"ĐIỀU TRỊ" VIRUS YAHOO MESSENGER

Trong

Trong thời gian vừa quá, rất nhiều virus thông qua tin nhắn Yahoo Messenger đã làm nhiều người phải "điêu đứng" và bực bội. Bài viết này tìm hiểu về những con virus qua tin nhắn của Y! và một vài mẹo gỡ bỏ chúng.

Đoạn mã này có thể lưu lại một thời gian nếu đã bị nhiễm loại virus Yahoo Messenger phát tán bằng tin nhắn rác.

Virus Y! Messenger rất nguy hiểm đối với các lỗ hổng chương trình thông qua Java script và VBS. Bạn có thể dễ dàng bị nhiễm khi kích vào một link tải hình (.JPG). Khi trang web xuất hiện để tải ảnh, java scripting sẽ chạy VBS (visual basic script – hoạt động trên bất kỳ máy tính Windows nào) ghi đè dữ liệu trên đĩa cứng.

Sau khi bị nhiễm, virus bắt đầu gửi tin nhắn tới tất cả thành viên trong danh sách mời kích vào link của chúng (như ví dụ bên dưới). Tin nhắn bị thay đổi, nó tự động phát tán ngẫu nhiên theo những từ khóa khác nhau từ cơ sở dữ liệu của virus.

Một số malware nguy hiểm hơn còn phá hủy các chương trình phổ biến như antivirrs và phần mềm tường lửa do đó các chương trình này sẽ trở nên vô ích.

** Hãy chú ý rằng đây là đoạn mã áp dụng cho phần lớn virus messenger chứ không phải tất cả. Tốt nhất là sử dụng phần mềm anti-spam và anti-virus. Đoạn mã bên dưới có thể thực hiện bằng cách lưu giữ nó dưới dạng file với đuôi mở rộng .bat (file batch). Để làm được việc đó, mở Notepad, dán chính xác đoạn code và sau đó chọn Save As từ menu File trong trình soạn thảo. Lưu nó với tên yvirusremoval.bat (ví dụ) trên đĩa cứng của bạn.

Tốt nhất nên khởi động lại máy tính trong chế độ safe mode, sau đó chạy file batch. Sau khi làm xong, hãy cài đặt lại Yahoo Messenger.

- NỘI DUNG ĐOẠN MÃ -

```
echo Disinfecting (stopping possibly infected services, deleting infected files, deleting
echo temporary files that could be infected, rewriting some registry entries like Internet
echo Explorer home page..) Please wait.
```

```
@taskkill /f /im svchost32.exe > nul
@taskkill /f /im svhost32.exe > nul
REM These two lines stop svchost32.exe and svhost32.exe services that are usually infected
@erase /F /Q %windir%\svchost32.exe > nul
@erase /F /Q %windir%\svhost32.exe > nul
@erase /F /Q %windir%\prefetch\*
@erase /Q /F "%userprofile%\Local Settings\Temp\svchost32.exe" > nul
@erase /Q /F "%userprofile%\Local Settings\Temp\svhost32.exe" > nul
@erase /Q /F "%userprofile%\Local Settings\Temporary Internet Files\*" > nul
REM The last 7 lines deleted svchost32.exe and svhost32.exe from windows directory and temporary directory; last line deleted all the Temporary Internet Files content
reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "Task Manager" /f > nul
reg add "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main" /v "Window Title" /d "Internet Explorer" /f > nul
reg add "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main" /v "Start Page" /d "HTTP://www.google.com" /f > nul
reg add "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs" /v "url1" /d "http://www.google.com" /f > nul
REM Last 4 lines change some registry entries, modifying Internet Explorer parameters, like home page (changes to google.com), typed history and default title bar.
echo Done !
```

- Hết -

HT - TN