NHỮNG VỊ TRÍ ẨN NÚP CỦA VIRUS VÀ TROJAN TRONG QUÁ TRÌNH KHỞI ĐỘNG

1. Thư mục START-UP: Windows mở tất cả các chương trình từ thư mục Start Up trong Start Menu. Thư mục này rất dễ thấy trong phần Programs của Start Menu. Chú ý là tôi không nói Windows "khởi chạy" mọi chương trình nằm trong thư mục Start Up. Tôi nói rằng n&

1. Thư mục START-UP: Windows mở tất cả các chương trình từ thư mục Start Up trong Start Menu. Thư mục này rất dễ thấy trong phần Programs của Start Menu. Chú ý là tôi không nói Windows "khởi chạy" mọi chương trình nằm trong thư mục Start Up. Tôi nói rằng n&

1. Thư mục START-UP: Windows mở tất cả các chương trình từ thư mục Start Up trong Start Menu. Thư mục này rất dễ thấy trong phần Programs của Start Menu. Chú ý là tôi không nói Windows "khởi chạy" mọi chương trình nằm trong thư mục Start Up. Tôi nói rằng nó "mở". Ở đây có sự khác biệt quan trọng. Tất nhiên là các chương trình điển hình trong thư mục Start Up sẽ chạy. Nhưng bạn có thể có các shortcut của chúng trong Start Up dưới dạng tài liệu chứ không phải là chương trình. Ví dụ nếu bạn đặt một tài liệu dạng Word trong thư mục Start Up, Word sẽ chạy và tự động mở nó trong quá trình khởi động hệ thống. Nếu bạn đặt một file WAV, phần mềm nghe nhạc sẽ chạy bản nhạc đó khi máy khởi động. Và nếu bạn đặt một Web-page Favourites, Internet Explorer (hay một browser khác bạn chọn) IE sẽ chạy và mở trang Web cho bạn tương tự như trên. (Các ví dụ dẫn ra ở đây có thể đặt shortcut một cách dễ dàng như là một file WAV, một tài liệu Word, v.v...) 2. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "Run" của Windows Registry. Các thành phần trong "Run" (và trong các phần khác của Registry trong danh sách bên dưới) có thể là các chương trình hay các file mà máy tính mở như trong giải thích của phần 1 ở trên. 3. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "RunServices" của Registry. 4. REGISTRY: Windows thực hiện tất cả các lệnh trong phần "RunOne" của Registry. 5. REGISTRY: Windows thực hiện tất cả các lệnh trong khu vực "RunServicesOne" của Registry. (Windows dùng hai khu vực "Runone" chỉ để chạy các chương trình thời gian đơn, thông thường trong phần khởi động hệ thống tiếp theo sau khi cài đặt một chương trình). 6. REGISTRY: Windows thực hiện các lệnh trong khu vực HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %* của Registry. Lệnh nhúng ở đây sẽ mở khi bất kỳ file chạy nào được thực thi. Có thể có những file khác: [HKEY_CLASSES_ROOT\exefile\shell\open\command] ="\"%1\" %*" [HKEY_CLASSES_ROOT\comfile\shell\open\command] ="\"%1\" %*" [HKEY_CLASSES_ROOT\batfile\shell\open\command] ="\"%1\" %*" [HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] ="\"%1\" %*" [HKEY_CLASSES_ROOT\piffile\shell\open\command] ="\"%1\" %*" [HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] ="\"%1\" %*" [HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] ="\"%1\" %*" [HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] ="\"%1\" %*" [HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] ="\"%1\" %*" [HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] ="\"%1\" %*" Nếu các khoá không có giá trị "\"%1\" %*" như trên và bị thay đổi một số thứ kiểu như "\"somefilename.exe %1\" %*" thì chúng sẽ tự động gọi một file đặc tả. 7. File BATCH: Windows thực hiện tất cả các lệnh trong các file Winstart BAT đặt trong thư mục Windows. (Hầu hết những người sử dụng và phần lớn những người thành thạo Windown đều không biết đến file này. Nó có thể không tồn tại trong hệ thống của bạn, nhưng bạn có thể tạo ra nó một cách dễ dàng. Chú ý rằng một số phiên bản của Windows gọi thư mục Windows là "WinNT"). Tên file đầy đủ là: WINSTAR.BAT. 8. File INITIALIZATION: Windows thực hiện các lệnh tại dòng "RUN=" trong file WIN.INI đặt ở thư mục Windows (hay WinNT). 9. File INITIALIZATION: Windows thực hiện các

lệnh tại dòng "LOAD=" trong file WIN.INI đặt ở thư mục Windows (hay WinNT). Nó cũng chạy các lệnh tại "shell=" trong System.ini hoặc c:\windows\system.ini. [boot] shell=explorer.exe C:\windows\filename Tên file theo kiểu explorer.exe sẽ bắt đầu bất cứ khi nào Windows khởi động. Với Win.ini, các tên file có thể được dành cho một không gian đáng kể, mỗi tên lưu trữ trên một dòng. Nó làm giảm khả năng các tên file có thể bị tìm thấy. Thông thường đường dẫn đầy đủ của file nằm trong mục nhập vào này, nếu không hãy kiểm tra lại trong thư mục Windows. 10. RELAUCHING: Windows khởi chạy lại các chương trình đang sử dụng khi hệ thống Shutdown. Windows không thể làm điều này với phần lớn các chương trình không phải của Microsoft. Nhưng nó thực hiện dễ dàng với Internet Explorer và với Windows Explorer, chương trình quản lý file và folder xây dựng trong Windows. Nếu bạn đang mở Internet Explorer khi hệ điều hành tắt, Windows sẽ mở lại đúng trang đó sau khi bạn khởi động lại hệ thống. (Nếu điều này không xảy ra trong máy tính của bạn, một người nào đó đã tắt tính năng này. Dùng Tweak UI, chương trình quản lý giao diện người dùng miễn phí của Microsoft Windows để tái kích hoạt thiết lập "Remember Explorer settings" hay dưới tên gọi nào đó khác trong phiên bản Windows của bạn). 11. TASK SCHEDULER: Windows thực hiện các lệnh chạy tự động trong Windows Task Scheduler (hay bất kỳ bộ lập lịch nào khác bổ sung hay thay thế Task Scheduler). Task Scheduler là một bộ phận chính thức của tất cả các phiên bản Windows, ngoài trừ phiên bản đầu tiên của Windows 95. Nhưng nếu cài đặt thêm Microsoft Plus Pack thì Windows 95 cũng có Task Scheduler. 12. SECONDARY INSTRUCTIONS: Các chương trình Windows khởi chạy tại thời điểm khởi động có thể tự do khởi chạy các chương trình "con" bên trong nó. Về mặt kỹ thuật, đây không phải là các chương trình do Windows khởi chạy. Nhưng chúng thường không thể phân biệt được với các chương trình tự động chạy thông thường nếu chúng được khởi chạy ngay sau khi chương trình "cha" chạy 13. Phương pháp C:\EXPLORER.EXE C:\EXPLORER.EXE Windows tải chương trình explorer.exe (luôn đặt trong thư mục Windows) trong suốt tiến trình khởi động. Tuy nhiên, nếu c:\explorer.exe tồn tại nó sẽ được thực thi thay vì Windows explorer.exe. Nếu c:\explorer.exe bị ngắt, người dùng thực tế bị lock out khỏi hệ thống của họ sau khi chúng khởi động lại. Nếu c:\explorer.exe là một trojan, nó sẽ được thực thi. Không giống như các phương thức tự động khởi động lại máy trong các virus khác, nó không cần bất kỳ file hay thanh ghi nào thay đổi. File này đơn giản chỉ phải đặt lại tên là: c:\explorer.exe. 14. Các phương thức Additional: Các phương thức tự động khởi động lại máy Additional. Hai phương thức đầu tiên được dùng bởi Trojan SubSeven 2.2. HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\explorer\Usershell folders Icq Inet [HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test] "Path"="test.exe" "Startup"="c:\\test" "Parameters"="" "Enable"="Yes" [HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\] This key specifies that all applications will be executed if ICQNET Detects an Internet Connection. [HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap] ="Scrap object" "NeverShowExt"="" Khoá này thay đổi đuôi mở rộng file của bạn.