CHƯƠNG 3

PHẦN MỀM MÃ ĐỘC

Bộ môn: Tin học quản lý
Khoa Thống kê – Tin học
Đại học Kinh Tế - Đại học Đà Nẵng

NỘI DUNG CHƯƠNG 3

1. Tổng quan về phần mềm mã độc
2. Giải pháp tổng thể phòng chống phần mềm mã độc
3. Phương pháp phát hiện và loại trừ phần mềm mã độc

1. Tổng quan về phần mềm mã độc

1. Khái quát về phần mềm mã độc
2. Phân loại phần mềm mã độc và tác hại của phần mềm mã độc

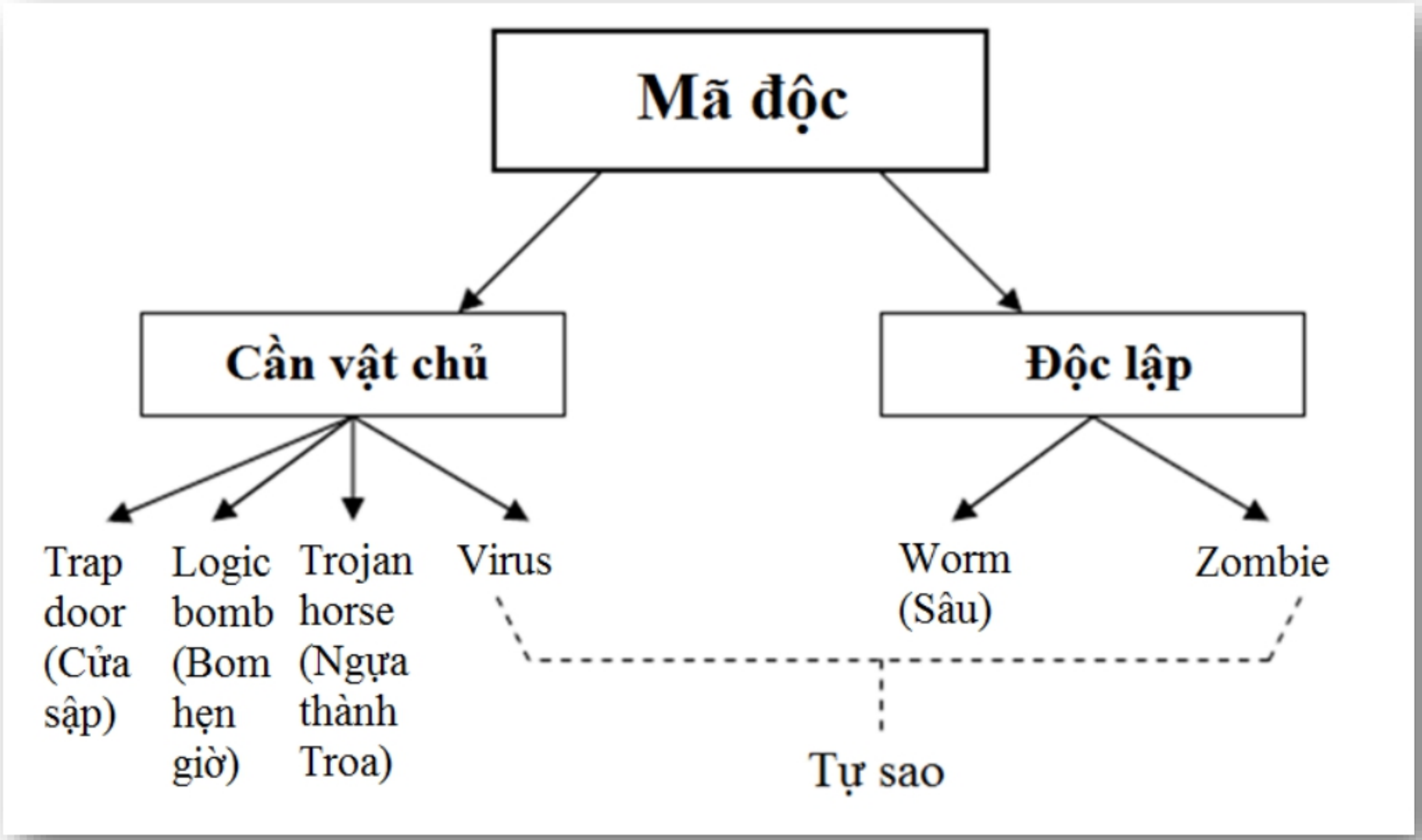
1.1. Khái quát về phần mềm mã độc

- Để tấn công/thâm nhập mạng, hacker thường sử dụng các ‘trợ thủ’ như virus, worm, trojan horse, backdoor…
- Mã độc (malicious code): tập mã thực thi tự chủ, không đòi hỏi sự can thiệp của hacker
- Các bước tấn công/thâm nhập mạng:
  - Hacker thiết kế mã độc
  - Hacker gửi mã độc đến máy đích
  - Mã độc đánh cắp dữ liệu máy đích, gửi về cho hacker
  - Hacker tấn công hệ thống đích

1.2. Phân loại phần mềm mã độc – Tác hại

- Phân loại mã độc theo đặc trưng thi hành:
  - Lệ thuộc ứng dụng chủ (need to host)
  - Thực thi độc lập (standalone)
- Phân loại mã độc theo khả năng tự sao:
  - Tự sao
  - Không tự sao

1.2. Phân loại phần mềm mã độc – Tác hại



1.2. Phân loại phần mềm mã độc – Tác hại

❑ Cửa sập (Trap door)

- ❖ "Cửa vào" bí mật của các chương trình
- ❖ Cho phép những người biết "cửa vào" có thể truy cập, bỏ qua các thủ tục an ninh thông thường
- ❖ Đã được sử dụng phổ biến bởi các nhà phát triển
- ❖ Là mối đe dọa trong các chương trình, cho phép khai thác bởi những kẻ tấn công
- ❖ Rất khó để chặn trong HĐH
- ❖ Đòi hỏi phát triển & cập nhật phần mềm tốt

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Bom hẹn giờ (Logic bomb)

- ❖ Mã được nhúng trong các chương trình hợp lệ
- ❖ Đoạn mã tự kích hoạt khi thỏa điều kiện hẹn trước (ngày tháng, thời gian...)
- ❖ Trước khi thoát khỏi hệ thống, hacker thường cài lại bom hẹn giờ nhằm xóa mọi chứng cứ, dấu vết thâm nhập
- ❖ Khi được kích hoạt, thường gây thiệt hại cho hệ thống: sửa đổi / xóa các file / đĩa
- ❖ Kỹ thuật bom hẹn giờ cũng được virus máy tính khai thác phổ biến: virus Friday, Chernobyl (24/04), Michelangelo (06/03), Valentine...

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Ngựa thành Troa (Trojan)

- ❖ Chương trình có ẩn tác dụng phụ, thường là bề ngoài hấp dẫn như trò chơi, nâng cấp phần mềm
- ❖ Khi chạy thực hiện một số tác vụ bổ sung:
  - Cho phép kẻ tấn công truy cập gián tiếp
- ❖ Thường được sử dụng để truyền bá một virus/sâu hoặc cài đặt một backdoor
- ❖ Hoặc đơn giản chỉ để phá hủy dữ liệu

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Ngựa thành Troa và cổng

- ❖ Mỗi Ngựa thành Troa sử dụng cổng Port(s) làm dấu hiệu nhận dạng và liên lạc với hacker
- ❖ Quét cổng (0-65535) trên máy đích để thu thập các thông tin: danh sách cổng chuẩn, dịch vụ sử dụng, hệ điều hành sử dụng, các ứng dụng đang sử dụng, tình trạng an ninh hệ thống…
- ❖ Ví dụ: Nếu cổng 80 mở, máy tính đang kết nối vào dịch vụ HTTP

1.2. Phân loại phần mềm mã độc – Tác hại

- **Ngựa thành Troa - hacker**
  - Báo cáo tình hình, thông tin hệ thống cho hacker
  - Nhận nhiệm vụ từ hacker thông qua cổng trjPort(s)
  - Các trojan tiêu biểu: Back Orifice, NetBus, QAZ...

Trojan Name	Protocol	Port Number
Back Orifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Sockets de Troie	TCP	5000, 5001 or 50505
Masters Paradise	TCP	3129, 40421, 40422, 40423 and 40426

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Virus máy tính

- ❖ Đoạn mã thực thi ghép vào chương trình chủ và giành quyền điều khiển khi chương trình chủ thực thi
- ❖ Virus được thiết kế nhằm nhân bản, tránh né sự phát hiện, phá hỏng/thay đổi dữ liệu, hiển thị thông điệp hoặc làm cho hệ điều hành hoạt động sai lệch

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Hoạt động của virus

❖ Các pha:

- Không hoạt động - chờ đợi sự kiện kích hoạt
- Lan truyền - sao chép mình tới chương trình/đĩa
- Kích hoạt – theo sự kiện để thực thi payload
- Thực thi – theo payload

❖ Chi tiết phụ thuộc các máy/HĐH cụ thể

- Khai thác các đặc trưng/điểm yếu

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Cấu trúc của virus

```
program V :=
    {goto main;
    1234567;
    subroutine infect-executable :=     {loop:
                    file := get-random-executable-file;
                    if (first-line-of-file = 1234567) then goto loop
                    else prepend V to file; }
   subroutine do-damage :=     {whatever damage is to be done}
   subroutine trigger-pulled := {return true if some condition holds}
   main: main-program :=       {infect-executable;
                                if trigger-pulled then do-damage;
   next:                        goto next;}
}
```

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Các kiểu virus

- ❖ Có thể phân loại theo cách tấn công của chúng
  - Virus ký sinh
  - Virus thường trú bộ nhớ
  - Virus boot sector
  - Lén lút
  - Virus đa hình
  - Virus macro

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Virus ký sinh

- ❖ Loại virus ký sinh vào các tập tin thi hành (com, exe, pif, scr, dll...) trên hệ thống đích
- ❖ Ứng dụng chủ (host application) có thể bị nhiễm virus vào đầu file, giữa file hoặc cuối file
- ❖ Khi hệ thống thi hành một ứng dụng chủ nhiễm:
  - Pay-load nắm quyền sử dụng CPU
  - Vir-code thực thi các thủ tục phá hoại, sử dụng dữ liệu trong Vir-data
  - Trả quyền sử dụng CPU cho ứng dụng chủ

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Boot virus

- ❖ Boot-virus: loại virus nhiễm vào mẫu tin khởi động (boot record - 512 byte) của tổ chức đĩa
- ❖ Multi-partite: loại virus tổ hợp tính năng của virus ký sinh và boot virus, nhiễm cả file lẫn boot sector

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Macro virus

- ❖ Đính vào các tập tin dữ liệu có sử dụng macro, data virus tự động thực hiện khi tập dữ liệu nhiễm được mở bởi ứng dụng chủ
- ❖ Các data virus quen thuộc:
  - Microsoft Word Document: doc macro virus
  - Microsoft Excel Worksheet: xls macro virus
  - Microsoft Power Point: ppt macro virus
  - Adobe Reader: pdf script virus
  - Visual Basic: vb script virus
  - Java: java script virus
  - Startup file: bat virus…

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Email virus

- ❖ Lây lan bằng cách sử dụng email với tập tin đính kèm có chứa một virus macro
  - Ví dụ Melissa
- ❖ Kích hoạt khi người dùng mở tập tin đính kèm
- ❖ Hoặc tệ hơn, ngay cả khi thư xem bằng cách sử dụng tính năng kịch bản trong email agent
- ❖ Thường nhắm vào Microsoft Outlook mail agent & các tài liệu Word/Excel

1.2. Phân loại phần mềm mã độc – Tác hại

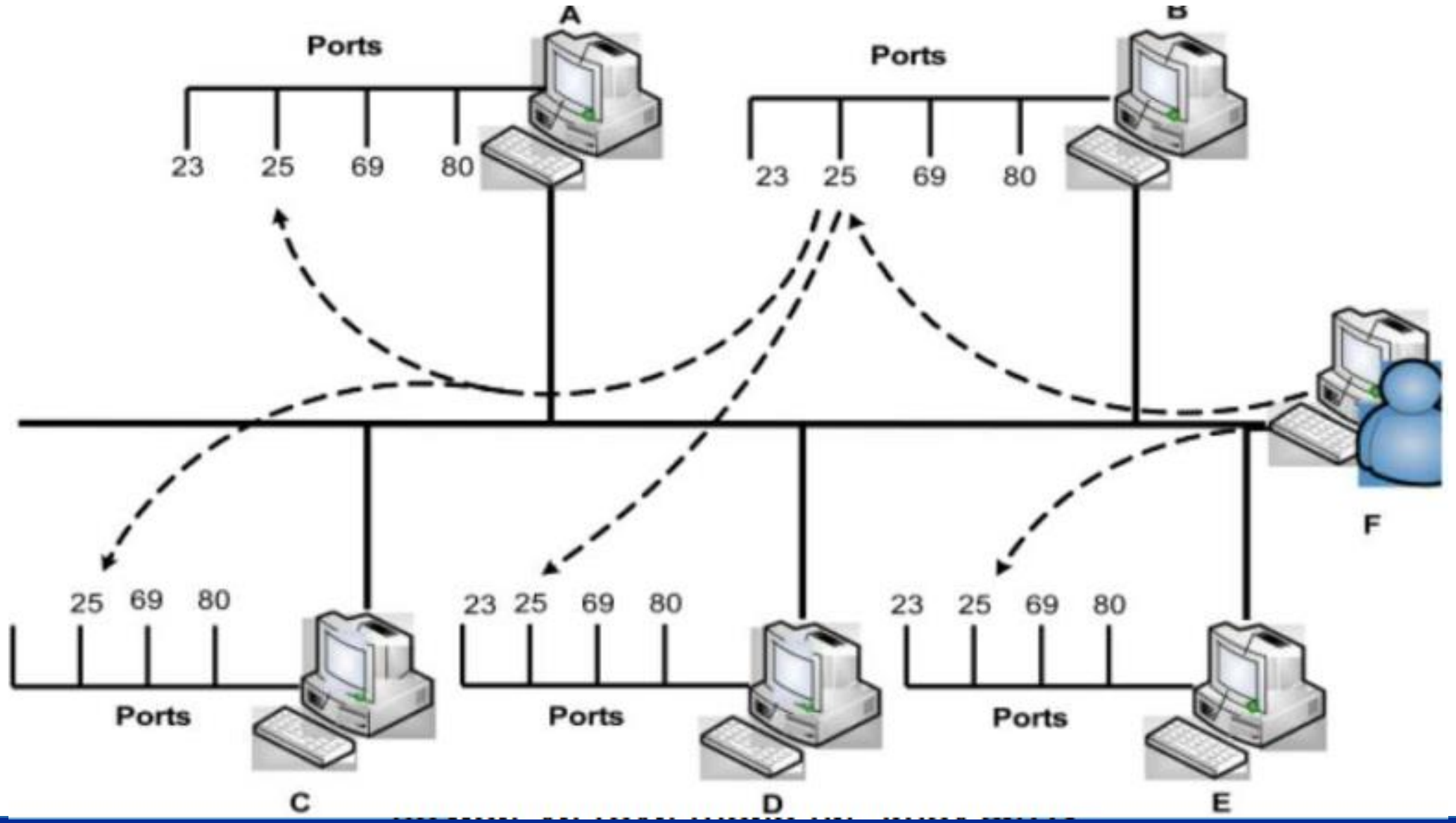
❑ Sâu (worm)

- ❖ Tập mã lệnh khai thác nối kết mạng, thường trú trong bộ nhớ máy đích, lây nhiễm và lan truyền từ hệ thống này sang hệ thống khác
- ❖ Lợi dụng quyền hạn người dùng để phát tán hoặc khai thác lỗ hổng hệ thống
- ❖ Cách thức lan truyền: email, chat room, Internet, P2P
- ❖ Được sử dụng rộng rãi bởi hacker để tạo **zombie**

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Sâu (worm)

❖ Một mô hình lây lan của sâu:



1.2. Phân loại phần mềm mã độc – Tác hại

❑ Một số sâu mạng điển hình

❖ Nimda và Code Red (2001) tấn công Microsoft's Internet Information Server (IIS) Web Server:

- Quét mạng để tìm các máy dễ tổn thương, Nimda tạo ra tài khoản guest với quyền quản trị trên máy nhiễm
- Code Red hủy hoại các website, suy thoái hiệu năng hệ thống, gây mất ổn định do sinh ra nhiều thread và tiêu tốn băng thông

❖ SQL Slammer (2003) khai thác tràn buffer trong Microsoft's SQL Server và Microsoft SQL Server Desktop Engine (MSDE), làm máy nhiễm sinh ra lượng dữ liệu lưu thông khổng lồ

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Một số sâu mạng điển hình

- ❖ Blaster (2003): khai thác tràn bộ đệm trong Microsoft Distributed Component Object Model (DCOM), Remote Procedure Call (RPC), gây mất ổn định và tự động khởi động máy
- ❖ Sasser (2004) khai thác tràn bộ đệm trong Microsoft's LSAS service (port 139), làm máy nhiễm tự động khởi động lại
- ❖ Zotob (2005) lợi dụng tính dễ bị tấn công của dịch vụ Plug- and-play của Microsoft Windows để lan truyền qua mạng

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Hoạt động của sâu

❖ Các pha hoạt động tương tự như của virus:

- Không hoạt động - chờ đợi sự kiện kích hoạt
- Lan truyền - sao chép mình tới chương trình/đĩa
  - Tìm kiếm các hệ thống khác để lây nhiễm
  - Thiết lập kết nối đến mục tiêu từ xa
  - Tự sao chép vào hệ thống từ xa
- Kích hoạt – theo sự kiện để thực thi payload
- Thực thi – theo payload

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Rootkit

- ❖ Rootkit: bộ công cụ (kit) giúp hacker khống chế hệ thống ở mức cao nhất (root)
- ❖ Rootkit có thể sửa đổi các khối cơ sở của một OS như kernel, các driver liên lạc hoặc thay thế các chương trình hệ thống được dùng chung bởi các phiên bản rootkit
- ❖ Một số rootkit được cài đặt như công cụ quản trị máy ảo, sau đó nạp OS nạn nhân vào máy ảo khiến anti-virus không thể phát hiện nó
- ❖ Hacker sử dụng rootkit để cài đặt các chương trình điều khiển từ xa mạnh mẽ

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Backdoor và Key logger

- ❖ Backdoor (cửa hậu): loại mã độc được thiết kế cho phép truy xuất hệ thống từ xa
- ❖ Key logger (thám báo bàn phím): ban đầu dùng giám sát trẻ con sử dụng mạng, về sau biến thể thành công cụ đánh cắp mật khẩu
- ❖ Trojans, rootkit và các chương trình hợp thức (như key logger) đều có thể được dùng để cài đặt backdoor

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Spyware và Adware

- ❖ Spyware (phần mềm gián điệp): rất đa dạng, thường không gây nguy hại về mặt dữ liệu
- ❖ Tác hại của spyware:
  - Rò rỉ thông tin cá nhân
  - Tiêu thụ tài nguyên máy đích
  - Hệ thống mất ổn định
- ❖ Spyware lây nhiễm qua download phần mềm
- ❖ Adware: spyware quảng cáo

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Phần mềm tống tiền (Ransomware)

- ❖ Lây nhiễm vào máy tính giống cách của sâu mạng và hạn chế người dùng truy cập vào máy tính hoặc các tập tin
- ❖ Đòi một khoản tiền chuộc để loại bỏ hạn chế
- ❖ Một số hình thức ransomware không thực sự hạn chế truy cập; chỉ hiển thị một thông điệp để lừa người dùng vào trả tiền
- ❖ Với một số ransomware, trả tiền chuộc sẽ không loại bỏ các hạn chế; trong các trường hợp khác, những hạn chế có thể được loại bỏ mà không cần phải trả tiền chuộc

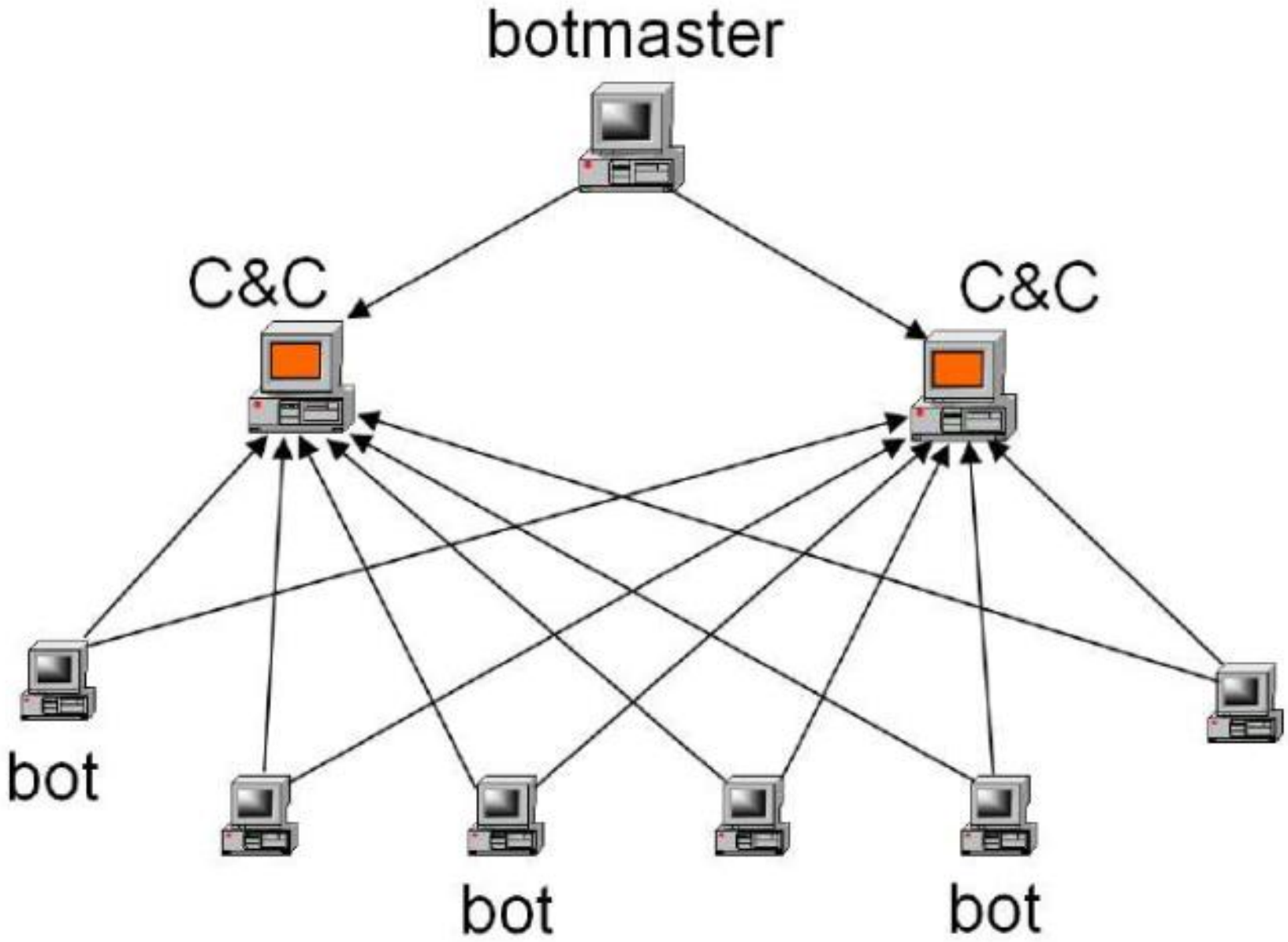
1.2. Phân loại phần mềm mã độc – Tác hại

❑ Bot và Botnet

- ❖ Virus/worm payload:
  - Cài đặt chương trình *bot* trên máy nạn nhân
- ❖ Bot biến máy tính nạn nhân thành một *zombie*, khi đó kẻ tấn công có thể điều khiển được từ xa.
- ❖ Rất nhiều zombie tập hợp thành *botnet* – thường bao gồm hàng trăm nghìn PC

1.2. Phân loại phần mềm mã độc – Tác hại

❑ Bot và Botnet



2. Giải pháp tổng thể phòng chống phần mềm mã độc

1. Chính sách
2. Nhận thức của người dùng
3. Loại bỏ điểm yếu
4. Loại bỏ các nguy cơ

2.1. Chính sách

- Đảm bảo có các chính sách ngăn chặn phần mềm mã độc và phổ biến chúng cho người dùng trong hệ thống thông tin.
- Một số chính sách như:
  - Các phương tiện truyền tin phải được quét loại bỏ mã độc trước khi mang vào công ty sử dụng
  - Các file đính kèm trong email phải được lưu lại và quét mã độc trước khi mở ra trên máy tính
  - Các ứng dụng và hệ điều hành phải được cập nhật các bản vá liên tục, kịp thời
  - …

2.2. Nhận thức người dùng

- Nâng cao nhận thức người dùng về các nguy cơ từ phần mềm mã độc có thể giảm bớt khả năng và mức độ nghiêm trọng của các sự cố đến từ phần mềm mã độc
- Các chương trình nâng cao nhận thức người dùng trong hệ thống thông tin được triển khai định kỳ để nâng cao nhận thức người dùng
- Một số các hoạt động nhận thức cần triển khai như:
  - Không mở các email và file đính kèm đáng ngờ hoặc từ các nguồn gửi đáng ngờ
  - Không vào các trang Web đen/ không tin cậy
  - Không mở các file với đuôi thực thi được, ví dụ .com, .exe, .pif, .bat, .vbs, …

2.3. Loại bỏ điểm yếu

- Quản lý bản vá
  - Là cách phổ biến nhất để loại bỏ các lỗi đã phát hiện trên các phần mềm hoặc hệ điều hành
- Cấp quyền tối thiểu
  - Quy tắc về quyền tối thiểu giúp hệ thống duy trì mức cấp phép vừa đủ hoạt động cho các người dùng và tiến trình. Giúp cho việc ngăn chặn phần mềm mã độc do chúng cần các quyền quản trị hệ thống
- Các phương pháp bảo vệ hệ thống khác
  - Loại bỏ các dịch vụ không cần thiết
  - Bỏ các chia sẻ file
  - Bỏ các tài khoản mặc định
  - Xác thực trước khi truy cập dịch vụ, tài nguyên

2.4. Loại bỏ các nguy cơ

1. Sử dụng phần mềm diệt virus
2. Sử dụng các công cụ phát hiện và loại bỏ phần mềm mã độc
3. Hệ thống IPS
4. Tường lửa và bộ định tuyến
5. Cấu hình ứng dụng

2.4.1 Sử dụng phần mềm diệt virus

- Các phần mềm diệt virus là phương pháp phổ biến nhất để đảm bảo loại bỏ các nguy cơ từ phần mềm mã độc
- Các tính năng bao gồm
  - Quét các thành phần quan trọng của hệ thống như boot sector, các file khởi động
  - Theo dõi hệ thống trong thời gian thực
  - Theo dõi hành vi của các phần mềm phổ dụng như Web, email, chat
  - Quét các file để kiểm tra virus và các phần mềm mã độc phổ biến
  - Thực hiện các hành động loại bỏ, cô lập, ngăn ngừa phần mềm mã độc
- Các công cụ: Windows Defender, Kaspersky AV, Avira, …

2.4.2 Sử dụng công cụ phát hiện và loại bỏ phần mềm mã độc

❖Các công cụ này được xây dựng nhằm vào một hoặc một số loại mã độc cụ thể mà phần mềm diệt virus không phát hiện và loại trừ được như các Spyware, rootkit,…

2.4.3 Sử dụng hệ thống IPS

- Các hệ thống IPS sử dụng các chữ ký của các loại tấn công cùng với phân tích về mạng và các giao thức để phát hiện ra các hành vi độc hại
- Các hệ thống IPS giúp ngăn chặn phần mềm mã độc thông qua việc phát hiện và chặn các mối đe dọa chưa biết.
- IPS giúp bảo vệ các thành phần không được phần mềm diệt virus bảo vệ như DNS.
- IPS giúp chặn các lưu lượng lớn phát sinh từ phần mềm mã độc (ví dụ, worm)

2.4.4 Tường lửa và bộ định tuyến

- Tường lửa được dùng để bảo vệ mạng và hệ thống khỏi các mối đe dọa từ bên ngoài
- Tường lửa giúp bảo vệ các mục tiêu không được phần mềm diệt virus và IPS theo dõi bảo vệ.
- Tường lửa giúp chặn các phần mềm mã độc với các địa chỉ IP cụ thể, ví dụ worm muốn download các Trojan về hệ thống
- Các tường lửa trên host có thể ngăn phần mềm mã độc phát tán, ví dụ ngăn chặn việc gửi nhiều email đồng thời do worm hay virus tạo ra

2.4.4 Tường lửa và bộ định tuyến

- Bộ định tuyến thường đứng trước tường lửa để thực hiện các hoạt động kết nối Internet
- Bộ định tuyến thực hiện các kiểm tra đơn giản cho các hoạt động mạng, như lọc đầu vào, đầu ra, giúp ngăn chặn một vài phần mềm mã độc
- Hoặc được cấu hình để ngăn chặn một số hành vi phát tán worm qua các dịch vụ mạng cụ thể

2.4.5 Cấu hình ứng dụng

- Nhiều phần mềm mã độc sử dụng các tính năng của các ứng dụng phổ biến như email client, trình duyệt Web, hay soạn thảo văn bản để lây nhiễm và phát tán.
- Người dùng cần vô hiệu hóa các tính năng không cần thiết để hạn chế khả năng phát tán của phần mềm mã độc
- Một số hành động như:
  - Chặn các file đính kèm đáng ngờ từ email
  - Lọc spam
  - Lọc nội dung Web
  - Hạn chế Web cookie
  - Chặn Web pop-up
  - …

3. Phương pháp phát hiện và loại trừ phần mềm mã độc

1. Phương pháp nhận biết hệ thống máy tính bị nhiễm phần mềm mã độc
2. Phương pháp loại trừ phần mềm mã độc

3.1. Phương pháp nhận biết hệ thống máy tính bị nhiễm phần mềm mã độc

1. Quét các cổng mở đáng ngờ
2. Quét các tiến trình chạy đáng ngờ
3. Quét các registry đáng ngờ
4. Quét các trình điều khiển thiết bị đáng ngờ
5. Quét các dịch vụ đang chạy trên hệ thống đáng ngờ

3.1. Phương pháp nhận biết hệ thống máy tính bị nhiễm phần mềm mã độc

6. Quét các chương trình khởi động đáng ngờ
7. Quét tập tin và thư mục đáng ngờ
8. Quét các hoạt động mạng đáng ngờ
9. Quét các file hệ điều hành có thay đổi đáng ngờ
10. Quét trojan bằng các chương trình phát hiện trojan
11. Quét virus bằng các chương trình diệt virus

3.1.1 Quét các cổng đáng ngờ

- Trojan sử dụng các cổng rảnh rỗi để kẻ tấn công duy trì kết nối
- Cần kiểm tra các kết nối đến các địa chỉ IP đáng ngờ
- Công cụ: netstat, currport, TCPView

3.1.2 Quét các tiến trình chạy đáng ngờ

- Trojan ngụy trang bản thân bằng chính các dịch vụ hoặc giấu các tiến trình hoạt động của mình
- Trojan đưa mã vào các tiến trình khác để sinh ra các tiến trình không thể nhìn thấy
- Sử dụng các công cụ giám sát tiến trình để phát hiện: Task manager, What is running?

3.1.3 Quét các registry đáng ngờ

- Windows thực hiện tự động chạy các lệnh trong một số mục registry khi khởi động
- Quét các giá trị registry cho các mục đáng ngờ liên quan đến Trojan do chúng chèn dữ liệu để chỉ dẫn thực hiện hoạt động
- Sử dụng các công cụ quét registry: regshot

3.1.4 Quét các trình điều khiển thiết bị đáng ngờ

- Trojan được cài đặt cùng với các trình điều khiển thiết bị tải về từ các nguồn không tin cậy
- Quét và xác minh các trình điều khiển đáng ngờ xem có phải chính hãng không
- Công cụ: Driverview, Driverscanner

3.1.5 Quét dịch vụ đáng ngờ chạy trên hệ thống

- Trojan sinh ra các dịch vụ của Windows cho phép kẻ tấn công truy cập và điều khiển trái phép hệ thống từ xa.
- Thông thường các dịch vụ này bị đổi tên trong giống các dịch vụ bình thường của hệ thống.
- Sử dụng các kỹ thuật rootkit để khóa các registry để ẩn tiến trình độc hại.
- Giám sát và phát hiện bằng công cụ: SrvMan, Process Hacker.

3.1.6 Các hoạt động quét khác

- Quét các chương trình khởi động đáng ngờ
  - Với các công cụ như Autorun, Starter
- Quét tập tin và thư mục đáng ngờ
  - Các công cụ kiểm tra tính toàn vẹn của các file và thư mục như Tripwire, Sigverif, WinMD5
- Quét các hoạt động mạng đáng ngờ
  - Theo dõi các hoạt động mạng đến các địa chỉ đáng ngờ
  - Theo dõi lưu lượng mạng đáng ngờ
  - Các công cụ: Capsa Network Analyzer

3.2. Phương pháp xử lý, loại trừ phần mềm mã độc

❖ Các pha trong xử lý phần mềm mã độc

Vòng đời ứng phó sự cố

3.2.1 Chuẩn bị

- Các tổ chức nên thực hiện các biện pháp chuẩn bị để đảm bảo rằng họ có khả năng ứng phó hiệu quả với các sự cố phần mềm độc hại. Gồm các công việc sau:
  - Phát triển chính sách xử lý sự cố phần mềm độc hại cụ thể và các thủ tục xác định vai trò và trách nhiệm của tất cả các cá nhân và tập thể có thể được tham gia vào việc xử lý sự cố phần mềm độc hại.
  - Thường xuyên tổ chức đào tạo và thực hành về các vấn đề liên quan đến phần mềm độc hại.
  - Xây dựng và duy trì các kỹ năng liên quan đến việc xử lý phần mềm độc hại, như hiểu biết về phương pháp lây nhiễm phần mềm độc hại và các công cụ phát hiện phần mềm độc hại.

3.2.1 Chuẩn bị

- Tạo điều kiện thông tin liên lạc và phối hợp bằng cách chỉ định trước một vài cá nhân hay một nhóm nhỏ chịu trách nhiệm điều phối phản ứng của tổ chức về các sự cố phần mềm độc hại.
- Thành lập một số cơ chế truyền thông để phối hợp giữa các bộ xử lý sự cố, cán bộ kỹ thuật, quản lý, và người dùng có thể được duy trì trong các sự kiện bất lợi.
- Thiết lập một điểm liên lạc để trả lời câu hỏi về tính hợp pháp của các cảnh báo về phần mềm độc hại.
- Chuẩn bị các công cụ phần cứng và phần mềm cần thiết để hỗ trợ trong việc xử lý sự cố phần mềm độc hại.

3.2.2 Phát hiện và phân tích

- Web server bị đánh sập
- Người dùng phàn nàn về việc chậm truy cập vào máy chủ trên Internet, cạn kiệt tài nguyên hệ thống, truy cập đĩa chậm, hoặc hệ thống khởi động chậm
- Phần mềm diệt virus phát hiện một host bị nhiễm sâu và tạo ra một cảnh báo
- Quản trị viên hệ thống nhìn thấy tên tập tin với các ký tự khác thường
- Host ghi lại một sự thay đổi cấu hình kiểm tra trong nhật ký của mình

3.2.2 Phát hiện và phân tích

- Bất cứ khi nào người dùng cố gắng chạy một trình duyệt Web, máy tính xách tay của người dùng tự khởi động lại
- Người quản trị e-mail thấy một số lượng lớn các e-mail bị trả về với nội dung đáng ngờ
- Các kiểm soát an toàn như phần mềm chống virus và tường lửa cá nhân bị vô hiệu hóa trên các host
- Quản trị mạng thấy có độ lệch bất thường từ các lưu lượng mạng điển hình.

3.2.2 Phát hiện và phân tích

- Giám sát phần mềm có hại và công cụ cảnh báo an toàn (ví dụ, phần mềm chống virus, IPS) để phát hiện tiền thân của sự cố phần mềm độc hại, có thể cung cấp cho các tổ chức cơ hội ngăn chặn sự cố bằng cách thay đổi các biện pháp an ninh
- Xem xét dữ liệu từ các nguồn chính của các chỉ dẫn sự cố phần mềm độc hại, bao gồm các báo cáo người dùng, báo cáo nhân viên IT, và các công cụ bảo mật (ví dụ, phần mềm chống virus, IDS), và tương quan dữ liệu giữa các nguồn để xác định hoạt động có hại liên quan.

3.2.2 Phát hiện và phân tích

- Phân tích sự cố phần mềm độc hại nghi ngờ và xác nhận phần mềm độc hại là nguyên nhân của từng vụ việc, vì không có chỉ báo nào là hoàn toàn tin cậy. Sử dụng nguồn dữ liệu thứ cấp khi cần để xem xét các hoạt động hoặc thu thập thêm thông tin.
- Xây dựng bộ công cụ tin cậy được cập nhật thường xuyên để xác định phần mềm độc hại, danh sách các tiến trình đang chạy và thực hiện các hoạt động phân tích khác.
- Thiết lập tập các tiêu chí ưu tiên để xác định mức độ đáp ứng thích hợp với các loại sự cố liên quan đến phần mềm độc hại khác nhau.

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Ngăn chặn (Containment)

❖ Có hai thành phần chính: ngăn chặn sự lây lan của phần mềm độc hại và ngăn chặn thiệt hại thêm cho hệ thống.

❖ **Người sử dụng tham gia.** Việc cung cấp cho người dùng các hướng dẫn về cách xác định sự lây nhiễm và những biện pháp nhận biết máy bị nhiễm là rất hữu ích; Tuy nhiên, các tổ chức không phụ thuộc nhiều vào người dùng để xác định các sự cố phần mềm độc hại.

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Ngăn chặn (Containment)

❖ **Tự động phát hiện.** Các công nghệ tự động, như phần mềm chống virus, lọc e-mail, và các phần mềm phòng chống xâm nhập, thường có thể chứa sự cố phần mềm độc hại. Trong một sự cố lớn, nếu phần mềm độc hại không thể được xác định bởi bản cập nhật phần mềm chống virus, thì các tổ chức cần phải được chuẩn bị để sử dụng các công cụ bảo mật khác.

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Ngăn chặn (Containment)

❖ **Vô hiệu hóa dịch vụ.** Các tổ chức nên được chuẩn bị để đóng hoặc khóa dịch vụ được sử dụng bởi phần mềm độc hại có chứa một sự cố và cần phải hiểu được hậu quả của việc làm đó. Đồng thời cần được chuẩn bị để đối phó với vấn đề gây ra bởi các tổ chức khác khi họ vô hiệu hóa dịch vụ của họ để ứng phó với một sự cố phần mềm độc hại.

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Ngăn chặn (Containment)

❖ **Vô hiệu hóa kết nối.** Các tổ chức nên được chuẩn bị để đặt các hạn chế bổ sung trên kết nối mạng chứa sự cố phần mềm độc hại, nhận ra các ảnh hưởng mà những hạn chế có thể có đối với các hoạt động của tổ chức.

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Loại bỏ (Eradication)

❖ Mục tiêu là xóa bỏ phần mềm mã độc khỏi hệ thống đã bị nhiễm.

❖ Chuẩn bị các biện pháp, kế hoạch loại bỏ trong một khoảng thời gian có thể hàng tuần cùng với các biện pháp khôi phục các dữ liệu, các hệ thống đang hoạt động

- Sử dụng nhiều biện pháp đồng thời cho việc xóa bỏ
- Chuẩn bị cấu hình lại các hệ thống: hệ điều hành, các ứng dụng và khôi phục dữ liệu từ các nguồn lưu trữ

3.2.3 Ngăn chặn, loại bỏ và khôi phục

❑ Khôi phục

❖ Hai khía cạnh chính của việc khôi phục từ các sự cố phần mềm độc hại là khôi phục chức năng và dữ liệu của hệ thống bị lây nhiễm; và loại bỏ các biện pháp ngăn chặn tạm thời.

- Các tổ chức nên xem xét các kịch bản xấu nhất có thể và xác định phương pháp khôi phục nên thực hiện.
- Xác định khi nào loại bỏ các biện pháp ngăn chặn tạm thời, chẳng hạn như các dịch vụ hoặc kết nối bị đình chỉ, thường là một quyết định khó khăn trong các sự cố phần mềm độc hại lớn
- Đội ứng phó sự cố nên cố gắng duy trì các biện pháp ngăn chặn tại chỗ cho đến khi ước tính về các hệ thống bị lây nhiễm và các hệ thống dễ bị lây nhiễm là đủ thấp mà sự cố tiếp theo không quá nghiêm trọng.

3.2.4 Hoạt động sau sự cố

- Do việc xử lý sự cố phần mềm độc hại có thể cực kỳ tốn kém nên việc các tổ chức xem xét các bài học về những sự cố phần mềm độc hại lớn là đặc biệt quan trọng.
  - Nắm được bài học sau việc xử lý sự cố phần mềm độc hại giúp cải thiện khả năng xử lý sự cố và phòng chống phần mềm độc hại
  - Thay đổi chính sách bảo mật
  - Thay đổi cấu hình phần mềm
  - Thay đổi trong việc phát hiện phần mềm độc hại và triển khai phần mềm phòng chống