cmd & virus

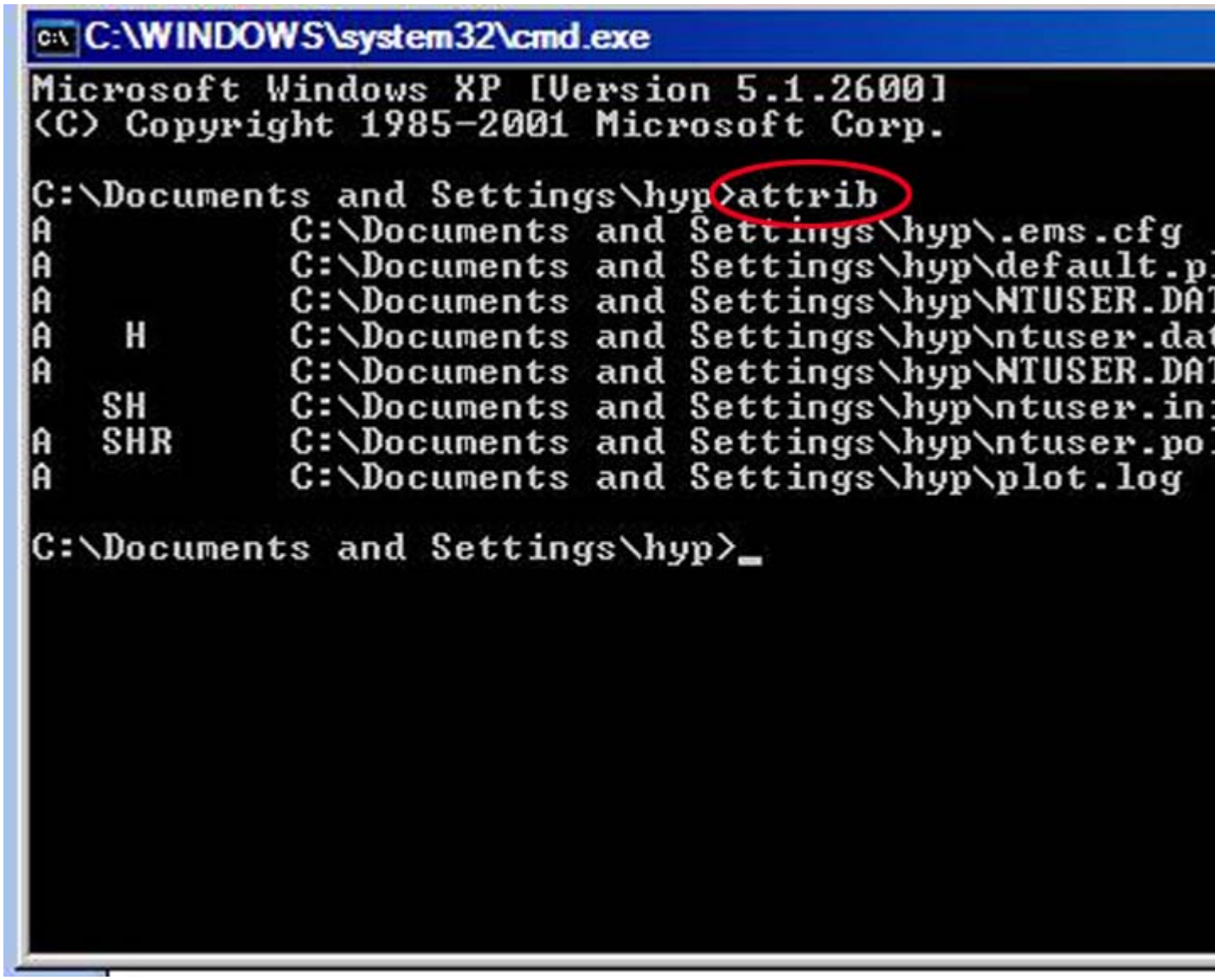
Jan 25, '10 12:05 AM

for everyone

loikaw virus က ရှင်းရတာ လွယ်ပါတယ်။ နောက်ပေါ်တဲ့ anti virus တွေလည်း loikaw ကိုတွေ့ နေကြပါပြီ... အားပေးတာကတော့ cmd ထဲမှာ ဂင်ရှင်းပါ..အသုံးပြုချင်တဲ့လူတွေအတွက် ကျွန်တော်တင်ပေးပါ့မယ်.. window key + R ပြီးတာနဲ့ cmd ရိုက်လိုက်ပေါ့..

တစ်ခုတော့ရှိတာပေါ့ cmd ထဲမှာ သုံးလို့ ရတဲ့ switch တွေကို နားလည်ရင်ပိုကောင်းပါတယ်.. cmd ထဲမဂင်ခင်မှာ အရင်ဆုံး msconfig ကို Run box ထဲမှာ အရင်ရိုက်ပြီး startup tag ထဲက ဗိုင်းရပ်ကို စပြီး မောင်းတဲ့ loikaw.exe ကို ဖြုတ်ပစ်ရပါမယ်။ loikaw.exe က task manager ကို ပိတ်ပစ်လိုက်ပါတယ်..

Run နေတဲ့ ဗိုင်းရပ်ကို အရင် ရပ်ပစ်ရပါမယ်.. Virus ရဲ့ သဘောတရားအတိုင်း source ကို နှစ်ပိုင်းခွဲထားတယ်.. တစ်ခုက Hard disk မှာ နေတယ်.. နောက်တစ်ခု က system (RAM) ထဲမှာ Run နေတယ်.. ကျွန်တော်တို့ က အရင်ဆုံး Hard Disk ထဲက ကောင်ကို အရင် ဖျက်ပစ်ရပါမယ်။ အဲဒီကောင်က window boot တက်တိုင်း သူက စပြီး အလုပ်လုပ်ရတာပါ။ သူမရှိရင် ဗိုင်းရပ်စ်က နိုးမှာမဟုတ်ပါဘူး.. သူက hidden file ပါ... မတွေ့ နိုင်ပါဘူး.. Windows ထဲမှာရယ် system32 ထဲမှာ ရယ် document and settings ထဲမှာ အကုန်ရှာရပါမယ်... အဲလိုရှာဖို့အတွက် သုံးရမှာက cmd ပါ။

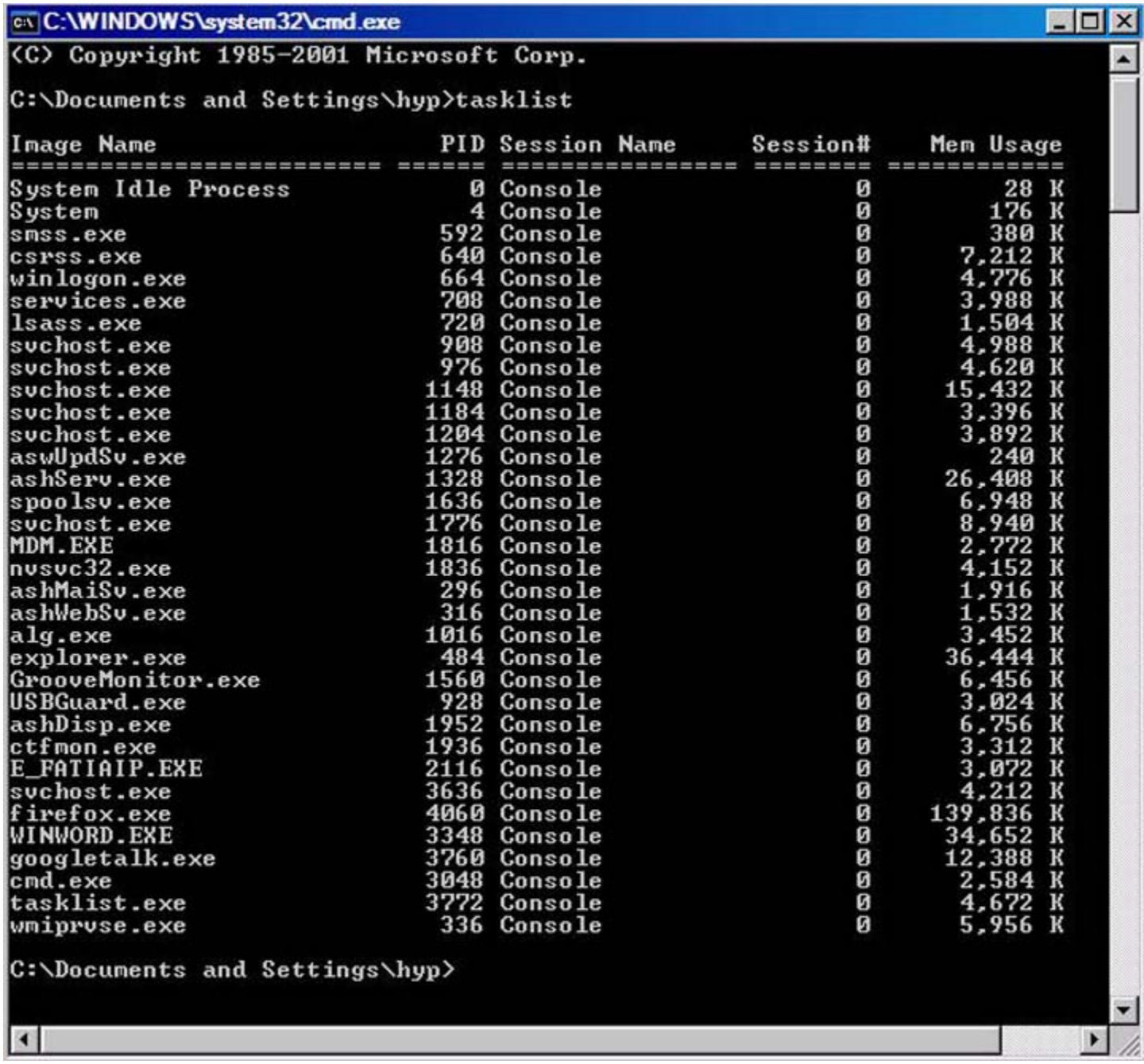


Task manager ကို ခေါ်ရန်ပထမနည်းလမ်း

တစ်ခုကို သတ်ရင် တစ်ခုက ပြန်နှိုးတယ်.. task manager ကို ပြန်ခေါ်နိုင်ဖို့အတွက် gpedit.msc ကို Run box ထဲမှာ ရိုက်ထည့်ပါ။ user configuration အောက်က administrative templates မှာ ရှိတဲ့ system အောက်က Ctr+Alt+Del Option မှာ Remove Task Manager ကို Disable လုပ်ပါ။ ပြီး ရင် Run box ထဲမှာ gpupdate ဆိုပြီး group Policy ကို update လုပ်ပါ။ ပြီးရင် Task Manager ကို ခေါ်ကြည့်ပါ။

မရခဲ့လျှင် -----

Task List ကို အသုံးပြုခြင်း



ကျွန်တော်တို့အတွက် virus process များကို ရပ်နိုင်ဖို့အတွက် Task List တစ်ခုလုံးကျန် ပါသေးတယ်။ Task list သည် cmd ထဲမှာ ပင်သုံးရခြင်းဖြစ်ပါသည်။

cmd ထဲတွင် Tasklist ဟု ရိုက်လိုက်ပါ။ Tasklist များကျလာလျှင် PID No. ကို
လိုက်၍ Task kill လုပ်နိုင်ပါတယ်။ ဗိုင်းရပ်စ် ရဲ့ process
ကိုအတိအကျသိဖို့တော့လိုတယ်...Taskkill /f /(PID No.) အနေဖြင့် ဗိုင်းရပ်စ်
လုပ်ငန်းစဉ်များကို ရပ်ပစ်လို့ရပါတယ်။

ဗိုင်းရပ်လုပ်ငန်းစဉ်များကို ရပ်လိုက်တာနဲ့ infected file တွေကို ဖျက်လို့ရပါပြီ... Cmd ကို အသုံး
ပြုပြီးဖျက်ရမှာဖြစ်ပါတယ်။

Cmd ထဲမှာ ဖျက်နည်းကတော့...

အရင်ဆုံးcmd ထဲဝင်ပါ။ document and settings ကိုအရင်ရှာကြည့်ပါ.. ရိုက်ရမယ့် command
ကတော့ attrib ပါ။

A = archive file ပါ။

H = Hidden file ပါ။

S= System file ပါ။

R = Read only file ပါ။

Virus တွေက ASHR အနေနဲ့ရှိနေတတ်ပါတယ်။ တစ်ခါတစ်လေ တစ်အားသတိထားရတယ်..
virus လား system file လားဆိုတာ.. မှားဖျက်ရင် windows
တက်တော့မှာမဟုတ်ပါဘူး..

သတိထားပါ။ ပုံမှန်ရှိရမယ့်ဖိုင်မဟုတ်ရင် ဖျက်သာဖျက်ပစ်ပါ။
ဖျက်တဲ့အခါလည်းသတိထားပါ။ ဘာလို့လဲဆိုတော့ တစ်ချို့တစ်ချို့သော virusတွေက
system file ကို hidden လုပ်ပြီး သူကတော့ system fileတွေ နေရာမှာ
ဝင်ယူနေတတ်တယ်..အထူးသဖြင့် folder ယောင်ဆောင်တဲ့ဗိုင်းရပ်တွေပေါ့.. cmd

ထဲမှာ ဖျက်တဲ့ command ကို အောက်မှာဖော်ပြပေးထား ပါတယ်။

Del ပါ။ force က /f ပါ။ S ဖိုင်တွေကို ဖျက်ဖို့အတွက် R ဖိုင်တွေကိုဖျက်ဖို့အတွက်လိုပါလိမ့်မယ်။

Switch တွေကို ကြည့်ချင်ရင်တော့ del /f /a (ဖျက်ချင်သောဖိုင်နာမည် အပြည့်အစုံ)

Del /? ကတော့ del နဲ့ တွဲသုံးနိုင်သော switch တွေကို အကုန်ပြောပြပါလိမ့်မယ်။


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\hyp>Help |more
For more information on a specific command, type HELP command-name
ASSOC Displays or modifies file extension associations.
AT Schedules commands and programs to run on a computer.
ATTRIB Displays or changes file attributes.
BREAK Sets or clears extended CTRL+C checking.
CACLS Displays or modifies access control lists (ACLs) of files.
CALL Calls one batch program from another.
CD Displays the name of or changes the current directory.
CHCP Displays or sets the active code page number.
CHDIR Displays the name of or changes the current directory.
CHKDSK Checks a disk and displays a status report.
CHKNTFS Displays or modifies the checking of disk at boot time.
CLS Clears the screen.
CMD Starts a new instance of the Windows command interpreter.
COLOR Sets the default console foreground and background colors.
COMP Compares the contents of two files or sets of files.
COMPACT Displays or alters the compression of files on NTFS partit
CONVERT Converts FAT volumes to NTFS. You cannot convert the
current drive.
COPY Copies one or more files to another location.
DATE Displays or sets the date.
DEL Deletes one or more files.
DIR Displays a list of files and subdirectories in a directory
DISKCOMP Compares the contents of two floppy disks.
DISKCOPY Copies the contents of one floppy disk to another.
DOSKEY Edits command lines, recalls Windows commands, and creates
ECHO Displays messages, or turns command echoing on or off.
ENDLOCAL Ends localization of environment changes in a batch file.
ERASE Deletes one or more files.
EXIT Quits the CMD.EXE program (command interpreter).
FC Compares two files or sets of files, and displays the diff
between them.
FIND Searches for a text string in a file or files.
FINDSTR Searches for strings in files.
FOR Runs a specified command for each file in a set of files.
FORMAT Formats a disk for use with Windows.
FTYPE Displays or modifies file types used in file extension ass
GOTO Directs the Windows command interpreter to a labeled line
batch program.
GRAFTABL Enables Windows to display an extended character set in gr
mode.
HELP Provides Help information for Windows commands.
IF Performs conditional processing in batch programs.
LABEL Creates, changes, or deletes the volume label of a disk.
MD Creates a directory.
MKDIR Creates a directory.
MODE Configures a system device.
MORE Displays output one screen at a time.
MOVE Moves one or more files from one directory to another dire
PATH Displays or sets a search path for executable files.
PAUSE Suspends processing of a batch file and displays a message
POPD Restores the previous value of the current directory saved
PRINT Prints a text file.
PROMPT Changes the Windows command prompt.

နောက်တစ်ခုအနေနဲ့တော့ cmd ထဲမှာ သုံးနိုင်သော switch တွေအကုန်လုံးကို ဒီ command နဲ့ ရှာကြည့်ပါ ။ နောက်စမ်းသပ်ကြည့်ပါ။ cmd က ပျော်စရာကောင်းပါလိမ့်မယ်။