

TROJAN, BACKDOOR VIRUS VÀ WORM

Khoa Công nghệ thông tin và Truyền thông
Trường Đại học Cần Thơ

Phần A

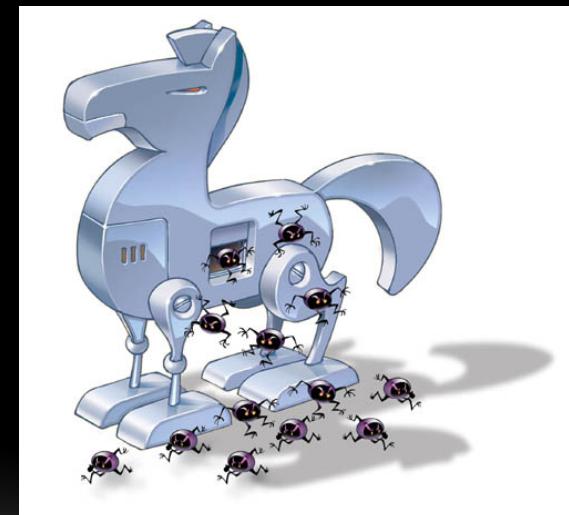
TROJAN VÀ BACKDOOR

TROJAN VÀ BACKDOOR

- Trojan và backdoor là gì.
- Kênh công khai và bí mật.
- Các loại trojan.
- Biện pháp đối phó trojan.
- Tổng kết.

TROJAN

- Trojan là một chương trình độc hại được cải trang như một chương trình vô hại.
 - Trojans được sử dụng để đánh cắp dữ liệu hoặc phá hoại hệ thống mục tiêu.
- ❖ Trojan thường được gắn vào:
- Phần mềm miễn phí
 - Công cụ gỡ bỏ phần mềm gián điệp
 - Phần mềm tối ưu hóa hệ thống
 - Âm nhạc, hình ảnh, trò chơi và video



BACKDOOR

- Backdoor là một chương trình cho phép hacker truy cập trở lại hệ thống sau đó.
- Backdoor có thể được nhúng vào trong một trojan độc hại
- Kỹ thuật phổ biến nhất để che giấu backdoor trong hệ điều hành Windows là thêm một dịch vụ mới có vẻ vô hại để chạy backdoor này.

KÊNH CÔNG KHAI VÀ BÍ MẬT

- Hacker có thể giao tiếp với backdoor thông qua các kênh công khai hoặc bí mật.
 - Kênh công khai (overt channel) là cách thông thường và hợp pháp mà các chương trình giao tiếp trong một hệ thống máy tính hoặc mạng.
 - Kênh bí mật (covert channel) sử dụng các chương trình hay các kênh giao tiếp theo một cách không theo quy chuẩn hoặc dự kiến.

CÁC LOẠI TROJAN PHỔ BIẾN

- **Remote Access Trojans (RATs)**: Được sử dụng để truy cập từ xa vào một hệ thống.
- **Data-Sending Trojans**: Được sử dụng để tìm dữ liệu trên một hệ thống và gửi dữ liệu cho hacker.
- **Destructive Trojans**: Được sử dụng để xóa hoặc làm hỏng các tập tin trên một hệ thống.
- **Denial-of-Service Trojans**: Được sử dụng để khởi động một cuộc tấn công từ chối dịch vụ.

CÁC LOẠI TROJAN PHỔ BIẾN

- **Proxy Trojans:** Sử dụng máy nạn nhân làm điểm xuất phát để truy cập hoặc phá hoại các hệ thống khác.
- **FTP Trojans:** Được sử dụng để tạo ra một máy chủ FTP nhằm sao chép các tập tin vào một hệ thống.
- **Security Software Disabler Trojans:** Được sử dụng để ngăn chặn phần mềm diệt virus.

CÁC LOẠI TROJAN



CÁCH PHÁT TÁN TROJAN

- Trojan được đóng gói cùng với các gói phần mềm khác. Khi người dùng tải gói phần mềm này về, trojan sẽ được tự động cài đặt lên hệ thống.
- Nạn nhân bị bẫy bởi những pop-up quảng cáo. Cho dù có nhấn YES hay NO thì trojan vẫn được cài vào máy.
- Hacker gửi trojan đính kèm trong email.
- Thỉnh thoảng khi nạn nhân nhấp chuột vào các loại tập tin khác như thiệp chúc mừng, phim, ảnh khiêu dâm thì trojan sẽ được âm thầm cài đặt lên hệ thống.

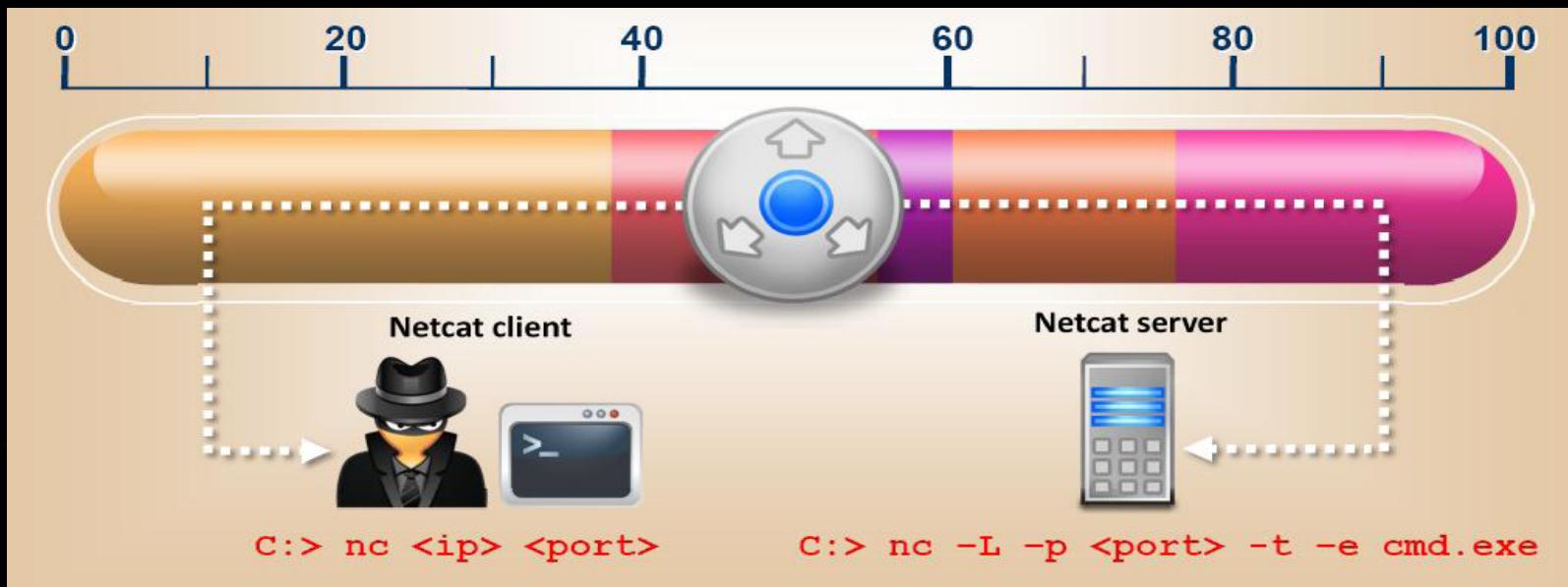
CÁCH PHÁT TÁN TROJAN



Ví dụ về cách đóng gói và phát tán Trojan

VÍ DỤ: COMMAND SHELL TROJAN

- Command Shell Trojan cho phép điều khiển từ xa một shell trên máy nạn nhân.
- Máy chủ trojan được cài trên máy của nạn nhân, trong đó nó mở một cổng cho hacker kết nối đến.
- Máy trạm trojan được cài trên máy hacker cho phép chạy lệnh shell trên máy nạn nhân.



COMMAND SHELL TROJAN: NCAT

The image shows two separate Windows Command Prompt windows. The top window has its title bar set to 'C:\Windows\system32\cmd.exe - ncat.exe -l -k -p 8888 -t -e cmd.exe'. It contains the command 'C:\Users\Phi\Downloads>ncat.exe -l -k -p 8888 -t -e cmd.exe'. The bottom window has its title bar set to 'C:\Windows\system32\cmd.exe - ncat localhost 8888'. It displays the output of the ncat listener, including the Windows version (Version 6.1.7601), copyright information (Copyright © 2009 Microsoft Corporation. All rights reserved.), and a directory listing of the 'Downloads' folder on drive C. The directory listing includes files like 'LANsurveyor-v10-Eval.zip', 'ManageEngine_OpManager.exe', 'ManageEngine_OpManager_64b', 'nc110.tgz', 'ncat-portable-5.59BETA1', 'ncat-portable-5.59BETA1.zip', 'ncat.exe', 'nmap-7.12-setup.exe', and 'test'.

```
C:\Windows\system32\cmd.exe - ncat.exe -l -k -p 8888 -t -e cmd.exe
C:\Users\Phi\Downloads>ncat.exe -l -k -p 8888 -t -e cmd.exe

C:\Windows\system32\cmd.exe - ncat localhost 8888
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation. All rights reserved.

C:\Users\Phi\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9044-779A

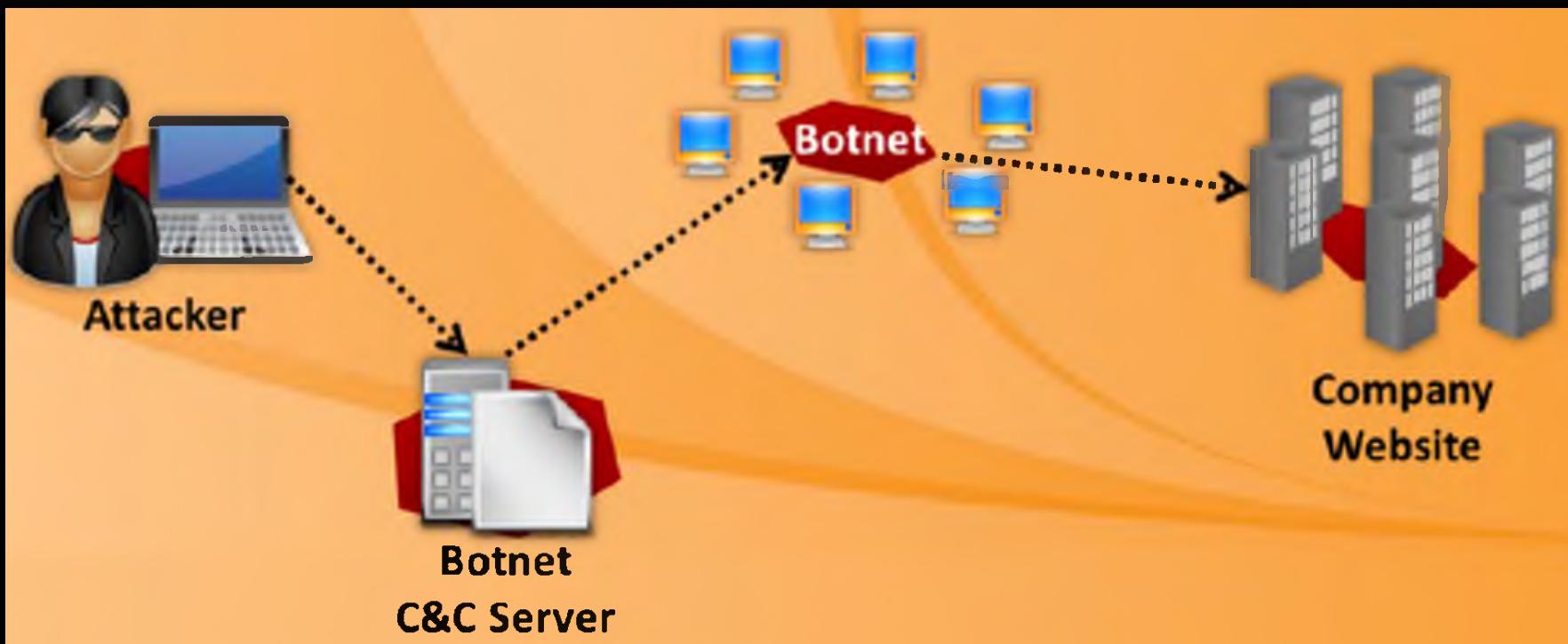
 Directory of C:\Users\Phi\Downloads

07/11/2016  12:02 PM    <DIR>
07/11/2016  12:02 PM    <DIR>
07/11/2016  12:29 AM           31,143,685 LANsurveyor-v10-Eval.zip
07/11/2016  01:21 AM           105,306,064 ManageEngine_OpManager.exe
07/11/2016  01:20 AM           107,302,040 ManageEngine_OpManager_64b
07/11/2016  11:39 AM            75,267 nc110.tgz
07/11/2016  11:48 AM    <DIR>      ncat-portable-5.59BETA1
07/11/2016  11:48 AM           666,933 ncat-portable-5.59BETA1.zip
06/30/2011  01:52 PM           1,667,584 ncat.exe
07/10/2016  01:57 PM           26,426,084 nmap-7.12-setup.exe
07/11/2016  12:02 PM    <DIR>      test
```

VÍ DỤ: BOTNET TROJAN

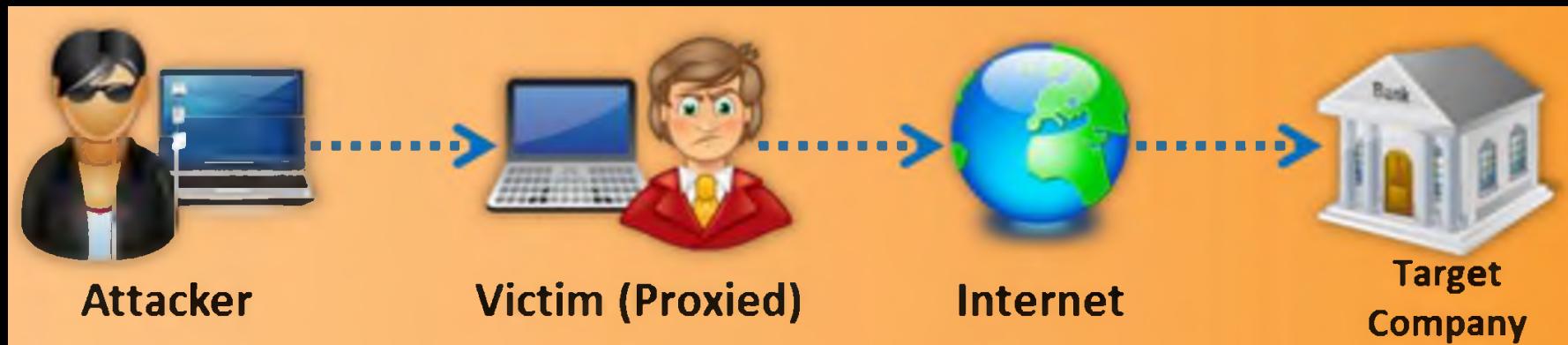
- Botnet Trojan lây nhiễm lên một số lượng lớn các máy tính trên một phạm vi địa lý rộng lớn, tạo ra một mạng bot được điều khiển thông qua trung tâm Command and Control (C&C)
- Botnet được sử dụng để phát động các cuộc tấn công như: từ chối dịch vụ (DoS), spamming, ...

VÍ DỤ: BOTNET TROJAN



VÍ DỤ: PROXY SERVER TROJAN

- Proxy server Trojan cho phép hacker sử dụng từ xa máy tính của nạn nhân như một Proxy để kết nối Internet.
- Proxy server Trojan, khi bị nhiễm, bắt đầu ăn một Proxy server trên máy tính của nạn nhân.



VÍ DỤ: FTP TROJAN

- FTP Trojan cài đặt FTP server trên máy nạn nhân để mở cổng FTP.
- Hacker có thể kết nối đến máy của nạn nhân bằng cách sử dụng cổng FTP để tải bất kỳ tập tin nào tồn tại trên máy tính của nạn nhân.



BIỆN PHÁP PHÒNG CHỐNG TROJAN

- Không tải về và thực thi các ứng dụng từ các nguồn không tin cậy
- Không mở tập tin đính kèm email nhận được từ những người gửi không rõ ràng.
- Cài đặt các bản vá lỗi và cập nhật bảo mật cho hệ điều hành và các ứng dụng.
- Quét đĩa CD/DVD và USB trước khi sử dụng.
- Chặn tất cả các cổng không sử dụng tại các máy chủ và tường lửa.