quan sát, chúng thay đổi các mục tiêu tấn công hàng ngày, đó có thể là các website thương mại, đôi khi là 1 website của 1 trường phổ thông.

Việc tấn công DDoS Việt Cơ được tiến hành theo trình tự:

1. Hacker sử dụng một trojan cài lên website khiêu dâm www.giac... .com. Trojan này lợi dụng một lỗ hổng của trình duyệt IE - bất cứ máy tính nào chưa update lỗi IE này, khi truy nhập vào www.giac....com sẽ lập tức bị Trojan tự động cài vào máy, trở thành zoombie (zoombie - thây ma sống- chỉ các máy tính bị xâm nhập và có thể bị điều khiển từ xa cho mục đích tấn công.). Có rất nhiều máy tính đã bị chiếm quyền điều khiển như vậy ở Việt Nam, tạo thành mạng BOTNET.

2. Mỗi khi máy tính nhiễm Trojan nối mạng Internet, Trojan này sẽ kết nối tới một địa chỉ định trước trên Internet là www.geocities.jp/blsbhost để lấy về các lệnh tấn công trong một file văn bản có tên là blvb.txt.

3. File này quy định các thông tin: Cần tấn công website nào? tấn công với tần xuất như thế nào… Như vậy khi cần tấn công website nào thì Hacker chỉ việc sửa đổi nội dung file blvb.txt là lập tức tất cả các máy tính bị chiếm điều khiển sẽ đồng loạt tấn công ồ ạt vào mục tiêu và website mục tiêu đó khó có thể chống đỡ nổi, dẫn đến không thể cung cấp dịch vụ được nữa (bị từ chối dịch vụ - DDos).



Hình 1: Sơ đồ hệ thống triển khai tấn công DDoS vào Vietco.com

**Trojan là gì?**

Trojan (hay Trojan horse), trước hết là một chương trình độc hại cho máy tính, được ngụy trang bằng một vỏ bọc tưởng chừng vô hại để tạo tin tưởng cho người dùng, từ đó sử dụng và vô tình máy tính bị nhiễm trojan, bị thu thập mọi dữ liệu từ bên thứ 3 để phục vụ cho mục đích xấu.

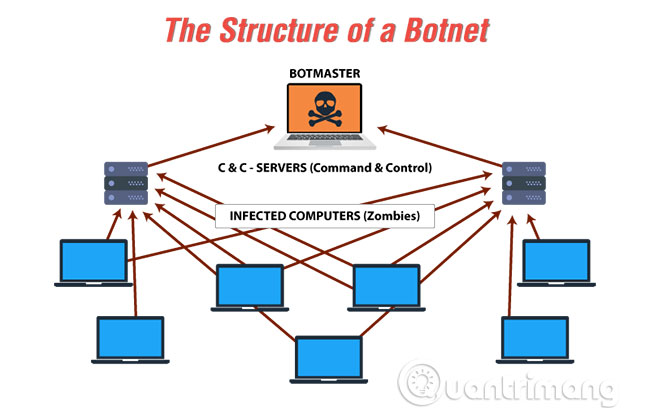
Trojan được lấy từ điển tích con ngựa thành Troia trong thần thoại Hy Lạp. Nội dung điển tích kể về sự thông minh của người Hy Lạp khi đã ẩn nấp vô số chiến binh trong thân con ngựa gỗ khổng lồ, khiến kẻ địch lầm tưởng đó là chiến tích thu được mà chủ quan, giúp quân Hy Lạp chiếm thành dễ dàng. Điều này cũng giống như cách thức hoạt động của trojan.

**BOTNET là gì?**

Từ “botnet” là sự kết hợp của hai từ, “robot” và “network”. Ở đây, một tên tội phạm mạng thực hiện vai trò của một “botmaster” sử dụng virus Trojan để xâm phạm bảo mật của một số máy tính và kết nối chúng vào mạng vì mục đích xấu. Mỗi máy tính trên mạng hoạt động như một “bot”, và được kẻ xấu kiểm soát để lây truyền malware, spam hoặc nội dung độc hại nhằm khởi động cuộc tấn công. Botnet còn được gọi là đội quân zombie vì các máy tính liên quan đang được điều khiển bởi một người khác không phải chủ sở hữu của chúng.

Nguồn gốc của botnet chủ yếu là để phục vụ như một công cụ trong các kênh Internet Relay Chat (IRC). Cuối cùng, những kẻ xấu sẽ khai thác các lỗ hổng có trong mạng IRC và các bot được phát triển. Điều này được cố ý tạo ra để thực hiện các hoạt động độc hại như ghi nhật ký về hành động nhấn phím, đánh cắp mật khẩu, v.v...

Cấu trúc của botnet thường có một trong hai dạng: Mô hình client - server (máy khách - máy chủ) hoặc mô hình peer-to-peer (ngang hàng).



Hình 2: Cấu trúc của BOTNET

Nguồn:

<https://www.bkav.com.vn/tin-tuc-noi-bat//-/view-content/151380/tim-ra-thu-pham-vu-tan-cong-ddos-vao-website-vietco-com>

<https://quantrimang.com/thu-pham-tan-cong-ddos-website-vietco-lo-mat-21075>

<https://quantrimang.com/trojan-la-gi-lam-sao-de-tranh-trojan-tan-cong-168699>

<https://quantrimang.com/botnet-hoat-dong-nhu-the-nao-36773>