Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan về an ninh mạng
2. Các phần mềm gây hại
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 vành đai
9. Tìm kiếm phát hiện xâm nhập

BÀI 2

CÁC PHẦN MỀM GÂY HẠI

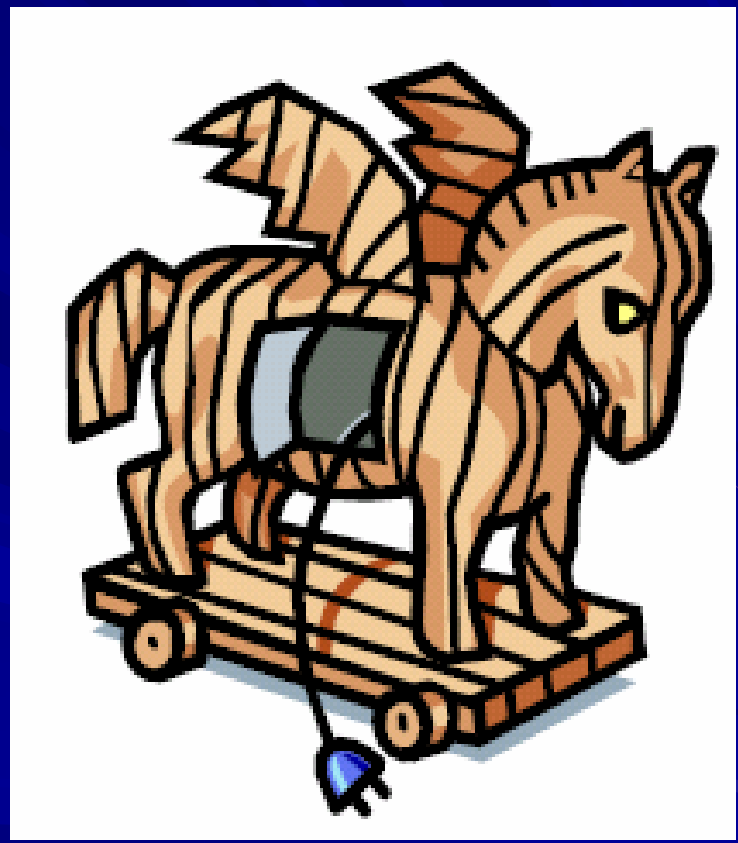
A. TROJAN VÀ BACKDOOR

Nội dung

1. Lịch sử hình thành Trojan
2. Khái niệm về Trojan
3. Phân loại Trojan
4. Một số Trojan phổ biến
5. Phòng chống Trojan
6. Một số cổng đi cùng các Trojan thông dụng
7. Bài tập

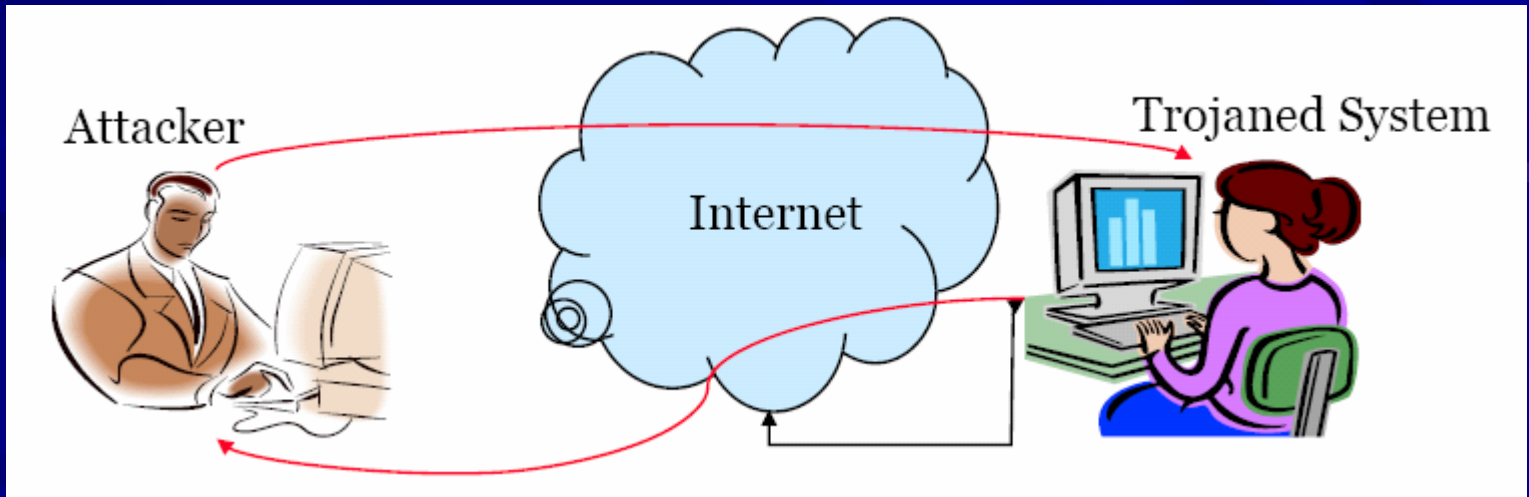
1. Lịch sử hình thành Trojan

- Ngựa Trojan trong truyền thuyết Hy Lạp cổ đại thế kỷ 17.
- Trojan trên máy tính được tạo ra đầu tiên là Back Orifice, có cổng xâm nhập là 31337.



2. Khái niệm về Trojan

- Trojan là chương trình gây tổn hại đến người dùng máy tính, phục vụ cho mục đích riêng nào đó của hacker.
- Thường hoạt động bí mật và người dùng không nhận ra sự hoạt động này.
- Công dụng hay gặp nhất của trojan là thiết lập quyền điều khiển từ xa cho hacker trên máy bị nhiễm trojan.



2. Khái niệm về Trojan

- Trojan không tự nhân bản như virus máy tính mà chỉ chạy ngầm trong máy bị nhiễm.
- Trojan thường làm chậm tốc độ máy tính, cấm chỉnh sửa registry…

2. Khái niệm về Trojan

Các con đường để Trojan xâm nhập vào hệ thống

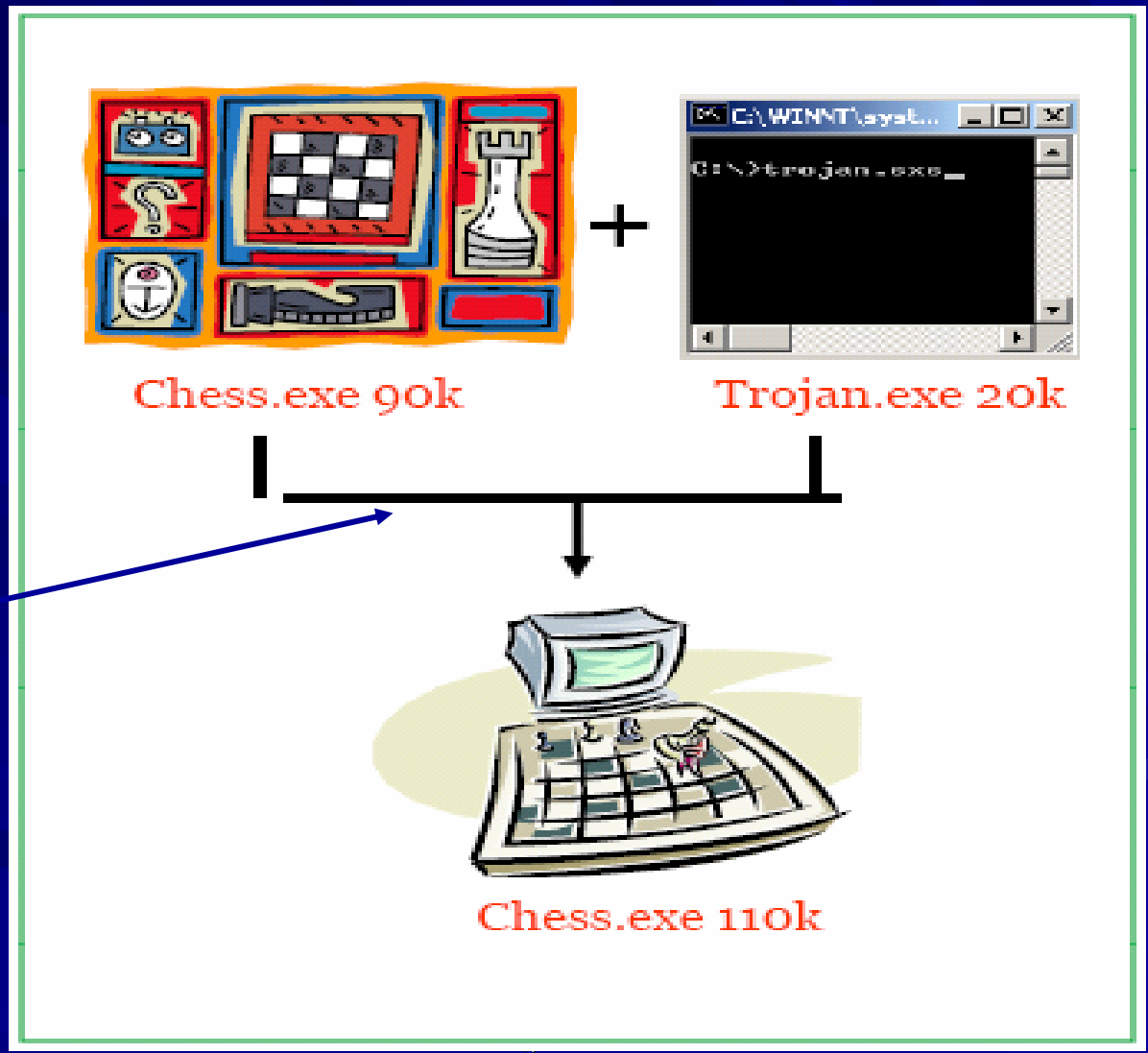
- Ứng dụng Messenger.
- File đính kèm.
- Truy cập vật lý.
- Duyệt Web và Email.
- Chia sẻ file.
- Phần mềm miễn phí.
- Download tập tin, trò chơi, screensaver từ internet…

2. Khái niệm về Trojan

Các con đường để Trojan xâm nhập vào hệ thống

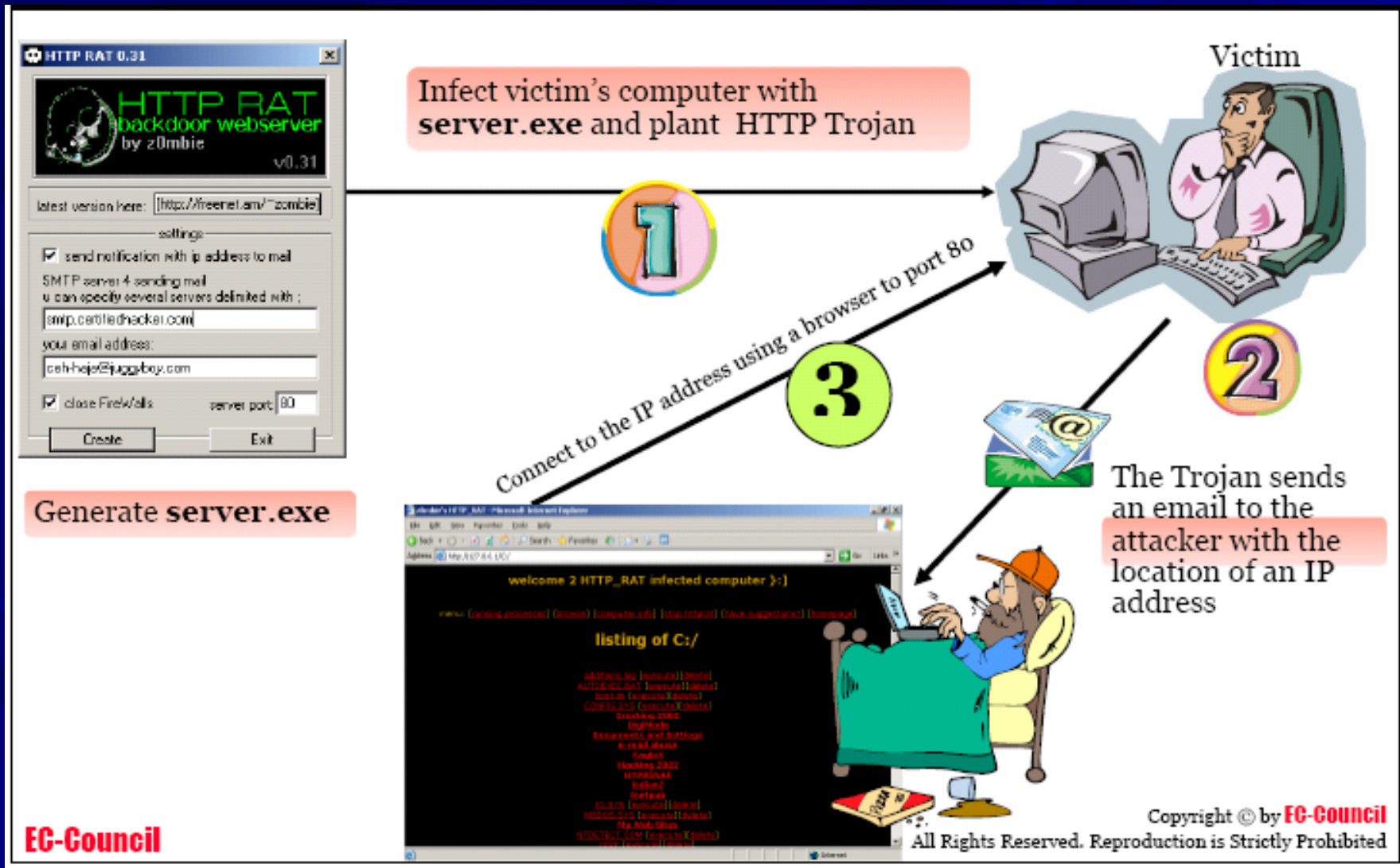
Graffiti.exe

One file exe maker



2. Khái niệm về Trojan

Các con đường để Trojan xâm nhập vào hệ thống



3. Phân loại Trojan

- Loại điều khiển từ xa (RAT)
- Keyloggers
- Trojan lấy cắp password
- FTP trojans
- Trojan phá hoại
- Trojan chiếm quyền kiểu leo thang

3.1. Trojan điều khiển từ xa (RAT)

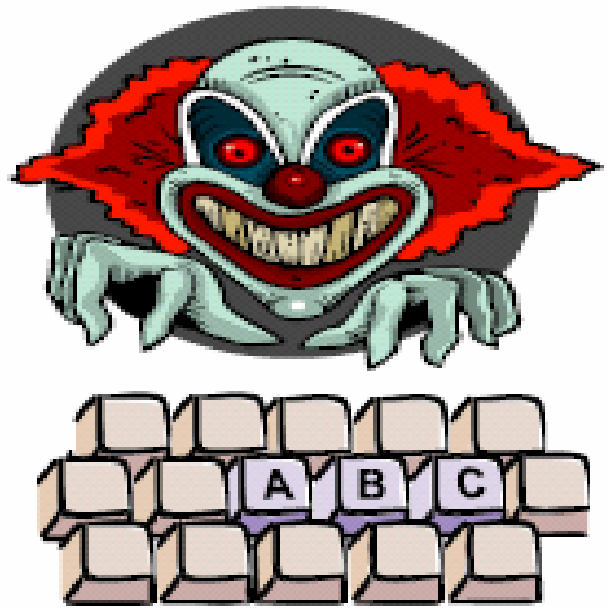
- RAT biến máy tính bị nhiễm trojan thành một server để máy tính client của hacker truy cập vào và nắm quyền điều khiển.
- Tự động kích hoạt mỗi khi máy tính hoạt động.
- Gồm 2 file, một cho server, một cho client.
- Thường được ngụy trang dưới một kiểu file bình thường nào đó để giấu kiểu exe.

3.1. Trojan điều khiển từ xa (RAT)

- Mỗi RAT thường chạy server dưới một cổng riêng biệt cho phép hacker thâm nhập vào máy bị nhiễm trojan và tiến hành điều khiển từ xa.
- Thường vô hiệu hoá việc chỉnh sửa registry nên khó xoá trojan này.
- Đôi khi có thể sử dụng trong việc quản lý máy tính từ xa.
- Phổ biến có Back Orifice, Girlfriend, Netbus…

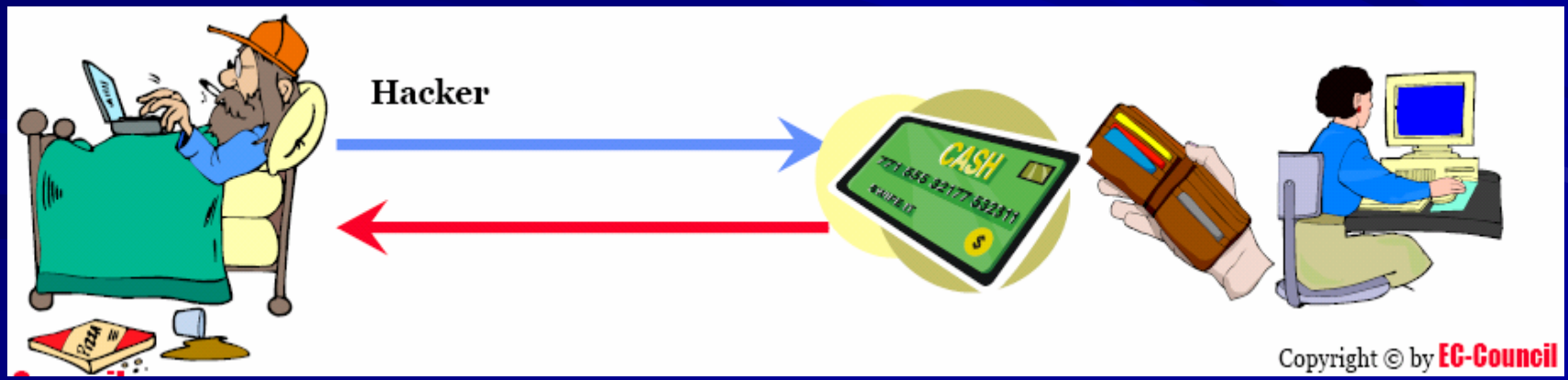
3.2. Keyloggers

- Keylogger bao gồm hai loại, một loại keylogger phần cứng và một loại là phần mềm.
- Nhỏ gọn, sử dụng ít bộ nhớ nên khó phát hiện.
- Hoạt động đơn giản, chủ yếu là ghi lại diễn biến của bàn phím rồi lưu lại trên máy hoặc gởi về cho hacker qua email.



3.2. Keyloggers

- Nếu dùng để giám sát con cái, người thân xem họ làm gì với PC, với internet, khi chat với người lạ thì keylogger là tốt.
- Khi sử dụng keylogger nhằm đánh cắp các thông tin cá nhân (tài khoản cá nhân, mật khẩu, thẻ tín dụng) thì keylogger là xấu.



3.2. Keyloggers

Một keylogger thường gồm ba phần chính:

- Chương trình điều khiển: điều phối hoạt động, tinh chỉnh các thiết lập, xem các tập tin nhật ký. Thông thường chỉ có thể gọi bằng tổ hợp phím tắt.
- Tập tin hook, hoặc là một chương trình monitor dùng để ghi nhận lại các thao tác bàn phím, capture screen.
- Tập tin nhật ký (log), nơi chứa đựng toàn bộ những gì hook ghi nhận được.

Ngoài ra, tùy theo loại có thể có thêm phần chương trình bảo vệ (protect), chương trình thông báo (report)…

3.2. Keyloggers

3.2. Keyloggers

3.3. Trojan ăn trộm password

- Ăn cắp các loại mật khẩu lưu trên máy bị nhiễm như mật khẩu của ICQ, IRC, Hotmail, Yahoo… rồi gởi về cho hacker qua email.
- Các loại trojan phổ biến là Barri, Kuang, Barok.

3.4. FTP Trojan

- Loại này mở cổng 21 trên máy bị nhiễm nên mọi người đều có thể truy cập máy này để tải dữ liệu.

3.5. Trojan phá hoại

- Mục đích chính là phá hoại
- Phá huỷ đĩa cứng, mã hoá các file
- Rất nguy hiểm, khó kiểm soát

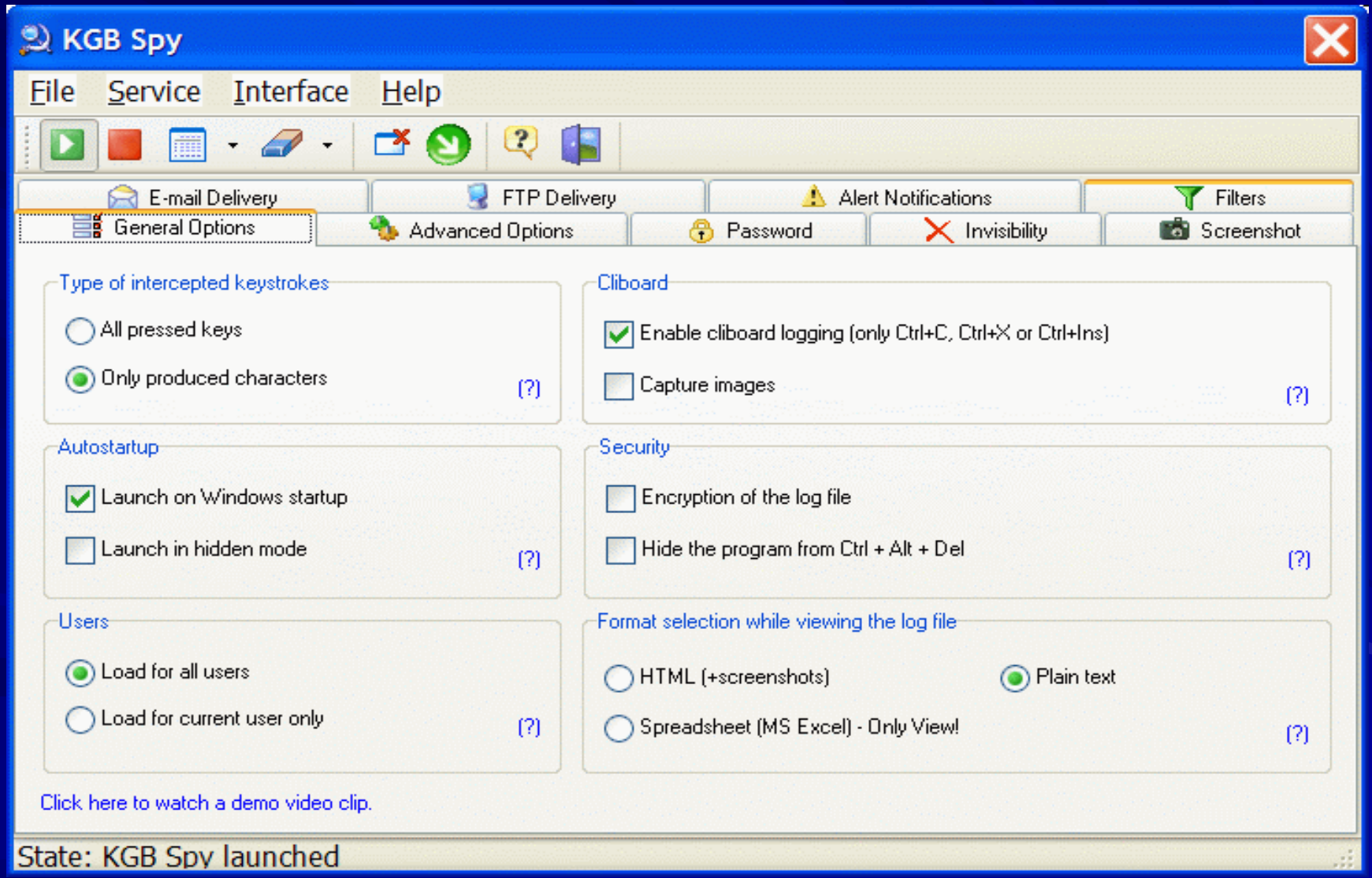
3.6. Trojan chiếm quyền kiểu leo thang đặc quyền

- Thường được gắn vào một ứng dụng hệ thống nào đó và sẽ cho hacker quyền cao hơn quyền đã có trong hệ thống khi ứng dụng này chạy.

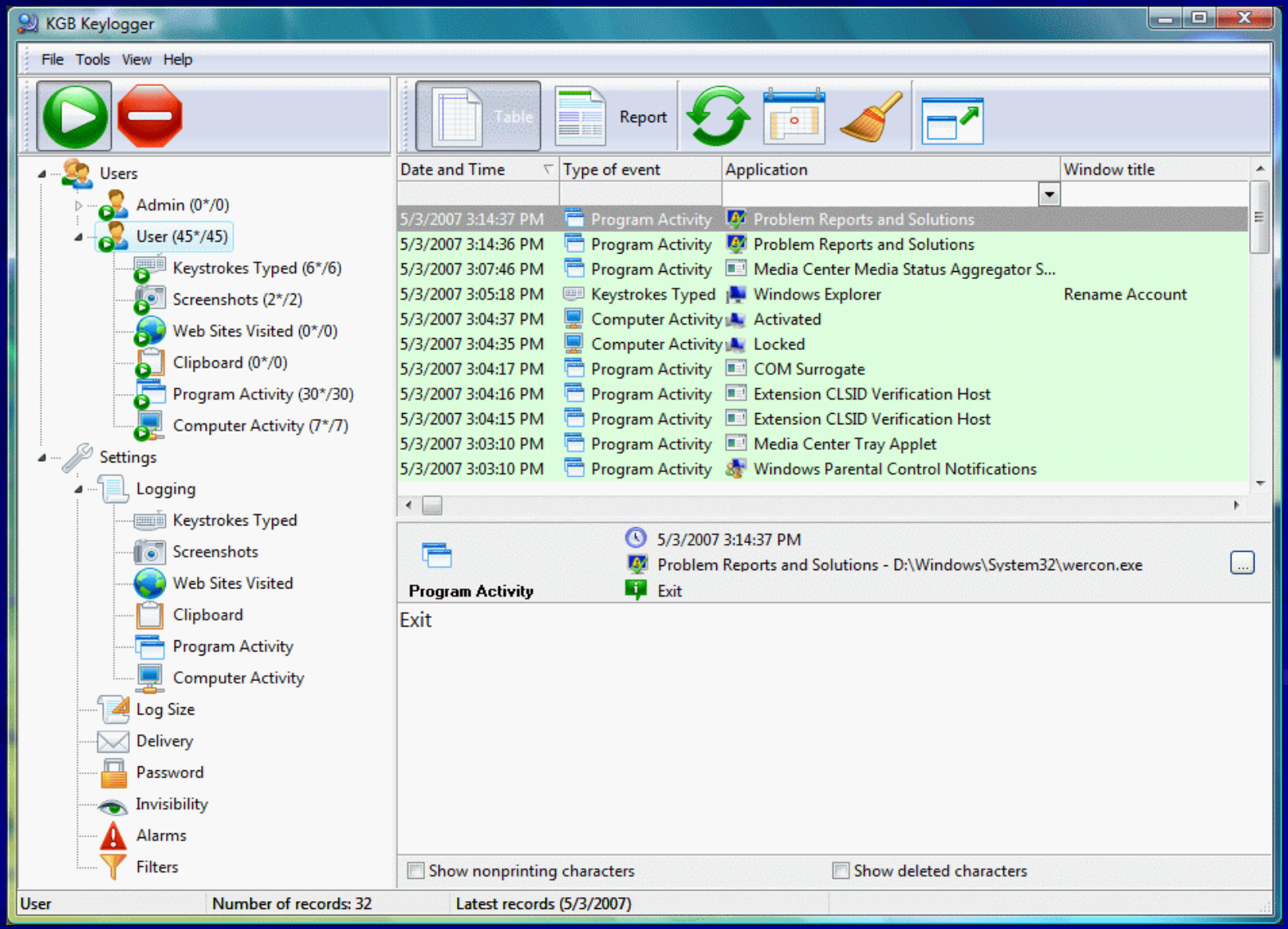
4. Một số Trojan phổ biến
KGB SPY

- Là loại trojan mạnh, được sử dụng rộng rãi. Version được cập nhật liên tục.
- Có thể theo dõi các phím nhấn, màn hình…
- Có các tab trong chương trình:
  - General options
  - Password
  - Email Delivery
  - Filters
  - Invisibility
  - Advanced options
  - Screenshot
  - FPT Delivery
  - Alert Notifications

4. Một số Trojan phổ biến
KGB SPY



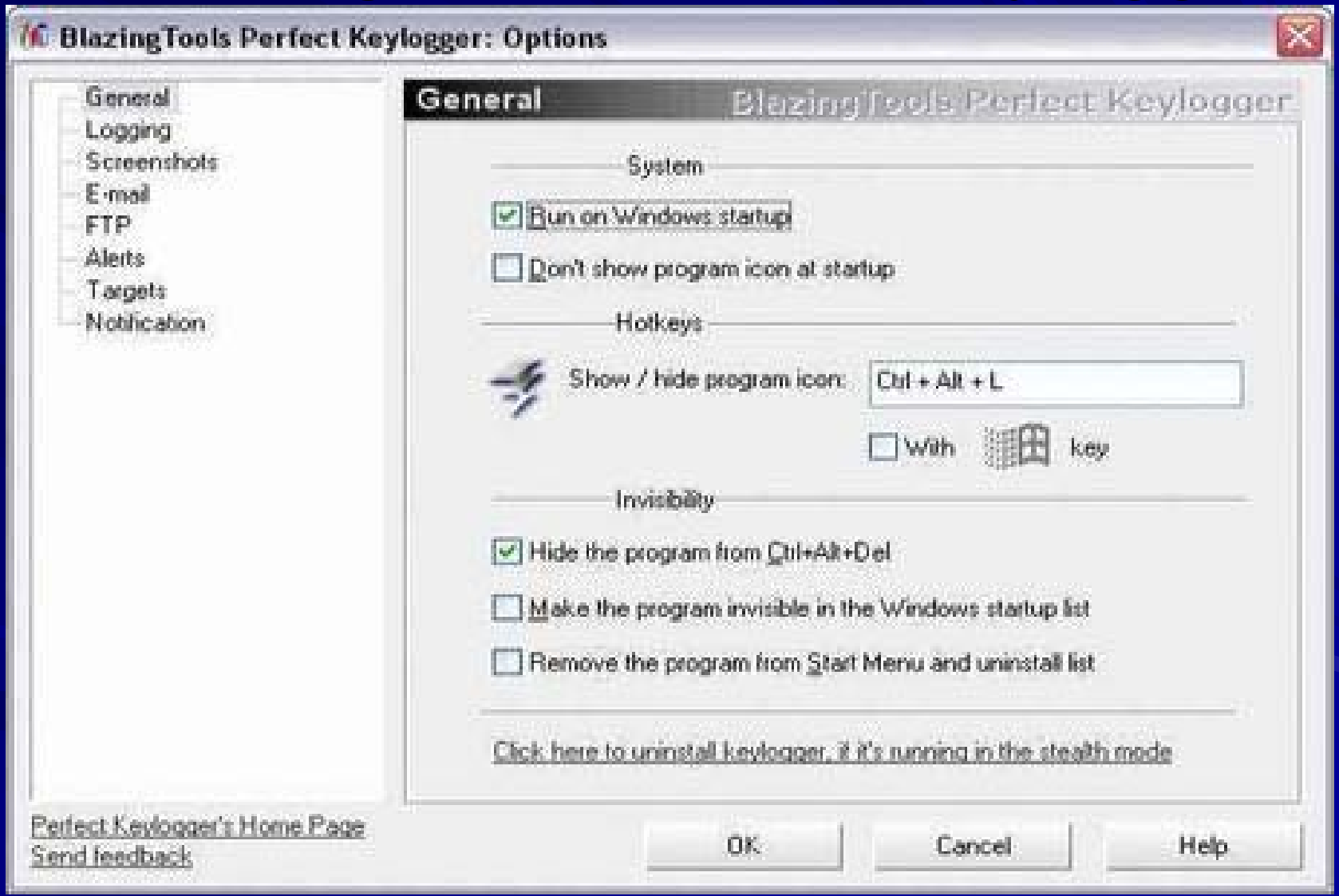
4. Một số Trojan phổ biến
KGB SPY



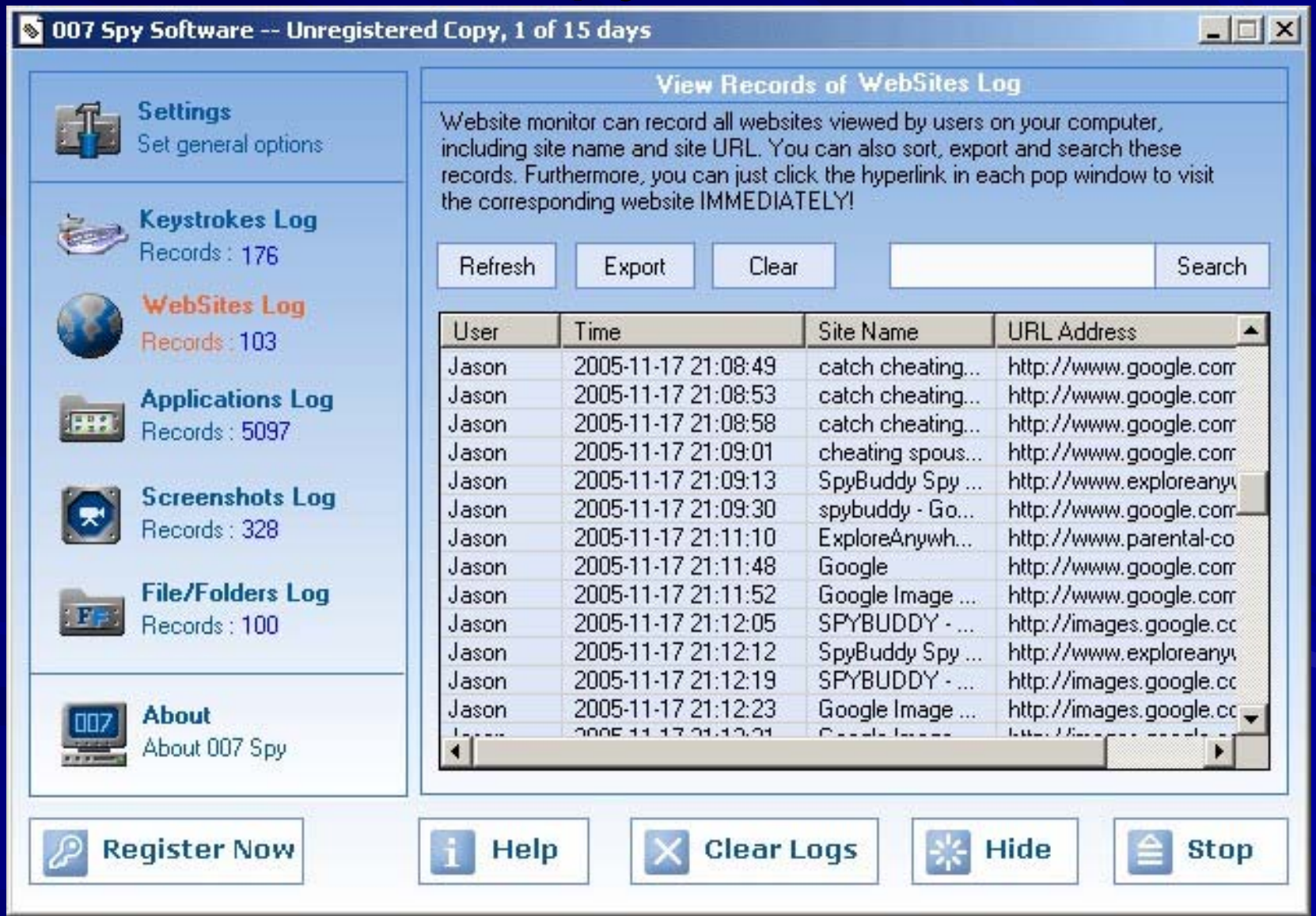
4. Một số Trojan phổ biến
Blazing Tool Perfect Keylogger

- Là một trojan mạnh, được sử dụng rộng rãi trên internet.
- Cho phép nhận thông tin từ máy bị nhiễm trojan từ email hoặc fpt server.
- Có thể lưu lại các phím nhấn, các link web, nội dung chat…

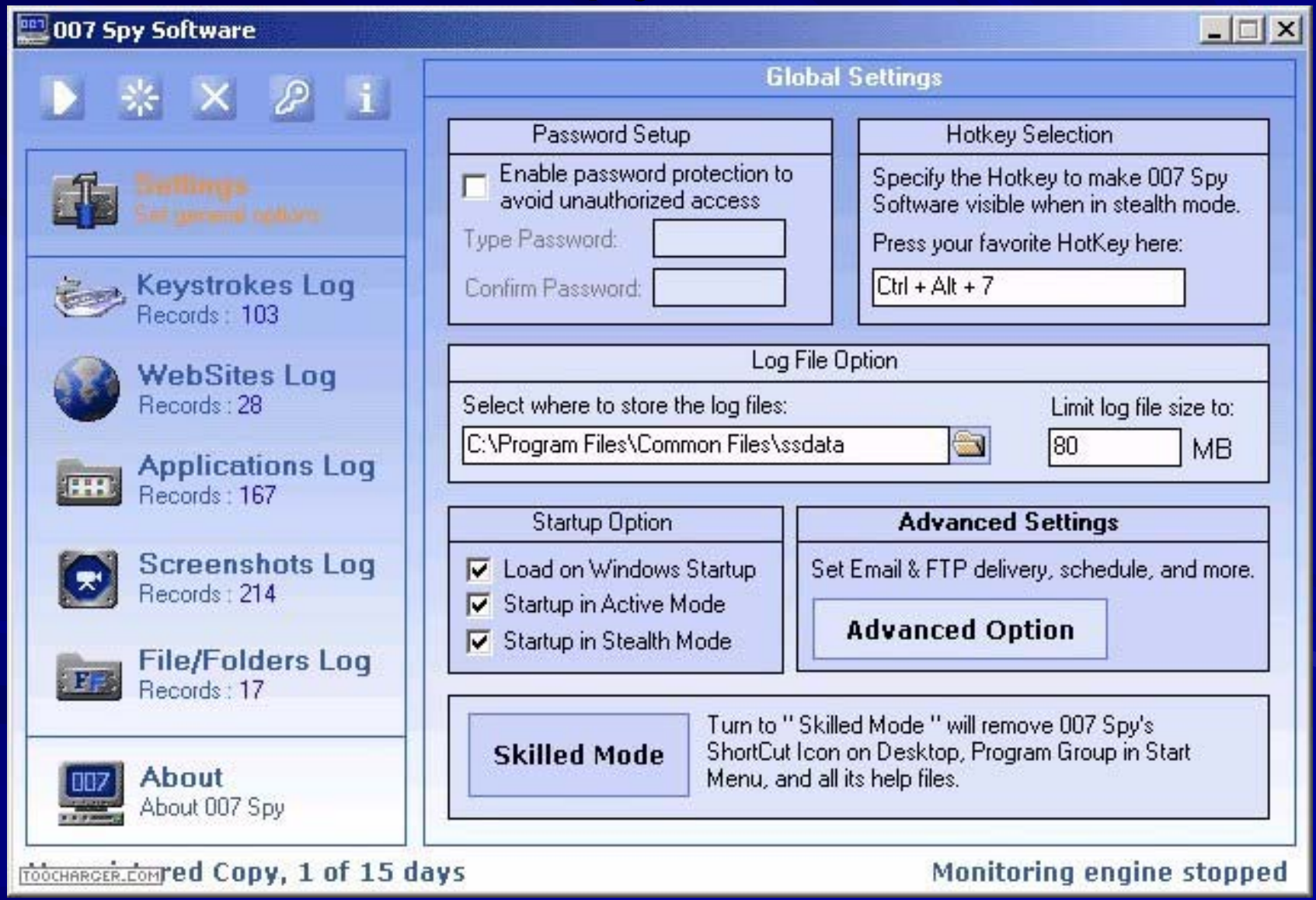
4. Một số Trojan phổ biến
Blazing Tool Perfect Keylogger



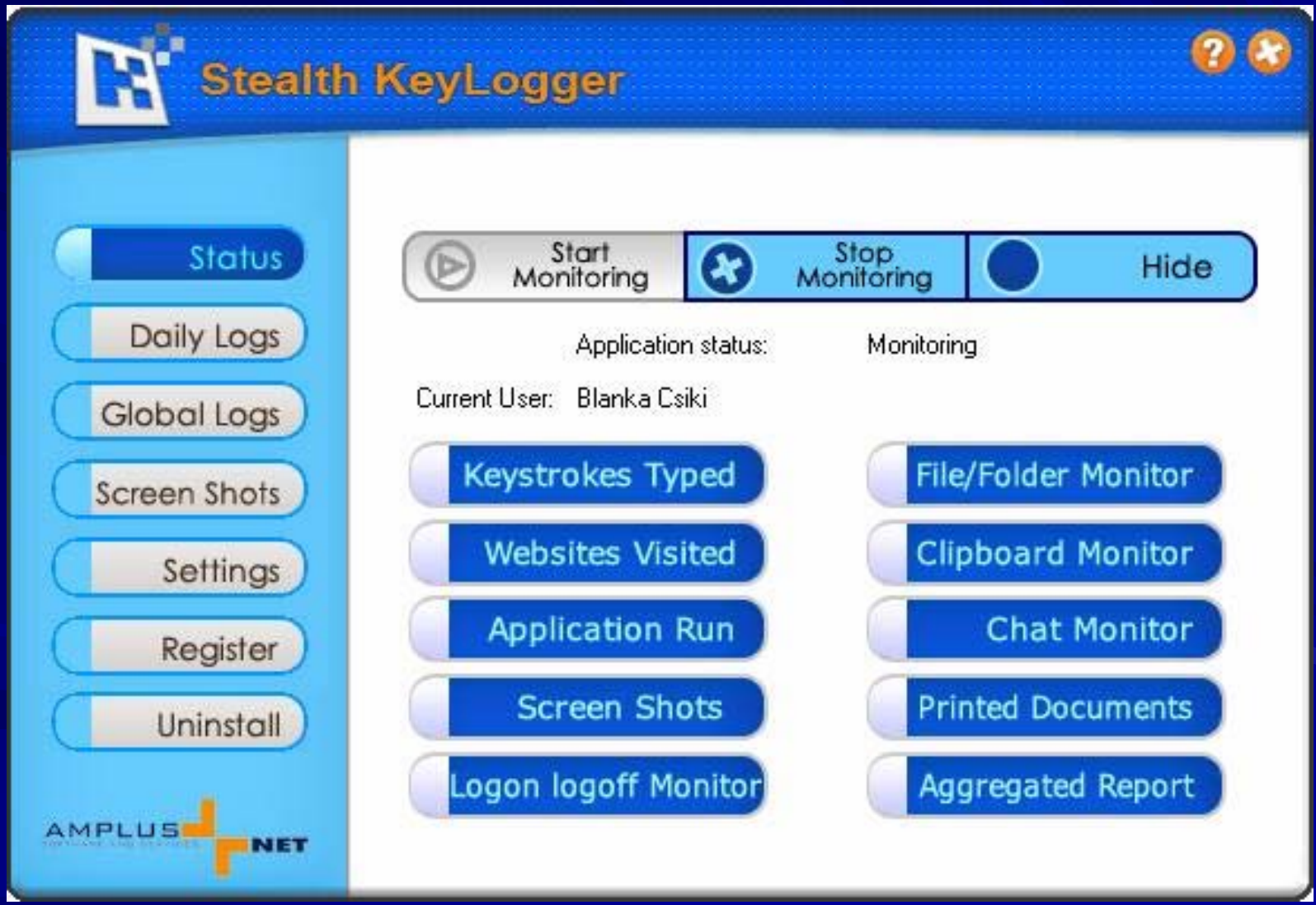
4. Một số Trojan phổ biến
007 Spy Software



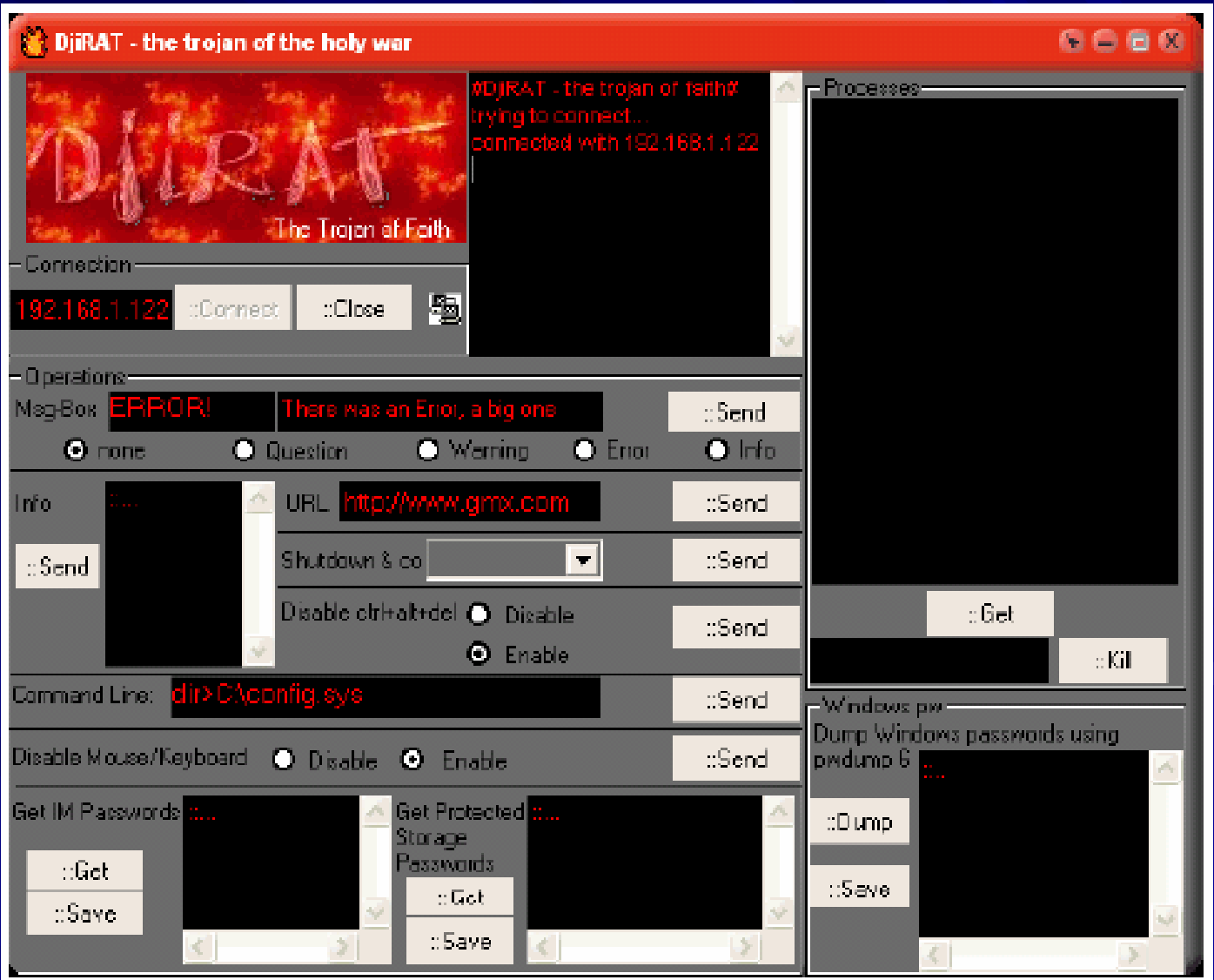
4. Một số Trojan phổ biến
007 Spy Software



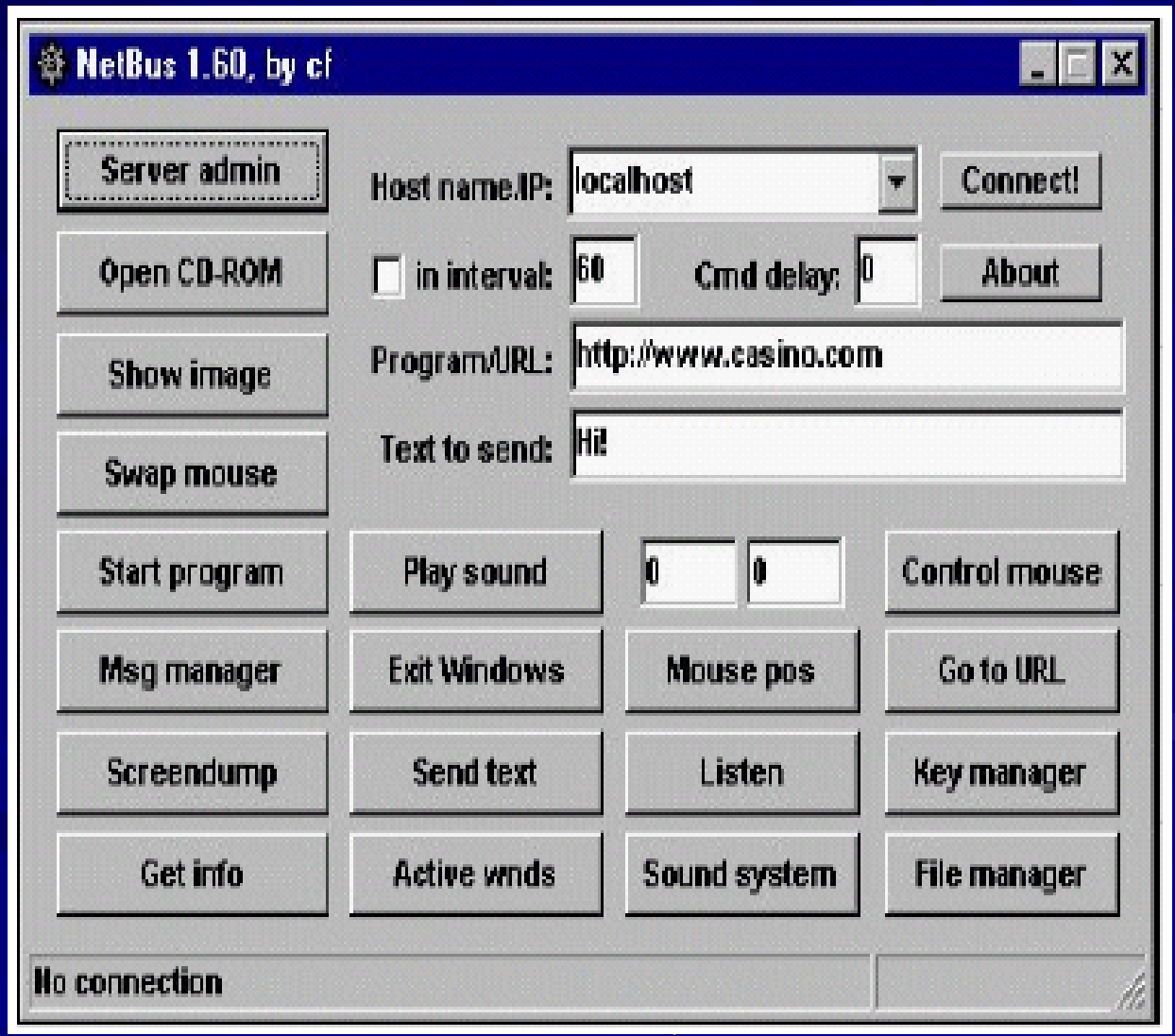
4. Một số Trojan phổ biến
Stealth Keylogger



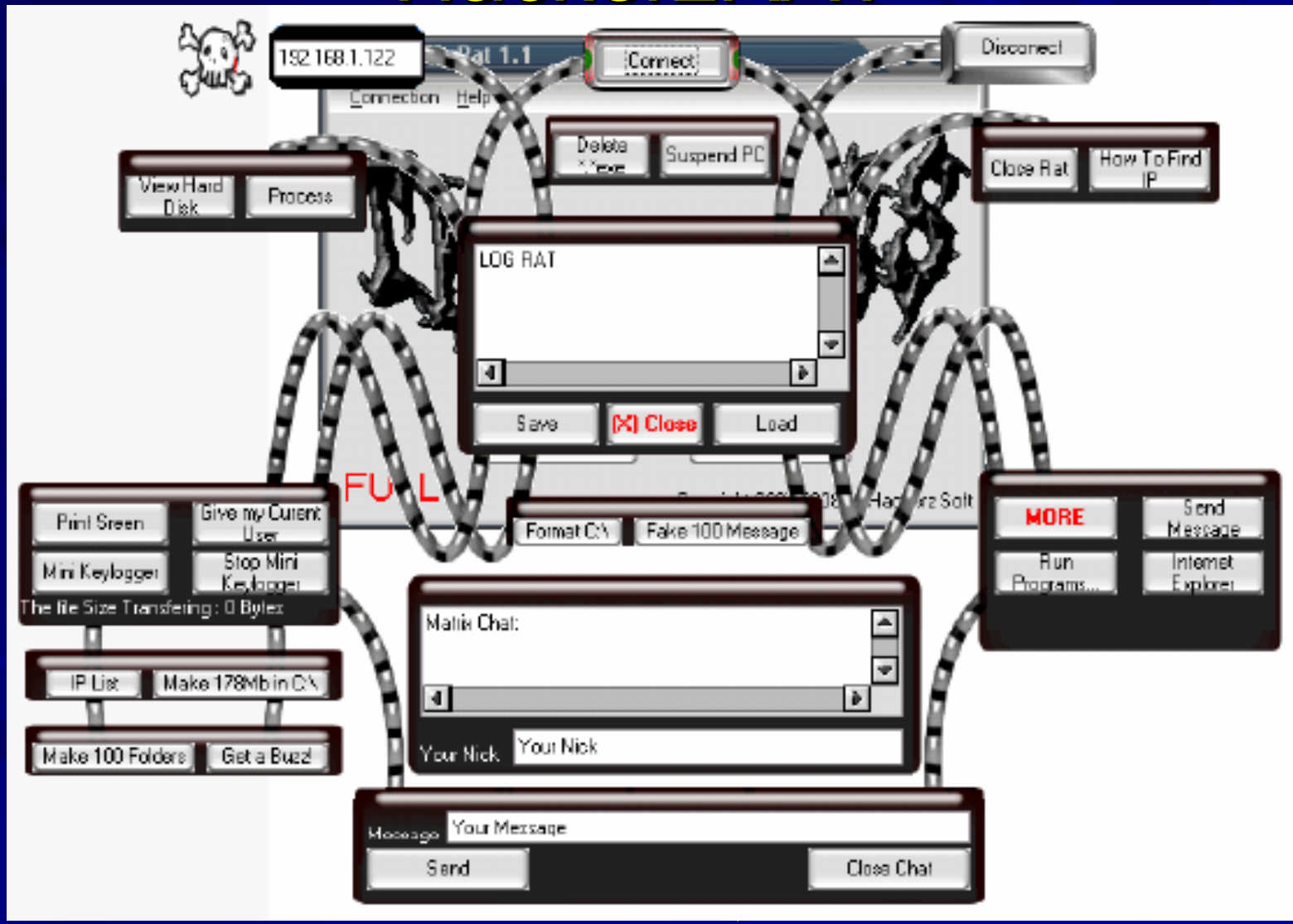
4. Một số Trojan phổ biến
DJI RAT



4. Một số Trojan phổ biến
NET BUS



4. Một số Trojan phổ biến
HackerzRAT



5. Phòng chống Trojan

- Hạn chế sử dụng chung máy tính, cài đặt mật khẩu bảo vệ.
- Không mở các tập tin lạ không rõ nguồn gốc, chú ý các file có phần mở rộng là exe, com, bat, scr, swf, zip, rar, gif…
- Không vào các trang web lạ.
- Không click vào các đường link lạ.
- Không cài đặt các phần mềm lạ.

5. Phòng chống Trojan

- Không download chương trình từ các nguồn không tin cậy.
- Luôn luôn tự bảo vệ mình bằng các chương chình chuyên dùng chống virus, chống spyware và dựng tường lửa khi đăng nhập Internet.
- Thường xuyên cập nhật đầy đủ các bản cập nhật bảo mật của hệ điều hành.

5. Phòng chống Trojan

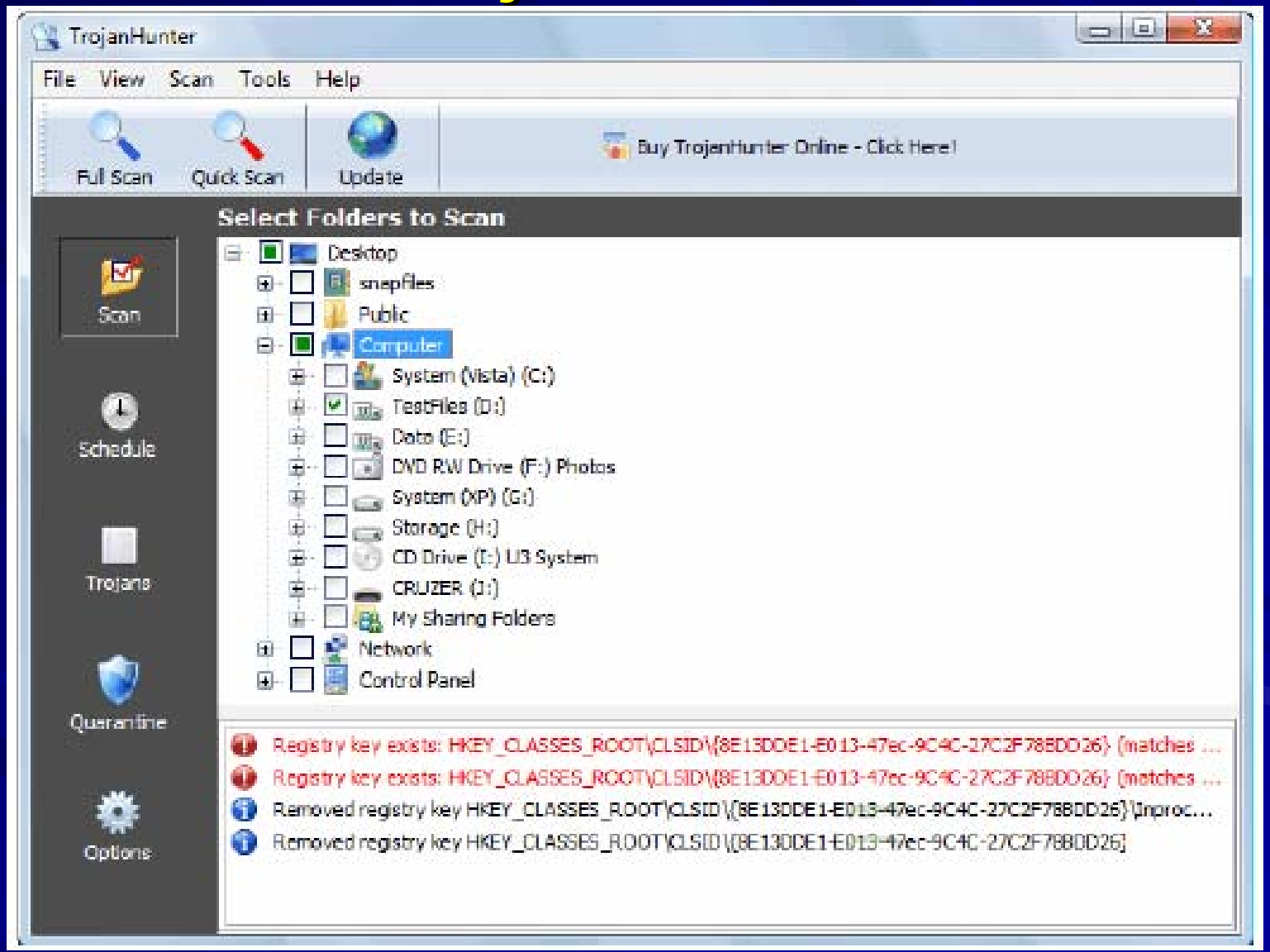
- Quét các port đang mở với các công cụ như Netstat, Fport, TCPView…
- Quét các tiến trình đang chạy với Process Viewer, What's on my computer, Insider…
- Quét những thay đổi trong Registry với MsConfig, What's running on my computer…
- Quét những hoạt động mạng với Ethereal, WireShark…
- Chạy các phần mềm diệt Trojan.

5. Phòng chống Trojan

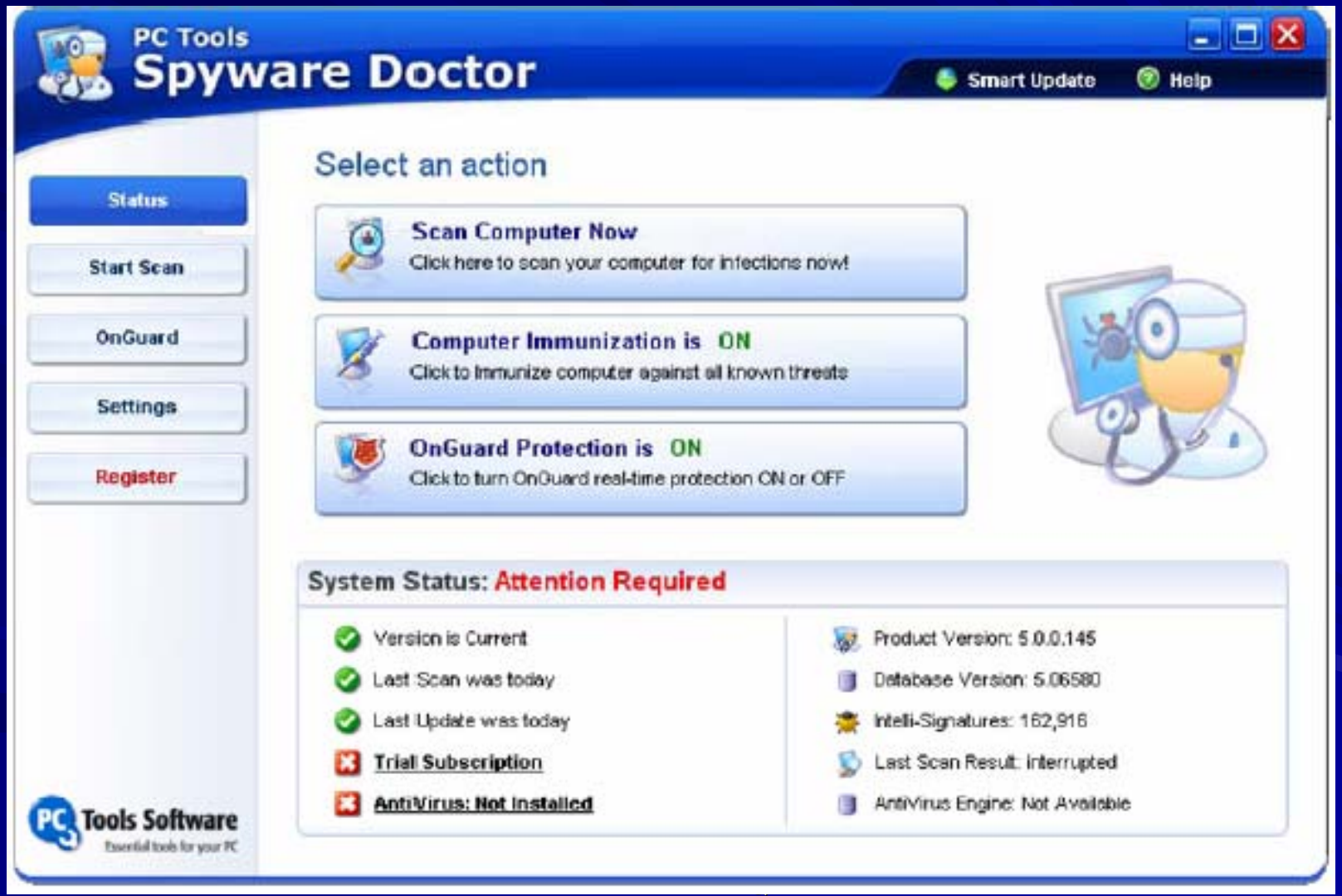
Below is the list of some of the anti-Trojan softwares that are available for trial:

- Trojan Guard
- Trojan Hunter
- ZoneAlarm f Win98&up, 4.530
- WinPatrol f WinAll, 6.0
- LeakTest, 1.2
- Kerio Personal Firewall, 2.1.5
- Sub-Net
- TAVScan
- SpyBot Search & Destroy
- Anti Trojan
- Cleaner

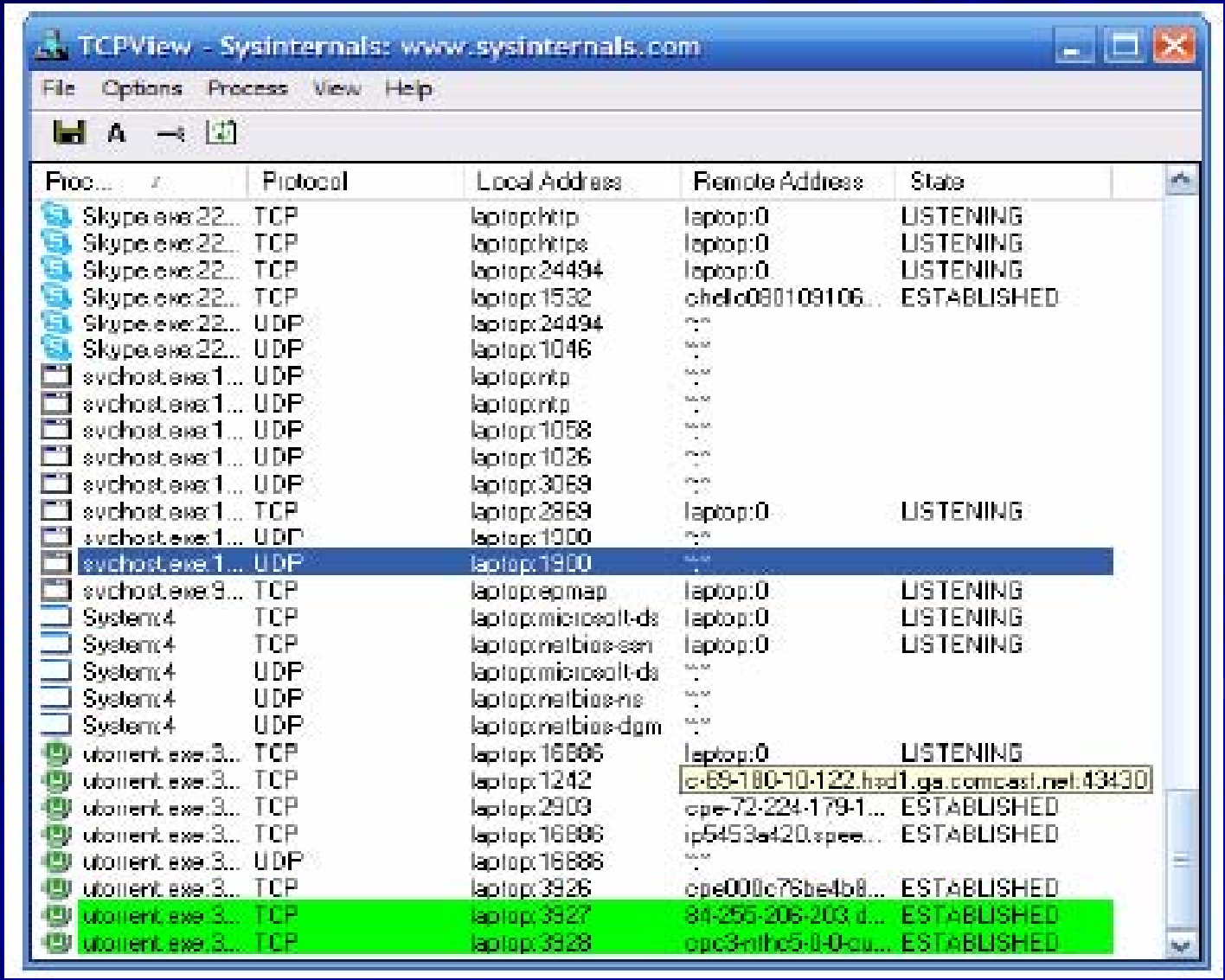
5. Phòng chống Trojan
Trojan Hunter



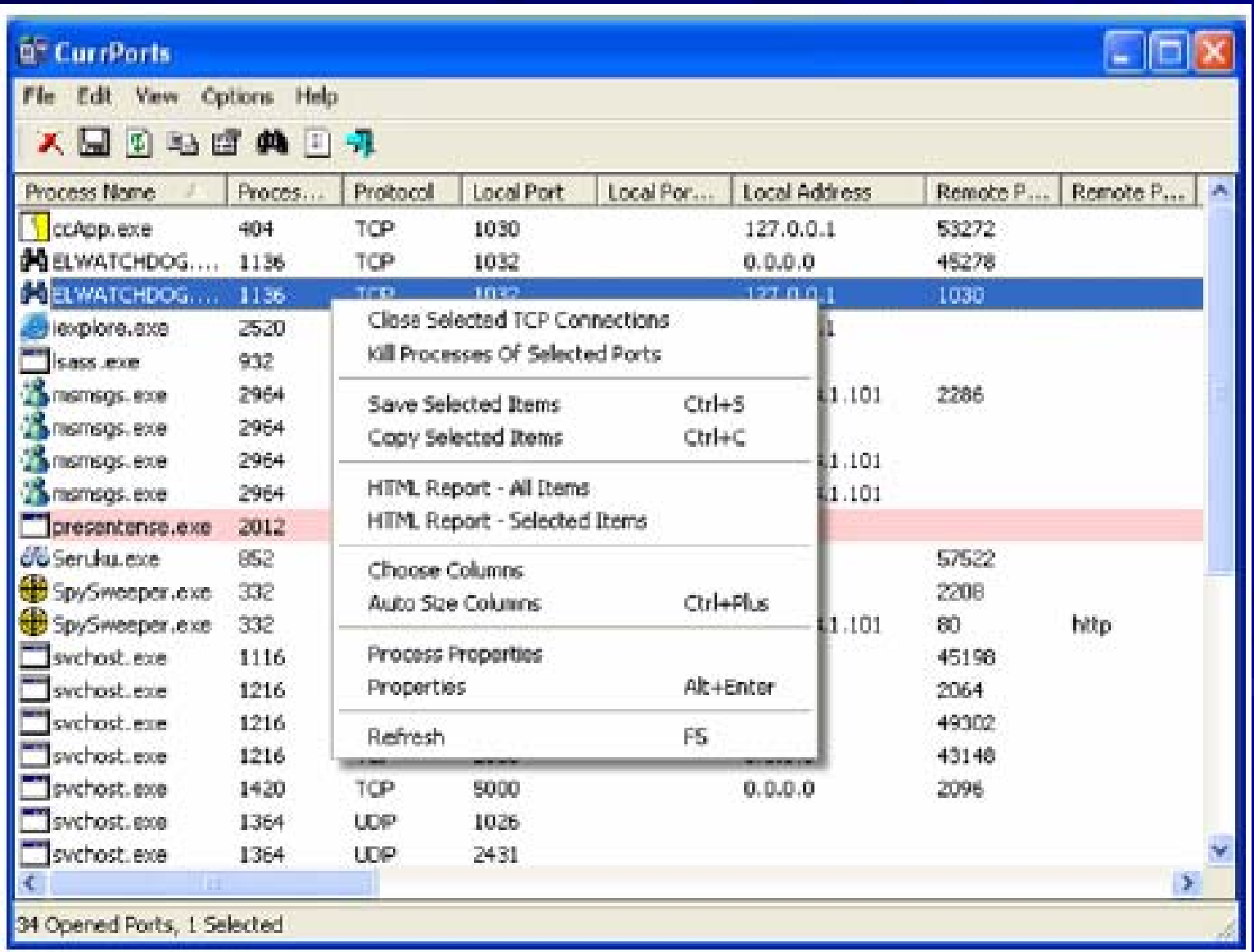
5. Phòng chống Trojan Spyware Doctor



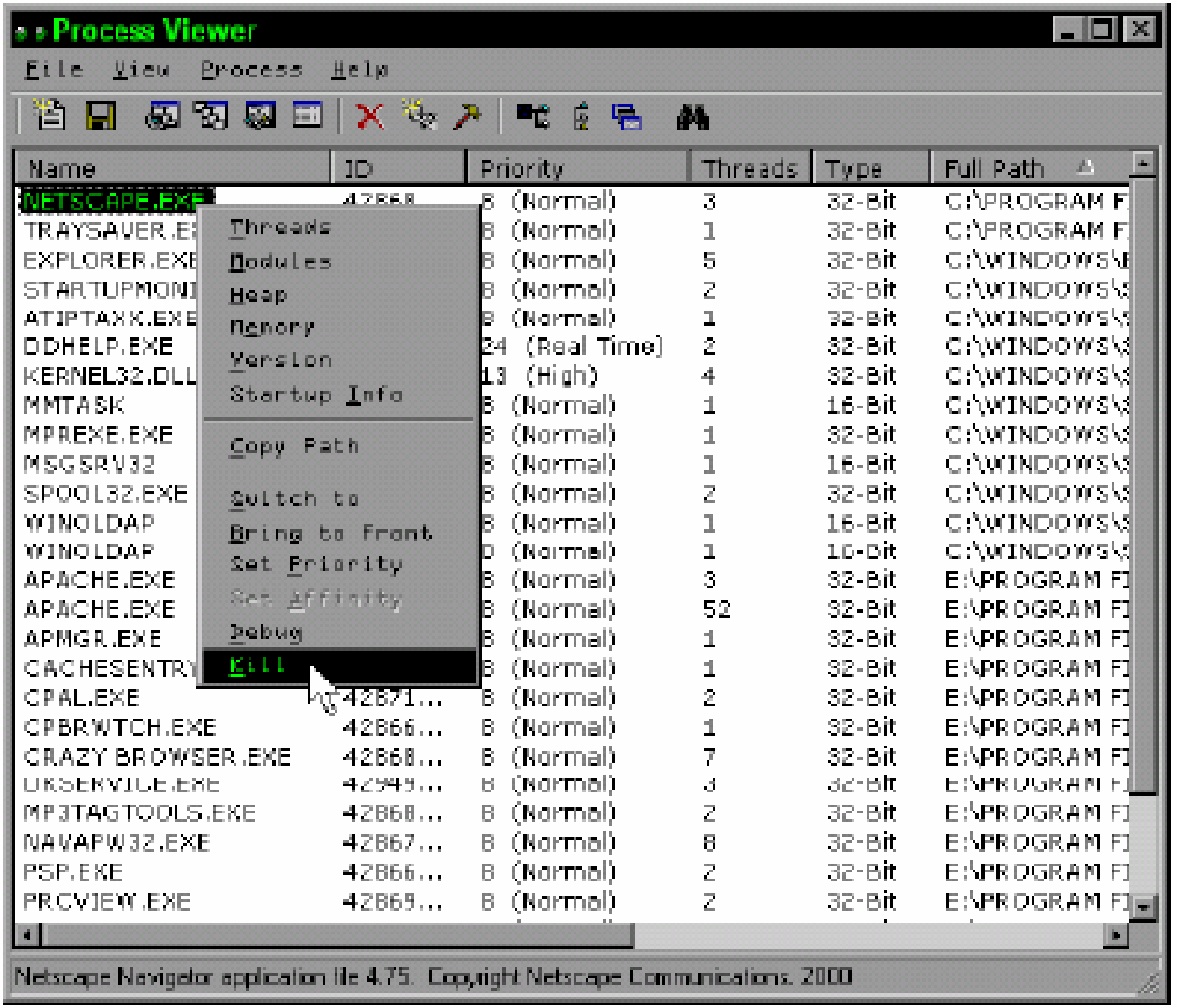
5. Phòng chống Trojan
TCPView



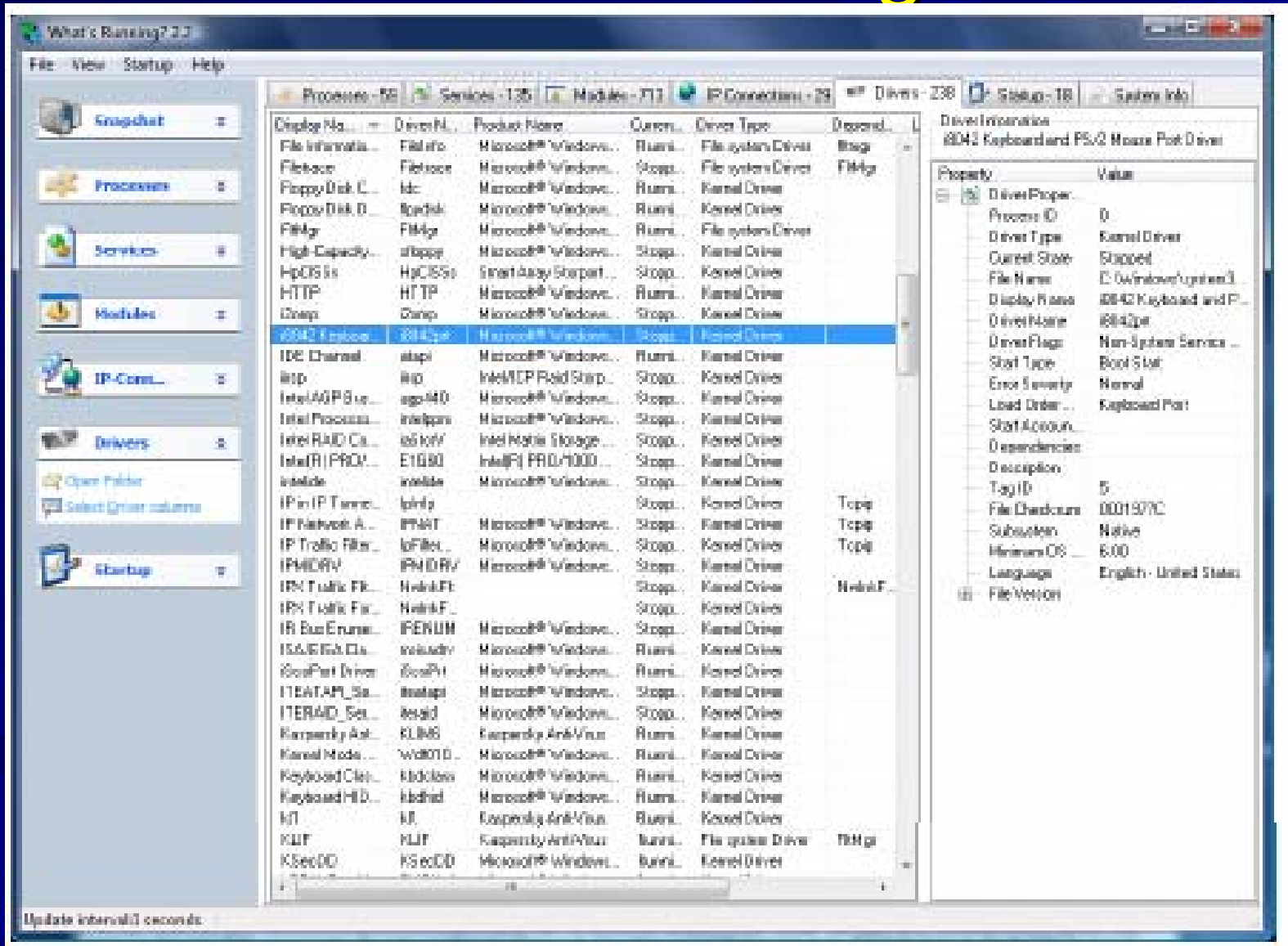
5. Phòng chống Trojan
CurrPorts Tool



5. Phòng chống Trojan
Process Viewer



5. Phòng chống Trojan
What's running



6. Một số cổng đi cùng các Trojan thông dụng

Trojan	Protocol	Ports
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
Masters Paradise	TCP	3129, 40421, 40422, 40423 and 40426

6. Một số cổng đi cùng các Trojan thông dụng

Satanz Backdoor|666	FTP99CMP|1492	WinCrash|4092	DeepThroat|6771
Silencer|1001	BackDoor|1999	ICQTrojan|4590	GateCrasher|6969
Shivka-Burka|1600	Trojan Cow|2001	Sockets de Troie|5000	Priority|6969
SpySender|1807	Ripper|2023	Sockets de Troie 1.x|5001	Remote Grab|7000
Shockrave|1981	Bugs|2115	Firehotcker|5321	NetMonitor|7300
WebEx|1001	Deep Throat|2140	Blade Runner|5400	NetMonitor 1.x|7301
Doly Trojan|1011	The Invasor|2140	Blade Runner 1.x|5401	NetMonitor 2.x|7306
Psyber Stream Server|1170	Phineas Phucker|2801	Blade Runner 2.x|5402	NetMonitor 3.x|7307
Ultors Trojan|1234	Masters Paradise|30129	Robo-Hack|5569	NetMonitor 4.x|7308
VooDoo Doll|1245	Portal of Doom|3700	DeepThroat|6670	ICKiller|7789

6. Một số cổng đi cùng các Trojan thông dụng

Portal of Doom|9872 Portal of Doom 1.x|9873 Portal of Doom 2.x|9874 Portal of Doom 3.x|9875 Portal of Doom 4.x|10067 Portal of Doom 5.x|10167 iNi-Killer|9989 Senna Spy|11000	Hack?99 KeyLogger|12223 GabanBus|1245 NetBus|1245 Whack-a-mole|12361 Whack-a-mole 1.x|12362 Priority|16969 Millennium|20001 NetBus 2 Pro|20034 GirlFriend|21544	Evil FTP|23456 Ugly FTP|23456 Delta|26274 Back Orifice|31337 Back Orifice|31338 DeepBO|31338 NetSpy DK|31339 BOWhack|31666 BigGluck|34324 The Spy|40412	Masters Paradise 1.x|40422 Masters Paradise 2.x|40423 Masters Paradise 3.x|40426 Sockets de Troie|50505 Fore|50766 Remote Windows Shutdown|53001 Telecommando|61466 Devil|65000 The tHing|6400

6. Một số cổng đi cùng các Trojan thông dụng

NetBus 1.x|12346	Gatecrasher |6969	Stealth Spy |555	BladeRunner | 5400
NetBus Pro 20034	Telecommando | 61466	Pass Ripper |2023	IcqTrojan | 4950
SubSeven|1243	Gjamer |12076	Attack FTP |666	InIkiller | 9989
NetSphere|30100	IcqTrojen| 4950	GirlFriend | 21554	PortalOfDoom | 9872
Silencer |1001	Priotrity |16969	Fore, Schwindler| 50766	ProgenicTrojan | 11223
Millenium |20000	Vodoo | 1245	Tiny Telnet Server| 34324	Prosiak 0.47 | 22222
Devil 1.03 |65000	Wincrash | 5742	Kuang |30999	RemoteWindowsShutdown | 53001
NetMonitor| 7306	Wincrash2| 2583	Senna Spy Trojans| 11000	RoboHack |5569
Streaming Audio Trojan| 1170	Netspy |1033	WhackJob | 23456	Silencer | 1001
Socket23 |30303	ShockRave | 1981		Striker | 2565

7. 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

7. 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

7. 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.

7. 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.

7. 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 chặn 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:

- 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.
- 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

Thank You !