An toàn Phần mềm
Phần mềm độc hại

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Phần mềm độc hại

- Các phần mềm độc hại thường gặp
- Các biện pháp ngăn chặn

An toàn Phần mềm

- Phần mềm độc hại
  - Các phần mềm độc hại thường gặp
  - Các biện pháp ngăn chặn

Phần mềm độc hại

- Chạy theo chủ định của người lập trình ra nó
- Chạy và phản ứng theo cách bất thường, không trông đợi từ phía người dùng
- Ẩn náu trong hệ thống, hoặc gắn vào các phần mềm không độc hại
- Có thể làm được mọi thứ mà một phần mềm có thể làm

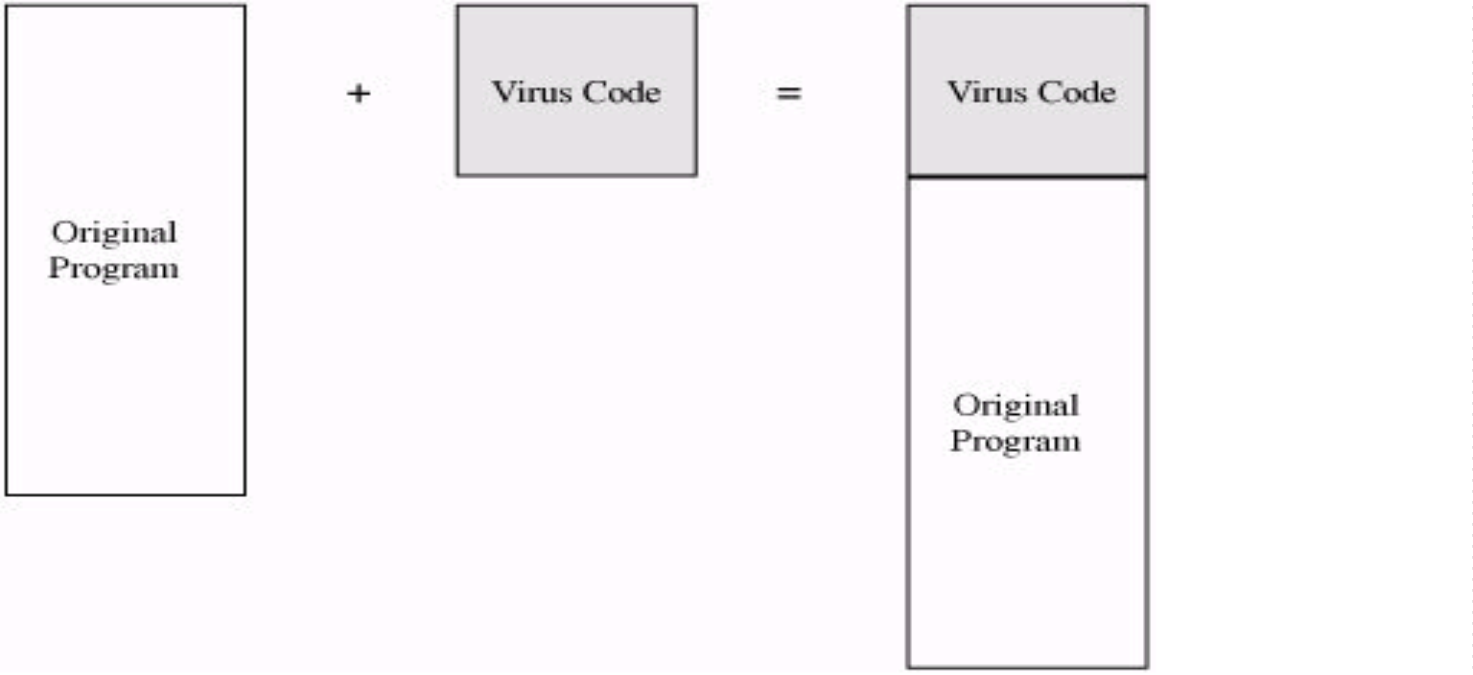
Các phần mềm độc hại thường gặp

- Vi rut (Virus)
  - Gắn vào một chương trình, phát tán bản sao ra khác chương trình khác
- Trojan horse
  - Có các tính năng bất thường
- Bom logic (Logic bomb)
  - Phát động khi điều kiện được thỏa mãn
- Bom thời gian (Time bomb)
  - Phát động khi đến hạn thời gian
- Trapdoor
  - Cho phép truy nhập trái phép các tính năng
- Sâu (Worm)
  - Phát tán bản sao qua mạng
- Thỏ (Rabbit)
  - Nhân bản đến khi không còn tài nguyên

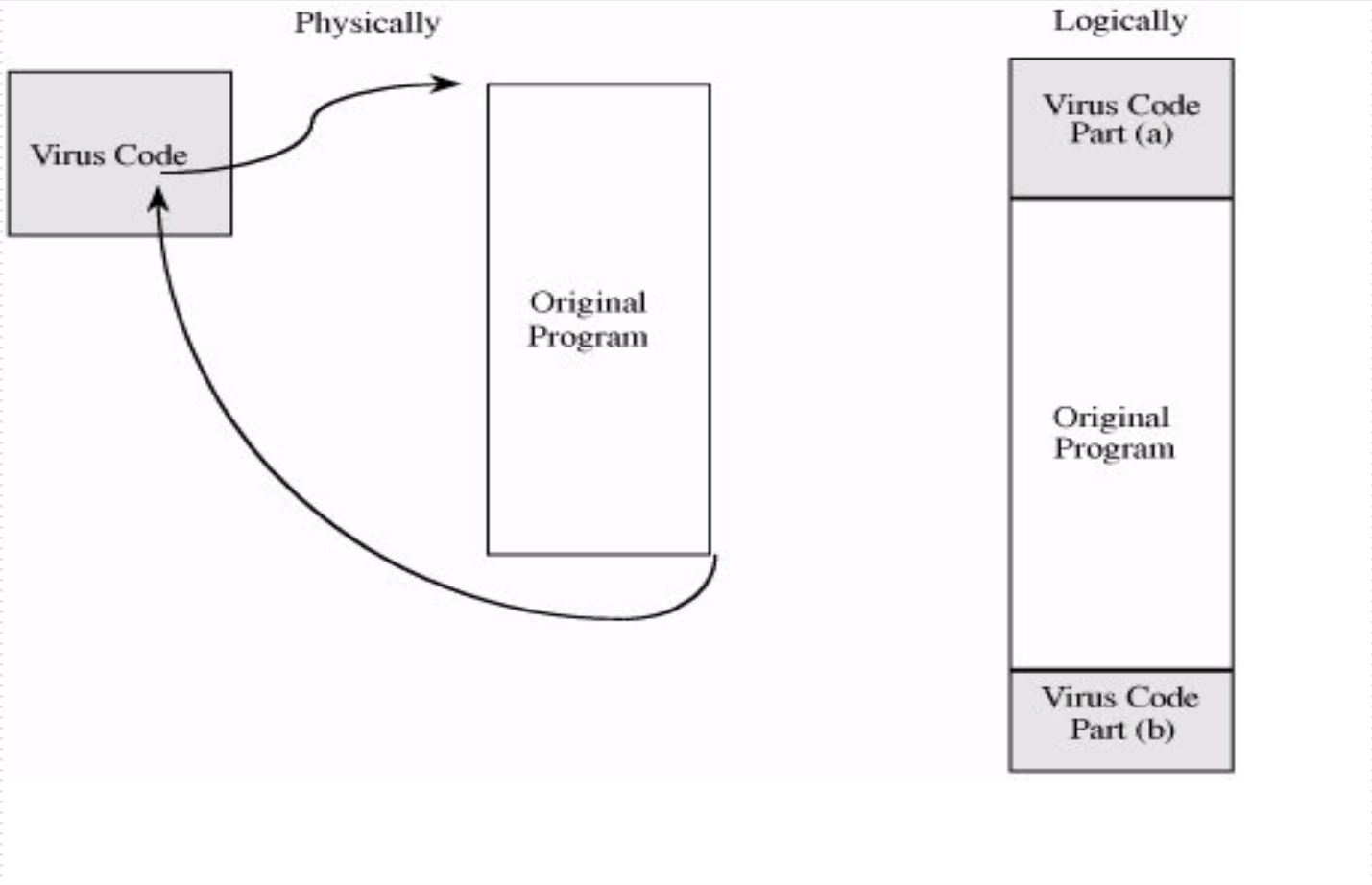
Virus

- Mã virus đính kèm mã một chương trình khác
- Virus chỉ gây hại khi được kích hoạt
  - Virus chạy khi mở tệp đính kèm trong e-mails, tệp ảnh, tệp đồ họa
- Virus chạy cùng với một chương trình khác (đã bị thay đổi mã) kích hoạt bởi người dùng

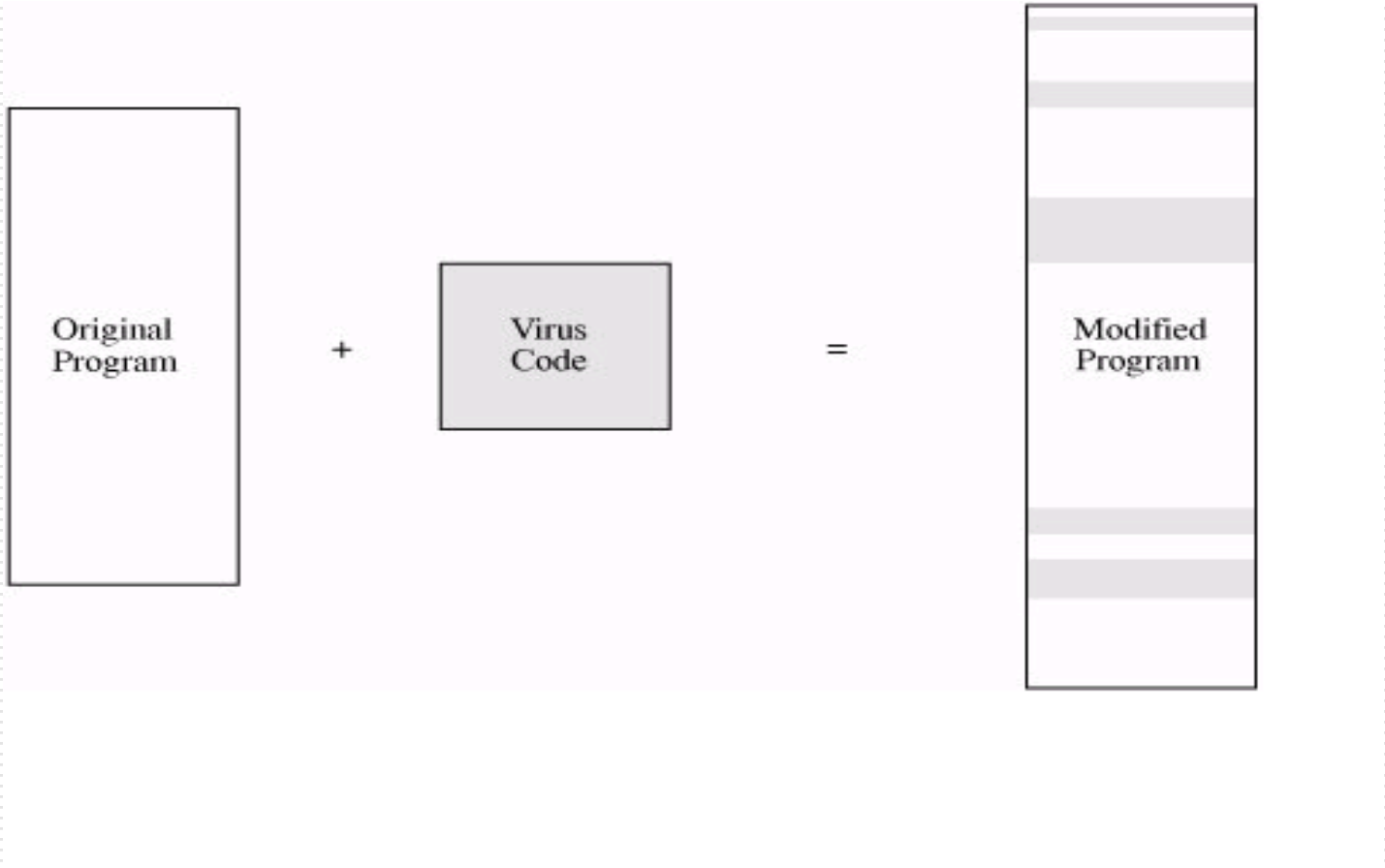
Mã virus nối vào mã chương trình



Mã virus bao quanh mã chương trình



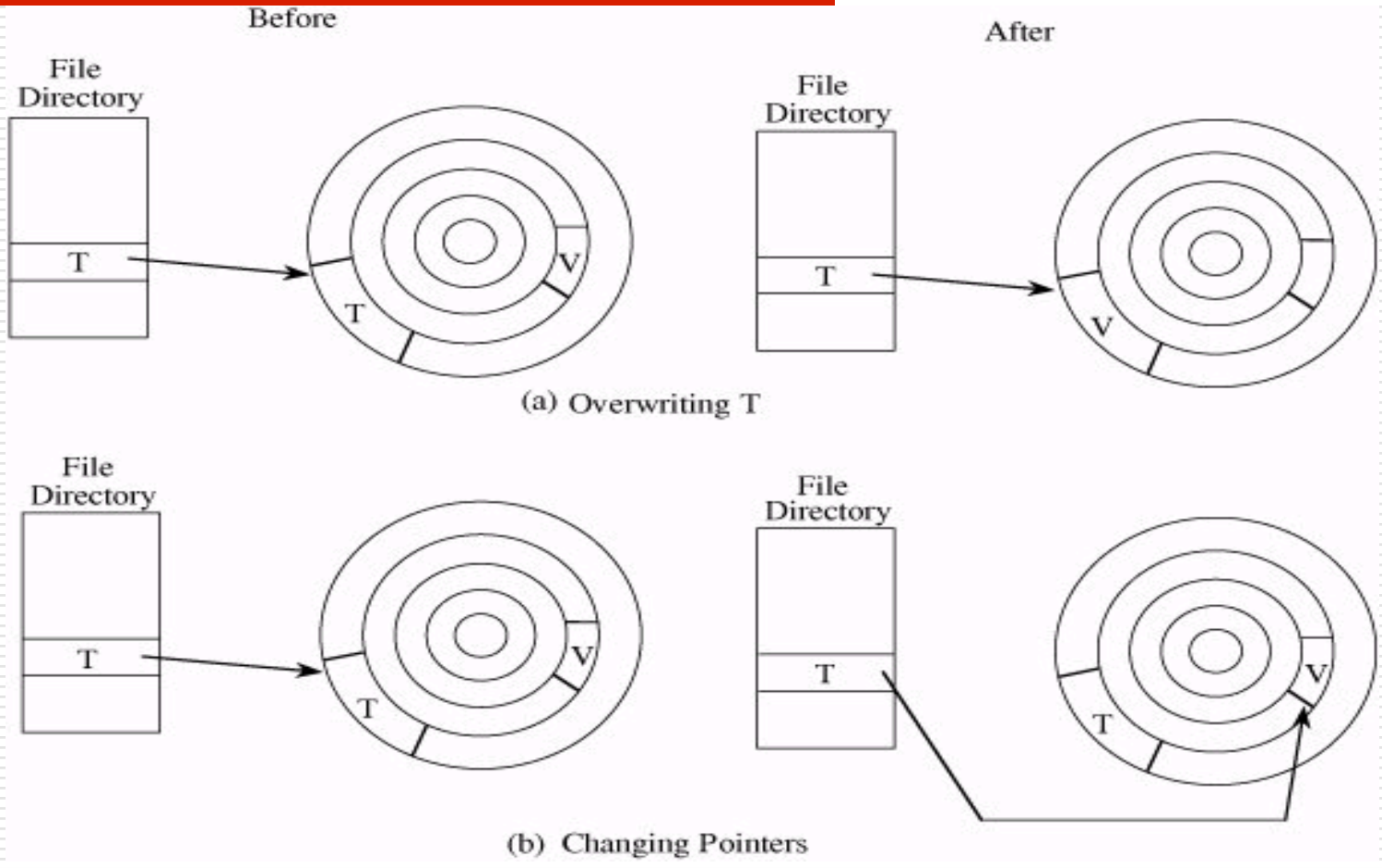
Mã virus tích hợp vào mã chương trình



Virus tài liệu

- Tài liệu
  - Slide
  - Spreadsheet
- Lệnh
  - Macro
  - Biến
  - Thủ tục
  - Truy nhập tệp, CSDL
  - Gọi hệ thống

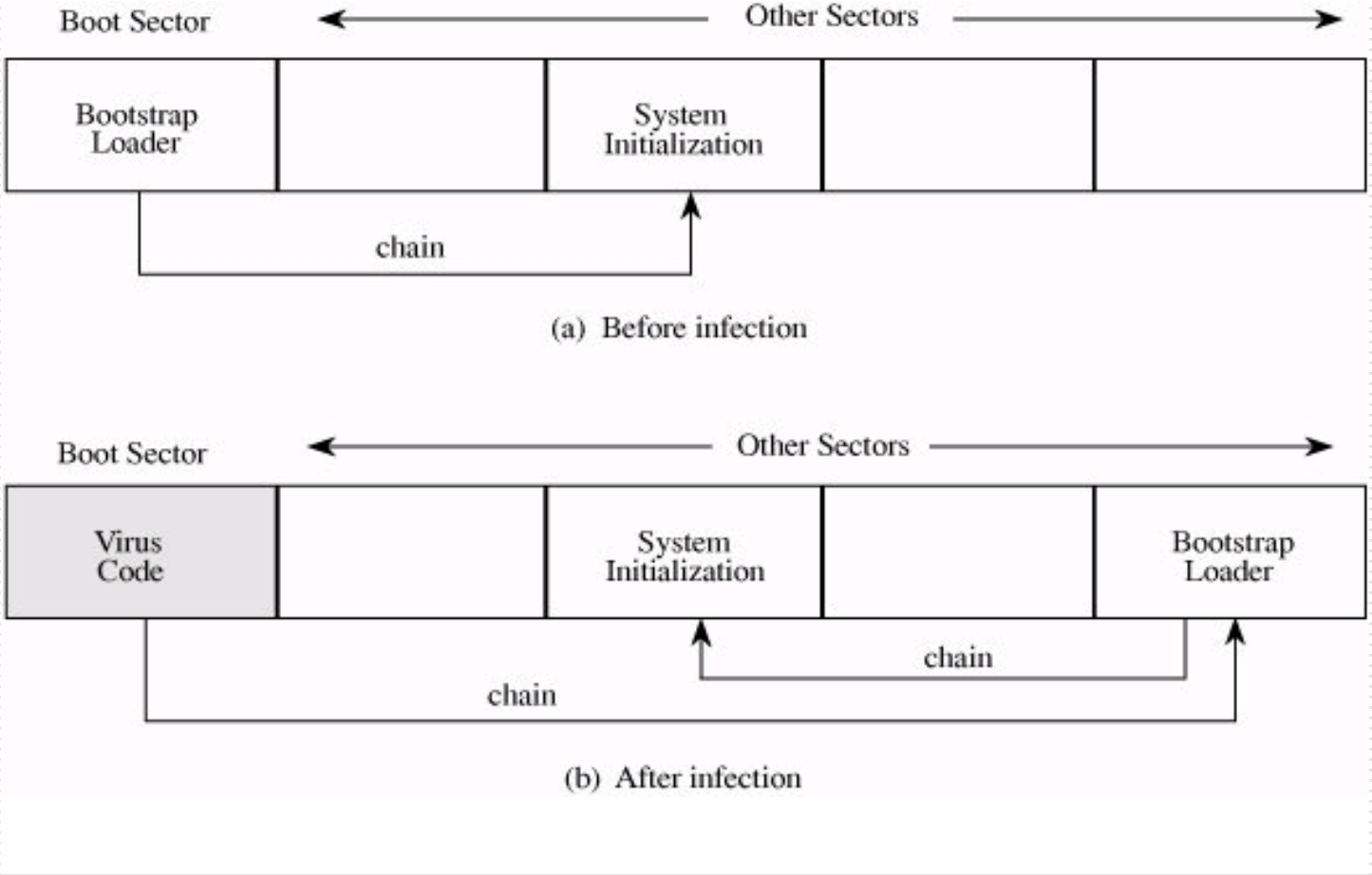
Virus đoạt quyền kiểm soát



Nơi ẩn náu Virus

- Vùng Boot (Boot Sector)
- Bộ nhớ (Memory-Resident)
- Ứng dụng (Application Program)
- Thư viện (Library)
- …

Boot Sector Virus



Dấu hiệu nhận biết Virus

- Mã virus có kiểu mẫu đặc biệt
  - Có thể nhận biết các đoạn mã của từng loại virus
  - Chương trình nhiễm virus sẽ lớn hơn chương trình ban đầu
  - Vị trí virus đính kèm không thay đổi
- Cách thức phát động và hậu quả

Cách thức phát động và hậu quả

- Đính kèm tệp
  - Thay đổi thư mục, tệp
- Xâm nhập trong bộ nhớ
  - Thay đổi bảng tín hiệu ngắt
  - Tải lên bộ nhớ khi có tín hiệu ngắt
- Lây lan qua đĩa
  - Đón tín hiệu ngắt, gọi hàm hệ thống
  - Thay đổi tệp hệ thống/tệp thực thi
- Phát tán lây lan
  - Lây lan vào vùng Boot, chương trình hệ thống, chương trình và dữ liệu
- Ẩn náu
  - Đón gọi hệ thống
  - Thay đổi kết quả
- ...

Các biện pháp ngăn chặn

- Sử dụng phần mềm thương mại từ nguồn tin cậy
- Kiểm thử phần mềm trên một máy tính/hệ thống tách biệt
- Mở tệp đính kèm chỉ khi nào biết rõ nguồn gốc
- Lưu ở nơi an toàn một phiên bản có thể tái tạo của hệ thống đang sử dụng
- Sử dụng phần mềm quét diệt virus

Một số ngộ nhận về virus

- Virus chỉ lây nhiễm trên các hệ thống MS Windows
- Virus không thể thay đổi các file “hidden” hoặc “read-only”
- Virus chỉ xuất hiện trong tệp dữ liệu, chương trình
- Virus chỉ phát tán thông qua qua đĩa, e-mail
- Virus không thể tồn tại trong bộ nhớ sau khi reboot power off/on
- Virus lây nhiễm trên phần cứng

Sâu

- Nhân bản và phát tán
  - Lây lan qua đĩa
  - Khai thác lỗi tràn bộ đệm của máy chủ Web (Microsoft IIS)
- Chạy như một chương trình độc lập
- Mục tiêu
  - Bôi nhọ trang Web
  - Phá hoại
  - Tấn công DOS, DDOS

Sự xuất hiện của sâu máy tính

- 02/11/1988: Morris
- 13/07/2001: Code Red
- 09/2001: Nimda
- 25/01/2003: Slammer
- 07/2010: Stuxnet

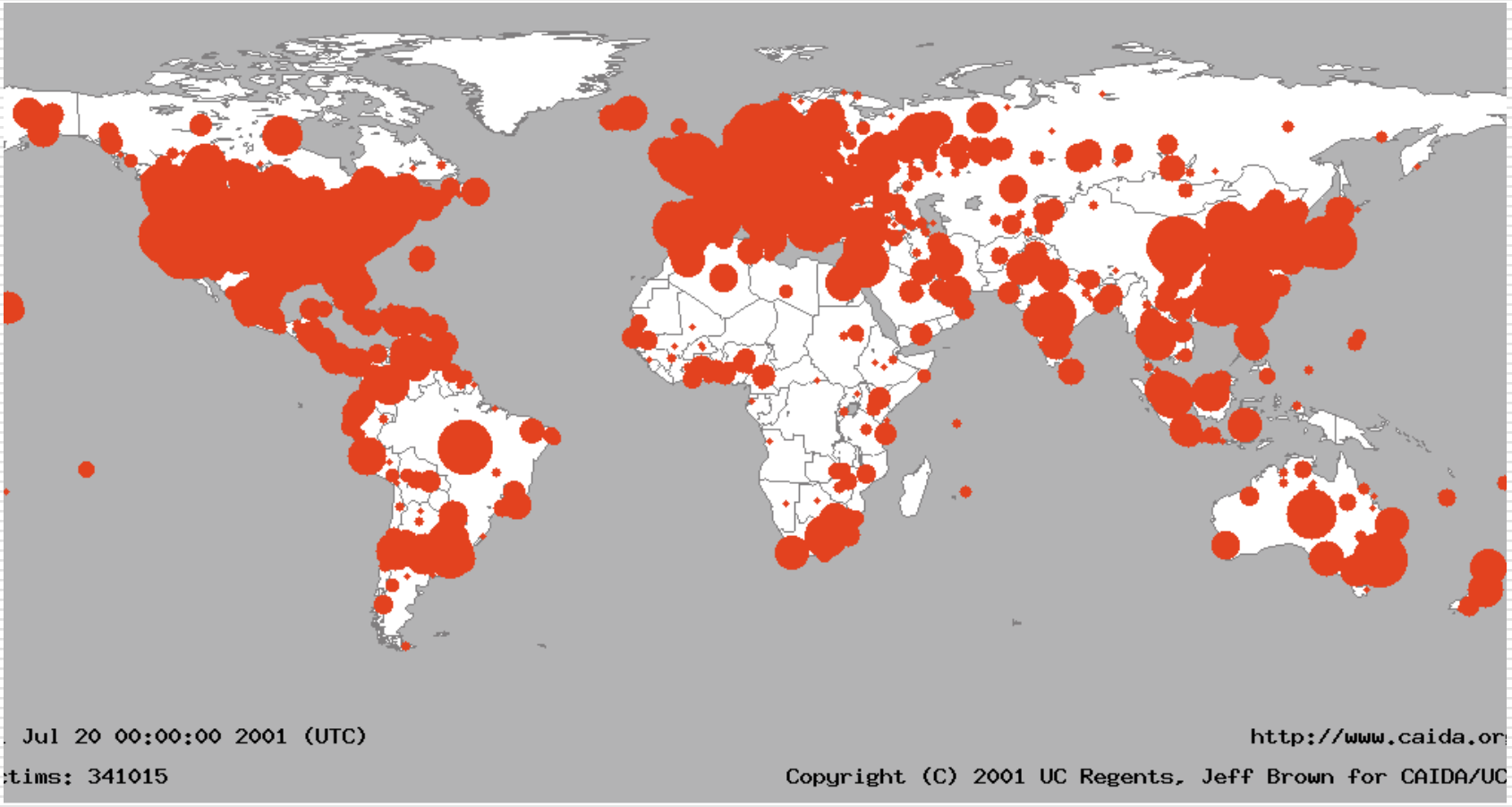
Code Red

/default.ida?
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%u
cdb3%u7801%u9090%u6858
%ucbd3%u7801%u9090%u9090%u8190%u00c3%u
0003%ub00%u531b%u53ff %u0078%u0000%u00=a
HTTP/1.0

Code Red

- Xuất hiện 13/07/2001
- Phát động
  - Kiểm tra ngày tháng năm
  - Từ ngày 1 đến 20 của tháng: phát tán
  - Từ ngày 21 đến cuối tháng: tấn công
    - Tràn kết nối vào *www.whitehouse.gov*
- Phát tán: vét cạn không gian địa chỉ IP trên 32 bit bằng cách tạo hạt giống ngẫu nhiên

Sau khi lây lan



Ngăn chặn Code Red

- Nhà trắng đưa ra biện pháp ngăn chặn Code Red bằng cách thay đổi địa chỉ IP của *www.whitehouse.gov*
- Code Red sẽ chết đối với những ngày từ ngày 21 đến cuối tháng
- Nhưng nếu hạt giống được Code Red chọn hợp lý thì vẫn có khả tiếp tục tấn công

Code Red 2

- Xuất hiện 04/08/2001
- Khai thác máy chủ Microsoft IIS
- Hoạt động như root backdoor, chống reboot
- Hậu quả: đánh sập Win NT/2K
- Vét cạn địa chỉ bằng cách ưu tiên địa chỉ lân cận

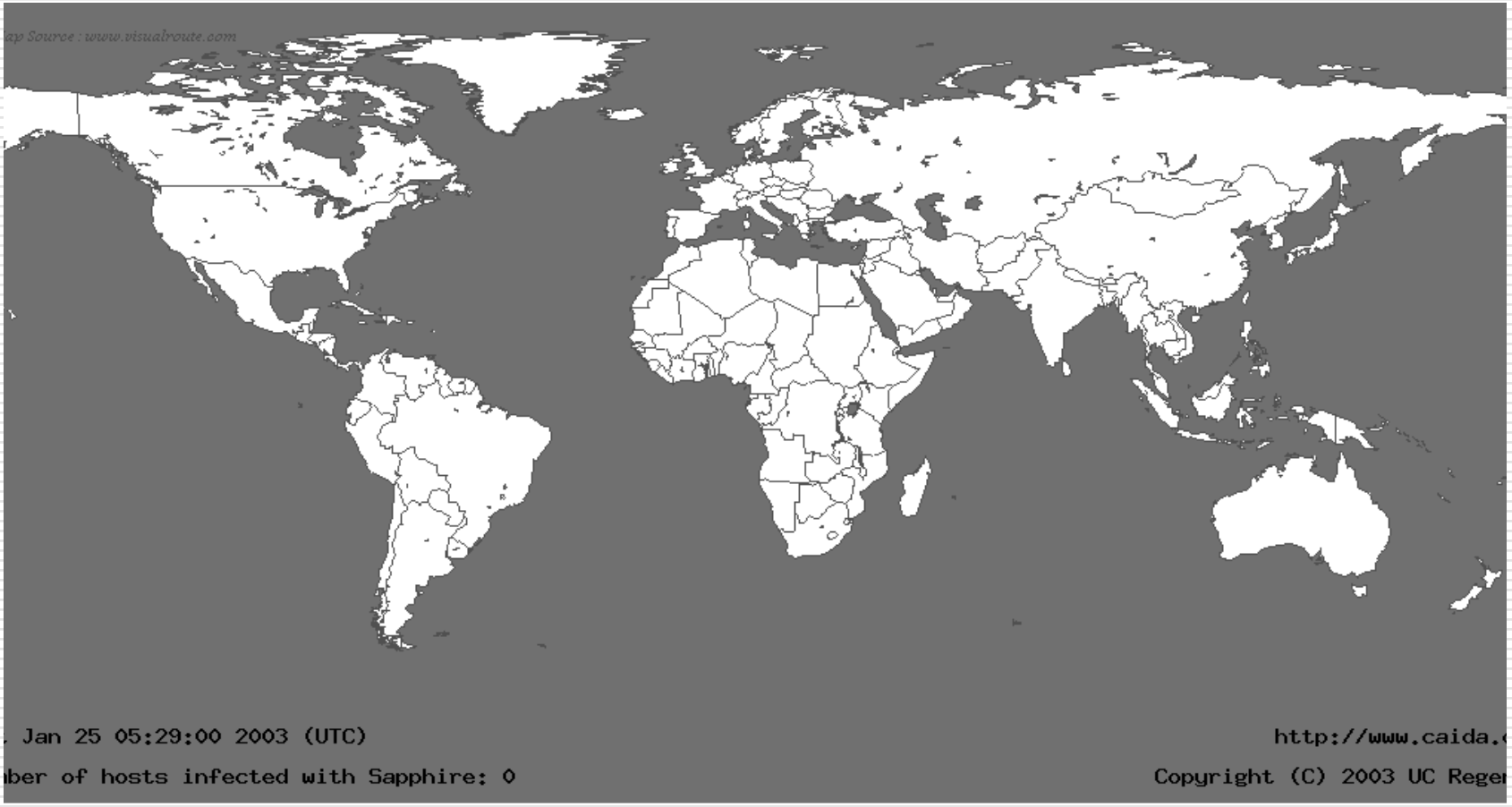
Nimda

- Xuất hiện 18/09/2001
- Phát tán
  - Tấn công máy chủ IIS như Code Red
  - Nhân bản qua email
  - Nhân bản qua mạng mở
  - Thay đổi nội dung các trang Web trên máy chủ bị lây nhiễm

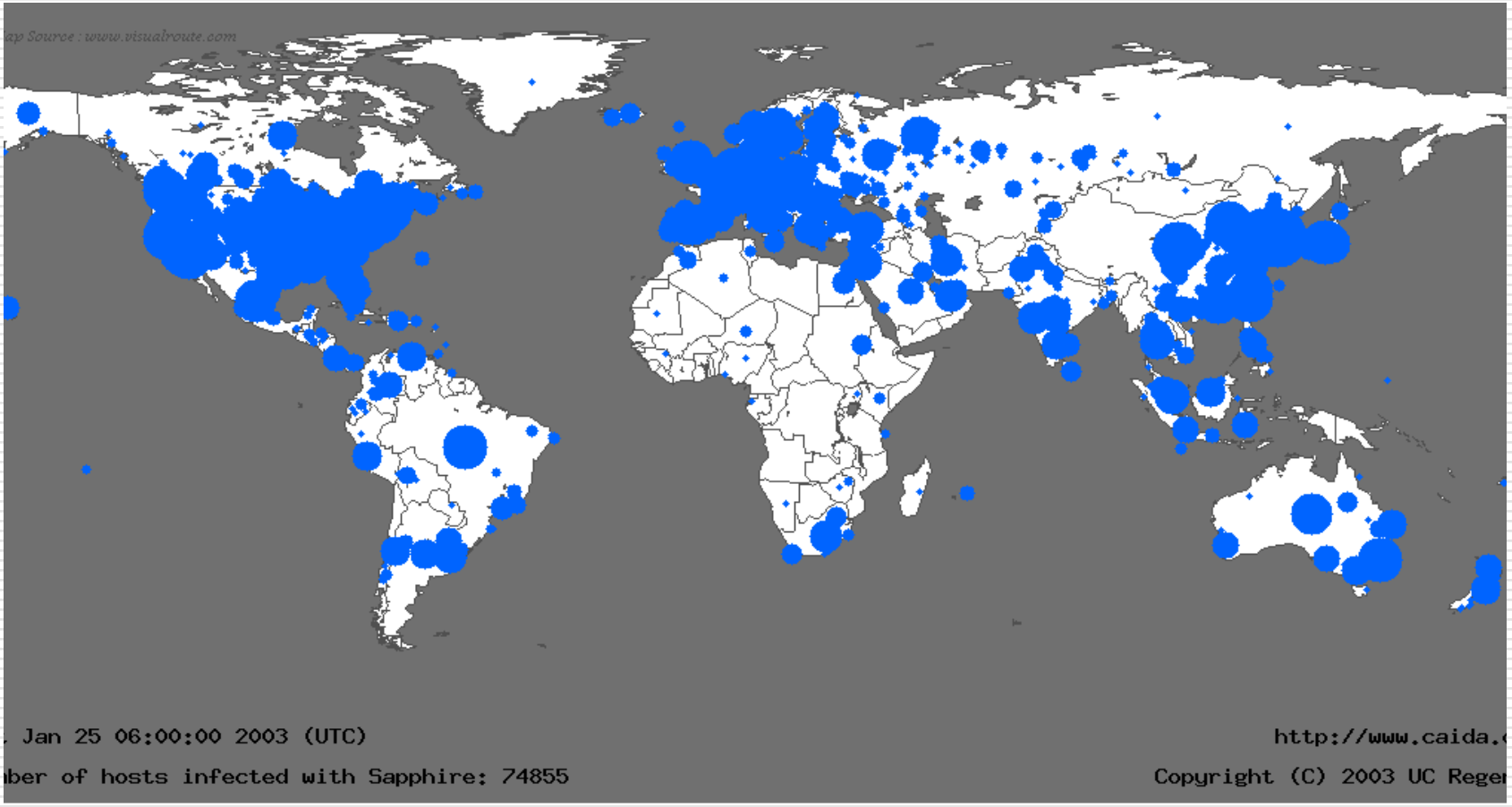
Slammer

- Xuất hiện 25/01/2003
- Phát tán
  - Khai thác các kết nối UDP
  - Sâu (376 bytes) vừa trong một gói tin
  - Tạo IP ngẫu nhiên và gửi chính nó
  - Tốc độ gửi nhanh, hàng trăm gói tin trong một giây
- Lây nhiễm 75 000 máy trong 30 phút, sâu lây lan với tốc độ nhanh nhất

Trước khi lây lan



30 phút sau khi lây lan



Stuxnet

- Xuất hiện 07/2010
- Phát tán
  - Đầu tiên qua USB
  - Phát tán qua mạng sử dụng Windows RPC
- Mục tiêu
  - Hệ thống SCADA: sử dụng trong các hệ thống kiểm soát điều khiển công nghiệp, năng lượng

Stuxnet

- Hoạt động
  - Quan sát hoạt động của hệ thống điều khiển biến tần
  - Nếu hệ thống hoạt động ở tần số 807-1210Hz
    - Máy gia tốc làm ở IRAN (và Phần Lan) dùng làm nặng Urunium để chế tạo cho bom nguyên tử
  - Tăng tấn số một cách từ từ lên 1410Hz
    - Làm hỏng máy gia tốc