VS

ဗိုင်းရပ်စ်များနှင့် ကာကွယ်ခြင်း....

ဧဝံ မေ သုတံ ၊ ကျွန်ုပ်သည် ဤသို့ ကြားနာ မှတ်သားခဲ့ရဖူးပါ၏

စီခရေဇီ
စုဆောင်းမျှဝေသည်။

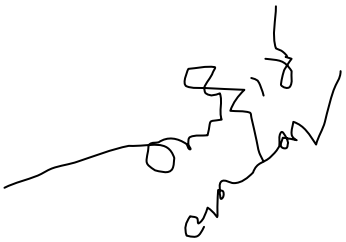
အထူးဝန်ခံတောင်းပန်ချက်

ကျွန်တော် မောင်စီခရေဇီသည် ဤစာစောင်ကို ကျွန်တော့်ပတ်ဝန်းကျင်၊ ကျွန်တော့်သူငယ်ချင်း မိတ်ဆွေ
ညီအစ်ကိုများထဲမှ မသိသေး၍ မေးမြန်းလာသမျှ ခနခန ဖြေရလွန်း၍ သက်သာစေရန် တစ်ကြောင်း၊

IT နယ်ပယ်သို့ စတင်ဝင်ရောက်ရန် ကြိုးစားနေသည့် လူငယ်လူရွယ်/ကျောင်းသူကျောင်းသားများ/ ယခုမှ
ကွန်ပျူတာအခြေခံကို စတင်လေ့လာသူများ/ ပိုင်းရပ်စ်နှင့်ပတ်သက်၍
အစိမ်းသက်သက်အတွေ့အကြုံမရှိသေးသူများ အတွက် အထောက်အကူဖြစ်စေရန် တစ်ကြောင်း၊
သတိမကပ်မိ၍ အခက်အခဲကြုံရခဲ့ရသူ သူငယ်ချင်းများအတွက် သတိကပ်လျှင် အလွယ်သာဖြစ်ကြောင်းကို
ပြောလို၍တစ်ကြောင်းကြောင့်သာ ရည်ရွယ်ရေးသားပါသည်။

တော်၍ တတ်၍ ရေးသားခြင်းမဟုတ်သလို ဆရာလုပ်ချင်၍ / နာမည်ကြီးချင်၍ရေးသားခြင်းလည်းမဟုတ်ပါ..
အားလုံးကို ကျွမ်းလွန်း၍လည်းမဟုတ်ပါ.. တွေ့ဖူးကြုံဖူးသမျှ သိဖူးမြင်ဖူးကြားဖူးသမျှ ဇဝံမေသုတံမျှသာ
ဖြစ်ပါသည်။

အရေးအသားများတွင် မည်သည့် ဆရာစဉ် သမားစဉ် /ပုဂ္ဂိုလ် တစ်ဦးတစ်ယောက်ပေါ်ထံကိုမျှ
မော်ကြွားစော်ကားလိုစိတ်မရှိပါ..
အသုံးအနှုန်း ဖော်ပြချက် စကားလုံးမှအစ မောက်မာ ရိုင်းပျ မှားယွင်းခဲ့သည်ရှိသော်
ကျွန်တော်ကသာလက်ဆယ်ဖြာမိုး၍ ရှိခိုးတောင်းပန်ပါသည် ...



တပ်ကြပ်ကြီးစာရေးအောင်ပိုင်မင်း
ကွန်ပျူတာဒီပလိုမာသင်တန်းအမှတ်စဉ်(၁)
သပြေရိပ်သာ (၂) တိုက် (၄၆-က)

မင်းလားကွ ဗိုင်းရပ်စ်

COMPUTER__CRAZY

ဘာလဲဟ ဗိုင်းရပ်စ် (Virus)

IT အခေါ် (Virus) ဗိုင်းရပ်စ် ဆိုသည်မှာ Computer လည်ပတ်မှုစနစ်ကို အနှောင့်အယှက် ပေးသော ပရိုဂရမ် ဖြစ်ပါသည်။ ဤပရိုဂရမ်များ ဝင်ရောက်နေသော စက်များအတွင်းတွင် Setting များ ပြောင်းလဲနေခြင်း၊ အသုံးပြုနေသော ဖိုင်များ ကွယ်ပျောက် (Hidden) ဖြစ်နေခြင်း၊ အသုံးပြုသူ User မှ ပြုလုပ်ခြင်းမဟုတ်ဘဲ ဖိုင်များ ပွားနေခြင်း အစရှိသဖြင့် နှောင့်ယှက်မှု ခံရစေပါသည်။ ဗိုင်းရပ်စ်များမှာ ဖန်တီးသူ၏ တိုက်ခိုက်လိုမှု အမျိုးအစားအလိုက် အန္တရာယ်ပေးနိုင်မှု အဆင့်အတန်း ကွာခြားကြပါသည်။ ကျိစယ်လို၍ နောက်ပြောင်ယုံမျှ ဖန်တီးထားသော Virus မှ အစပြု၍ ကိုယ်ရေး အချက်အလက်များ/ဖိုင်များပျက်စီးစေခြင်း အပါအဝင် Windows Operating System တစ်ခုလုံးကို ရပ်တန့်သွားအောင်၊ လည်ပတ်နိုင်ခြင်းမရှိတော့အောင် ဖန်တီးတိုက်ခိုက်သည့် Virus အဆုံး Virus ပေါင်းစုံတို့ကို ယနေ့အခါတွင် တွေ့ရှိနေရပါသည်။ Virus နှင့်ဆက်စပ်၍ World Wide Web ပေါ်တွင် အများဆုံးတွေ့ရှိရသည့် အနှောင့်အယှက် ပရိုဂရမ်များမှာ -

- **Adware (Advertising-supported software)**။ အင်တာနက်ကြော်ငြာများအတွက် အထောက်အပံ့ ဖြစ်စေသော ပရိုဂရမ်များ ဖြစ်ပါသည်။ Adware ပါဝင်သော Software ကို Install ပြုလုပ်မိသော ကွန်ပျူတာပေါ်တွင် ၎င်းပရိုဂရမ်များသည် အလိုအလျောက် လည်ပတ်ပြီး ကြော်ငြာ Internet webpage များကို ဖော်ပြစေသည်။ Download ပြုလုပ်စေသည်။ သို့ဖြစ်၍ ကွန်ပျူတာ၏ memory မလိုအပ်ပဲ Run နေသည့် ဤ ပရိုဂရမ်များကြောင့် စွမ်းဆောင်ရည် ကျဆင်းလာသည်။ စက်နေးလာသည်။ အလိုအလျောက်ပေါ်လာသော ကြော်ငြာစာမျက်နှာ များကြောင့် အလုပ်ရှုပ်ရသည်၊ စိတ်ရှုပ်ရသည်။ Adware များလာပါက ကွန်ပျူတာရပ်တန့်ခြင်း Hang ဖြစ်ခြင်းများ ဖြစ်လာနိုင်သည့်အတွက် အသုံးပြုသူ User အနေဖြင့် များစွာအခက်အခဲဖြစ်လာစေပါသည်။

- **Spyware** ။ တိုက်ခိုက်ခံရသူ၏ ကွန်ပျူတာပေါ်သို့ ပုန်းလျှိုးဝင်ရောက် Install ပြုလုပ်တတ်ပြီး User ၏ လှုပ်ရှားမှုများကို ကြားဖြတ် ဖမ်းယူထောက်လှမ်းခြင်း၊ တစ်စိတ်တစ်ဒေသ ထိန်းချုပ်ခြင်း၊ ကိုယ်ရေးအချက်အလက်များ၊ Account /Password များကိုခိုးယူပြီး User မသိအောင် ဖန်တီးသူထံသို့ ပြန်ပို့စေခြင်း အစရှိသည့်နှောင့်ယှက်မှုများကို ပြုလုပ်တတ်သောကြောင့် ပိုမို အန္တရာယ်ကြီးမားပါသည်။

- အလားတူ အနှောင့်အယှက်ပေးတတ်သော ပရိုဂရမ်များလည်း များစွာရှိပါသေးသည်.. အုပ်စုလိုက် ထင်ရှားသော အခေါ်အဝေါ်များမှာ - Trojans, Keyloggers, Hijacker, worms etc..

- အင်တာနက်ချိတ်ဆက်ထားခြင်းမရှိသော စက်များတွင် ဤကဲ့သို့ ပရိုဂရမ်များ Run နေလျှင် ကွန်ပျူတာမှာ အလွန်အမင်းလေးလံလာပါသည်။

ဘယ်သူတွေကို တိုက်တတ်သလဲ (အတိုက်ခိုက်ခံ ပစ်မှတ်များ)

အများအားဖြင့် Compter လုံခြုံရေးအကြောင်း မသိနားမလည်သူ အသုံးပြုစ User များ၊ ကလေးသူငယ်များ၊ ကွန်ပျူတာနှင့် အင်တာနက်ကို စသင်ခါစ Free download ဝါသနာရှင်လေးများ၊ ယုံလွယ်သူ ကျောင်းသားလူငယ်များ၊ အင်္ဂလိပ်စာကို သေချာမဖတ်ဘဲ Message မြင်တိုင်း Click နှိပ်တတ်သူ OK နှိပ်တတ်သူများ ခံရတတ်ပါသည်။ လူကြိုက်များသော တစုံတရာဖြင့် ဖျားယောင်းသွေးဆောင်ပြီးမှ ကွန်ပျူတာပေါ်တွင် မလိမ့်တပတ်ဖြင့် Install ပြုလုပ်စေခြင်းမျိုးကို အသုံးများပါသည်။

- ဥပမာ (၁) - မောင်ဖြူသည် အင်တာနက်အသုံးပြုတတ်ကာစ လူငယ်တစ်ဦးဖြစ်သည်။ အင်တာနက်ပေါ်တွင် ဘာမဆို ရနိုင်သည် ဟု ကြားဖူးနေသည်။ အင်တာနက် စာမျက်နှာများကိုဖွင့်ကြည့်ရင်း "လုံခြုံရေးအတွက် အလွန်အသုံးဝင်သည့် Software တစ်ခုကို Free Download လုပ်ခွင့်ပြုမည်" ဟု တွေ့သည်။ ယုံကြည်စွာ Download လုပ်လိုက်သည်၊ မစစ်ဆေးတော့ဘဲ Install ပြုလုပ်လိုက်သည်၊ သို့သော် ထို လုံခြုံရေး Software ဆိုသည်က အနှောင့်အယှက် Virus ဖြစ်နေသည်၊ Windows ပေါ်တွင် ကြော်ငြာစာမျက်နှာများ အလိုအလျောက် အဆက်မပြတ် ပေါ်လာသည်။ ကွန်ပျူတာမှာ အလွန်အမင်းလေးလံလာသည်။

- ဥပမာ (၂) - မောင်ညိုသည် ယနေ့ခေတ်တွင် IT ပညာနှင့် မကင်းကွာသင့်ကြောင်း သိရှိထားသည့် လူပျိုကြီးတစ်ဦးဖြစ်သည်။ IT ခေတ် အင်တာနက်တွင် အရွယ်ရောက်ပြီးသူများ (အထူးသဖြင့် ယောကျ်ားလေးဝါသနာရှင်များ) အကြည့်များသည့် Adault Site ဟုခေါ်သော လိင်မှုဆိုင်ရာ ဗီဒီယိုများ ရုပ်ပုံများ ကို ပြသ ရောင်းချသော / Free download လုပ်ခွင့်ပြုသော Web Site များ အများအပြားရှိသည်ဟု သိထားသည်။ ၎င်း Website များသို့ ဝင်ရောက်ကြည့်ရှုသည်၊ နှစ်သက်သော ဗီဒီယိုကို Download ပြုလုပ်သည့်အခါ ဗီဒီယိုဖိုင်ကို ကြည့်ရှုရန် လိုအပ်သော Software တစ်ခုကို Install ပြုလုပ်ရမည်ဟု တွေ့သည်။ ညွှန်ကြားချက်အတိုင်း ဆောင်ရွက်လိုက်သည်။ အဆိုပါ Software ဟု လိမ်ညာထားသော ဗိုင်းရပ်စ် ကူးစက်ခံရပါတော့သည်။

- ဥပမာ (၃) - မသင်းသင်းသည် ခင်မင်တတ်သော မိန်းကလေးတစ်ဦးဖြစ်သည်။ ယနေ့ အင်တာနက်ကို ဖွင့်ကြည့်သောအခါ မိမိ၏ Email Inbox ထဲတွင် အီးမေးလ်တစ်စောင်တွေ့သည်။ ခေါင်းစဉ်က Life is beauty ဟုတွေ့သည်။ စိတ်ဝင်စားသဖြင့် မစဉ်းစားတော့ဘဲ Click နှိပ်ပြီး ဖွင့်လိုက်သည်။ Link များကို နှိပ်ကြည့်လိုက်သည်။ It is too late now. Your life is no Longer-Beautiful ဟုပေါ်လာသည်။ ကွန်ပျူတာထဲမှ အချက်အလက်များ အားလုံး ပျက်စီးသွားပါသည်။

- ဥပမာ (၄) - မောင်ချောသည် ကွန်ပျူတာ ကျောင်းသားငယ်တစ်ဦးဖြစ်သည်။ Hacker ဟူသည့် ကွန်ပျူတာပညာရှင်များကို အလွန်အားကျသည်။ ယင်းတို့ကဲ့သို့ ဖြစ်လိုသည်။ ယင်းပုဂ္ဂိုလ်များသည် IT ပညာဖြင့် လူသားများအား ကူညီနိုင်သည်၊ တိုက်ခိုက်နိုင်သည်၊ မည်သည့်နေရာတွင်မည်သည့် Hacker က မည်သို့ အစွမ်းပြသွားသည် အစရှိသဖြင့် ကြားဖူးနေသည်၊ Hacker ဖြစ်ရန် ကြိုးစားနေလေသည်။ တနေ့တွင် မောင်ချော၏ Email ထဲသို့ စာတစ်စောင်ရောက်လာသည်။ သူတပါး၏ Email ကို Hack ပြီး ဝင်ကြည့်နိုင်သည့် နည်းလမ်းဟုရေးထားသည်။ လုပ်နည်းမှာ အလွန်လွယ်ကူပြီး မိမိတိုက်ခိုက်လိုသူ၏ Email adress ကိုဖော်ပြကာ မိမိ၏ Email account နှင့် Passwrod ကို ပို့ပေးယုံမျှဖြင့် သူတပါး Account ကို ဝင်ရောက်ကြည့်ရှုနိုင်မည်ဟု ဆိုထားသည်။ သို့ဖြစ်ရာ ညွှန်ကြားချက်အတိုင်း မိမိ၏ Account name နှင့် Password ကို ပေးလိုက်သည်။ လူကိုယ်တိုင်လာတောင်းလျှင်ပင် ပေးမည်မဟုတ်။ ယင်းနောက် ဘာမှ ထူးခြားမလာဘဲ Account သာ ခိုးယူခံလိုက်ရပေတော့သည်။ ၎င်း Web Program က မောင်ချော Account ထဲမှ Address Book ကိုဖတ်ပြီး ထိုထဲမှ မိတ်ဆွေများကို အလားတူ Email များ ပို့လေသည်။ မိမိမိတ်ဆွေမှ ပေးပို့သော Email မို့ ယုံကြည်ပြီး ခံရသည့်သူများ ခံရမည်။ သတိရှိသူများ လွတ်လိမ့်မည်။

ပျံ့ပွားပုံကတော့ လန့်သွားမယ် ယုံ

သက္ကရာဇ် ၂၀၀၀ နောက်ပိုင်းတွင် ဗိုင်းရပ်စ်ဖြင့် နှောင့်ယှက်ခံရမှုများ အလွန်များပြားလာပါသည်။ အများအားဖြင့် Online (World Wide Web) ပေါ်မှ စတင်ကူးစက်ခြင်းဖြစ်ပြီး ကွန်ပျူတာဆက်စပ်ပစ္စည်းများမှ တစ်ဆင့် Offline ကွန်ပျူတာများသို့ပါ ရောက်ရှိပြန့်ပွားလာပါသည်။ floppy disk များခေတ်က ပျံ့ပွားမှုနှုန်းထက် ယခု flash memory ခေတ်တွင် ပိုမိုမြန်ဆန်စွာ ပြန့်ပွားလာပါသည်။

ပထမဆုံး အင်တာနက်ချိတ်ဆက်ထားသောစက်တစ်လုံးမှာ Virus ကူးစက်ခံနေရပြီဆိုပါစို့..

- ထိုကွန်ပျူတာမှ ဥပမာ ဓါတ်ပုံဖိုင်များကို Print ထုတ်ယူရန် ဓါတ်ပုံဆိုင်သို့ flash Disk ဖြင့် ထည့်ပြီး သယ်ဆောင်သွား၏။ ထိုအခါ ကွန်ပျူတာထဲမှ ဗိုင်းရပ်စ်သည် flash Disk ပေါ်သို့ ကူးစက်ပြီး ပါလာ၏။
- ဓါတ်ပုံဆိုင်မှ User သည် ဗိုင်းရပ်စ် Scan နှင့် အခြားကာကွယ်မှုများကို Up to date မပြုလုပ်နိုင်ပါက ၎င်း၏ ကွန်ပျူတာထဲသို့ ဆက်လက်ကူးစက်၏။
- အခြား Customer များလည်း ဓါတ်ပုံထုတ်ရန် Flash Disk များ Flash Card များဖြင့် လာကြ၏။ ယင်းတို့၏ ပစ္စည်းများမှလည်း Virus ပါလာနိုင်၏။ ယင်းတို့ထံသို့လည်း စက်တွင်းရှိ Virus များ ကူးသွားနိုင်၏ ။

- ထိုသူများအားလုံး Flash Disk ကိုယ်စီဖြင့် အိမ်၊ ရုံး၊ ဌာန အသီးသီးသို့ ပြန်သွားကြပြီး သက်ဆိုင်ရာကွန်ပျူတာအသီးသီးတွင် အရင်းရောအမြတ်ပါ ပါလာသော သက်ဆိုင်ရာ ဗိုင်းရပ်စ်ပါသည့် Disk များ Card များကို ဆက်လက် အသုံးပြုကြ၏။
- ရုံးချင်း ၊ အိမ်ချင်း၊ အဖွဲ့ချင်း ဆက်လက် Share ပြုလုပ်ကြ၏ ။ ထိုအခါ..... ကာကွယ်နိုင်သူများ လွတ်ကြစေ။ မကာကွယ်နိုင်သူများ ခံကြစေ။
- MP3 , MP 4 အစရှိသည့် ကွန်ပျူတာနှင့်ဆက်စပ်ပစ္စည်းများ အသုံးပြုသူများလည်း.. ဤသို့ ဤနှယ်အတိုင်းပင်.....။
- Network တစ်ခုထဲရှိ Computer တစ်လုံးသို့ကူးစက်ပြီဆိုလျှင်လည်း အခြားကွန်ပျူတာများစွာ မှာ ဤသို့ဤနှယ်အတိုင်းပင်...။

Antivirus Software (ဗိုင်းရပ်စ်ကာကွယ်ရေး ဆော့ဖ်ဝဲများ)

IT လောကကြီးတွင် ဖျက်ဆီးသူရှိသလို စောင့်ရှောက်သူလည်းရှိ၏။ အခကြေးငွေဖြင့် ကာကွယ်ပေးသူလည်းရှိ၏။ စေတနာဖြင့် ကာကွယ်ပေးသူလည်းရှိ၏။ Virus, Spyware ဟူသည့် အဖျက် Program များ ပေါ်လာသော အခါ Antivirus, Antispysare ဟူသည့် ကာကွယ်တိုက်ဖျက်နိုင်သော Software များလည်း ပေါ်လာကြသည်။ အချို့ကား စိတ်ထားဖြူစင်သော ပညာရှင်များက ဖန်တီး ထုတ်လုပ်ပြီး အခမဲ့ ဖြန့်ဖြူးပေးသော Software များဖြစ်ကြသည်။ ၎င်းပုဂ္ဂိုလ်တို့၏ စွမ်းဆောင်ကူညီမှု အတွက် ကျေးဇူးတင် အသိအမှတ်ပြုပါက နည်းများမဆို လှူဒါန်း (Donate) နိုင်သည်။ မလှူလည်း ရပါသည်။ ဥပမာ- Hijack This , Spybot Search & Destory , etc...

အချို့ကား ကွန်ပျူတာလုံခြုံရေး အတွက် အခကြေးငွေပေးရသော Software များကို ထုတ်လုပ် ရောင်းချကြသည်။ အသစ်ပေါ်ထွက်လာသော ဗိုင်းရပ်စ်များကို ကာကွယ်နှိမ်နင်းရန် အချိန်နှင့်တပြေးညီ Update များ ထုတ်ပေးကြသည်။ Computer Security ဆိုင်ရာ အခြားအထောက်အပံ့များလည်း ပေးကြသည်။

အချို့ Software များသည် Virus ကိုသာ ရှာဖွေနှိမ်နင်း ကာကွယ်နိုင်သည်။ အချို့က Spyware, Adware တို့ကိုသာ ရှာဖွေနှိမ်နင်းကာကွယ်နိုင်သည်။ အချို့ကမူ ဘက်စုံကာကွယ်နိုင်သည်။ အရည်အသွေး အမျိုးမျိုး၊ ဈေးနှုန်းအမျိုးမျိုး.....။

ဘယ်လို Antivirus Software ကိုသုံးသည်ဖြစ်စေ.. သေနတ်ပစ်လျှင်ကျည်ပါရသလို Antivirus Software မှန်လျှင် Defination Update လုပ်ရပါသည်။ ဆိုလိုသည်မှာ 2006 ခုနှစ်က ထုတ်လုပ်ထားသော Software တစ်ခုကို Update မလုပ်ထားလျှင် 2008 ခုနှစ်မှထွက်ပေါ်လာသော နည်းပညာအသစ်နှင့် Virus ကို မသိပါ။ မသိ၍ မသတ်နိုင်ပါ.. ထို့ကြောင့် ကျည်မပါသောသေနတ် ဆောင်ထားသလိုဖြစ်ပါသည်။ ဆောင်ရတာတောင် လေးပါသေးသည်။ ထို့ကြောင့် ဘာကိုသုံးသုံး Update လုပ်ပြီးသုံးမှ ဖြစ်ပါမည်။

ကောင်းတာကိုလည်း ရွေးသုံးရပါမည်။ အင်တာနက် ချိတ်နိုင်သူများက တိုက်ရိုက် Download ပြုလုပ်သုံးစွဲပြီး မချိတ်ဆက်နိုင်သူများက ရရှိနိုင်သောဆိုင်တွင် ကူးယူသုံးစွဲရပေမည်။

လုပ်ပုံကာ လန်းပေစွ

စက်ထဲဝင်သွားသည့် ဗိုင်းရပ်စ်ဖိုင်တစ်ဖိုင် အလုပ်လုပ်ပုံလေးတွေက အန္တရာယ်ပေးရန် ရည်ရွယ်မှု အပေါ်မှာ မူတည်၍ မတူကြပါ။ သို့သော် ယခုအချိန်အထိတွေ့ဖူးသမျှထဲမှ ပြည့်ပြည့်စုံစုံ အလုပ်လုပ်သော ဗိုင်းရပ်စ်များ၏ လုပ်ပုံကိုင်ပုံ ဖြစ်နိုင်ချေများကို ဖော်ပြပါမည်-

- ဗိုင်းရပ်စ်အများစုသည် ကွန်ပျူတာအတွင်းသို့ Hidden (မမြင်နိုင်သော) ဖိုင်များအနေဖြင့်သာ ဝင်ရောက်ပါသည်။ Windows Explorer မှ Tool => Folder Options ကိုနှိပ်ပြီး View Tab ကိုဖွင့်ကာ => Advence Setting Area အတွင်းမှ Hidden files and folders အောက်မှ Show hidden files and folders-ON ကို ရွေးထားလိုက်ပါက ကွန်ပျူတာပေါ်ရှိ မည့်သည့် Hidden file ကိုမဆို မြင်နိုင်ပါသည်။ မြင်နိုင်က ဗိုင်းရပ်စ်ကို သတ်နိုင်မည်ဖြစ်ရာ အဆင့် အတန်းတခုရှိသော ဗိုင်းရပ်စ်သည် ကွန်ပျူတာထဲသို့ Run သွားသည်နှင့် တပြိုင်နက် Tool => Folder Options Menu ကို ဖျောက်ထားလိုက်ခြင်းဖြင့် မိမိအား ရှာတွေ့ရန်ကြိုးစားမှုကို အချည်းအနှီးဖြစ်စေပါသည်။
- အကယ်၍ ဗိုင်းရပ်စ်ဝင်ခဲ့သော် User က Run နေသည့် ဗိုင်းရပ်စ်ကို ရပ်ရန်အလို့ငှာ ကွန်ပျူတာကို Shut down/Restart ပြုလုပ်လိုက်ခြင်းဖြင့် ရပ်တန့်နိုင်သည့် အခြေအနေ တစ်ရပ် ရှိပါသည်။ သို့သော် အဆင့်အတန်းတစ်ခုရှိသည့် ဗိုင်းရပ်စ်သည် System Configuration Utility ရှိ Start Up နေရာတွင် ဗိုင်းရပ်စ်တည်ရှိသည့် ဖိုင်ပတ်လမ်းကြောင်းကို ထည့်သွင်းလိုက်သဖြင့် ကွန်ပျူတာကို ပြန်ဖွင့်လိုက်သည်နှင့်တပြိုင်နက် Virus ဖိုင်မှာ Run မြဲ Run နေစေပါသည်။ ဤနည်းဖြင့် ပြုလုပ်ချက်ကိုလည်း အနည်းငယ် နားလည်တတ်ကျွမ်းသည့် User က ပယ်ဖျက်နိုင်ပါသေးသည်။ ထို့ကြောင့် Windows ၏ အရေးအကြီးဆုံးနေရာဖြစ်သော Registry Editor တွင်လည်း ထပ်မံ ထည့်သွင်းလိုက်ပြန်ပါသည်။ ထည့်သွင်းပြီးနောက် Registry Editor ကို ပါ Disable ပြုလုပ်လိုက် ခြင်းဖြင့် Virus ကို ရပ်တန့်စေရန်ကြိုးစားမှုကို အချည်းအနှီးဖြစ်စေပါသည်။
- အဆင့်အတန်းတစ်ခုရှိသော ဗိုင်းရပ်စ်သည် Program တစ်ခုထဲ Run နေခြင်းမဟုတ်ပါ.. 3 ခု ထိရှိနိုင်ပါသည်။ ဥပမာ - A ,B , C ဟုဆိုကြပါစို့....။ A သည် အဖျက် Program ဖြစ်ပါသည်။ B သည် အဖျက် Program မဟုတ်ပါ။ ထို့ကြောင့် Antivirus က မဖမ်းပါ။ B သည် A ရှိမရှိကို စောင့်ကြည့်ပြီး မရှိတော့လျှင် ပြန်ရေးပေးပါသည်။ A ကိုဖျက်လိုက်ပါက B က A ကို ပြန်ရေးပေးနိုင်ပါသည်။ C ကတော့ A ကို အလိုအလျောက် Run စေရန် (Autorun) ဖိုင်ဟု အကြမ်းဖျင်း နားလည်ထားနိုင်ပါသည်။ ဤသည်မှာ ဥပမာအားဖြင့် ပြောပြခြင်းဖြစ်ပါသည်။ အားလုံးဒီအတိုင်းဟု ဆိုလိုခြင်းမဟုတ်ပါ။ ဤကဲ့သို့ ဖန်တီးမှုအားကောင်းလာသော ဗိုင်းရပ်စ်

များကို တိုက်ဖျက်ရန် အတွက် သက်ဆိုင်ရာ Antivirus ကို အမြဲတမ်း Database (Difination) Update ပြုလုပ်ပေးနေရပါမည်။

- ဗိုင်းရစ်စ် တစ်ခုသည် လက်ရှိ Run နေ /မနေ ကို သိရှိနိုင်သည့် နေရာတစ်ခု ရှိပါသေးသည်။ ၎င်းမှာ Windows Task Manager ဖြစ်ပါသည်။ ကွန်ပျူတာကို အတန်အသင့် ရင်းနှီးသူများသည် Task Manager ကိုလည်း သုံးစွဲတတ်ကြပါသည်။ Task Manager တွင် လက်ရှိ Program မည်မျှ အလုပ်လုပ်နေသည်ကို ကြည့်ရှုနိုင်ခြင်း၊ မည်သည့် Process များ မည်မျှ Run နေသည်ကိုလည်း သိရှိနိုင်ခြင်း ၊ Process အသစ်များကို Run စေနိုင်ခြင်း ၊ Run နေသော Process များကိုလည်း ရပ်တန့်ပစ်စေနိုင်ခြင်းအပြင် Computer သည် လက်ရှိ Memory မည်မျှ သုံးစွဲနေရသည်ကို သိရှိနိုင်ပါသည်။ သို့ဖြစ်ရာ ဗိုင်းရပ်စ်တစ်ခု Run နေမနေကို သိရှိရန် Ctrl + Alt + Delete ကို နှိပ်ပြီး Process Tab တွင် ကြည့်ရှုမှတ်သားကာ ရပ်တန့်နိုင်ပေသည်။ သို့သော် အဆင့်အတန်း တစ်ခုရှိသည့် Virus သည် Task Manager ကိုလည်း Disable ဖြစ်အောင် လုပ်လိုက်ပါသည်။ ထို့ကြောင့် ရပ်တန့်ရန်ကြိုးစားမှုကို အချည်းအနှီးဖြစ်စေပါသည်။
- သို့ဖြစ်ရာ အကျဉ်းချုပ်အားဖြင့် အတန်အသင့် အဆင့်ရှိသော Virus သည် ကွန်ပျူတာထဲသို့ ဝင်ရောက်သွားပြီးသည်နှင့် အောက်ဖော်ပြပါ လုပ်ရပ်များကို တပြိုင်တည်း လုပ်လိုက်လေ့ ရှိပါသည်။
  - Folder Options ကို ဖျောက်လိုက်သည်။
  - Registry Editor ကို Disable လုပ်လိုက်သည်။
  - Task Manager ကို Disable လုပ်လိုက်သည်။
  - Start up နှင့် Registry တို့တွင် ကွန်ပျူတာ Windows တက်သည်နှင့် Auto run စေသည်။

ဤသို့ အတည်တကျနေရာယူပြီးနောက်မှ အဓိကလုပ်ငန်းဖြစ်သော ဖျက်ဆီးခြင်း နှောင့်ယှက်ခြင်း လုပ်ငန်းပေါင်းစုံကို လုပ်ဆောင်ကြလေကုန်၏ ။ အချို့ကား file/folder များကို ဝှက်လိုက်ပြီး ယင်း file/folder များ၏ icon နှင့်အမည်များ ကိုအသုံးပြု၍ exe ဖိုင်များ ဆောက်ကြသည်။ ထောင်ချောက်ဆင်ခြင်းသဘောပင် ။ User က မိမိပြုလုပ်ထားသော ဖိုင်မှတ်၍ ဖွင့်သည်ရှိသော် Vires ကို တစ်ကြိမ် Run ပေးခြင်းဖြစ်လေသည်။ ဤကဲ့သို့ Run ပေးတိုင်း Virus သည် မိမိကိုယ်ကို ပုံတူများ ပွားပေးပြီး ပိုမို ရှုပ်ထွေးလာစေသည်။ အချို့ကား Windows စတက်လျှင် လိုအပ်သော ntdlr file ကဲ့သို့ မရှိမဖြစ်ဖိုင်မျိုးကို ဖျက်ပစ်လိုက်၏ ။ နောက်တစ်ကြိမ် Computer မှ Restart ဖြစ်သောအခါ ntdlr file missing ဟု ပြနေပြီး windows မတက်တော့ချေ..။ အချို့ကား file icon များကိုပြောင်းပစ်လေ၏။ အချို့ကား ပေါက်တတ်ကရ ပေါ်ချင်ရာတွေပေါ်ကုန်၏။ File ဟူသမျှ အားလုံးဖျက်ဆီးပစ်ခြင်းခံရသူများ ရှိခဲ့သည်။ အရေးကြီးသောဖိုင်များ ပျက်စီးသွားသဖြင့် အချိန်မီအလုပ်မပြီးရကား အလုပ် ပြုတ်သူများ၊ အရေးယူခံခဲ့ရသူများ ရှိခဲ့သည်။ အထူးသဖြင့် မြန်မာပြည်မှ ရွှေမြန်မာအမျိုးကောင်းသား မျိုးဆက်သစ်များထဲက တော်ရာတော်ကြောင်း ပညာ

ကို မသင်ဘဲ ဗိုင်းရပ်စ်ရေးသောနည်းကိုမှ လေ့လာ၍ ရေးကြသည့် မြန်မာပြည်ဖြစ် ဗိုင်းရပ်စ်များက ပို၍ ရက်စက်၏။ ဖအေ့မျက်နှာကို Ice-cream သုတ်၍ ခွေးဝဲစားနဲ့လျက်ခိုင်းသော သားသမီးမျိုး၏ ရက်စက်မှုမျိုးဖြစ်ပေသည်။ ရှက်တက်ကြပါစေ ။ ဤကား Virus ၏ အဓိက နှောင့်ယှက် ဖျက်ဆီးရေးလုပ်ငန်းပေါင်းစုံကို ကြုံဖူးသမျှ ပြောပြခြင်းဖြစ်သည်။ flash disk ကဲ့သို့ disk တစ်ခုခုလာထိုးလျှင် စက်ထဲရှိသမျှ ဗိုင်းရပ်စ်အားလုံး ထို disk ပေါ်သို့ ပွားပြီးလိုက်သွားကြ၏။ နောက်စက်တစ်လုံးသို့ ထို disk သွားထိုးလျှင် တပျော်တပါး ထိုစက်ပေါ်သို့ ကူးကြ၏ ။ ဤနည်းအားဖြင့် Virus သည် AIDS ကူးနည်းမျိုး ကူးစက်တတ်ပေကြောင်း မှတ်သားရပါသည်။

<u>မဖြစ်ခင်တား၍အကာအကွယ်ယူ</u>

ယနေ့ခေတ်အခါသမယ Antivirus/Antispyware များ မကောင်းဟု မပြောလိုပါ။ သူ့ဟာနဲ့သူ အလွန်ကောင်းကြပါသည်။ သို့သော် မည်မျှပင်ကောင်းကောင်း File sharing နှင့် ကင်းကင်းရှင်းရှင်း မနေနိုင်သူများအတွက် လုံခြုံသည်ဟူ၍မရှိပါ။ ကျွန်တော်တို့ပတ်ဝန်းကျင်တွင် ဤစနစ်ကြီးမျိုး တစ်ခု ရှိနေပါသည်။ ကျွန်တော်တို့ မသုံးမဖြစ် သုံးနေကြရပါသည်။ တစ်ဦးနှင့်တစ်ဦး file များ၊ ကောင်းမွန်သော Software များ Share ကြပါသည်။ Virus များလည်း ပွ ထ နေသည်ကို တွေ့နေရပါသည်။ စေတနာဖြင့် Kaspersky, Nortan, Avast, AVG ကဲ့သို့သော Software များအတွက် Update file များ ဖြန့်ဖြူးပေး နေသည် ကိုလည်း ဝမ်းသာစွာတွေ့ရပါသည်။ Virus များလည်း ပွားမြဲပွားနေသည်ကိုတွေ့ရပါသည်။ Online ပေါ်တွင် လွန်ခဲ့သည့် ၁၀ ရက်လောက်ကမှ စတင်ပေါ်ပေါက်လာသော ဗိုင်းရပ်စ်က ကျွန်တော်တို့ ရုံး/ဌာန အချို့မှ သူငယ်ချင်းများ၏ ကွန်ပျူတာတွင် Up to date ဝင်မွေနေသည်ကိုလည်း တွေ့ဖူးပါသည်။ အရမ်းခေတ်မီတယ်ခေါ်မလား၊ ဂုဏ်ယူဖွယ်ရာလား ၊ ထိုင်ကန်တော့ရမလား မပြောတတ်တော့ပါ..။ ဗိုင်းရပ်စ်ဟူသည် မီးကဲ့သို့ မလောင်ခင်တား၊ မဝင်ခင် တားရသည့်အမျိုးဖြစ်ကြောင်း သတိချပ်စေချင်ပါသည်။ ဖျက်ဆီးမှုပြင်းထန်သော ဗိုင်းရပ်စ်မျိုးကို ဝင်နေကြောင်း မသိလိုက်ဘဲ Infection ဖြစ်ပြီးကာမှ သိလျင် နောက်ကျသွားနိုင်ပါသည်။ ဖိုင်များ မပျက်လျှင်တောင် Windows ပြန်တင်ရသည့် အဖြစ်မျိုးနှင့် အချိန်နှင့်ငွေးညီ လုပ်ငန်းပြီးစီးရန် လိုအပ်နေသည့်အခါမျိုးတိုက်ဆိုင်လျင် မည်မျှ စိတ်ဆင်းရဲရသည်ကို ကြုံဖူးသူများ သိကြပါသည်။ ထို့ကြောင့် မဝင်ခင် တားပါ.. အကာအကွယ်အပြည့်ဖြင့် နေပါ။ ဝင်လာလျှင် ချက်ချင်းရှင်းပစ်ပါ။ flash disk လာလျှင် ဗိုင်းရပ်စ်ပါသည်ဟု အသေမှတ်ယူထားပါ။ Auto run box တက်လာလျှင် Cancel လုပ်ပစ်ပါ။ Antivirus ဖြင့် Scan ထိုးပါ။ တွေ့လျှင်သတ်ပါ။ မတွေ့လျှင်ပင် မသေချာသေးပါ။ ဤနေရာတွင် Winrar ဟုခေါ်သည့် လူသုံးများသော ဖိုင်ချုံ့ Software လေးကို သုံးပြီး flash disk ကို ထိုးပြီးပြီးချင်း browse လုပ်ကြည့်လျှင် Virus ကို မြင်နိုင်ပြီး စက်ထဲမမဝင်သေးခင် Shft+Del ဖြင့် ဖျက်ပစ်လိုက်နိုင်သည်ဆိုသည်ကို လူသိနည်းသေး၏။ ဆက်လက် ရှင်းပြသွားပါမည်။ အောက်မှာပြမယ့်နည်းတွေကိုကြည့်ပြီး စစ်ဆေးပါဦး..။ လုံးဝသေချာမှ flash disk , floppy disk , အစရှိသည်တို့ကိုသုံးပါဟု တိုက်တွန်းအပ်ပါသည်။

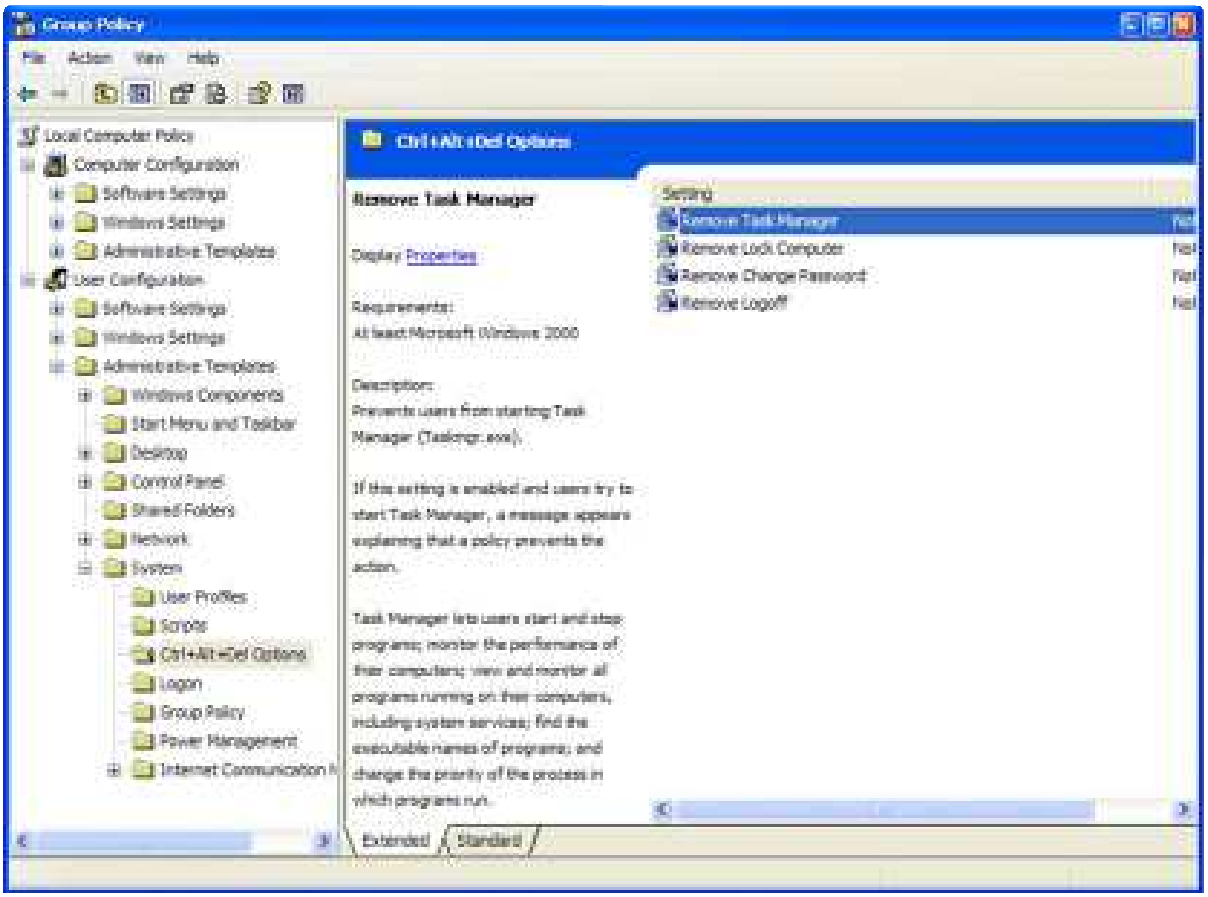
ဗိုင်းရပ်စ်များနှင့်ကခုန်ခြင်း

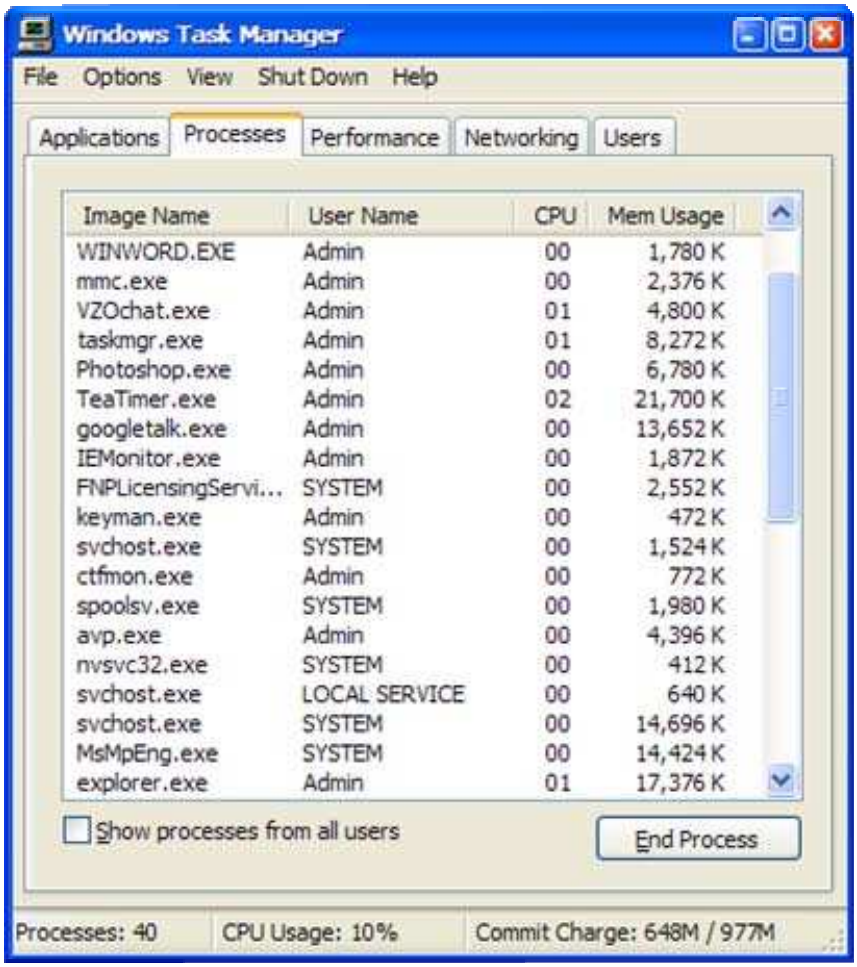
မိမိစက်အတွင်းမှာ ဗိုင်းရပ်စ်တစ်ကောင်ကောင် ဝင်နေတယ်လို့ ထင်ပါသလား။ သေချာပေါက် ဝင်နေပြီ ဆိုတာသိနေပါလျက်နဲ့ Antivirus က အဲဒီဗိုင်းရပ်စ်ကို မသိလို့ သတ်လို့မရ ဖြစ်နေပါသလား။ ဗိုင်းရပ်စ်ကို သေသေချာချာတွေ့နေလို့ Shift + Delete နဲ့ဖျက်တာတောင်မှ ပြန်ပြန်ပေါ်နေပါသလား။ တခုချင်း ကြည့်ရှုင်းသွားရအောင်....။

အပေါ်မှာပြောခဲ့တာတွေထဲက တခုခုဖြစ်နေပြီဆိုရင် မိမိစက်ဟာ ဗိုင်းရပ်စ်ထိထားပြီပြီးလို့ပဲ မှတ်ထား လိုက်ပါ။ တကယ်လို့ ဗိုင်းရပ်စ်နာမည်ကို သိတယ်ဆိုရင်တော့ အကောင်းဆုံးပေါ့။
ဗိုင်းရပ်စ်တစ်ခုဟာ စက်ထဲမှာ Run နေပြီဆိုရင် သူ့ကို ဒီအတိုင်း Shift + Delete နဲ့ ဖျက်လို့မရပါဘူး။ ပြန်ပေါ်ပါတယ်.. ။ အပြီးသတ်ချင်ရင် အရင်ဆုံး သူ့ရဲ့ Process ကို ရပ်ပစ်ရပါမယ်.. Keyboard က Ctrl+Alt+Del သုံးလုံးကိုတွဲနှိပ်လိုက်ပါ။ Windows Task manager ပေါ်လာရပါမယ်။ မပေါ်လာဘဲ အောက်က Massage ပေါ်လာရင်တော့ ဗိုင်းရပ်စ်ရှိတယ်ဆိုတာ ပိုသေချာပါပြီ..။

ဒါဆိုရင်တော့ Task Manager ကို ပြန်ဖွင့်ဖို့ လုပ်ရပါမယ်..။
Start =>Run ကို နှိပ်ပြီး gpedit.msc လို့ ရိုက်ထည့်ပြီး OK ကို နှိပ်လိုက်ပါ။

Group Policy Windows ပေါ်လာပါလိမ့်မယ်။ ဘယ်ဘက်အခြမ်းမှာ User Configuration ကို Double Click လိုက်ရင် အောက်ကို folder သုံးခု ထပ်ပြေကျသွားပါမယ်။ အဲဒီက Administrative Templates ကို ထပ်ပြီး Double Click လိုက်ရင် အောက်ကို folder တွေ ထပ် ပြေကျသွားပါမယ်။ ဟိုးအောက်ဆုံးမှာ System ဆိုတာရှိတယ်။ အဲဒါကို Double Click လိုက်ပါအုံး ထပ်ပြေကျသွားတဲ့ folder တွေထဲမှာ Ctrl+Alt+Del Options ကို Click တစ်ချက်နှိပ်လိုက်ပြီး Window ရဲ့ညာဘက်အခြမ်းမှာ Remove Task Manager ကို Double click နဲ့ ဖွင့်လိုက်ရပါမယ်..

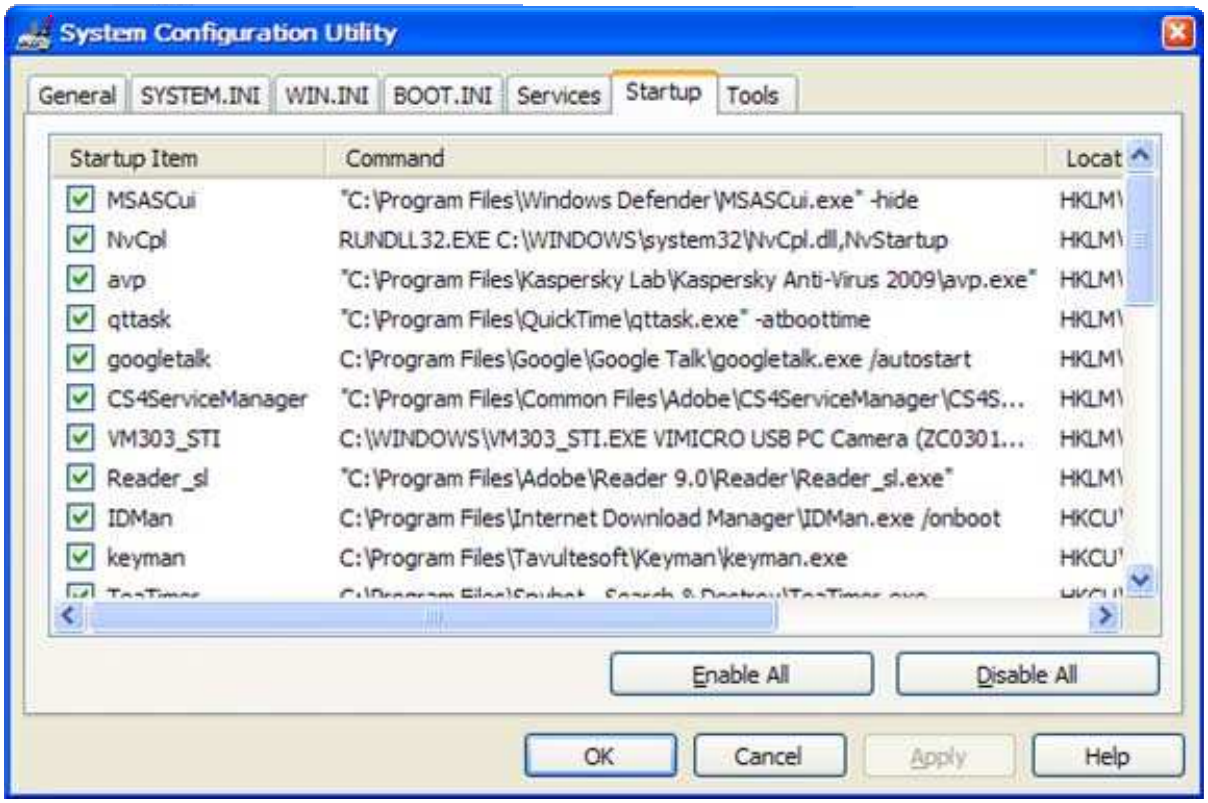




ထပ်ပွင့်လာတဲ့ Remove Task Manager Properties Dialog box မှာ Setting Tab ကိုနှိပ်ထားပြီး Disable radio button လေးကို ရွေးကာ Apply ကို Click လုပ်လိုက် ပါ။ ကဲ အခု Ctrl +Alt + Delete ကို ပြန်နှိပ်ကြည့် လိုက်ပါအုံး.. ပြန်ပေါ်လာတာ ကိုတွေ့ရပါ လိမ့်မယ် ဒါဆိုရင် Remove Task Manager Properties Dialog box ကို OK နှိပ်ပြီး ပိတ်လိုက်ပါမယ် ပြီးတော့ Windows Task Manager

မှာ Process Tab ကို နှိပ်ထားလိုက်ပါ။ ပြီးရင် အောက်မှာ လက်ရှိ Run နေတဲ့ Process တွေထဲက Virus process (ဥပမာ အခု ကျွန်တော်တို့ဆီမှာ ခေတ်စားနေတဲ့ chrome.exe) ပေါ်ကို Right Click ခေါက်ပြီး End Process Tree ကိုနှိပ်လိုက်ရင် Virus ဟာ သက်မဲ့ ဖြစ်သွားပါပြီ (ရပ်သွားပြီလို့ ဆိုလိုတာပါ)။

ကဲအခု ရပ်တန့်နေပြီဖြစ်တဲ့ ဗိုင်းရပ်စ်ကို အပြီးအပြတ် ဆက်ရှင်းလိုက်ရအောင်.. အထက်မှာကျွန်တော်တို့ ပြောခဲ့တယ်.. ဗိုင်းရပ်စ်ဟာ သူ့ကိုရပ်တန့်လိုက်ပြီဆိုရင် အလိုအလျောက် Windows စတက်တာနဲ့ Run နိုင်အောင် Windows Startup မှာ တည်နေရာဖိုင်ပတ်လမ်းကြောင်းကို သွားရေးထားတယ်လို့ ပြောခဲ့တယ်နော်။ အဲဒီတည်နေရာရေးမိတာကိုက အခုတော့ သူ့သေတွင်းသူတူးသလိုဖြစ်သွားပြီပေါ့။ ဘယ်နေရာမှာရှိသလဲဆိုတာကိုသွားကြည့်ရအောင်။ Start => Run ကို နှိပ်ပြီး msconfig လို့ ရိုက်လိုက်ပါ။ OK နှိပ်လိုက်ပါ..။ System Configuration Utility ပေါ်လာပါလိမ့်မယ်.. Startup Tab ကို နှိပ်လိုက်ပါ .. အဲဒီမှာ ဝင်းဒိုးစစတက်ချင်း Run မယ့်ဖိုင်တွေကို အမှန်ခြစ်လေးတွေခြစ်ထားတာ တွေ့ရပါမယ်၊ ဗိုင်းရပ်စ်ဖိုင် (ဥပမာ chrome.exe) ကိုလိုက်ရှာလိုက်ပေါ့။ တွေ့ပြီဆိုရင် အမှန်ခြစ်ကလေးကို ဖြုတ်လိုက် ဒါဆိုရင် နောက်တခါဝင်းဒိုးစတက်ရင် ဒီနေရာကနေ မ Run နိုင်တော့ဘူးပေါ့။ တဆက်ထဲမှာပဲ သူ့ရဲ့ဖိုင်ပတ်လမ်းကြောင်းကို မှတ်ခဲ့လိုက်မယ်၊ c:\program files\system 32\chrome.exe လို့ ရေးထားတယ်ဆိုတော့ အဲဒီမှာ သွားရှာပြီး ဖျက်ပစ်ယုံပဲပေါ့ ..

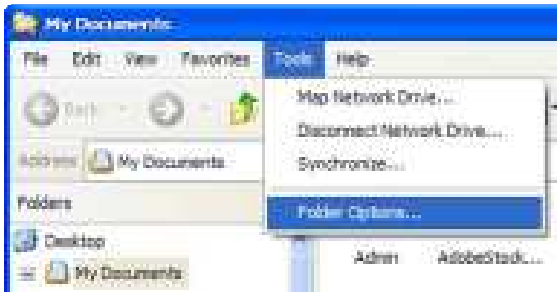


အခု Apply & OK နှိပ်ပြီးထွက်လိုက်ပါ။ Windows က Restart ချ မလားလို့ မေးပါလိမ့်မယ်။ လုပ်စရာနည်းနည်းကျန်သေးတဲ့အတွက် အဲဒီအတိုင်းလေးပဲ ဘာမှမလုပ်ဘဲ ထားလိုက်ပါအုံး..

အထက်စာမျက်နှာတွေမှာတုန်းက ကျွန်တော်တို့ ပြောခဲ့တယ်နော်.. Windows ရဲ့ Hidden ဖိုင်တွေကို ကြည့်လို့ရတဲ့ Folder Options Menu ကိုင် ဝိုင်းရပ်စ်က ဖျောက်ထားတတ်တယ်လို့..

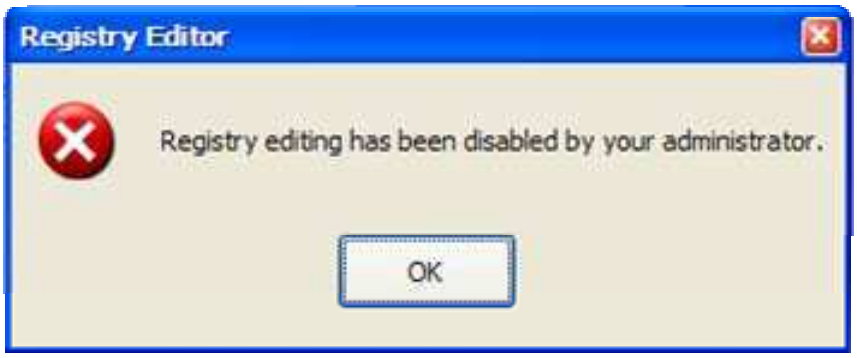
အခု အဲဒါလေးကိုလည်း ပြန်ပြင်ကြမယ်.. ထုံးစံအတိုင်း gpedit.msc ကို Run လိုက်ပါအုံး.. ပြီးရင်...

User Configuration => Administrative Templates => Windows Components => Windows Explorer ကို နှိပ်ထားပြီး ညာဘက်အခြမ်းက Removes the Folder Options menu item from the Tools menu ကို Double Click နဲ့ ဖွင့်လိုက်ပါ.. ထပ်ပေါ်လာတဲ့ box ထဲမှာ ထုံးစံအတိုင်း Disable ကိုနှိပ်ပြီး Aply ခေါ်လိုက်မယ် ၊ ပြီးရင် Start => Programs=> Accessories => Windows Explorer ကို ဖွင့်ကြည့်လိုက်ပါ ။ Tools Menu ကို နှိပ်ကြည့်လိုက်ရင် Folder Options Menu ကို တွေ့ရပြီပေါ့ဗျာ..

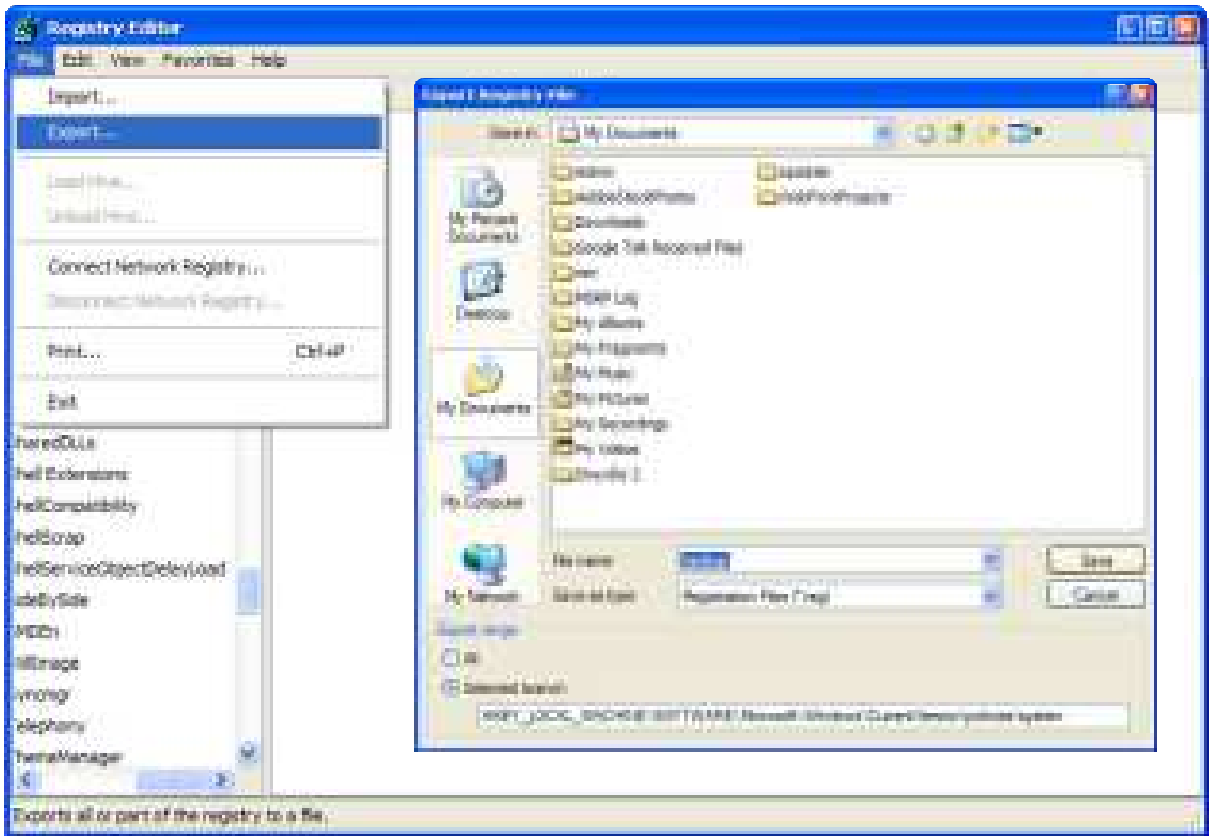


Folder Options Menu ကို တွေ့ပြီဆိုရင် Windows Hidden ဖိုင်တွေကို မြင်ရအောင် လုပ်ကြပါမယ်.. Tools menu အောက်က Folder Options ကို နှိပ်လိုက်ပါမယ်.. View Tab ကို Click လုပ်ထားပြီး Hidden files and folders အောက်က Show Hidden files and folders-ON ဆိုတာလေးကို Check လုပ်ပြီး Apply & OK နဲ့ ထွက်လိုက်မယ်.. ဒါဆိုရင် Hidden files တွေကို မြင်ပြီပေါ့...

အခု ဆက်လုပ်ရမှာကတော့ Registry Editor ထဲက Run ထားတဲ့ ဖိုင်ပတ်လမ်းကြောင်း ကို ဖျက်ပစ်ဖို့ပါ.. အဲဒီတော့ Startup မှာ ဖျက်ခဲ့ ပေမယ့် Registry ထဲမှာ မဖျက်ရသေး ရင် Virus က Run နေအုံးမှာပါဗဲ.. ဒါကြောင့် တခါထဲ အပြတ်ရှင်းရပါမယ်.. Start => Run ကနေ regedit လို့ ရိုက်လိုက်ပြီး OK ပေးလိုက်ပါ။ တကယ်လို့ Registry Editor ကို ဝိုင်းရပ်စ်က မပိတ်ထားခဲ့ရင် ပွင့်လာရမယ်.. ပိတ်ထားတယ်ဆိုရင် တော့ ဒီလိုပေါ်လာမယ်..



အဲဒါကို ပြင်ဖို့ အတွက် Start => Run ပြန်ခေါ်ပြီး gpedit.msc ပြန် ရိုက်ထည့် OK ပြန် ပေးလိုက်ရင် Gropu Policy ပြန်တက် လာမယ်.. ဘယ်ဘက် အခြမ်းက User configuration => Administrative Templates => System ကို နှိပ်ထားပြီး ညာဘက်အခြမ်းမှာ Prevent access to registry tools ကို ဖွင့်ပါမယ်.. ပွင့်လာလို့ ရှိရင် Setting Tab ကို ရွေးထားပြီး Disable radio button လေးကို တချက်နှိပ်လိုက်မယ်.. Apply & OK ပေးလိုက် မယ်.. ပြီးရင် Start => Run မှာ regedit လို့ ရိုက် ထည့်ပြီး OK လိုက်ရင် Registry Editor ပွင့်လာ ပါလိမ့်မယ်.. အခု အဓိကကျတဲ့အချက် တစ်ချက်ကို ပြောပါမယ်.. Windows Registry သည် ကွန်ပျူတာ လည်ပတ်ဖို့ အတွက် အရမ်းအရေးကြီးပါတယ် Key အချက်အလက်အားလုံးဟာ အထိ မခံပါဘူး အကြောင်း တစုံ တရာကြောင့် အဲဒီထဲက Key တွေကို မှား ဖျက်မိရင် ဒုက္ခတွေ့နိုင်ပါတယ်.. ဒါကြောင့် ဘာမှမလုပ်ခင်မှာ Registry ကို Back up လုပ်ထားပါ.. ဒါပေမယ့် သေမထူးနေမထူး ဝိုင်းရပ်စ်ထိထားတဲ့ ကွန်ပျူတာတစ်လုံး အတွက်ကတော့ ဒီထက်ဆိုးဖျက်မိလည်း ဘာမှတော့ ဖြစ်မလာတော့ပါဘူး.. အမှန်တကယ် သတိပေးချင်တာက သေချာစွာ စစ်ဆေးပြီးမှ ဖျက်ရပါမယ် ဆိုတာပါပဲ ကဲ.. registry backup လုပ်ရအောင်



File => Export ကို နှိပ်ပြီး ပေါ်လာတဲ့ box ထဲမှာ သတ်သတ်မှတ်မှတ် တစ်နေရာကိုရွေးပြီး Save လုပ်လိုက်ပါ..

အခုကျွန်တော်တို့ ဆက်လုပ်မှာက Registry ထဲမှာရေးထားတဲ့ Virus ရဲ့ ဖိုင်ပတ်လမ်းကြောင်းကို ရှာဖို့ပါပဲ.. အဲဒါကိုဖျက်မှ ဗိုင်းရပ်စ်ရဲ့ လက်စလက်နတွေက ပြတ်မှာလေ.. Regsiry Editor ရဲ့ ဘယ်ဘက်အခြမ်းမှာလည်း HKEY_CURRENT_USER ဆိုတာရှိပါတယ်.. အတိုကောက်အားဖြင့် HKCU လို့မှတ်လိုက်ရအောင်.. အဲဒါလေးကို အခုရေးပြမယ့်အစီအစဉ်အတိုင်း ဖြေချသွားမယ်..

HKCU => Software => Microsoft => Windows => Current Versions=> Run ကို click နှိပ်ထားမယ်.. ညာဘက်အခြမ်းမှာ ပေါ်နေတဲ့ Key တွေအားလုံးဟာ Windows စတက်တက်ချင်း Run မယ့် ဖိုင်တွေပါပဲ.. အဲဒီထဲမှာ ဗိုင်းရပ်စ်ဖိုင်အမည်ပါတဲ့ Key ကို လိုက်ရှာမယ်..ဖျက်မယ်.. မရှိရင် ဒါမှမဟုတ် ဖျက်ပြီးရင် ဘယ်ဘက်အခြမ်းကိုပြန်သွားမယ်..

HKEY_LOCAL _MACHINE ကိုလည်း HKLM လို့ မှတ်လိုက်မယ်နော်.. အဲဒါလေးကိုလည်း အခုရေးပြမယ့်အစီအစဉ်အတိုင်း ဖြေချသွားမယ်..

HKLM => Software => Microsoft => Windows => Current Versions=> Run ကို click နှိပ်ထားမယ်.. ညာဘက်အခြမ်းမှာ ပေါ်နေတဲ့ Key တွေအားလုံးဟာ Windows စတက်တက်ချင်း Run မယ့် ဖိုင်တွေပါပဲ.. အဲဒီထဲမှာလည်း ဗိုင်းရပ်စ်ဖိုင်အမည်ပါတဲ့ Key ကို လိုက်ရှာမယ်..ဖျက်မယ်.. မဖျက်ခင်မှာ ဖိုင်ပတ်လမ်းကြောင်းလေးကို သေချာစွာ မှတ်ခဲ့ပါ..

တခါတရံ ဗိုင်းရပ်စ်က Start Menu ထဲက Search ဆိုတာကိုလည်း ဖျောက်ထားတတ်တယ်.. ဒါမျိုးရှိနေရင်လည်း...

HKCU => Software => Microsoft => Windows => Current Versions=> policies => System ကို Click နှိပ်ထားပြီး ညာဘက်အခြမ်းမှာ nofind ဆိုတဲ့ key ကို ဖျက်လိုက်ရမှာပါ.. အဲဒီမှာ မရှိဘူးဆိုရင်တော့

HKLM => Software => Microsoft => Windows => Current Versions=> policies => System ကို Click နှိပ်ထားပြီး ညာဘက်အခြမ်းမှာ nofind ဆိုတဲ့ key ကို ဖျက်လိုက်ပါ.. ဆိုလိုတာက ကျွန်တော်တို့ Registry ကို ကောင်းကောင်းလေး နားလည်ထားရုံနဲ့ ကွန်ပျူတာကို လိုသလို ထိန်းချုပ်လို့ရတယ် ဆိုတာလေးပါ.. ပြီးတော့ Group Policy ကို ထိန်းချုပ်နိုင်တာရောပေါ့.. ကျွန်တော့်အမြင်ကတော့ Group Policy ကို သုံးတာက ပိုပြီးအန္တရာယ်ကင်းတယ်၊ လွယ်ကူရှင်းလင်းတယ်လို့ထင်ပါတယ်..။

ကဲ အခု Windows Registry ကို ပိတ်လိုက်မယ်..

ကဲ .. အခု ဗိုင်းရပ်စ်ကို တကယ်သွားပြီးသတ်တော့မယ်..

စောစောက မှတ်လာတဲ့ ဖိုင်ပတ်လမ်းကြောင်းအတိုင်း သွားပြီးတော့ ရှာလိုက်ပါ..

c:\windows\system32 ကိုဖွင့်ပြီး chrome.exe ကို လိုက်ရှာလိုက်ပါ တွေ့ရင် Shift+Delete နဲ့ ဖျက်လိုက်ပါ.. ပြီးသွားပါပြီ..ဗိုင်းရပ်စ်က သေသွားပါပြီ.. ဒါပေမယ့် အခု ကျွန်တော်ဥပမာထားပြောနေတဲ့

ဝိုင်းရပ်စ်က သာမန် နောင့်ယှက်တာလောက်ပဲ လုပ်တဲ့ ဝိုင်းရပ်စ်ပါ.. တချို့ ဝိုင်းရပ်စ်တွေက ဝင်းဒိုးစ်တက်ဖို့မရှိမဖြစ်လိုအပ်တဲ့ ဖိုင်တွေကို ဖျက်ပစ်တတ်တယ်လို့ ပြောခဲ့တယ်နော်.. အဲဒီတော့ ကိုယ့်စက်ထဲမှာ ဝင်ကိုက်သွားတဲ့ဝိုင်းရပ်စ်ဟာ ဝင်းဒိုးစ် Boot file တွေကို ဖျက်ဆီးသွားသေးသလားဆိုတာ စစ်ရအုံးမယ်.. တော်ကြာနေမှ ဝိုင်းရပ်စ်က သေပါပြီကွာဆိုပြီး Restart ချလိုက်ရင် နောက်တခါ ပြန်တက်လာတဲ့ အခါကျတော့ ဝင်းဒိုးစ်က မတက်တော့ရင် ခဲလေသမျှ ပဲရေပွ ဖြစ်အုံးမှာလေ.. အဲဒါကြောင့် Final Check အနေနဲ့ mycomputer=> Drive C: ကို ဖွင့်ကြည့်လိုက်ပါအုံး.. အဲဒီထဲမှာ

- ntdlr
- ntdetect.com
- boot.ini ဆိုတဲ့ ဖိုင် သုံးဖိုင် စုံမစုံကြည့်ပါ.. တစ်ဖိုင်ဖိုင်က လိုနေပြီဆိုရင်တော့ တခြားကွန်ပျူတာကနေ ကူးထည့်လိုက်ပါအုံး.. အဲဒီသုံးဖိုင် မစုံရင် နောက်တစ်ကြိမ် ဝင်းဒိုးတက်တော့မှာမဟုတ်ပါဘူး..

ကဲ စုံပြီဆိုရင်တော့ msconfig လုပ်တုန်းက Restart တောင်းထားတဲ့ဘောက်စ်ကို အခု လက်ခံပြီး စိတ်ချလက်ချသာ Restart ချလို့ရပါပြီ...

ညှပ်ကျန်ခဲ့တဲ့ မေးခွန်းတစ်ခု

အခုပြောခဲ့သမျှ မှာ Disable ဖြစ်နေတာတွေကို Group Policy (gpedit.msc) ကနေ ပြန်ဖွင့်လို့ ရတယ်ဆိုတာလေးတွေမှတ်မိကြတယ်နော်.. မေးခွန်းတခုက အဲဒီလို ထိန်းချုပ်နိုင်တဲ့ gpedit.msc ကိုရော ဝိုင်းရပ်စ်တစ်မျိုးမျိုးက Disable မလုပ်သွားနိုင်ဘူးလား ...

အဖြေက လုပ်သွားနိုင်ပါတယ်.. gpedit.msc တင်မက ရှိရှိသမျှ .msc command အားလုံးကို Disable လုပ်သွားတဲ့ ဝိုင်းရပ်စ်ကိုတောင် သူငယ်ချင်းတစ်ယောက်က တွေ့ဖူးပါသတဲ့.. အဲဒီတော့ ကျွန်တော်တို့ ဒီလို အဖြစ်မျိုးနဲ့ ခံရရင် ဘယ့်နယ်လုပ်ကြပါ့မလဲ.. သူကတော့ ကွန်ပျူတာကို Format ရိုက်ပစ်လိုက်တယ်လို့ပြောတယ်.. ကောင်းကြရော.. သူ့စက်ကတော့ဖြင့် အရေးကြီး Data မရှိလို့ နမြောစရာမလိုဘူးထင်ပါရဲ့.. ဒီတစ်ခါတော့ ခက်ပြီ.. အဲဒီတော့ သူ့ကို ပြန်ဖွင့်ဖို့ Windows Registry ကို ပြန်သွားရပါမယ်.. အဲဒီလိုပြန်သွားဖို့ကိုလည်း Registry ကို Disable လုပ်ထားသေးတော့ ဘာလုပ်ရအုံးမှာလဲ..

အဖြေ။ Administrator level ရှိတဲ့အကောင့်တစ်ခုကို အသစ်ဖွင့်လိုက်ပြီး လက်ရှိ အကောင့်ကနေ အကောင့် အသစ်ကို Switch လုပ်လိုက်ရပါမယ်.. အဲဒီမှာ Registry Disable မဖြစ်သေးတာကို တွေ့ရမှာဖြစ်ပြီး အဲဒီကနေ သွားပြင်ပေးရင်ဖြင့် gpedit.msc ကို ပြန်ဖွင့်လို့ရသွားမှာပါ.. ဒါကြောင့်

- Start => Setting => Control panel => User account ကို နှိပ်လိုက်ပါ။
- User Account Window ပေါ်လာတဲ့အခါကျတော့ create a new account ကို နှိပ်ပါ။

- နောက်ထပ် တဆင့်ပေါ်လာရင်တော့ Name the new account အောက်က လေးထောင့်ဘောက်စ်လေးထဲမှာ နာမည်အသစ်တစ်ခု ပေးလိုက်ပါ.. ကျွန်တော်ကတော့ ဥပမာအနေနဲ့ crazy လို့ ပေးလိုက်ပါတယ်.. ဗိုင်းရပ်စ်ကြောင့် ရှူးနေပြီ ဆိုတဲ့သဘောပေါ့ ပြီးတော့ Next ကို နှိပ်တယ်..။

- နောက်တစ်ဆင့်ကို ရောက်သွားတဲ့အခါကျတော့ Pick an account type ဆိုတဲ့အောက်မှာ Computer Administrator ဆိုတာကို ရွေးရပါမယ်..။ ဒီနေရာမှာ

  - Computer Administrator နဲ့ Limited တို့သည် လုပ်ပိုင်ခွင့်ချင်း မတူပါဘူး.. Administrator က ကွန်ပျူတာကို ကြိုက်သလိုလုပ်လို့ရတယ်.. Software တင်တာ၊ ဖြုတ်ချတာ၊ အရေးကြီးတဲ့ Setting တွေ ပြင်ခွင့်ရှိတာ၊ Limited User တွေကို ထိန်းချုပ်လို့ရတာ၊ အဲဒီ User တွေရဲ့ ဖိုင်တွေကို ကြည့်ရှုခွင့်၊ ပြင်ခွင့်၊ ဖျက်ခွင့်ရှိတာ၊ အဲဒီ User တွေရဲ့ ကွန်ပျူတာသုံးစွဲမှုကို အစစအရာရာလိုပဲ ကန့်သတ်လို့ရတာတွေ ရှိပါတယ်။

  - Limited User ကတော့ Administrator ရဲ့ ကန့်သတ်မှုအောက်မှာပဲ နေရပါတယ်။ Software တင်ခွင့်/ဖြုတ်ချခွင့်မရှိ၊ Administrator ရဲ့ဖိုင်တွေကို ကြည့်ခွင့်မရှိ၊ Windows Setting တွေကို ပြင်ခွင့် မရှိပါ။

  အဲဒီတော့ ပြင်ချင်တာပြင်လို့ရအောင် Computer Administrator ကို ရွေးခြင်းဖြစ်ပါတယ်။ ရွေးပြီးရင် Create Account ကို နှိပ်လိုက်ပါ ။ ဒါဆိုရင် User account windows ထဲမှာ crazy ဆိုတဲ့နာမည်နဲ့ အကောင့်အသစ်တစ်ခု ပေါ်လာပါပြီ..။ Admin ဆိုတာကတော့ ကျွန်တော်တို့ လက်ရှိအကောင့်ပါ။ ကွန်ပျူတာတစ်လုံးနဲ့ တစ်လုံး တူမှာတော့မဟုတ်ဘူးနော်.. အသေမှတ်မထားပါနဲ့..၊ တချို့ကွန်ပျူတာတွေဆိုရင် အကောင့်တွေ အများကြီး ဆောက်ထားသေးတယ်။

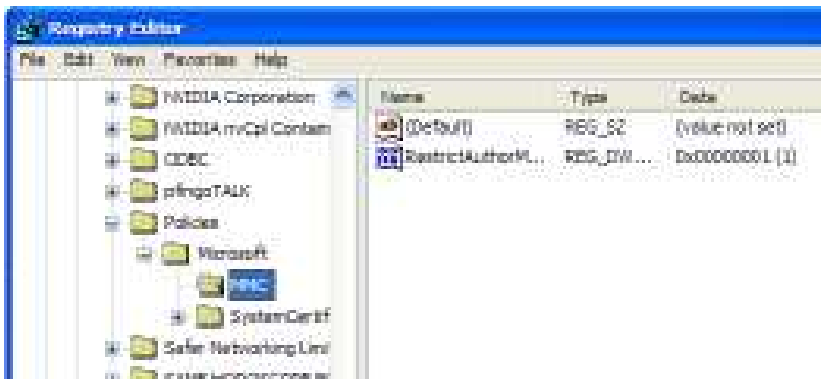
- ကျွန်တော်တို့ အခုဆောက်လိုက်တဲ့အကောင့်အသစ်ဟာဆိုရင် Registry တို့ Taskmanager တို့ ပိတ်ဆို့ခြင်းမခံရသေးပါဘူး.. အသစ်စက်စက်လေးပေါ့နော်.. အဲဒီအကောင့်လေးနဲ့ ကွန်ပျူတာကို ပြန်တက်ပြီး လက်ရှိ Admin ဆိုတဲ့အကောင့်ရဲ့ Disable ဖြစ်နေတဲ့ Setting တွေကို ပြန်ပြင်ရမှာပါ။

- Start => log off Admin ကို ရွေးလိုက်ပါတယ်.. အဲဒီမှာ log off box ပေါ်လာပါတယ်.. Switch to user ဆိုတာလေးကို နှိပ်လိုက်ပါမယ်.. User ပြောင်းသုံးမယ်ဆိုတဲ့သဘောပေါ့.. နှိပ်လိုက်တဲ့အခါမှာ Admin နဲ့ crazy ဆိုပြီး User နှစ်ခု ပေါ်လာပါတယ်.. အဲဒီမှာ ကျွန်တော်တို့က အကောင့်အသစ် crazy ကို ရွေးပေးလိုက်ပါတယ်... ဒါကြောင့် Windows ဟာ crazy ဆိုတဲ့အကောင့်နဲ့ ပြန်တက်လာတာကိုတွေ့ရပါတယ်..

- ကဲ အခု Start => Run မှာ Regedit လို့ ရိုက်ထည့်ပြီး OK ကြည့်ရင် Registry Editor ပွင့်လာပြီပေါ့ဗျာ..

- ဒီတော့ ဆက်လုပ်ရမှာက Admin ဆိုတဲ့ User ဆီမှာ ပိတ်နေတဲ့ .msc ပြင်ဆင်ခွင့် Key ကို လိုက်ရှာရမယ်နော်..

HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC ကို Click လုပ်ထားပြီး ညာဘက်အခြမ်းက RestrictAuthorMode ဖျက်ပစ်လိုက်ရပါမယ်.. အကယ်၍များပေါ့လေ.. ကိုယ့် ကိုယ်ပိုင်စက်ပဲ ဘာမှ ထူးထူးခြားခြား ကလိထားတာမရှိဘူးဆိုရင် MMC ဆိုတဲ့ Key တစ်ခုလုံးကိုပါ ဖျက်ပစ်လိုက်လို့ ရပါတယ်.. အဲဒီ MMC အောက်မှာ ရေးထားတဲ့ Dword Value



တွေ အားလုံးဟာ .msc command တွေနဲ့ ပတ်သက်တဲ့ အရာတွေကို ကလိထားတာ ဖြစ်လို့ပါပဲ.. ဆက်လက်ပြီး HKEY_USER အောက်က ဖိုဒါတွေ အားလုံးမှာလည်း အထက်ပါ လမ်းကြောင်း အတိုင်း လိုက်ရှာပြီး ဖျက်ပစ်ရပါမယ်..

HKEY_USER\.DEFAULT\Software\Policies\Microsoft\MMC
HKEY_USER\.S-1-5-18\Software\Policies\Microsoft\MMC
HKEY_USER\.S-1-5-19\Software\Policies\Microsoft\MMC
HKEY_USER\.S-1-5-20\Software\Policies\Microsoft\MMC
HKEY_USER\.S-1-5-21\Software\Policies\Microsoft\MMC , etc.....

စက်တစ်လုံးနဲ့ တစ်လုံးကွဲလွဲတာရှိကောင်းရှိမယ်.. HKEY_USER အောက်က အားလုံးမှာသာ ရှာပြီးရှင်းပါ။

- တတ်နိုင်ရင်တော့ တခြား Start up Key လိုဟာတွေကိုပါ .. တခါထဲရှာသတ်ခဲ့ရင် အကောင်းဆုံးပေါ့.. ဒါဆို ဗိုင်းရပ်စ်သတ်တဲ့ကိစ္စပါ တခါထဲ ပြီးသွားမယ်လေ..

- အခုဆိုရင် စက်ကို စစ်ဆေးစရာရှိတာ စစ်ဆေးပြီး (boot file တွေ စုံမစုံစစ်ဖို့နဲ့ တဖိုင်ဖိုင်ပျက်နေပြီဆိုရင် တခြားကွန်ပျူတာထဲက ကူးထည့်ဖို့ကို ပြောတာပါ) Restart ချလို့ ရပါပြီ.. ပြန်တက်လာတဲ့အခါမှာ Admin အကောင့်နဲ့ ပြန်ဝင်ပါ.. ဒါဆိုရင် Admin အကောင့်မှာ .msc command တွေ ပြန်သုံးလို့ ရပြီပေါ့။ .msc command တွေ ခေါ်လို့ရမှတော့ Group Policy တွေခေါ်ပြင်လို့ရပြီပေါ့.. ။ အဲဒါရမှတော့ Registry , Task Manager , Folder Options အစရှိတဲ့ Setting ပေါင်းစုံကို လေ့လာထားရင်ထားသလို ပြန်ပြင်လို့ရပြီပေါ့ဗျာ..

- ထပ်ပြီးသတိပေးပါရဲ့ Atnivirus အကောင်းဆုံးလို့ နာမည်ကြီးတာကို ရှာပြီး ကွန်ပျူတာမှာ တင်ထားပါ... အမြဲ Defination Update လုပ်ပေးပါ.. အနည်းဆုံး တစ်ပတ်တကြိမ် Scan စစ်ပါ။ တွေ့ရင်နှိမ်နင်းပါ.. သာမန်အားဖြင့် နှိမ်နင်းလို့မရရင် အခုဖော်ပြခဲ့တဲ့နည်းအတိုင်း လက်ဗလာနဲ့ သတ်ပါ။ Flash Disk တို့ Floppy Disk တို့ကို သတိကြီးစွာထားပြီးသုံးစွဲပါ...။

- အခုတင်ပြခဲ့တာတွေဟာ အလယ်အလတ်တန်းနဲ့ အချို့အမြင့်တန်း ထိခိုက်မှုရှိတဲ့ ဗိုင်းရပ်စ်တွေကို Manual လက်ဗလာနဲ့ သတ်ဖို့ပါ... တကယ်လို့ Windows ရဲ့ Control panel ကိုပါ ဗိုင်းရပ်စ်က ပိတ်သွားပြီ ဆိုရင်တော့ ကျွန်တော်တို့ User အကောင့်အသစ်တောင် မဆောက်နိုင်တော့ပါဘူး.. ဒါမျိုးဆိုရင်တော့ Windows ရဲ့ Autoexec.bat ကိုသုံးတဲ့ .bat ဖိုင်ကို ကိုယ်တိုင်ဖန်တီးရေးသားပြီး Disable ဖြစ်နေတဲ့ Setting တွေကို ပြန်ဖွင့်ရမှာပါ.. အဲဒီအကြောင်း ပြည့်ပြည့်စုံစုံနဲ့ အသေးစိတ်တွေကိုတော့ နောက်မှပဲ တောင်းဆိုသူများလည်းရှိမှ၊ ကျွန်တော်ကိုကူညီပေးမယ့် သူလည်း ရှိမှသာ ကျွန်တော် ဆက်ရေးနိုင်ပါတော့မယ်။

ပြီးသွားရင်တော့ မိမိစက်မှာတင်ထားတဲ့ Antivirus Software က ရှာလို့မတွေ့တဲ့ ဒါမှမဟုတ် တွေ့သော်လည်း မသတ်နိုင်တဲ့ ဗိုင်းရပ်စ်ကို လက်နဲ့သက်တဲ့ ကိစ္စပြီးဆုံးသွားပြီမို့

မင်းလားကွ ဗိုင်းရပ်စ်..!!!

လို့သာ (ဘယ်သူမှကြားအောင် ခပ်တိုးတိုးလေး.....) ကြုံးဝါးလိုက်ပါတော့လို့ မြှောက်ပေးလိုက်ပါတယ်..

သတိ သတိ ဆင်ခြင်သိ

နောက်ထပ်လာမယ့် flash disk တွေကို စက်ထဲ ထိုးထည့်လိုက်ပြီဆိုတာနဲ့ Auto run box တက်လာရင် Cancel ပေးလိုက်ပါ.. ။ winrar Software လေးကိုတင်ထားပါ.. အဲဒါလေးကိုဖွင့်ပြီး သူ့ရဲ့

Address bar လေးကနေ အခုထိုးလိုက်တဲ့ flash disk ကို Browse လုပ်ကြည့်ပါ ကိုယ်မသိတဲ့ဖိုင်တွေ ပါလာပြီဆိုရင် ဒါမှမဟုတ် ကိုယ်သိတဲ့ ဖိုင်းရပ်စ်တွေ ပါလာပြီဆိုရင် ဖျက်ပစ်ပါ.. ကိုယ့် disk မဟုတ်ဘူးဆိုလည်း ဝိုင်ရှင်ကို ပြောပြီး ဖျက်ပစ်ပါ..။ အဖျက်မခံရင် ကိုယ့်စက်ထဲလည်း အဝင်မခံပါနဲ့။ ပြန်သာပေးလိုက်ပါ။ ဖျက်ပစ်ပြီး တဲ့အခါ အဲဒီ flash disk ကို Remove လုပ်လိုက်ပါ။ ပြီးမှ ပြန်တပ်ပါ.. ။ Winrar နဲ့ ပြန် စစ်ကြည့်လိုက်အုံး.. ပြန်ပေါ်နေရင် ဖိုင်းရပ်စ်က ကိုယ့်စက်ထဲရောက်နေပြီလို့သာမှတ် ... အစကနေ ပြန်သတ်.. ။ သေသွားပြီးရင် flash disk ထဲမှာရောက်သွားတဲ့အကောင်ကို လက်စတုန်းသတ်ပစ်ပါ.. ။ သံသရာကို မလည်စေနဲ့တော့.. ကိုယ့်ဆီမှာပဲ ဖြတ်ပစ်လိုက်..။ flash disk တစ်ခုကို ထိုးလိုက်တာနဲ့ Auto ဖိုဒါပွင့်သွားတယ်ဆိုရင် ချက်ချင်း msconfig တို့ regedit တို့ကို ပြန်စစ်ပါ.. Task Manager ကိုပြန်စစ်ပါ.. ။ ထိပြီဆိုပြန်သတ် .. လက်သွက်ပါစေ..

ဒဏ်ရာများနှင့် ကခုန်ခြင်း

ဖိုင်းရပ်စ်တစ်ကောင် ဟာ စက်ထဲကို မဝင်တာအကောင်းဆုံးပါပဲ.. ဝင်ပြီးမှဆိုရင် အဲဒီဖိုင်းရပ်စ် သေသွားပြီဆိုရင်တောင် ကွန်ပျူတာမှာ ဒဏ်ရာတွေ ကျန်ခဲ့တတ်ပါတယ်.. Antivirus Software တချို့ဟာလည်း ဖိုင်းရပ်စ်ကို ပဲသတ်ပေးပါတယ်.. ဒဏ်ရာတွေကိုတော့ မကုပေးပါဘူး ကျန်တော်ခံခဲ့ရဖူးလို့ သိတာပါ.. ဥပမာ အထက်မှာ ပြောခဲ့တဲ့ Registry Disable ဖြစ်တာမျိုး၊ Task Manager Disable ဖြစ်ပြီးကျန်တာမျိုးအစရှိသဖြင့်ပေါ့.... မှတ်မိသလောက်တော့ ပြောပြတာပါ.. အခုလို လက်နဲ့သတ်လိုက်လံ ပြုပြင်တတ်တဲ့အခါကျတော့ ဖြစ်ကျန်ခဲ့တဲ့ ဒဏ်ရာလေးတွေကို သက်သာလာ စေတယ်.. ပြီးတော့ ဖိုင်းရပ်စ်သေသွားပြီးနောက်ပိုင်းမှာ ကွန်ပျူတာကို ထိန်းချုပ်နိုင်စွမ်းတွေလည်း အလိုအလျောက်လိုက်ပြီး မြင့်မားလာတော့မယ်ပေါ့..

IT နယ်မှာ ဒီဂါထာလေးအမြဲရွတ်နေပါဗျာ....

ဥုံ.....သတိ .. သတိ .. အမြဲရှိ.. သတိမရှိ....ဆော်ခံထိ..။