Trường Đại Học Công Nghệ Thông Tin

NHẬP MÔN BẢO ĐẢM VÀ AN NINH THÔNG TIN

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan
2. a. Các phần mềm gây hại – Trojan
   b. Các phần mềm gây hại – Virus
3. Các giải thuật mã hoá dữ liệu
4. Mã hoá khoá công khai và quản lý khoá
5. Chứng thực dữ liệu
6. Một số giao thức bảo mật mạng
7. Bảo mật mạng không dây
8. Bảo mật mạng ngoại vi

Bài 2b

CÁC PHẦN MỀM GÂY HẠI - VIRUS

VIRUS MÁY TÍNH

NỘI DUNG

- Tổng quan về Virus máy tính
- Các kỹ thuật của Virus máy tính
- Các kỹ thuật của Virus máy tính trên mạng
- Phòng chống Virus máy tính
- Một số bài tập

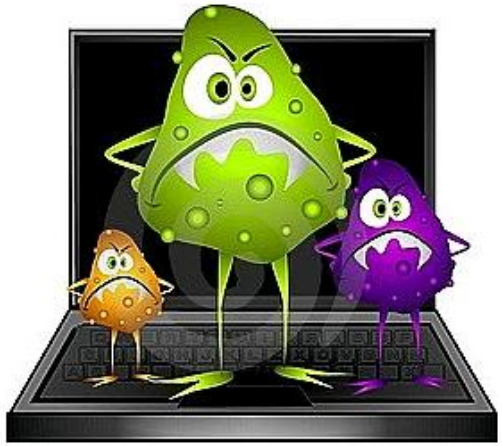
1. Tổng quan về Virus máy tính

- Virus máy tính là gì?
- So sánh Virus, Worm, Zombie, Trojan

1. Tổng quan về Virus máy tính

- Chương trình Virus thường thực hiện các bước sau:
  - Tìm cách gắn vào đối tượng chủ, sửa đổi dữ liệu sao cho virus nhận được quyền điều khiển mỗi khi chương trình chủ được thực thi.
  - Khi được thực hiện, virus tìm kiếm những đối tượng khác, sau đó lây nhiễm lên những đối tượng này.
  - Tiến hành những hoạt động phá hoại, do thám.
  - Trả lại quyền thi hành cho chương trình chủ hoạt động như bình thường.

1. Tổng quan về Virus máy tính



Đối tượng lây nhiễm

- Các file chương trình .BAT, .EXE, .COM, …
- Các tài liệu văn bản Word, Excel, PowerPoint, …

Cung khởi động của đĩa

1. Tổng quan về Virus máy tính

Year of Discovery	Virus Name
1981	Apple II Virus- First Virus in the wild
1983	First Documented Virus
1986	Brain, PC-Write Trojan, & Virdem
1989	AIDS Trojan
1995	Concept
1998	Strange Brew & Back Orifice
1999	Melissa, Corner, Tristate, & Bubbleboy
2003	Slammer, Sobig, Lovgate, Fizzer, Blaster/Welchia/Mimail
2004	I-Worm.NetSky.r, I-Worm.Baqle.au
2005	Email-Worm.Win32.Zafi.d, Net-Worm.Win32.Mytob.t

1. Tổng quan về Virus máy tính

- Năm 1949: John von Neumann (1903-1957) phát triển nền tảng lý thuyết tự nhân bản của một chương trình cho máy tính.
- Năm 1981: Các virus đầu tiên xuất hiện trong hệ điều hành của máy tính Apple II.
- Năm 1983: Tại Đại Học miền Nam California, Fred Cohen lần đầu đưa ra khái niệm *computer virus*.
- Năm 1986: Virus "the Brain", virus cho máy tính cá nhân (PC) đầu tiên, được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (*boot sector*) của một dĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ dĩa mềm.

1. Tổng quan về Virus máy tính

- Năm 1987: Virus đầu tiên tấn công vào command.com là virus "Lehigh".
- Năm 1988: Virus Jerusalem tấn công đồng loạt các đại học và các công ty trong các quốc gia vào ngày thứ Sáu 13. Đây là loại virus hoạt động theo đồng hồ của máy tính.
- Tháng 11.1988, Robert Morris, 22 tuổi, chế ra worm chiếm cứ các máy tính của ARPANET, làm tê liệt khoảng 6.000 máy. Morris bị phạt tù 3 năm và đóng phạt 10.000 USD.
- Năm 1990: Norton giới thiệu chương trình thương mại chống virus đầu tiên.

1. Tổng quan về Virus máy tính

- Năm 1991: Virus đa hình (*polymorphic virus*) ra đời đầu tiên là virus "Tequilla". Loại này biết tự thay đổi hình thức của nó, gây ra sự khó khăn cho các chương trình chống virus.
- Năm 1995: Virus văn bản (*macro virus*) đầu tiên xuất hiện. Macro virus là loại virus viết ra bằng ngôn ngữ lập trình Visual Basic cho các ứng dụng (VBA) và tùy theo khả năng, có thể lan nhiễm trong các ứng dụng văn phòng của Microsoft như Word, Excel, PowerPoint, OutLook,....
- Năm 1998, virus Melissa, tấn công hơn 1 triệu máy, lan truyền bởi một tệp đính kèm kiểu Word bằng cách đọc và gửi đến các địa chỉ của Outlook trong các máy đã bị nhiễm virus.

1. Tổng quan về Virus máy tính

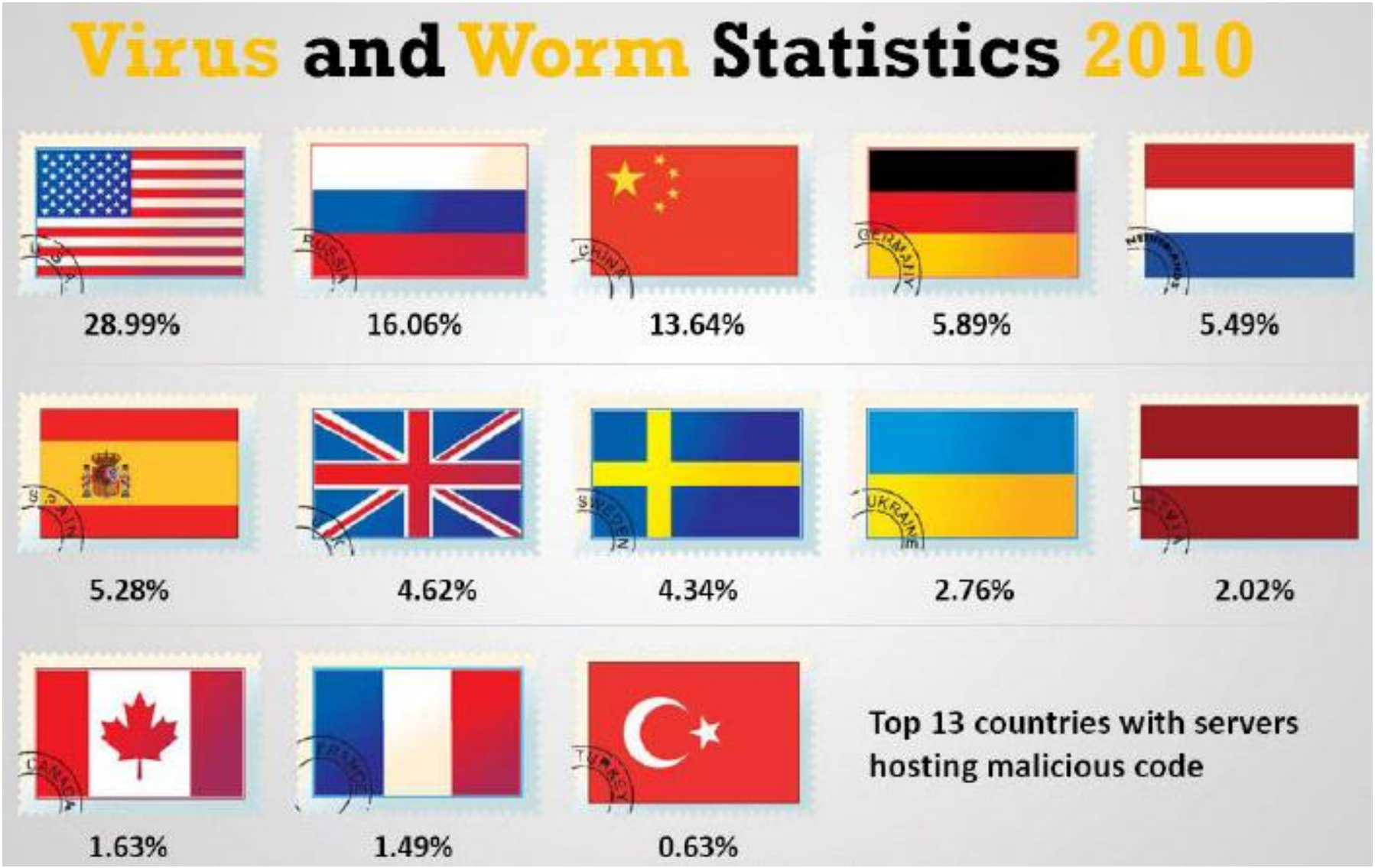
- Năm 2000: Virus Love Bug, còn có tên ILOVEYOU xuất hiện. Đây là một loại macro virus. Tác giả của virus này là một sinh viên người Philippines.
- Năm 2002: Tác giả của virus Melissa là David L. Smith, bị xử 20 tháng tù.
- Năm 2003: Virus Slammer, một loại worm lan truyền với vận tốc kỉ lục, truyền cho khoảng 75 ngàn máy trong 10 phút.
- Năm 2004: xuất hiện worm Sasser. Với virus này thì người ta không cần phải mở đính kèm của điện thư mà chỉ cần mở lá thư là đủ cho nó xâm nhập vào máy. Tác giả của worm này chỉ mới 18 tuổi, Sven Jaschan, người Đức.

1. Tổng quan về Virus máy tính

Top 10 Viruses (2008)

- W32/Detnat
- W32/Netsky
- W32/Mytob
- W32/Bagle
- W32/MyWife
- W32/Virut
- W32/Zafi
- W32/MyDoom
- W32/Lovegate
- W32/Bagz

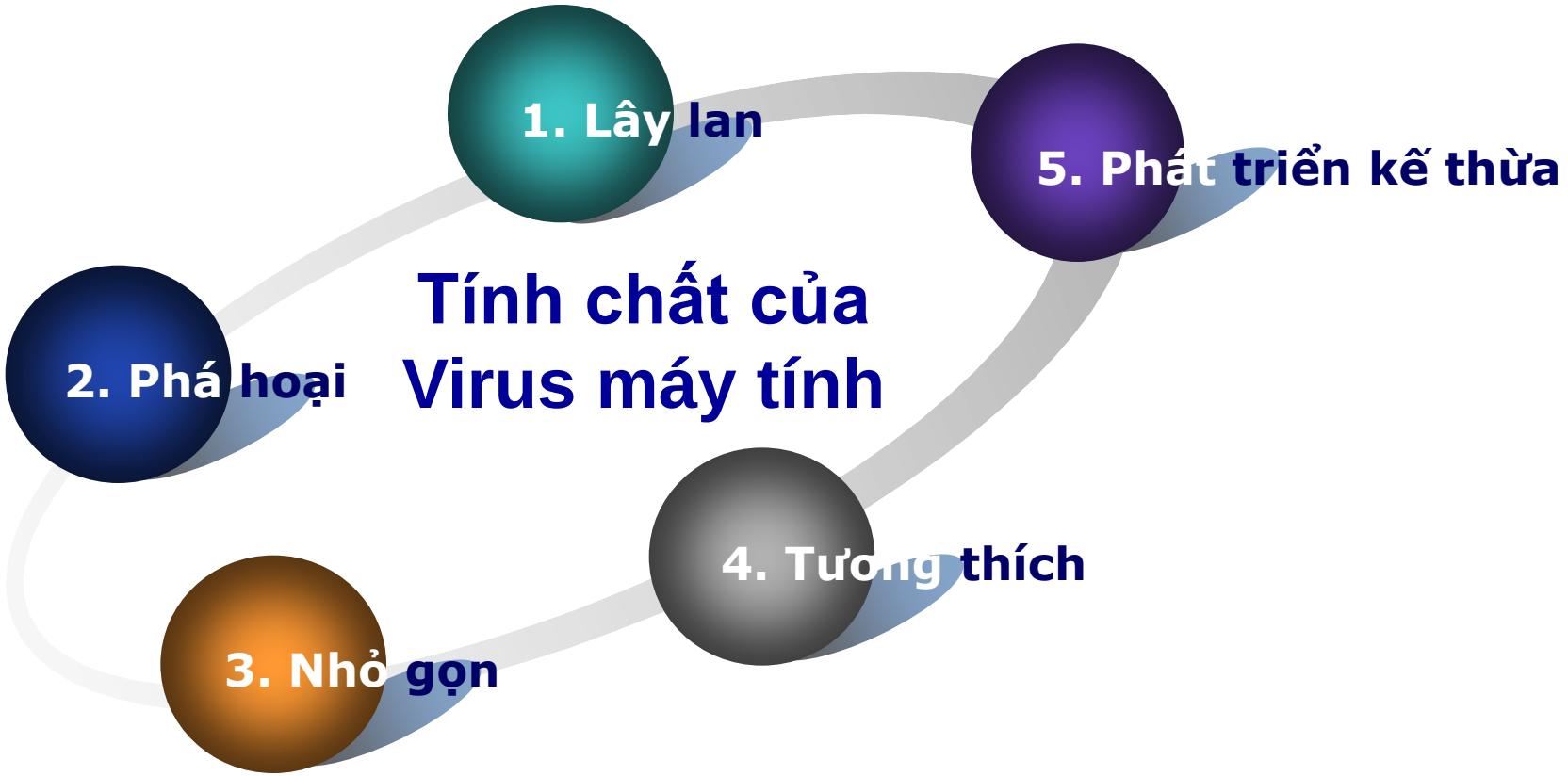
1. Tổng quan về Virus máy tính



1. Tổng quan về Virus máy tính

- Virus máy tính và mạng máy tính:
  - Virus máy tính có khả năng sử dụng những tính năng của hệ điều hành/ứng dụng để truyền bá, lây nhiễm trên mạng -> khả năng lây lan nhanh chóng và rộng rãi.
  - Virus máy tính có khả năng tiến hành những hoạt động phá hoại, do thám trên mạng máy tính, gây ảnh hưởng nghiêm trọng đến sự ổn định, tin cậy và an toàn của mạng.

1. Tổng quan về Virus máy tính



1. Tổng quan về Virus máy tính

1. Tổng quan về Virus máy tính

- **Một cách phân loại khác**:

1. System Sector or Boot Virus: lây nhiễm trên cung boot của đĩa.
2. File Virus: lây nhiễm trên các file thực thi.
3. Macro Virus: lây nhiễm trên các tập tin word, excel, access…
4. Source Code Virus: ghi đoạn code của Trojan đè hoặc nối tiếp vào đoạn code của tập tin chủ.
5. Network Virus: tự phát tán theo email bằng cách sử dụng lệnh và các giao thức của mạng máy tính.

1. Tổng quan về Virus máy tính

- **Một cách phân loại khác**:

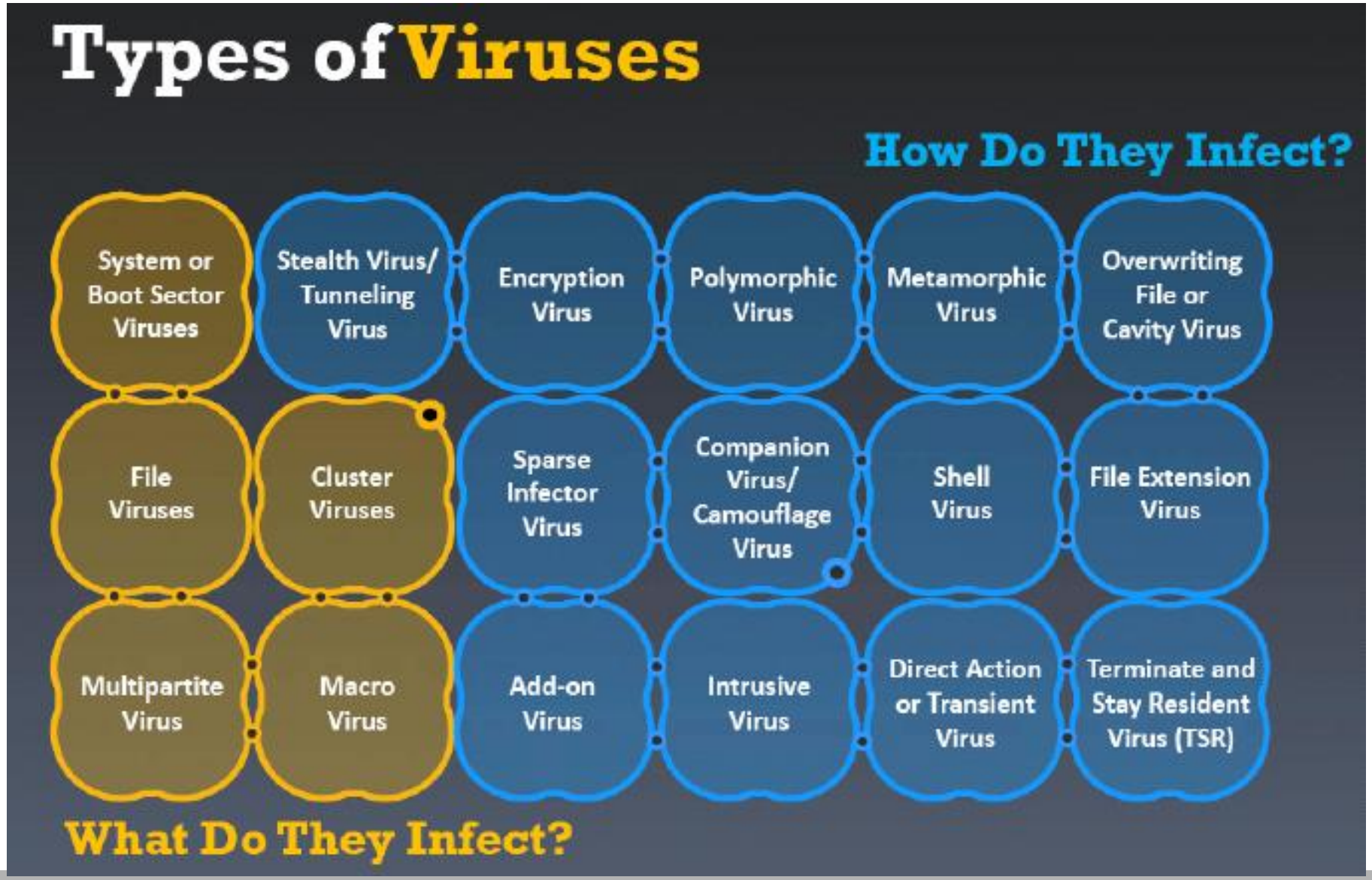
6. Stealth Virus: có thể ẩn với các chương trình chống virus.
7. Polymorphic Virus: có thể thay đổi đặc điểm của nó với mỗi lần lây nhiễm.
8. Cavity Virus: duy trì kích thước file không thay đổi trong khi lây nhiễm.
9. Tunneling Virus: tự che giấu dưới những dạng anti-virus khi lây nhiễm.
10. Camouflage Virus: ngụy trang dưới dạng những ứng dụng chính hãng của người dùng.

1. Tổng quan về Virus máy tính

- **Một cách phân loại khác**:

11. Shell Virus: đoạn mã của virus sẽ tạo thành một shell xung quanh đoạn mã của chương trình bị lây nhiễm, tương tự như một chương trình con trên chương trình gốc nguyên thủy.
12. Add-on Virus: ghi đoạn mã của nó nối tiếp vào điểm bắt đầu của chương trình bị lây nhiễm và không tạo ra thêm bất kỳ thay đổi nào khác.
13. Intrusive Virus: viết đè đoạn code của nó lên một phần hoặc hoàn toàn đoạn code của file bị lây nhiễm.

1. Tổng quan về Virus máy tính



1. Tổng quan về Virus máy tính

Klez Virus (1)

Klez virus arrives as an email attachment that automatically runs when viewed or previewed in Microsoft Outlook or Outlook Express

It is a memory-resident mass-mailing worm that uses its own SMTP engine to propagate via email

Its email messages arrive with randomly selected subjects

It spoofs its email messages so that they appear to have been sent by certain email accounts, including accounts that are not infected

1. Tổng quan về Virus máy tính

Klez Virus (3)

Rebecca double clicks the attached executable in the email

Upon execution, this worm drops a copy of itself as WINK*.EXE in the Windows System folder

- (Where * is a randomly generated variable length string composed of alphabetical characters. For example, it may drop the copy as WINKABC.EXE)

1. Tổng quan về Virus máy tính

Klez Virus (4)

Autorun Techniques

- This worm creates the following registry entry so that it executes at every Windows startup:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  Winkabc

It registers itself as a process so that it is invisible on the Windows Taskbar

On Windows 2000 and XP, it sets itself as a service by creating the following registry entry:

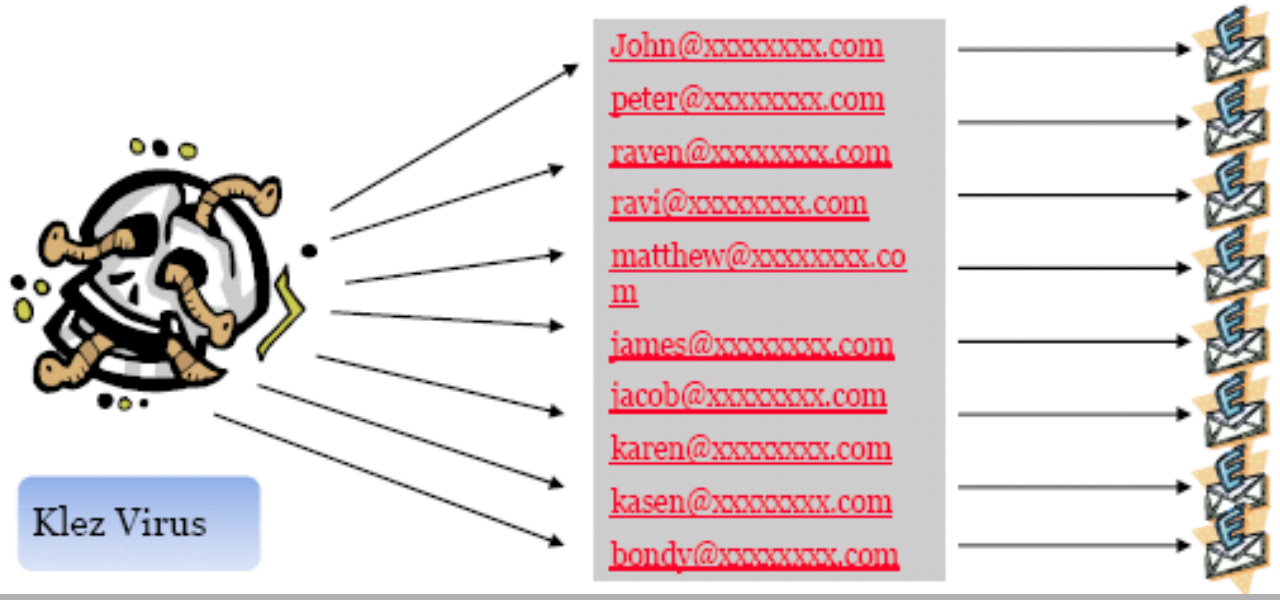
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services Winkabc

1. Tổng quan về Virus máy tính

Klez Virus (5)

Payload

- Once the victim's computer is infected, the Klez virus starts propagating itself to other users through Microsoft Outlook contact list



1. Tổng quan về Virus máy tính

Disk Killer

Disk Killer is a destructive, memory resident, Master Boot Record (MBR)/Boot Sector infecting virus

It spreads by writing copies of itself to 3 blocks on either a floppy diskette or hard disk

These blocks are marked as bad in the File Allocation Table (FAT) so that they cannot be overwritten

The MBR is patched so that when the system is booted, the virus code is executed and it can attempt to infect any new diskettes

1. Tổng quan về Virus máy tính

- Cấu trúc một chương trình Virus đơn giản

```
1.    program V := {
2.          12345;
3.          goto main;
4.          subroutine infect := {
5.                loop:
6.                P := get-random-host-program;
7.                if (the second line of P = 12345;)
8.                   then goto loop
9.                   else insert lines 1-27 in front of P;
10.         }
11.         subroutine break-out := {
12.               modify selected files;
13.               delete selected files;
14.               ...
15.         }
16.         subroutine infection-condition := {
17.               return true if certain conditions are satisfied;
18.         }
19.         subroutine breakout-condition := {
20.               return true if certain conditions are satisfied;
21.         }
22.   main: main-program := {
23.               if infection-condition then infect;
24.               if breakout-condition then break-out;
25.               goto next;
26.         }
27.   next:
28.   the original host program ...
29.   }
```

1. Tổng quan về Virus máy tính

- Check for previous infection
  - Check whether the file is already infected or not
  - This is useful in avoiding multiple infections of the same file
  - Example code to check a previous infection:

```
mov     ah,3Fh                          ; Read first three
mov     cx, 3                           ; bytes of the file
lea     dx, [bp+offset buffer]          ; to the buffer
int     21h

mov     ax, 4202h                       ; SEEK from EOF
xor     cx, cx                          ; DX:CX = offset
xor     dx, dx                          ; Returns filesize
int     21h                             ; in DX:AX

sub     ax, virus_size + 3
cmp     word ptr [bp+offset buffer+1], ax
jnz     infect_it

bomb_out:
mov     ah, 3Eh                                 ; else close the file
int     21                                      ;  and go find another
```

1. Tổng quan về Virus máy tính

- Covering tracks
  - Restore file attributes, time and date to avoid detection
  - Following code can be used to restore file attributes:

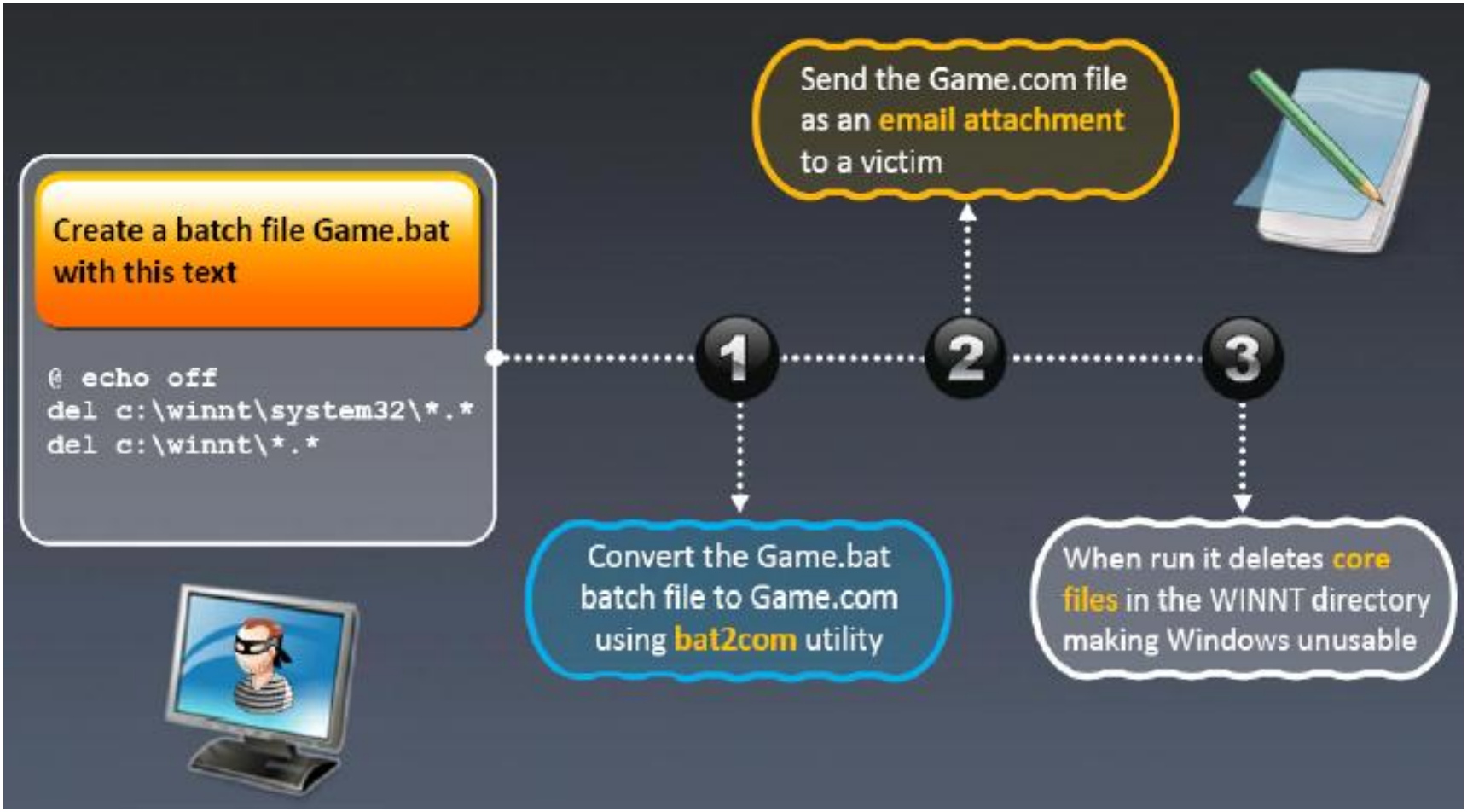
```
mov     ax, 5701h                       ; Set file time/date
mov     dx, word ptr [bp+f_date]        ; DX = date
mov     cx, word ptr [bp+f_time]        ; CX = time
int     21h

mov     ah, 3eh                         ; Handle close file
int     21h

mov     ax, 4301h                       ; Set attributes
lea     dx, [bp+offset DTA + 1Eh]; Filename still in DTA
xor     ch, ch
mov     cl, byte ptr [bp+f_attrib]; Attribute in CX
int     21h
```

1. Tổng quan về Virus máy tính

Viết một chương trình virus đơn giản



1. Tổng quan về Virus máy tính

Công cụ viết virus

Virus creation programs and construction kits can automatically generate viruses

There are number of Virus construction kits available in the wild

Some virus construction kits are:

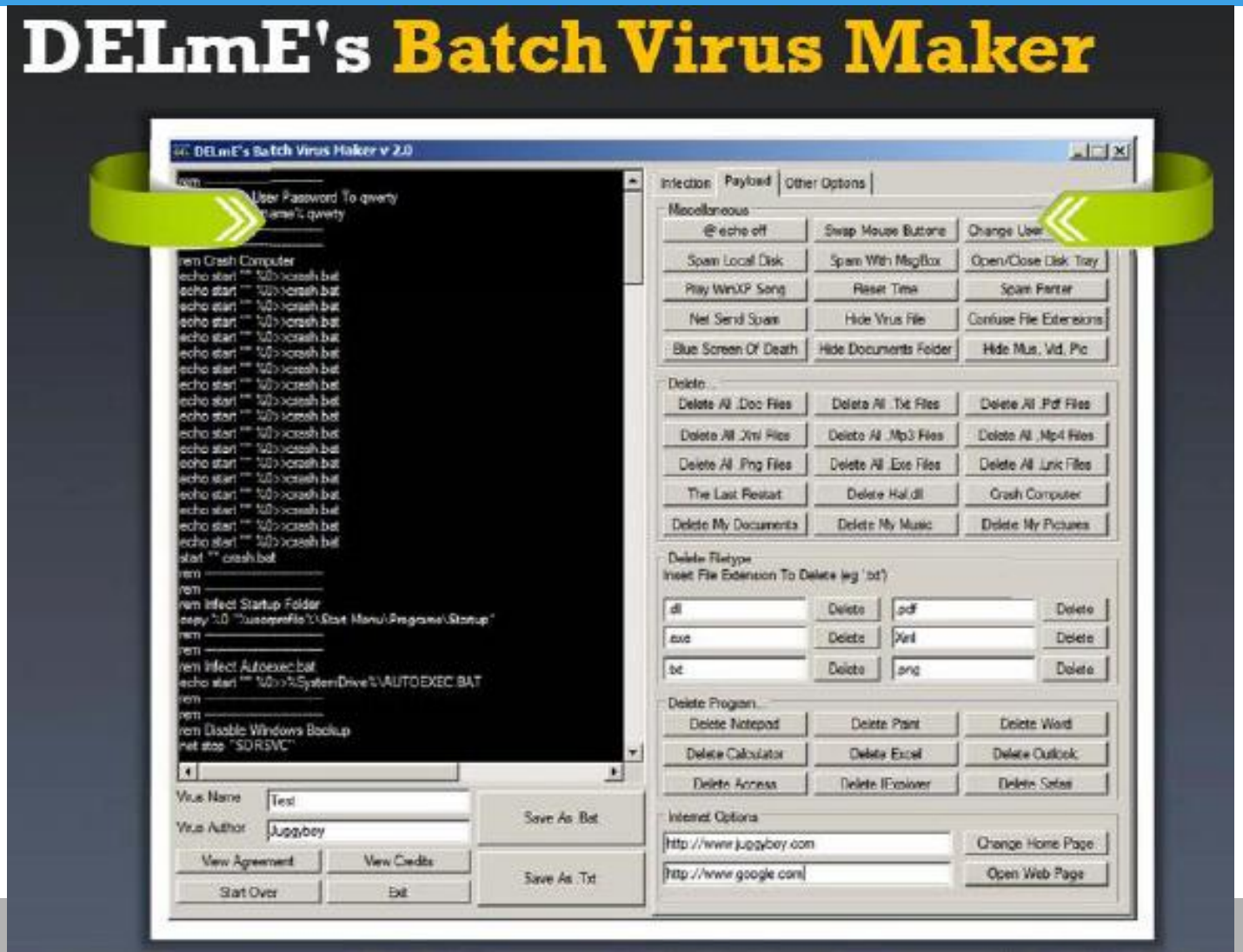
- Kefi's HTML Virus Construction Kit
- Virus Creation Laboratory v1.0
- The Smeg Virus Construction Kit
- Rajaat's Tiny Flexible Mutator v1.1
- Windows Virus Creation Kit v1.00

1. Tổng quan về Virus máy tính

Công cụ viết virus

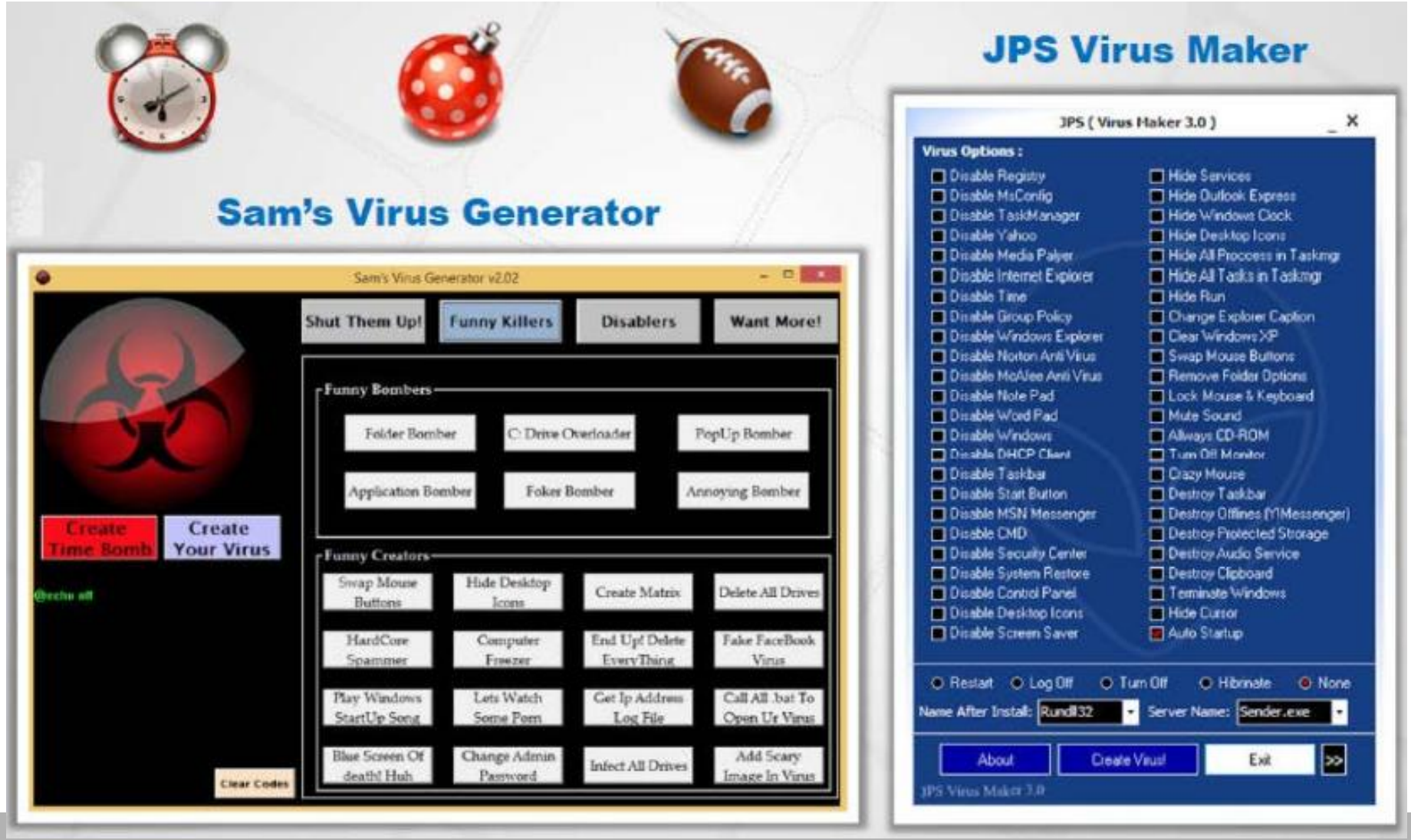
1. Tổng quan về Virus máy tính

Công cụ viết virus



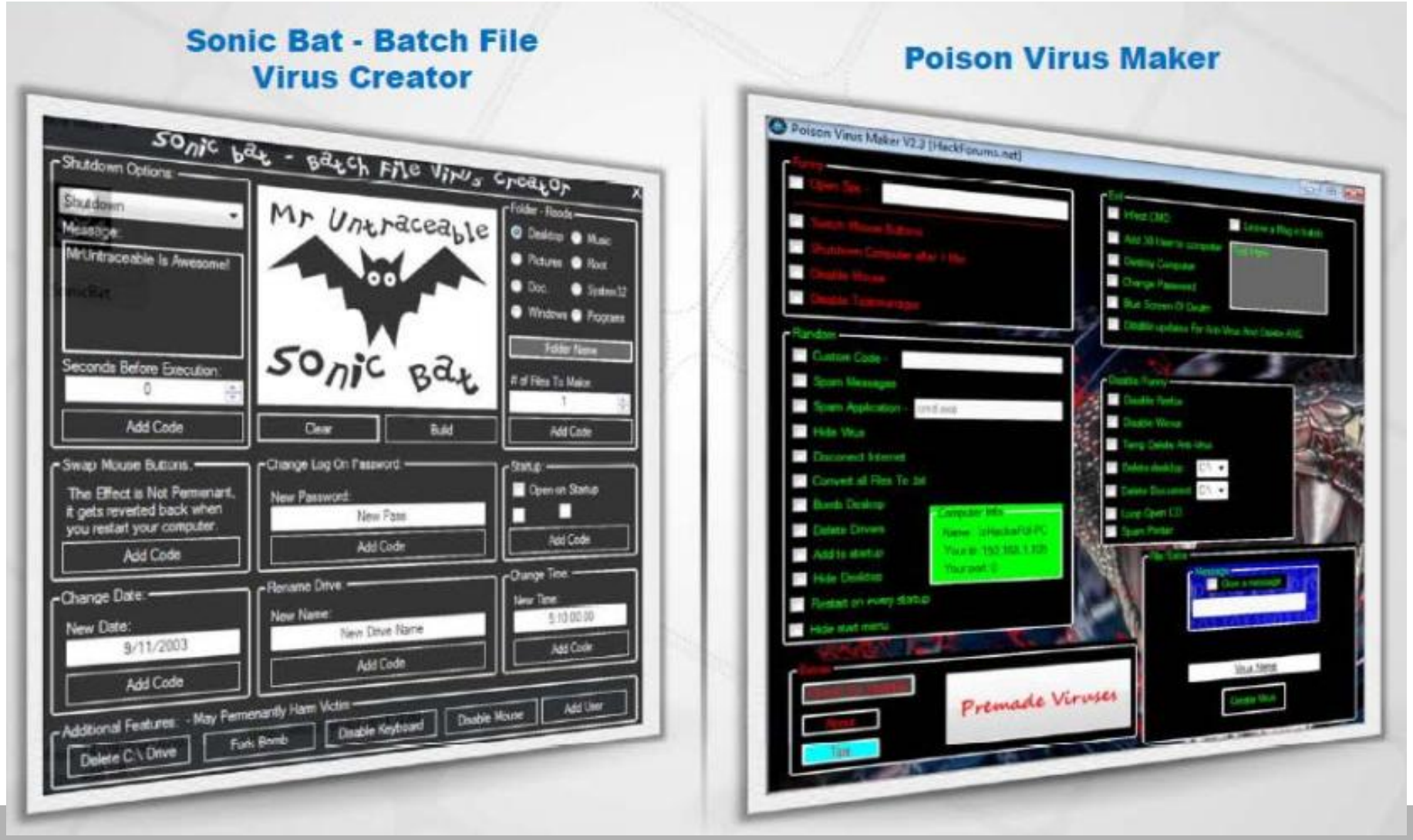
Virus

Sam's Virus Generator and JPS Virus Maker



Virus

Sonic Bat - Batch File Virus Creator and Poison Virus Maker



Worm

1

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction

Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system

2

3

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks

Worm

How is a Worm Different from a Virus?

Replicates on its own

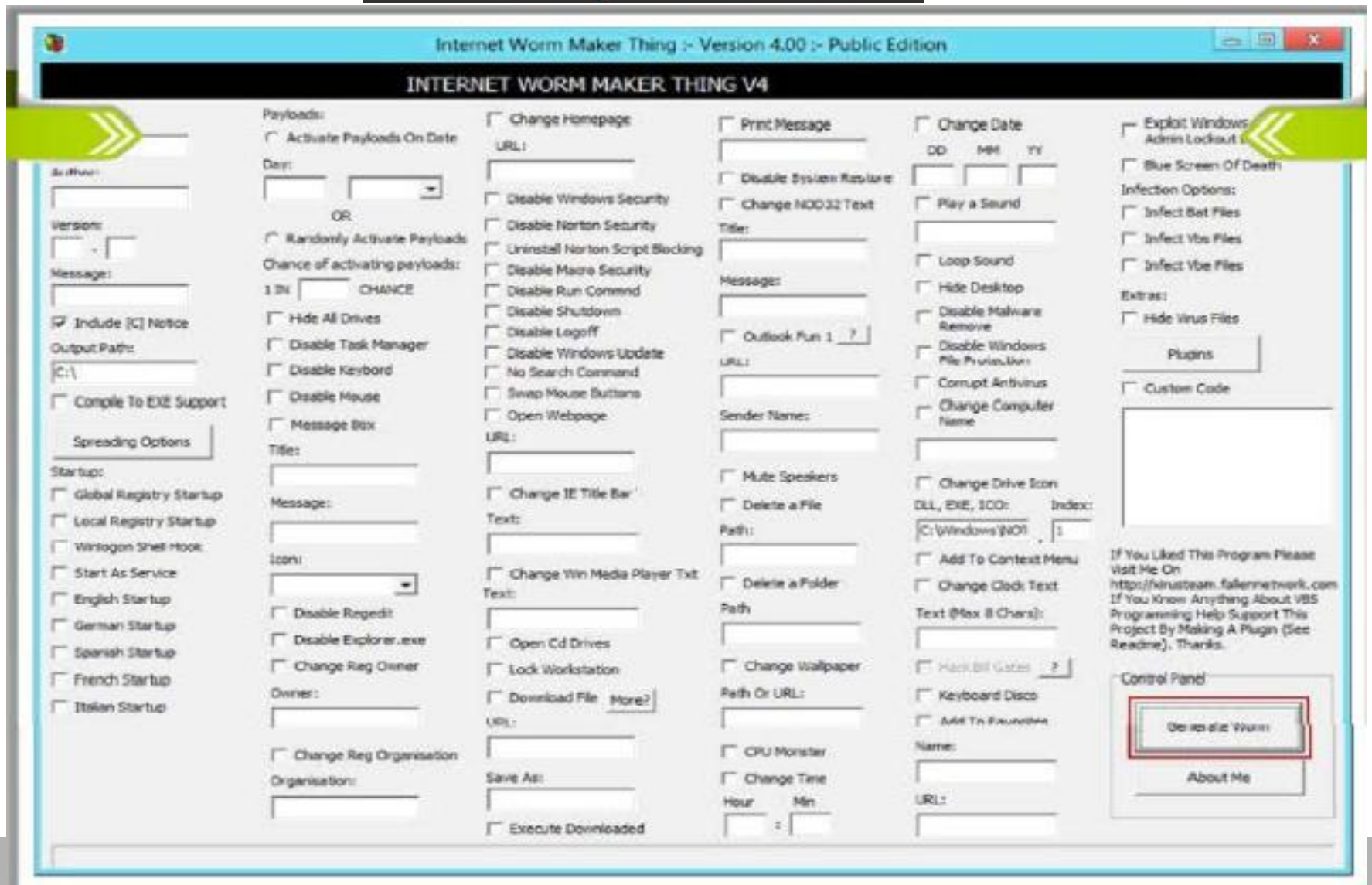
A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs

Spreads through the Infected Network

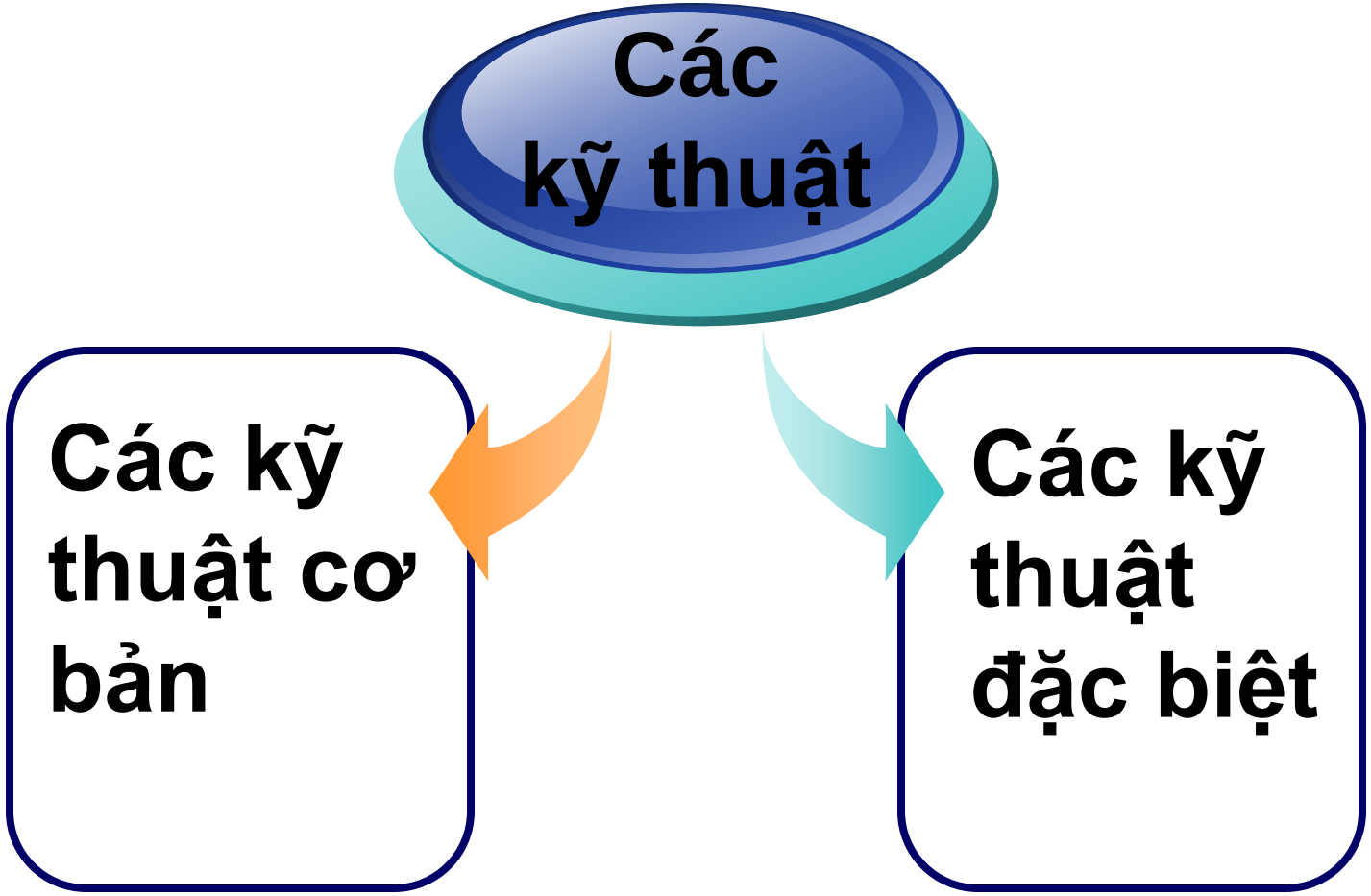
A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Worm

Worm Maker: Internet Worm Maker Thing



2. Các kỹ thuật của Virus máy tính



2. Các kỹ thuật của Virus máy tính

Các kỹ thuật cơ bản

1. Kỹ thuật lây nhiễm
2. Kỹ thuật định vị trên vùng nhớ
3. Kỹ thuật kiểm tra sự tồn tại
4. Kỹ thuật thường trú
5. Kỹ thuật mã hoá
6. Kỹ thuật nguỵ trang
7. Kỹ thuật phá hoại
8. Kỹ thuật chống bẫy
9. Kỹ thuật tối ưu

2. Các kỹ thuật của Virus máy tính

1. **Kỹ thuật lây nhiễm**

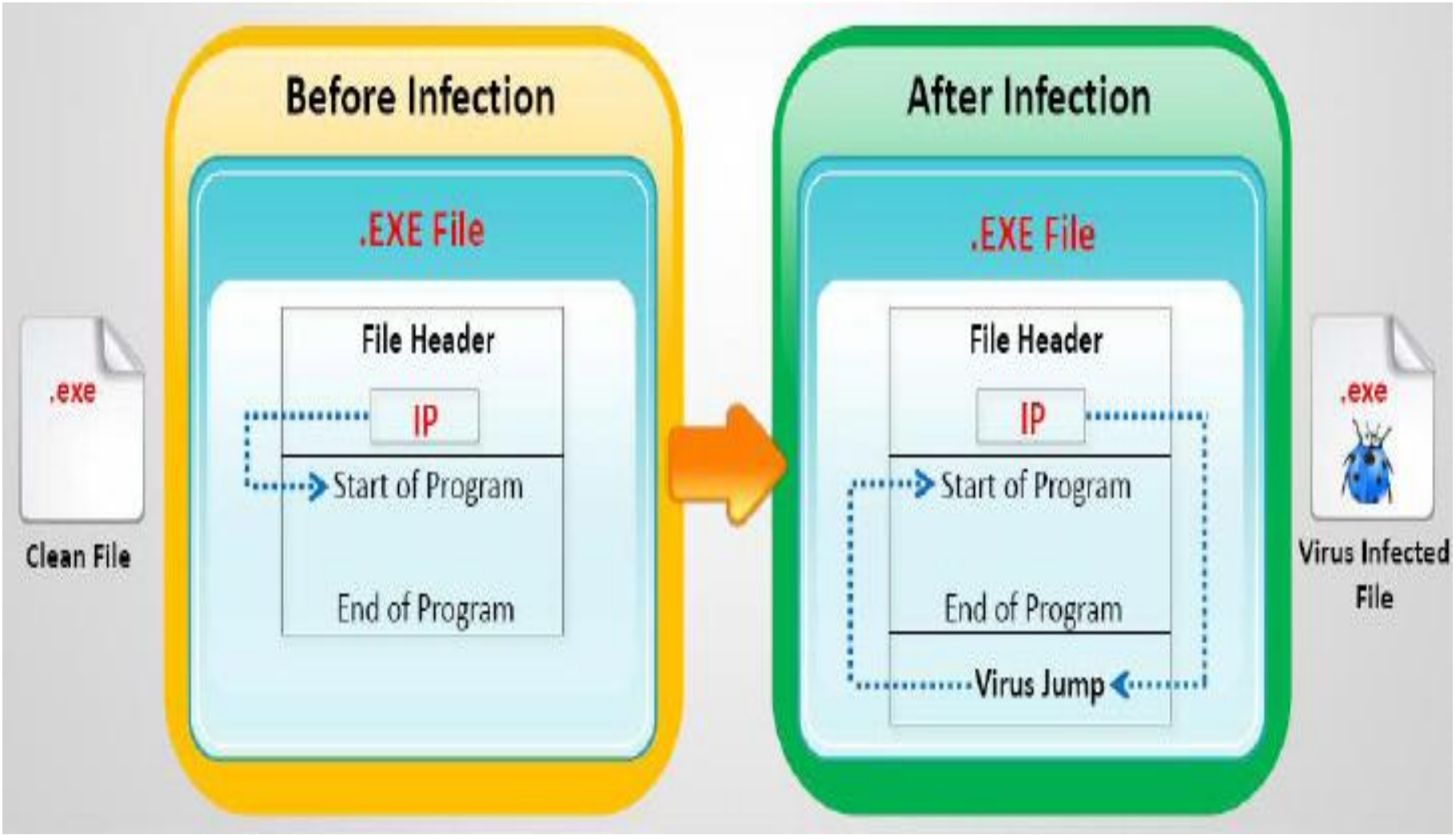
   Là kỹ thuật cơ bản cần phải có của mỗi virus. Có thể đơn giản hoặc phức tạp tuỳ loại virus.

- Kỹ thuật lây nhiễm Boot Record / Master Boot của đĩa: thay thế BR hoặc MB trên phân vùng hoạt động với chương trình virus.
- Kỹ thuật lây nhiễm file thi hành: chương trình virus sẽ được ghép vào file chủ bằng cách nối thêm, chèn giữa, điền vào khoảng trống, ghi đè…

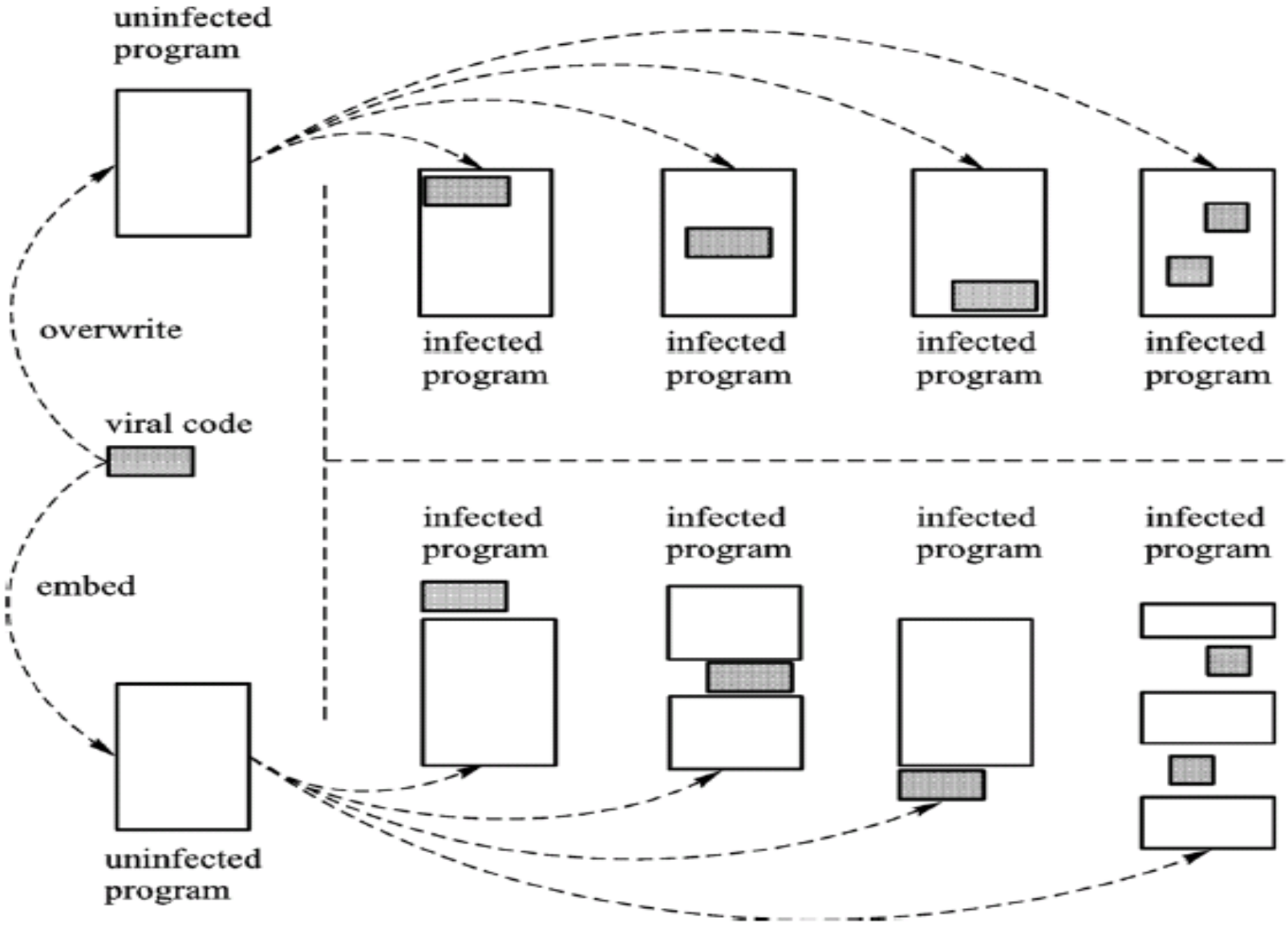
2. Các kỹ thuật của Virus máy tính

- **Thuật toán thường dùng để lây nhiễm một file .COM:**
  - Mở file
  - Ghi lại thời gian/ngày tháng/thuộc tính
  - Lưu trữ các byte đầu tiên (thường là 3 byte)
  - Tính toán lệnh nhảy mới
  - Đặt lệnh nhảy
  - Chèn thân virus chính vào
  - Khôi phục thời gian/ngày tháng/thuộc tính
  - Đóng file.

2. Các kỹ thuật của Virus máy tính



2. Các kỹ thuật của Virus máy tính



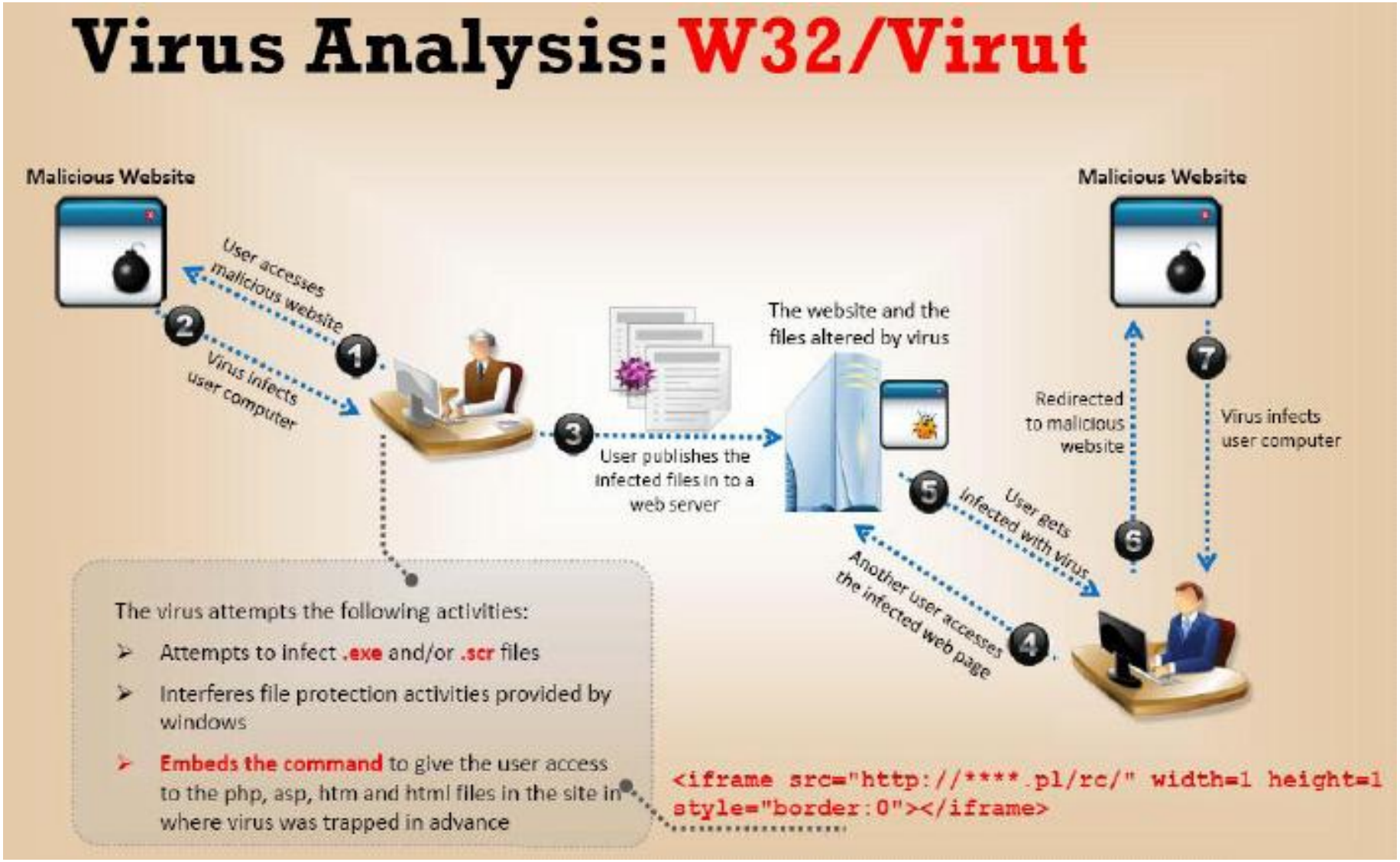
2. Các kỹ thuật của Virus máy tính

```
.rsrc:0042603E loc_42603E:                             ; CODE XREF: start+30↓j
.rsrc:0042603E                  cmp     dword ptr [ebx+4Eh], 'sihT'
.rsrc:00426045                  jnz     short loc_426053
Program control flow :00426047  mov     eax, [ebx+3Ch]
.rsrc:0042604A                  add     eax, ebx
.rsrc:0042604C                  cmp     word ptr [eax], 'EP'
.rsrc:00426051                  jz      short loc_426058
.rsrc:00426053
.rsrc:00426053 loc_426053:                             ; CODE XREF: start+29↑j
.rsrc:00426053                  sub     ebx, 100h
.rsrc:00426059                  jnp     short loc_42603E
.rsrc:0042605B ; ---------------------------------------------------------------
.rsrc:0042605B
.rsrc:0042605B loc_426058:                             ; CODE XREF: start+35↑j
.rsrc:0042605B                  mov     edx, [eax+78h]
```

Virus locates the offset to the PE header of Kernel32.dll

```
.rsrc:00426069 LocateGetProcAddress:                   ; CODE XREF: start:loc_426090↓j
.rsrc:00426069                  lodsd
.rsrc:0042606A                  add     eax, ebx
.rsrc:0042606C                  cmp     dword ptr [eax-1], 74654700h
.rsrc:00426073                  jnz     short loc_426090
.rsrc:00426075                  cmp     dword ptr [eax+3], 'corP'
.rsrc:0042607C                  jnz     short loc_426090
.rsrc:0042607E                  cmp     dword ptr [eax+7], 'rddA'
.rsrc:00426085                  jnz     short loc_426090
.rsrc:00426087                  cmp     dword ptr [eax+0Bh], 'sse'
.rsrc:0042608E                  jz      short GetProcAddressFound
.rsrc:00426090
.rsrc:00426090 loc_426090:                             ; CODE XREF: start+57↑j
.rsrc:00426090                                         ; start+60↑j ...
.rsrc:00426090                  loop    LocateGetProcAddress
.rsrc:00426092                  pop     ecx
.rsrc:00426093                  pop     ebp
.rsrc:00426094                  retn
.rsrc:00426095 ; ---------------------------------------------------------------
.rsrc:00426095
.rsrc:00426095 GetProcAddressFound:                    ; CODE XREF: start+72↑j
.rsrc:00426095                  sub     [esp+0Ch+var_C], ecx
```

2. Các kỹ thuật của Virus máy tính



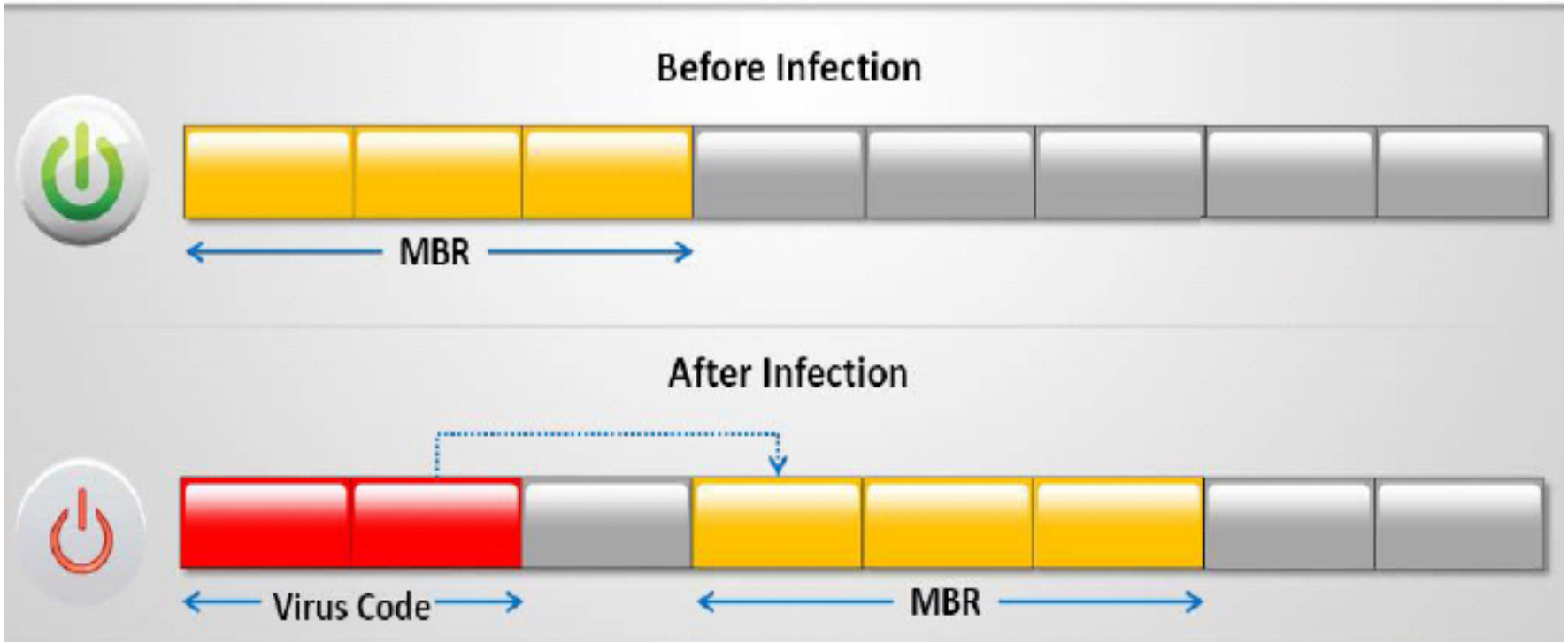
2. Các kỹ thuật của Virus máy tính

2. Kỹ thuật định vị trên vùng nhớ

- Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment:offset mới.
- Là một kỹ thuật quan trọng đối với các chương trình virus dạng mã máy (virus Boot, virus file). Virus macro và virus Script thực chất là các lệnh của chương trình ứng dụng nên không cần tiến hành kỹ thuật này.

2. Các kỹ thuật của Virus máy tính

- Boot sector virus **moves MBR to another location** on the hard disk and copies itself to the original location of MBR
- When system boots, **virus code is executed first** and then control is passed to original MBR



2. Các kỹ thuật của Virus máy tính

3. Kỹ thuật kiểm tra sự tồn tại

- Mỗi virus chỉ nên lây nhiễm/kiểm soát một lần để đảm bảo không làm ảnh hưởng đến tốc độ làm việc của máy tính.
- Virus phải kiểm tra sự tồn tại của chính mình trước khi lây nhiễm hoặc thường trú.
  - **Kiểm tra trên đối tượng bị lây nhiễm**
  - **Kiểm tra trên bộ nhớ**
- Kỹ thuật kiểm tra thường là:
  - **Dò tìm đoạn mã nhận diện trên file hoặc bộ nhớ.**
  - **Kiểm tra theo kích thước hoặc nhãn thời gian của file.**

2. Các kỹ thuật của Virus máy tính

4. Kỹ thuật thường trú

- Các virus boot phải phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, biến, vùng đệm.
- Các virus file cần phải kiểm tra xem chương trình đã thường trú chưa, nếu chưa sẽ định rõ vùng nhớ muốn sử dụng, copy phần virus vào bộ nhớ, sau đó khôi phục file chủ và trả quyền điều khiển về cho file chủ.

2. Các kỹ thuật của Virus máy tính

5. **Kỹ thuật mã hoá:**

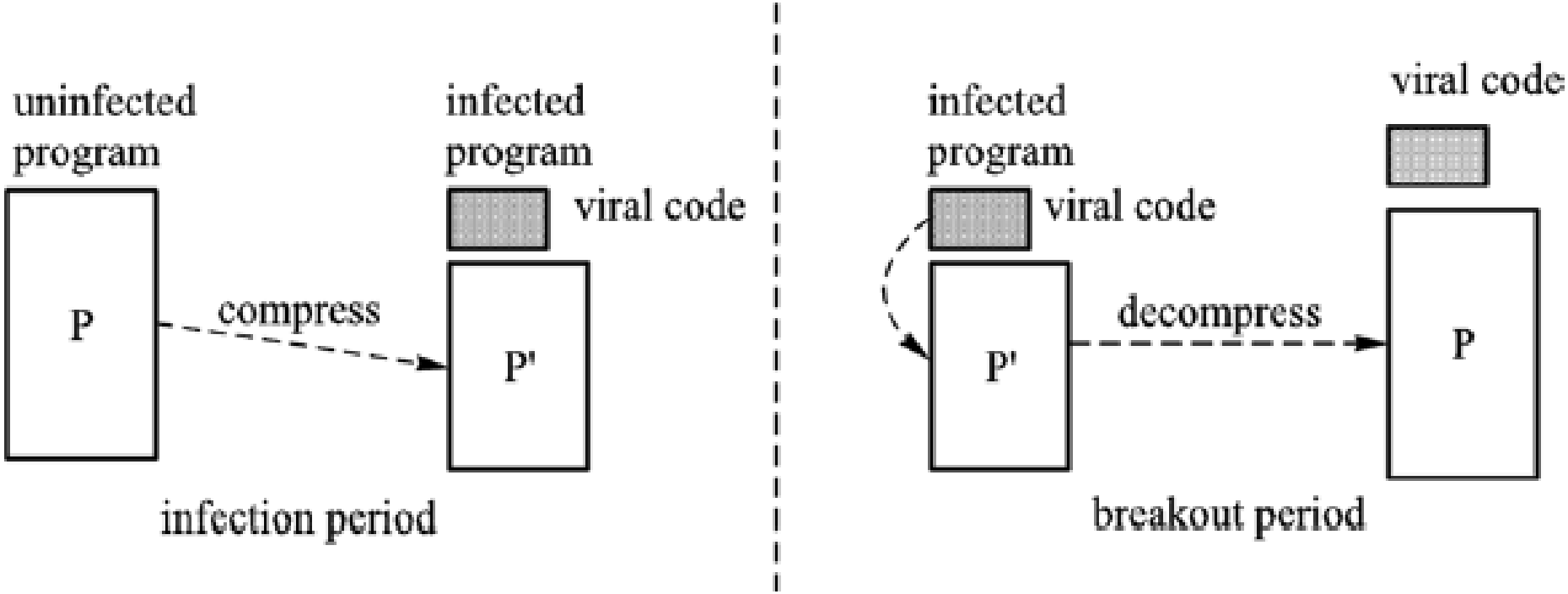
- Nhằm che giấu mã lệnh thực sự của chương trình virus. Thủ tục mã hoá cũng chính là thủ tục giải mã.

6. **Kỹ thuật nguỵ trang:**

- nhằm giấu giếm, nguỵ trang sự tồn tại của virus trên đối tượng chủ.
- Những virus sử dụng kỹ thuật này thường chậm bị phát hiện nên có khả năng lây lan mạnh.

2. Các kỹ thuật của Virus máy tính

- Sơ đồ nén file chủ để nguỵ trang sự tồn tại của Virus:
  - Kiểm tra kích thước file chủ định lây nhiễm
  - Nén file chủ
  - Gắn đoạn mã cần lây nhiễm vào file chủ
  - Có thể chèn thêm những đoạn ký tự vô nghĩa khi kích thước file chủ + virus vẫn nhỏ hơn kích thước file chủ nguyên thuỷ.
  - Giải nén file chủ trước khi file này thực thi.



2. Các kỹ thuật của Virus máy tính

7. Kỹ thuật phá hoại:

- Đa dạng
- Phá hoại dữ liệu trên máy tính
- Phá hỏng một phần máy tính

8. Kỹ thuật chống bẫy:

- Chọn lọc file trước khi lây nhiễm theo một số tiêu chí nào đó nhằm tránh những file bẫy của chương trình Antivirus.
  - Không lây nhiễm các file có số trong tên file
  - Không lây nhiễm những chương trình sử dụng nhiều mã lệnh đặc biệt.

2. Các kỹ thuật của Virus máy tính

- Không lây nhiễm các file có tên liên tục (ví dụ aaaaa.com…).
- Không lây nhiễm các file liên tục có cùng kích thước.
- Không lây nhiễm các file ở thư mục gốc.
- Không lây nhiễm các file có lệnh nhảy và lệnh gọi zero.
- ….

9. Kỹ thuật tối ưu:

❖ Gồm các kỹ thuật viết mã và thiết kế nhằm tối ưu chương trình về tốc độ và kích thước.

2. Các kỹ thuật của Virus máy tính

Các kỹ thuật đặc biệt

1. Kỹ thuật tạo vỏ bọc
2. Kỹ thuật đa hình
3. Kỹ thuật biến hình
4. Kỹ thuật chống mô phỏng
5. Kỹ thuật chống theo dõi

2. Các kỹ thuật của Virus máy tính

1. **Kỹ thuật tạo vỏ bọc:**

- Là kỹ thuật chống gỡ rối / dịch ngược mã lệnh virus nhằm chống lại phần mềm antivirus.
- Thường mã hoá hoặc sử dụng các lệnh JMP và CALL để chương trình lộn xộn, phức tạp.
- Sử dụng các thủ tục giả để phân tích viên gặp khó khăn khi phân biệt các tác vụ…

2. Các kỹ thuật của Virus máy tính

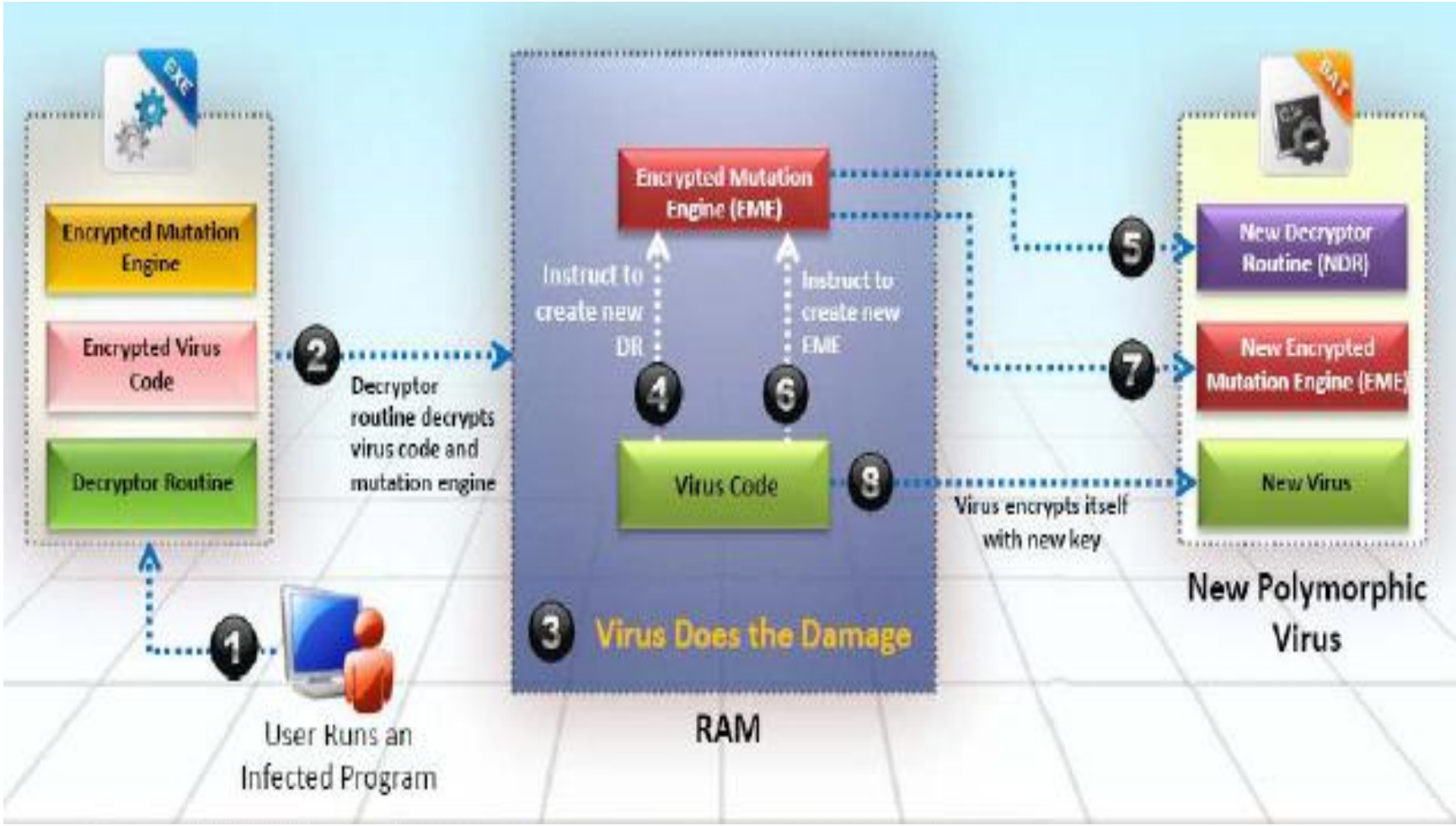
2. Kỹ thuật đa hình:

- Là kỹ thuật chống lại phương pháp dò tìm đoạn mã mà các chương trình antivirus thường sử dụng để nhận dạng một virus đã biết bằng cách tạo ra các bộ giải mã khác biệt.

3. Kỹ thuật biến hình:

- Cũng là một kỹ thuật chống lại các kỹ thuật nhận dạng của chương trình antivirus bằng cách sinh ra cả đoạn mã mới hoàn toàn.
- Là một kỹ thuật khó, phức tạp.

2. Các kỹ thuật của Virus máy tính



2. Các kỹ thuật của Virus máy tính

4. Kỹ thuật chống mô phỏng và theo dõi:

- Một số chương trình antivirus hiện đại sử dụng phương pháp heuristic để phát hiện virus dựa trên hành vi của chương trình. Kỹ thuật này nhằm chống lại sự phát hiện của chương trình antivirus như vậy.
- Thông thường là chèn thêm những đoạn mã lệnh "rác" không ảnh hưởng đến logic của chương trình xen kẻ giữa những mã lệnh thực sự.

3. Các kỹ thuật của Virus máy tính trên mạng

1. **Kỹ thuật lây nhiễm trên mạng**

- Sử dụng hàm GetLogicalDriveStrings để lây lan qua các ổ đĩa chia sẻ từ xa được ánh xạ thành ổ đĩa cục bộ.
- Sử dụng các hàm API để liệt kê các ổ đĩa mà người sử dụng đã kết nối.

3. Các kỹ thuật của Virus máy tính trên mạng

2. **Kỹ thuật phát tán virus trên mạng**

- Sử dụng sự phổ biến của thư điện tử
- Chặn các hàm API hỗ trợ mạng

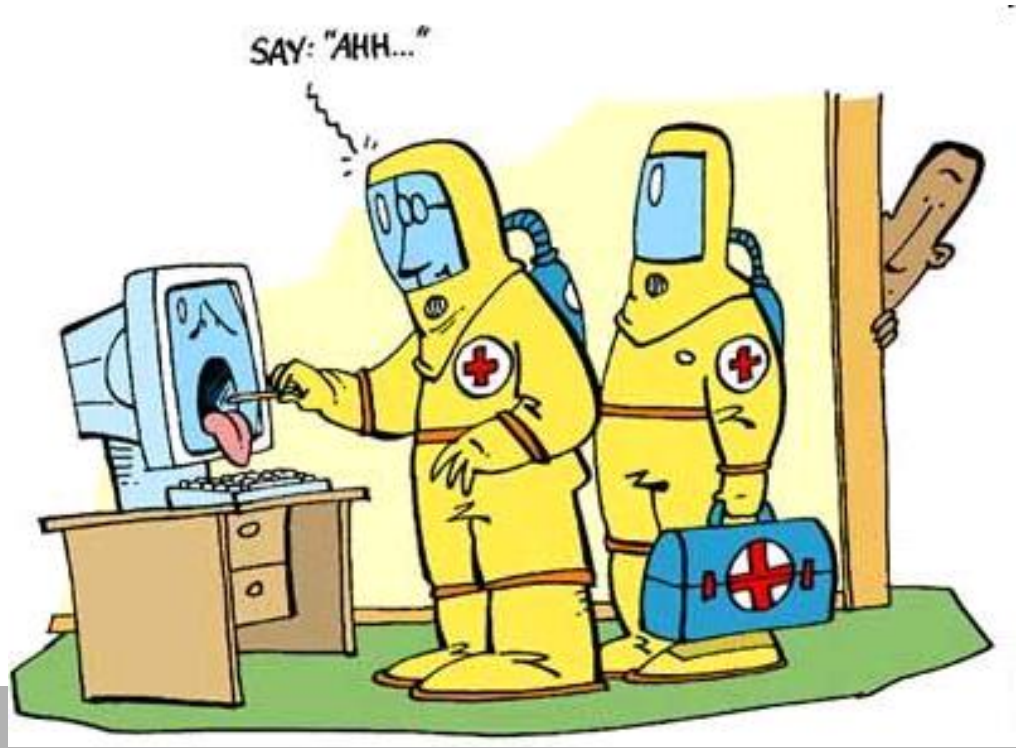
3. **Kỹ thuật phá hoại trên mạng**

- Tạo các cổng nghe đợi sẵn để virus có thể tiến hành các hoạt động phá hoại hay do thám như lấy trộm mật khẩu, khởi động máy, phá hoại hệ thống…
- Tấn công từ chối dịch vụ (DOS)
- …

4. Phòng chống virus máy tính

1. **Ý nghĩa:**

- Đảm bảo máy tính hoạt động ổn định.
- Chống mất cắp các thông tin mật.
- Bảo vệ dữ liệu an toàn.



4. Phòng chống virus máy tính

2. Các dấu hiệu máy tính nhiễm virus:

- Máy không khởi động được hoặc không vào Windows được.
- Máy hoặc ứng dụng dễ bị treo
- Máy chạy chậm hơn bình thường, ổ cứng đọc liên tục.
- Không in được
- Máy báo thiếu file nào đó.
- Xuất hiện nhiều file lạ không rõ nguồn gốc.
- Thông báo thiếu bộ nhớ
- Mất dữ liệu…

4. Phòng chống virus máy tính

3. Cách phòng chống virus máy tính:

- Hạn chế sử dụng đĩa mềm hoặc USB không rõ nguồn gốc mà chưa có sự kiểm tra bằng các phần mềm diệt virus.
- Không cài đặt các phần mềm không cần thiết hoặc download từ trên mạng về.
- Không sử dụng các phần mềm không có bản quyền.
- Không nên mở xem các thư điện tử lạ.
- Phải cài các phần mềm chống virus tốt nhất.
- Phải sao lưu dữ liệu thường xuyên
- …

4. Phòng chống virus máy tính

Run Port Monitor

Run File Monitor

Run the virus in this monitored environment

Run Network Monitor

Run Registry Monitor

4. Phòng chống virus máy tính

- Các chương trình tìm diệt Virus sẽ quét các tập tin thực thi, tập tin office, tập tin đính kèm E-mail, các tập tin được download và những dạng tập tin khác có thể trở thành host của Virus (Hostable files).
- Các phương pháp quét chuẩn bao gồm:
  - Basic scanning:
    - Tìm chữ ký của virus đã được biết đến trong các tập tin hostable, bao gồm cả cấu trúc, định dạng, các mẫu, và những đặc trưng khác.
    - Kiểm tra kích thước của các file hệ thống đã bị thay đổi để phát hiện nhiễm virus.

4. Phòng chống virus máy tính

- Heuristic scanning: quét các đoạn mã đáng ngờ trong các tập tin thực thi dựa trên công nghệ heuristics.
- ICV scanning:
  - Sử dụng giải thuật HMAC để tính toán giá trị kiểm tra tính toàn vẹn của tập tin thực thi chưa bị nhiễm virus và một khoá mã hoá cố định.
  - Một giá trị ICV được nối vào cuối của tập tin thực thi không bị nhiễm virus.
  - Các virus không biết mật mã sẽ không thể thay đổi ICV.
  - Khi một tập tin bị nhiễm virus, giá trị ICV của nó sẽ thay đổi so với giái trị ICV nguyên thuỷ.

4. Phòng chống virus máy tính

Virus Detection Methods

Scanning

Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus

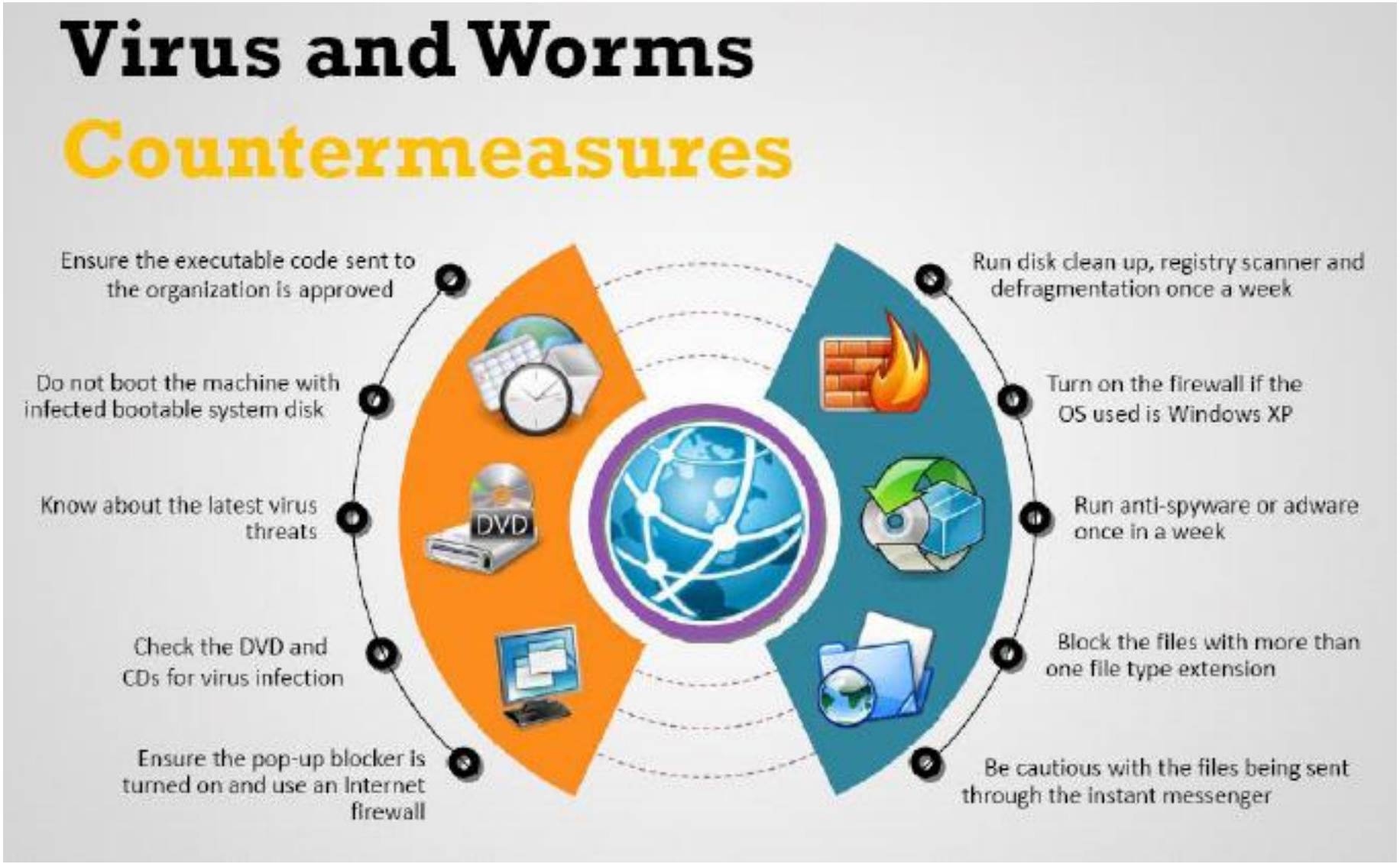
Integrity Checking

Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors

Interception

The interceptor monitors the operating system requests that are written to the disk

4. Phòng chống virus máy tính



4. Phòng chống virus máy tính

4. Phòng chống virus máy tính

C|EH™ Certified Ethical Hacker

Virus Analysis - IDA Pro Tool

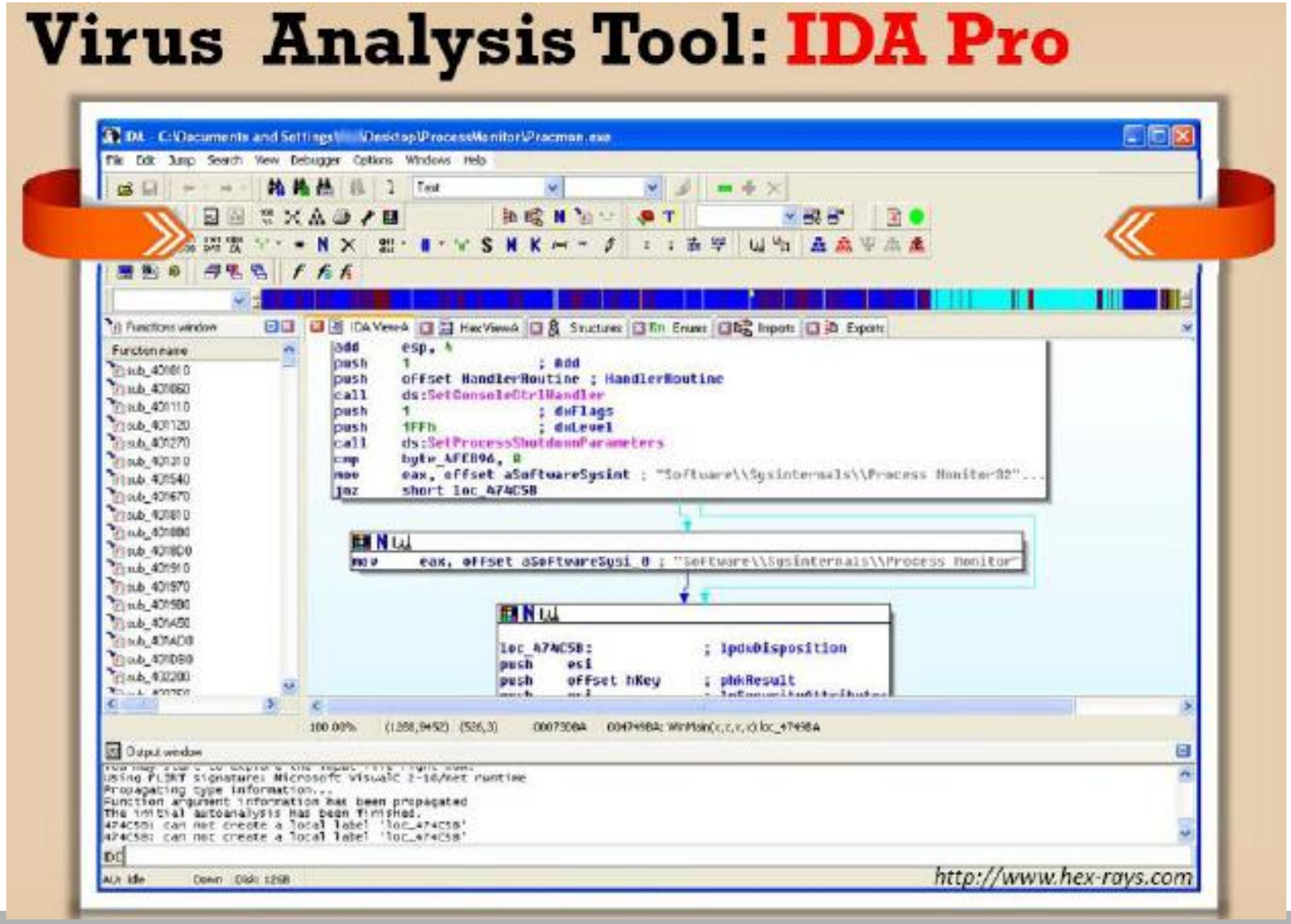
It is a dissembler and debugger tool that supports both Windows and Linux platforms

It is an interactive, programmable, extendible, multi-processor

Used in the analysis of hostile code and vulnerability research and software reverse engineering

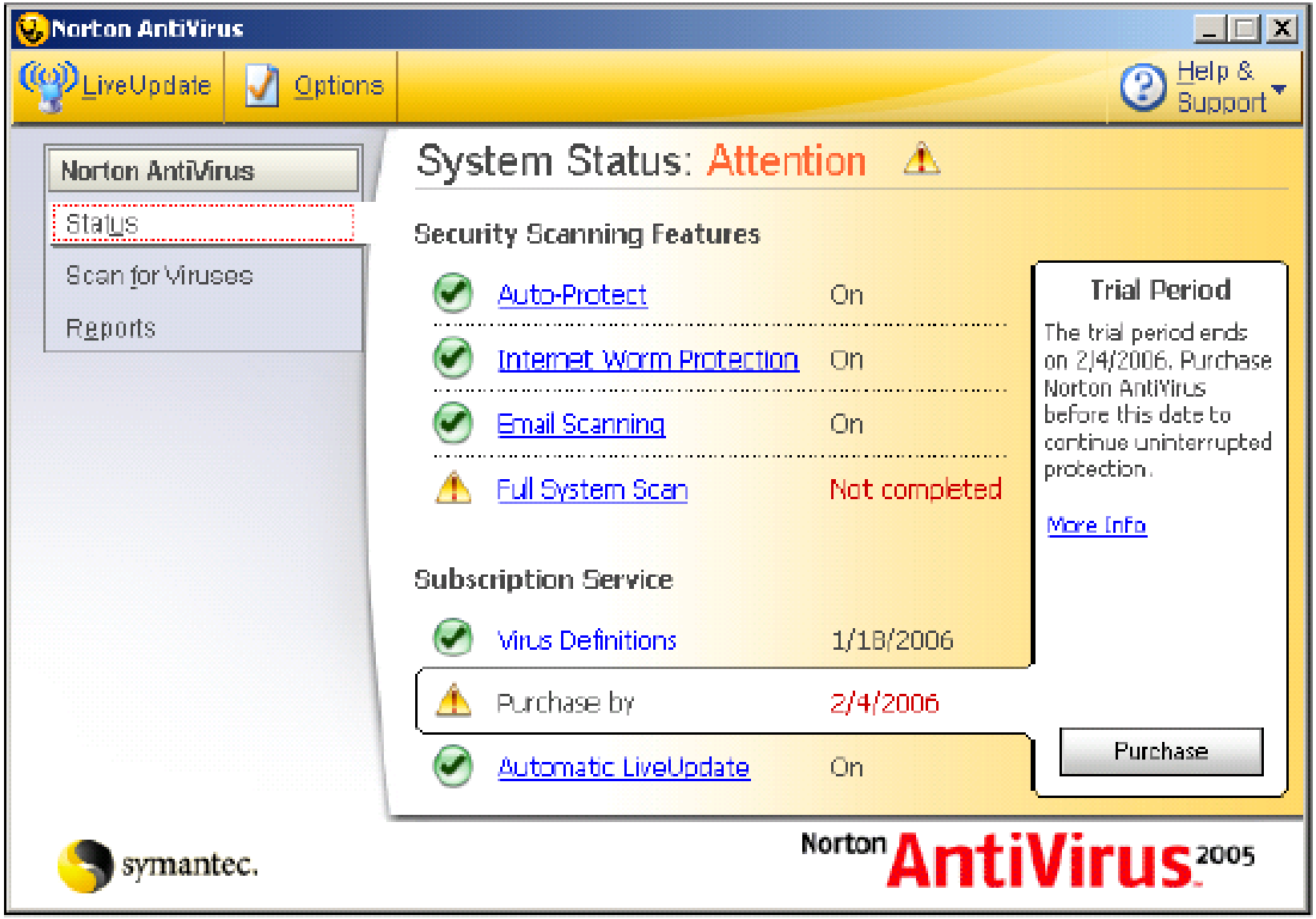
Allows automated unpacking/ decrypting of protected binaries

4. Phòng chống virus máy tính

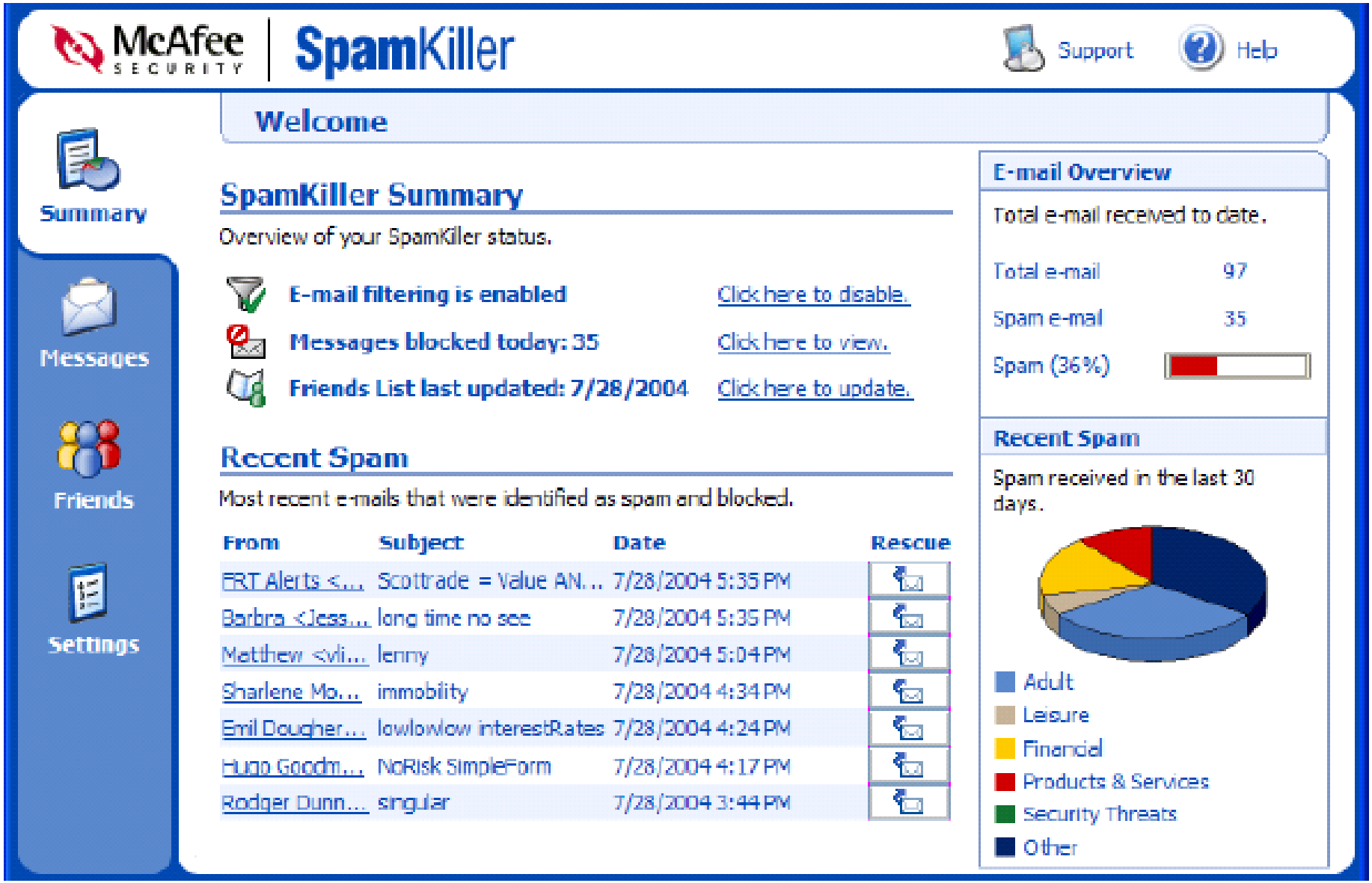


4. Phòng chống virus máy tính

4. Phòng chống virus máy tính



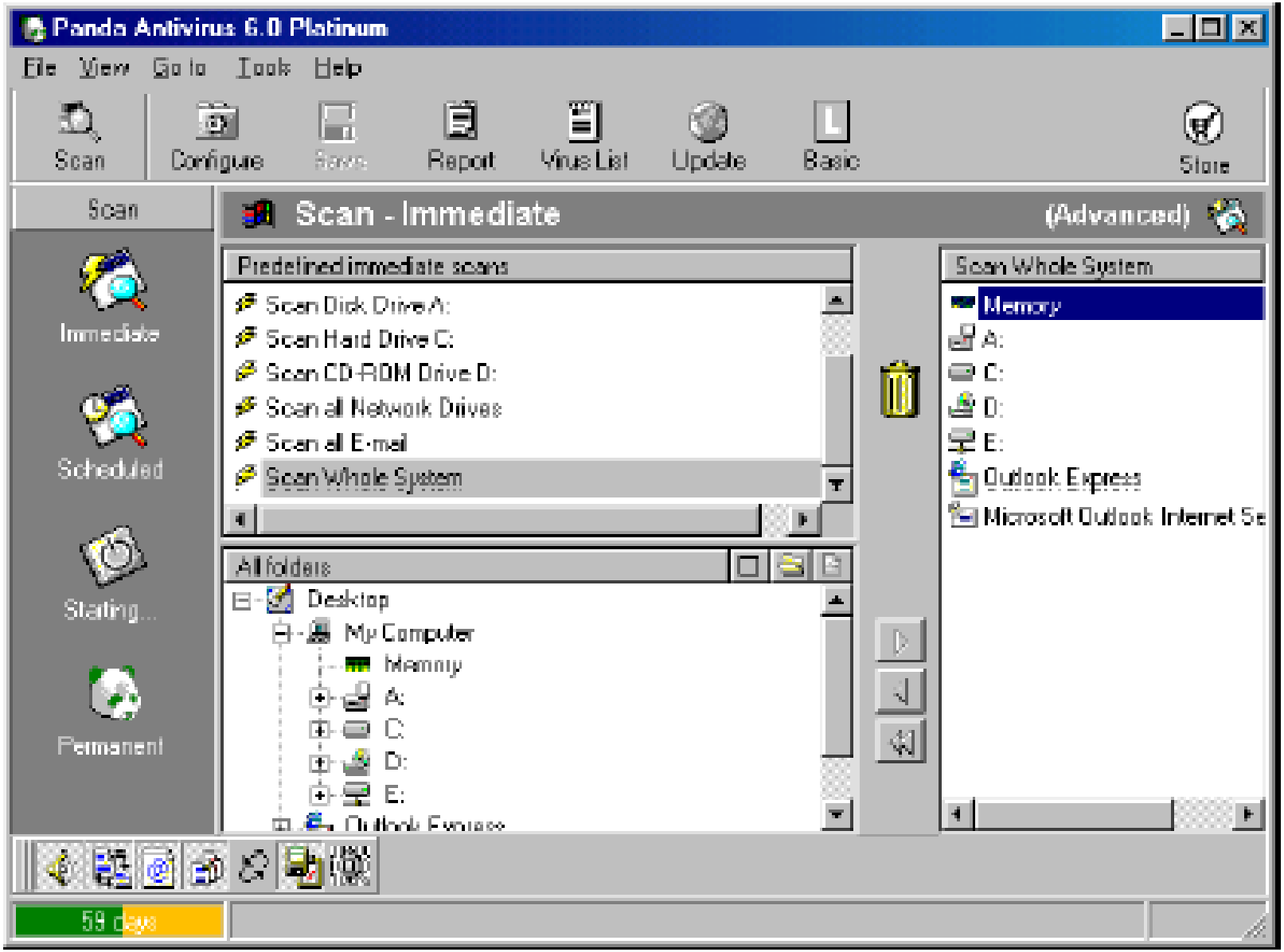
4. Phòng chống virus máy tính



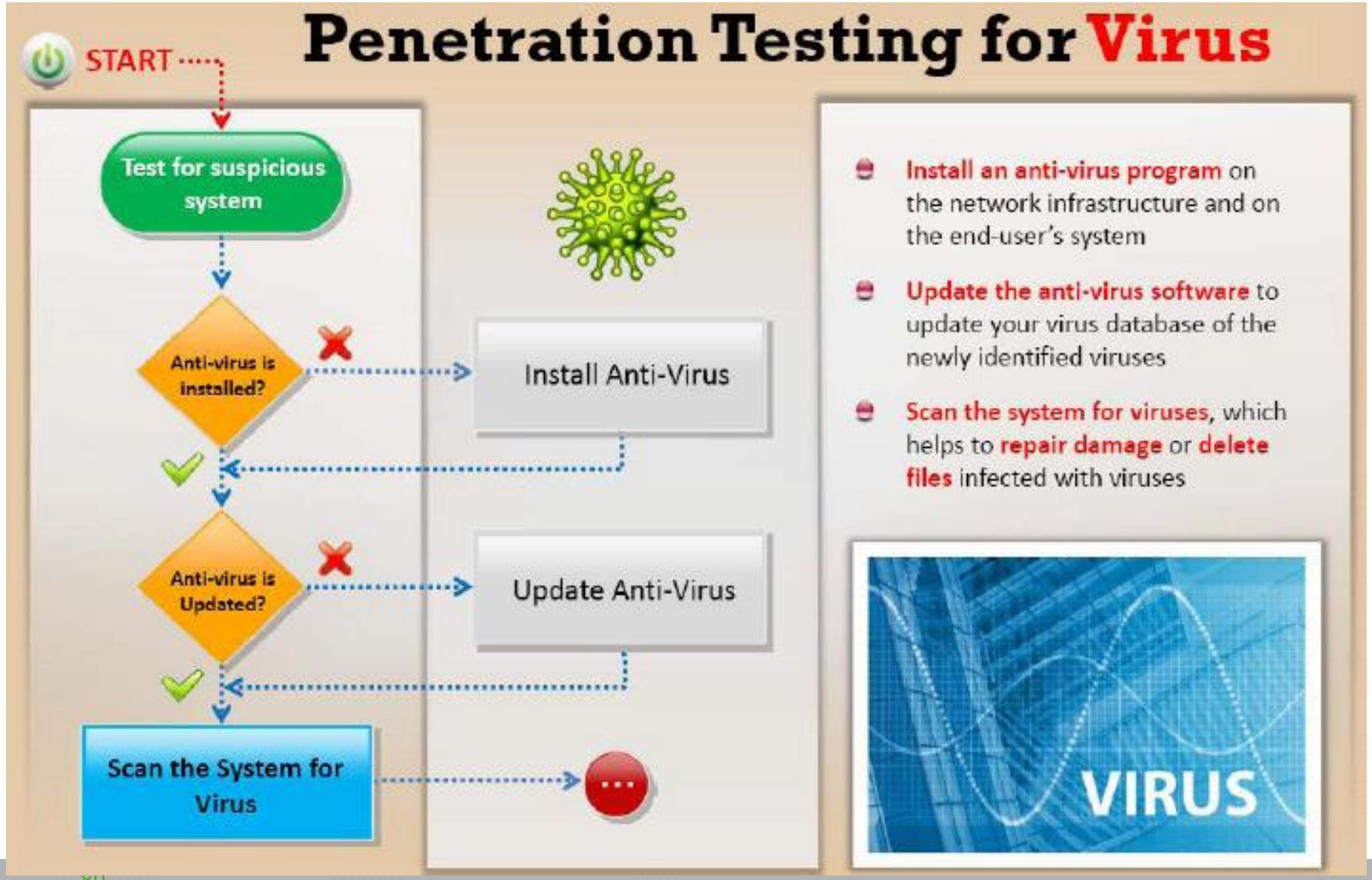
4. Phòng chống virus máy tính

4. Phòng chống virus máy tính

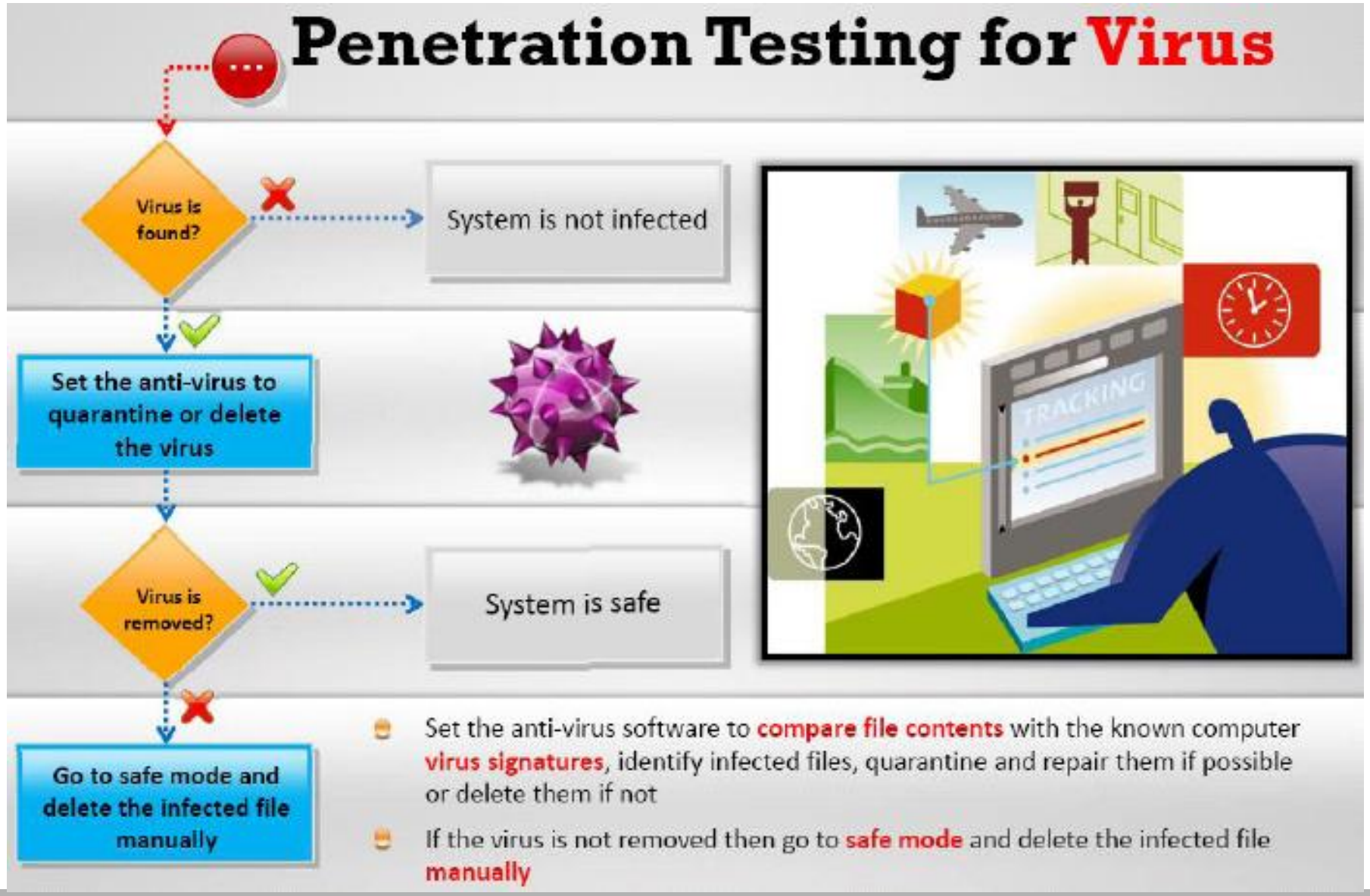
4. Phòng chống virus máy tính



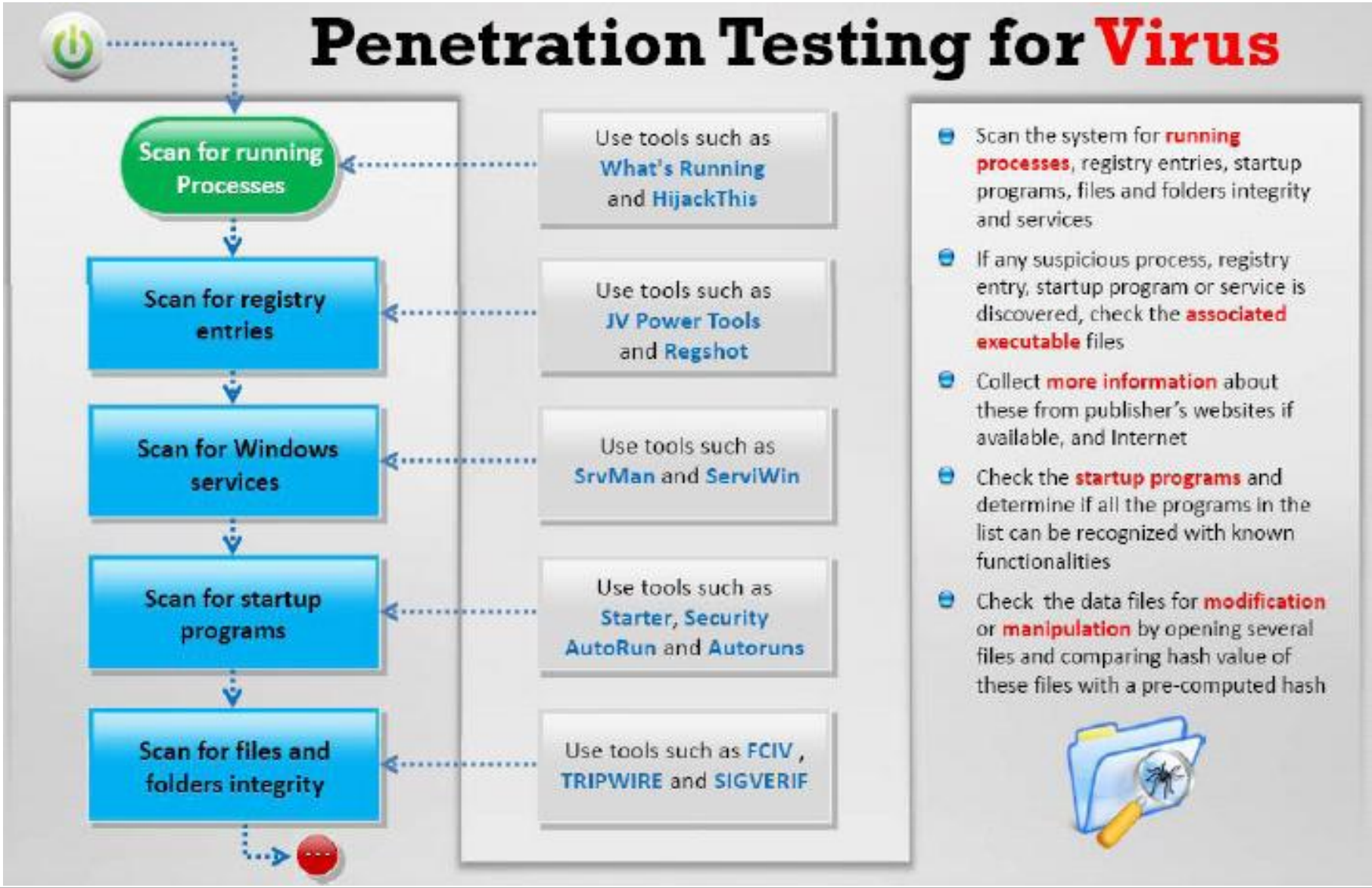
4. Phòng chống virus máy tính



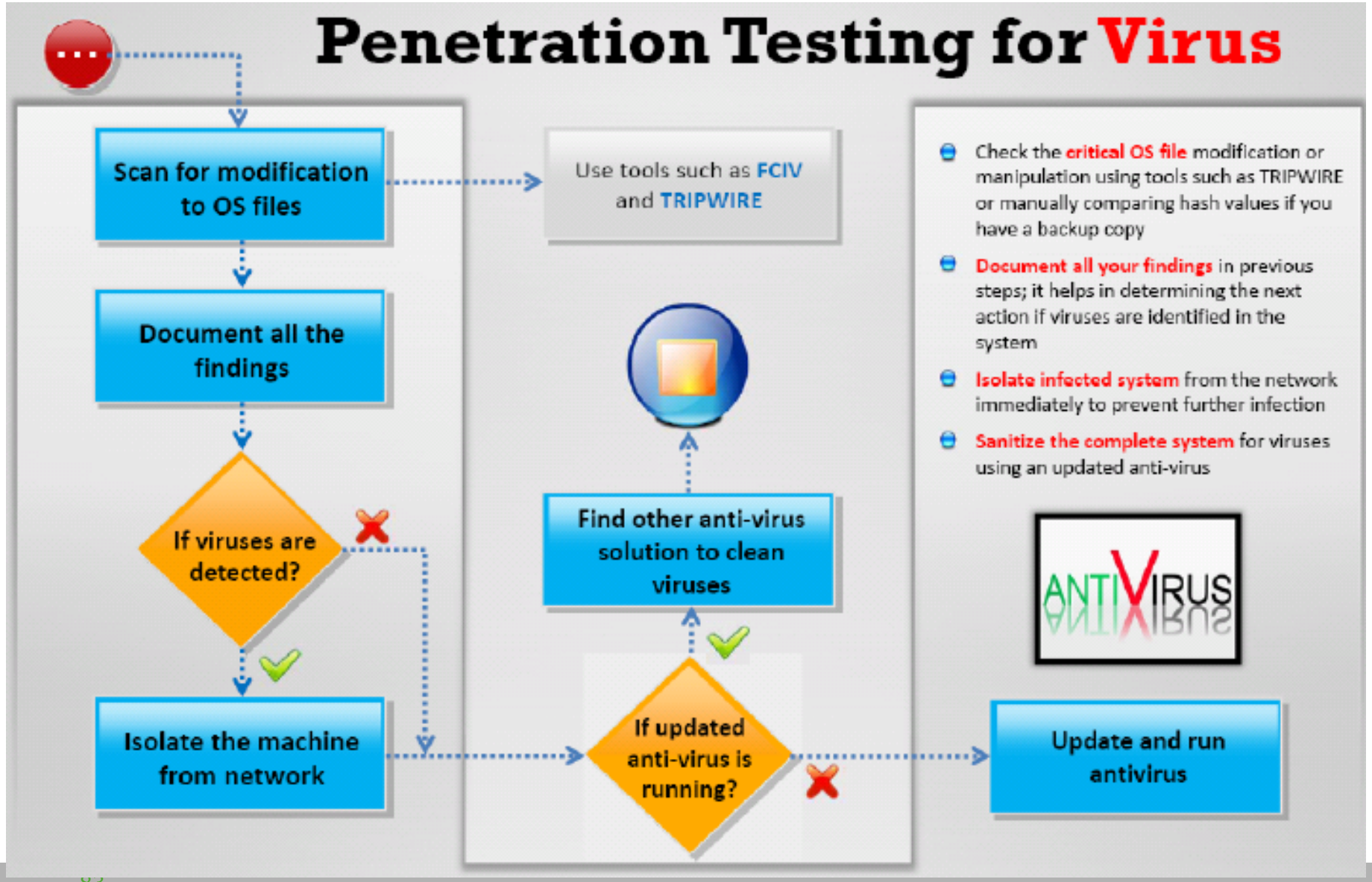
4. Phòng chống virus máy tính



4. Phòng chống virus máy tính



4. Phòng chống virus máy tính



4. Phòng chống virus máy tính

Anti-virus Tools

AVG Antivirus
http://free.avg.com

Norton AntiVirus
http://www.symantec.com

BitDefender
http://www.bitdefender.com

F-Secure Anti-Virus
http://www.f-secure.com

Kaspersky Anti-Virus
http://www.kaspersky.com

Avast Pro Antivirus
http://www.avast.com

Trend Micro Internet Security Pro
http://apac.trendmicro.com

McAfee AntiVirus Plus
http://home.mcafee.com

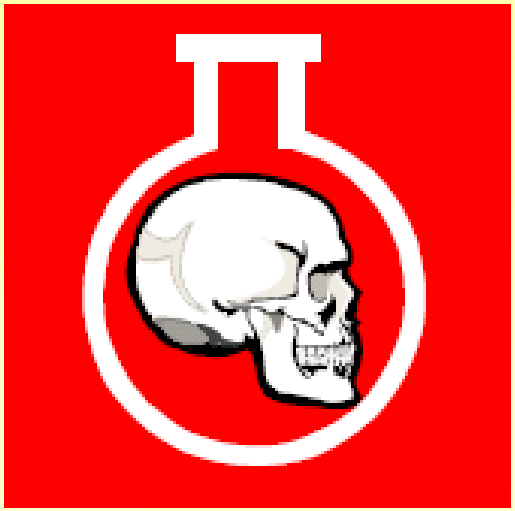
4. Phòng chống virus máy tính

- Aladdin Knowledge Systems http://www.esafe.com/
- Central Command, Inc. http://www.centralcommand.com/
- Computer Associates International, Inc. http://www.cai.com
- Frisk Software International http://www.f-prot.com/
- Trend Micro, Inc. http://www.trendmicro.com
- Norman Data Defense Systems http://www.norman.com
- Panda Software http://www.pandasoftware.com/
- Proland Software http://www.pspl.com
- Sophos http://www.sophos.com

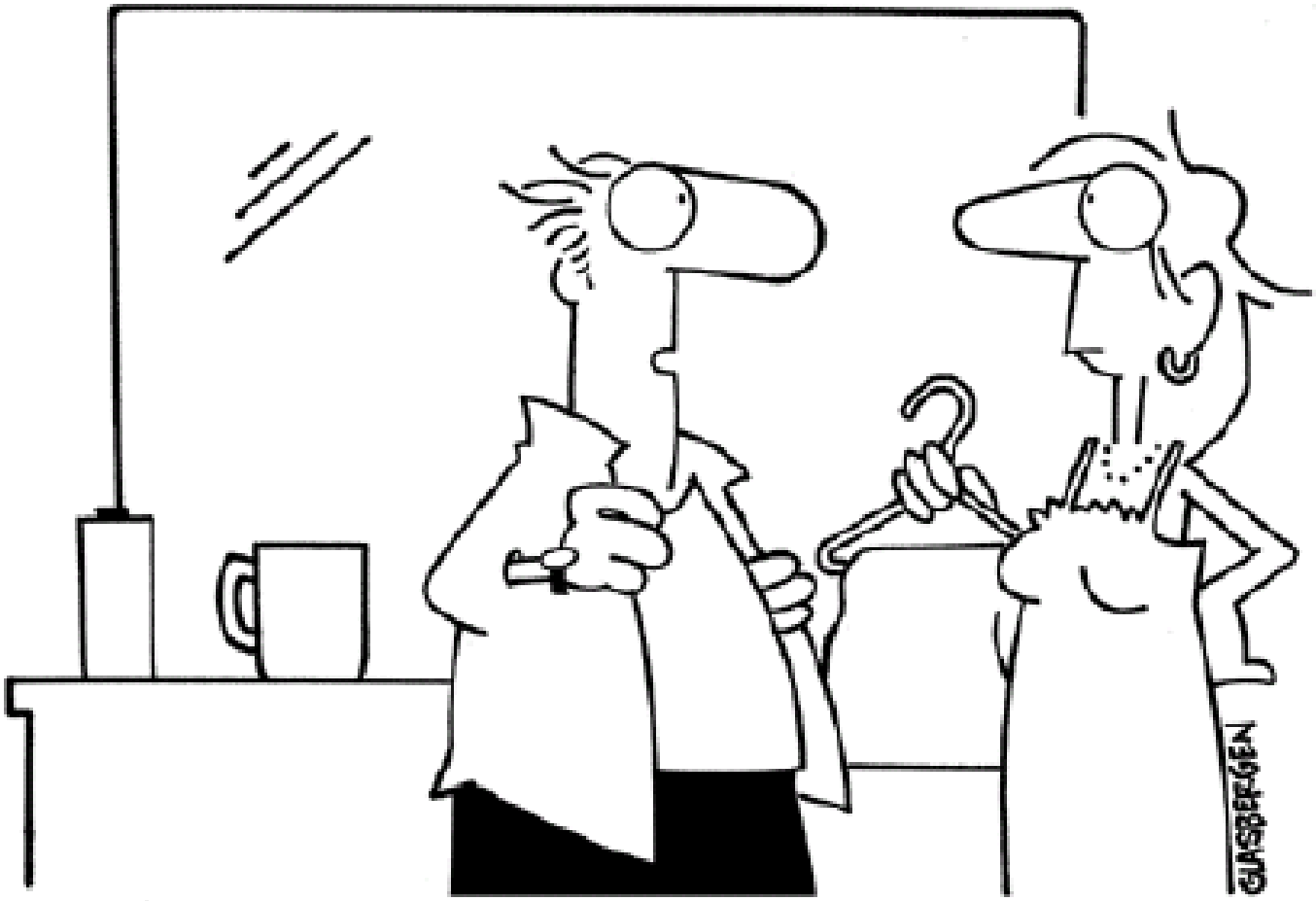
4. Phòng chống virus máy tính

The following databases can be useful if you are looking for specific information about a particular virus:

Proland - Virus Encylopedia
http://www.pspl.com/virus_info/
Norman - Virus Encylopedia
http://www.norman.com/Virus/en-us
AVG - Virus Encyclopedia
http://www.grisoft.com/doc/Virus+Encyclopaedia/lng/us/tpl/tpl01
Virus Bulletin - Virus Encyclopedia
https://www.virusbtn.com/login
F-Secure Virus Info Center
http://www.f-secure.com/vir-info/
McAfee - Virus Information Library
http://vil.mcafee.com/
Panda Software - Virus Encyclopedia
http://www.pandasoftware.com/library/
Sophos Virus Information
http://www.sophos.com/virusinfo/
Symantec AntiVirus Research Center
http://www.symantec.com/avcenter/index.html
Trend Micro - Virus Encyclopedia
http://www.antivirus.com/vinfo/virusencyclo/default.asp



4. Phòng chống virus máy tính



"I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it's time to go home."

5. Bài tập

1. Dưới đây liệt kê một số Worm phổ biến và port tương ứng. Tìm kiếm tài liệu liên quan và mô tả cách hoạt động của 5 Worm khác nhau trong danh sách.

port	protocol layer	name
445	TCP	Zotob
1080	TCP	MyDoom.B
2041	TCP	W32/korgo
2745	TCP	Bagle.C
3067	TCP	W32/korgo
3127	TCP	MyDoom.A
3128	TCP	MyDoom.B
5554	TCP	Sasser–FTP server
8080	TCP	MyDoom.B
8998	UDP	Sobig.F
9898	TCP	Dabber
9996	TCP	Sasser–remote shell
10080	TCP	MyDoom.B

5. Bài tập

2. Dưới đây liệt kê một số Trojan phổ biến và port tương ứng. Tìm kiếm tài liệu liên quan và mô tả cách hoạt động của 5 Trojan khác nhau trong danh sách.

port	protocol layer	name
1243	TCP	SubSeven
1349	UDP	Back Orifice DLL
1999	TCP	SubSeven
2583	TCP and UDP	WinCrash
6711	TCP	SubSeven
6776	TCP	SubSeven
8787	TCP and UDP	Back Orifice 2000
12345	TCP	NetBus
12346	TCP	NetBus Pro
27374	UDP	SubSeven
54320	TCP and UDP	Back Orifice 2000
54321	TCP and UDP	Back Orifice 2000
57341	TCP and UDP	NetRaider

5. Bài tập

3. Xây dựng những quy tắc ACL để chặn các Worm và các Trojan (đã nêu trong bài 1 và 2) xâm nhập vào mạng nội bộ.
4. Mô tả chức năng quét Heuristic để tìm Virus.
5. Mô tả sự giống nhau và khác nhau trong cách hoạt động giữa các phần mềm McAfee VirusScan và Norton AntiVirus.
6. Tìm kiếm từ các trang web có liên quan danh sách Virus và Trojan mới xuất hiện trong 2 tuần qua. Nêu một số đặc điểm chính của chúng.
7. Giải thích tại sao System Administrator không nên sử dụng một tài khoản người dùng có mật khẩu super-user để duyệt Web hoặc gởi và nhận E-Mail.

5. Bài tập

8. Web 2.0 xuất hiện vào năm 2004, đại diện cho thế hệ thứ hai của công nghệ Web. Bảng dưới đây mô tả vài kỹ thuật tương ứng giữa Web 2.0 và Web 1.0 thế hệ trước:

Web 1.0 technology	Web 2.0 technology
personal Web pages blogs	blogs
Akamai	BitTorrent
mp3.com	Napster
DoubleClick	Google AdSense
Britannica Online	Wikipedia
content management systems	wikis

Web 2.0 có cùng một số vấn đề về bảo mật như Web 1.0 và còn phát sinh thêm một số vấn đề mới. Tìm các tài liệu liên quan và mô tả 5 vấn đề bảo mật trong Web 2.0.

5. Bài tập

9. Vào trang http://www.microsoft.com/downloads, download về và cài đặt trên máy tính các phần mềm:
    1. Windows Defender
    2. Microsoft Security Essentials

- Chạy Windows Defender để quét Spyware, giải thích cơ chế hoạt động của phần mềm này.
- Đánh giá Microsoft Security Essentials với một số phần mềm tương tự phổ biến nhất hiện nay về:
    1. Khả năng chống mã độc hại
    2. Tường lửa tích hợp vào IE
    3. Hệ thống giám sát mạng để tăng khả năng ngăn chận tấn công từ bên ngoài
    4. Tiêu tốn tài nguyên, thời gian hoạt động…

5. Bài tập

10. Trong hệ điều hành Windows, cookies của trình duyệt IE được lưu trữ trên ổ đĩa C trong thư mục Documents and Settings. Vào thư mục là tên người dùng, vào thư mục Cookies. Chọn và mở ngẫu nhiên một tập tin cookie. Giải thích những gì bạn thấy, và trả lời các câu hỏi:
    1. Nếu cookie được truyền tới các máy chủ Web dưới dạng plaintext, liệt kê và mô tả các mối đe dọa bảo mật tiềm tàng mà người dùng có thể sẽ gặp.
    2. Nếu người dùng được phép chỉnh sửa các tập tin cookie lưu trữ trên máy tính cục bộ, liệt kê và mô tả các mối đe dọa bảo mật tiềm tàng có thể xảy ra cho các máy chủ Web.

5. Bài tập

11. Nêu chức năng và cách sử dụng các công cụ:

- Netstat
- Fport
- TCPView
- CurrPorts Tool
- Process Viewer
- What's running
- One file exe maker

5. Bài tập

12. Thực hiện các bài lab trong CEH v8

- Module 6: Trojans and Backdoors
- Module 7: Virus and Worms

5. Bài tập

1. Lập bảng so sánh đặc điểm của Trojan, Virus, Worm.
2. Liệt kê các biện pháp phòng chống Trojan và Virus theo thứ tự ưu tiên từ cao đến thấp.
3. Tìm và nêu đặc điểm của 6 loại mã độc (2 virus, 2 worm, 2 trojan) xuất hiện trong thời gian gần đây (ghi chú nguồn tham khảo).