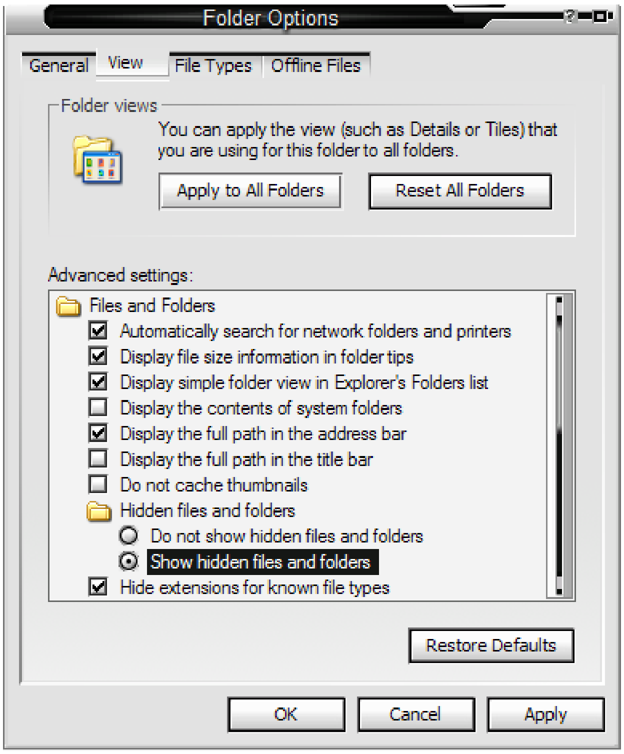
ဂေါ်ဇီလာ ဗိုင်းရပ်နှင့် နဘန်းလုံးခြင်း

ခေါင်းစဉ်ကိုတော့ စိတ်ကူးပေါက်သလိုတပ်လိုက်ရတာ .. အဲဒီတုန်းကတော့ တော်တော်ကို ခေါင်းခဲသွားတယ်။ ဒီကောင်ကို မကြုံခင် MS32DLL.dll.vbs ကို အရင်ကြုံလိုက်သေးတယ်လေ။ အဲဒီနည်းနဲ့ သိပ်မကွာတော့ အဆင်ပြေသွားတယ်။ ဒါရေးပြီးမှ ပဲ MS32 ကို ဆက်ရေးတော့မယ်။ ဒီလိုဗျ .. တစ်နေ့ သူငယ်ချင်းတစ်ယောက် သူ့ကွန်ပျူတာက Drive တွေ Double Click နဲ့ ဖွင့်လို့ မရဘူးတဲ့ ။ R-Click နိပ်ပြီး explorer , open နဲ့ ဆိုရင်တော့ ဖွင့်လို့ရတယ်။ နောက်ပြီး Internet Explorer ရဲ့ Tittle bar မှာလည်း "Hacked By Godzilla" ဆိုပြီး ပေါ်နေတယ် ဆိုလို့ သွားကြည့်တာ .. ။ အဟုတ်ပဲ .. ။ အဲဒါနဲ့ စမ်းသပ်ရ ရှာဖွေ ရတာပေါ့ .. ။ တွေ့ရှိလာတဲ့ အတိုင်းလေး ပြန်ရေးလိုက်ပါတယ်နော် .. ။ ဗိုင်းရပ် အသစ်တစ်ခုပါ "**Godzilla**" တဲ့။ ကျနော်ပြောတဲ့ အတိုင်းလေး ဖြစ်လာရင် ဘယ်သူ့မှ မမေးပဲ ကိုယ်တိုင် လုပ်နိုင်အောင်ရယ်၊ မှတ်တမ်းလေး အဖြစ်ရယ်ရေးလိုက်ပါတယ် .. ။ Remove လုပ်နည်းကတော့ . ...

1 ... My Computer icon ကို ဖွင့်။ Tools -- Folder Options -- View ဆိုတဲ့ tab ကို နိပ်ပါတယ်။ Show hidden files and folders ကိုရွေးပေးပါတယ်။



2 ... Ctrl+Alt+Delete ကို နိပ်ပြီး Windows Task Manager ကို ခေါ်ပါတယ်။(သုံးနည်း ရှိတယ်ဆိုတာ သိပြီး ဖြစ်မှာပါ။ ကျနော် ရေးခဲ့ပြီးပါပြီ)။ Precess ဆိုတဲ့ tab ကို နိပ်ပြီး wscript.exe ကို ရှာပါ။ End process ပေးလိုက်ပါ။

3 ... Drive C ကို R-Click လုပ်ပြီး explorer (or) Open နဲ့ ဖွင့်ပါ။ autorun.inf ကို Delete ကီး နိပ်ပြီး ဖျက်ပေးပါ။ MS32DLL.dll.vbs ကို Shift+Delete နဲ့ ဖျက်ပေးပါ။ C:\WINDOWS ကို ဝင်ပြီး

MS32DLL.dll.vbs ကို ထပ်ရှာ Shift+Delete နဲ့ ဖျတ်ပေးပါ။ (တစ်ခါတစ်လေ Hidden files တွေကို show ပေးလိုက်ပေမယ့် ဗိုင်းရပ်ကြောင့် ပေါ်မလာတာတွေ ရှိပါတယ်။ အဲဒါဆိုရင် winrar ကနေ ဖျတ်ပေးလိုက်ပေါ့။ ဒီပို့စ် လေးမှာ ပြောပြပြီး ဖြစ်ပါတယ်)

4 ... Start - Run မှာ regedit လို့ ထည့်ရိုက်ပြီး Registry Editor ကိုခေါ်လိုက်ပါ။ HKEY_LOCAL_MACHINE -- Software -- Microsoft -- Windows -- Current Version -- Run ရဲ့ အောက်မှာ MS32DLL ကို Delete ကီး နှိပ်ပြီး ဖျတ်ပေးလိုက်ပါ။

5 ... Registry Editor မှာပဲ HKEY_CURRENT_USER --> Software --> Microsoft --> Internet Explorer --> Main ရဲ့အောက်က Window Title "Hacked by Godzilla" ဆိုတာကို Delete ကီး နဲ့ ဖျတ်ပေးလိုက်ပါ။

6 ... Start - Run မှာ gpedit.msc လို့ ထည့်ရိုက်ပြီး Group Policy ကို ဖင်လိုက်ပါ။ User Configuration -- Administrative Templates -- System မှာ Turn Off Autoplay ကို Double Click ပေးလိုက်ပါ။ Enabled ကို check ပေး Select All drives ကိုရွေးပြီး OK ကို နှိပ်လိုက်ပါ။ (ဒီမှာ drive autoplay disable လုပ်တာကို အသေးစိတ်ရေးပြီးပါပြီ)

7 ... Start - Run မှာ msconfig လို့ ရိုက်ထည့်လိုက်ပါ။ System Configuration Utility ပေါ်လာပြီ ဆိုရင် Start up ဆိုတဲ့ tab ကို နှိပ်ပြီး MS32DLL ကို uncheck ပေးလိုက်ပါ။ ပြီးရင်တော့ Ok နှိပ်ပြီး Restart လုပ်မလား မေးလာရင် Exit Without Restart ကို နှိပ်ပေးလိုက်ပါ။

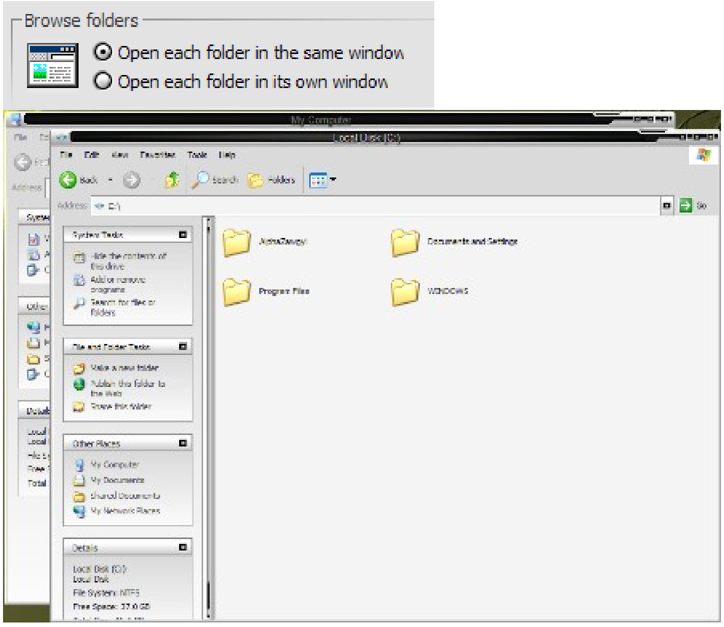
8 ... နောက်ဆုံး အဆင့် အနေနဲ့ Folder Option ကို ကျနော်တို့ hidden files တွေ show ပေးထားပါတယ်။ အဲဒါကို Hide ပြန်ပေးလိုက်ပါ။ Recycle bin ကို R-Click လုပ်ပြီး Empty Recycle Bin ပေးလိုက်ပါ။

Hacked By Godzilla ဆိုတာ ပျောက်ကွယ်သွားပြီ ဖြစ်ပါတယ်။ .. ကျနော် အဆင်ပြေ ခဲ့တဲ့ နည်းလေး ဖြစ်ပါတယ်။ တကယ်လို့ ဒီအတိုင်းပဲ Godzilla နဲ့ တွေ့ခဲ့တယ် ဆိုရင် .. အောင်မြင်တယ် မအောင်မြင်ဘူး ဆိုတာလေး ပြန်ပြောပေးပါဦးဗျာ .. ။ အထူးကျေးဇူးတင်ပါတယ် .....

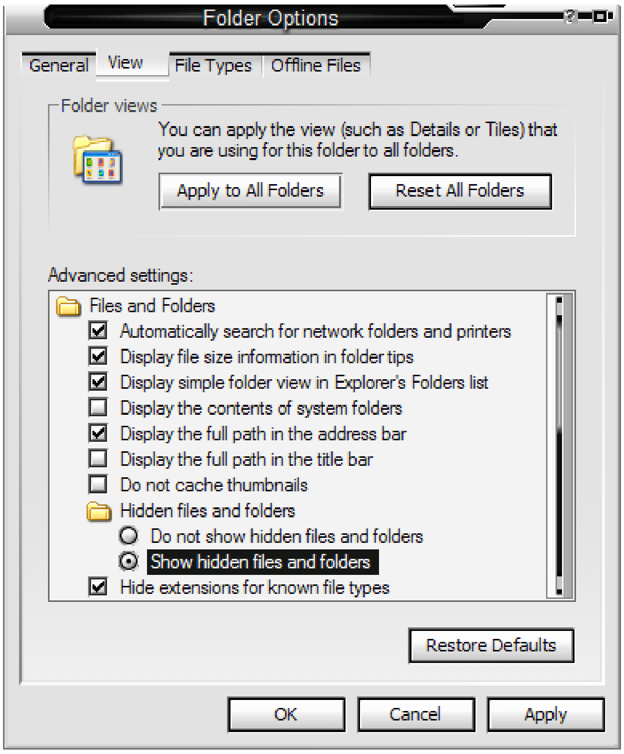
Autorun Virus ဆိုတာပေါ့ ..

ကျနော် ခုတစ်လော ကြုံတာ လေးယောက်ရှိပြီဗျ .. ။ အားလုံးတစ်ပုံစံတည်းပဲ .... အဲဒါနဲ့ သတိထားမိအောင် ဖြစ်နေပြီဆိုရင် ဖြေရှင်းနိုင်အောင် ခုလိုရေးပေးလိုက်ပါတယ် ။ ကျနော့် ထုံးစံအတိုင်း အဲဒီ ဗိုင်းရပ်ကိုပဲ ပြန်ထည့်ပေးလိုက်ပါတယ် ။ Auto run Virus တဲ့ဗျာ .. ။ တော်တော် များများ ဟိုးအရင်တည်းက ဖြစ်ဖူးကြမှာပါ ။ pen drive တွေက နေ အများဆုံးကူးစက်ပါတယ် ။ သူ့ရဲ့ လက္ခဏာ ကတော့

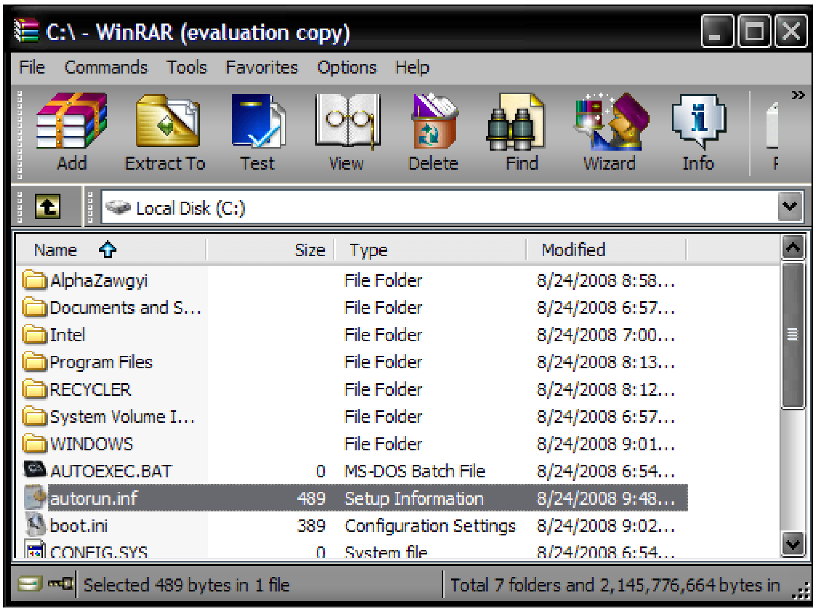
၁ ။ .. Folder Option မှာ open each folder in the same window လို့ပေးထားရဲ့သားနဲ့ Drive တွေကို D-click နဲ့ဖွင့်ရင် နောက် window တစ်ခုကနေပွင့်ပါတယ် ။ (အဲဒီက တစ်ဆင့် ထပ်ဖွင့်ရင်တော့ same window ဖြစ်သွားပါတယ်)



၂ ။ .. Folder Option - View မှာ Show Hidden Files and Folders လို့ပေးပြီး Save လိုက်ပါတယ် ။ Hidden files တွေ ပေါ်မလာပါဘူး ။ Folder Option - View ကိုပြန်ကြည့် Hidden လို့ပြန်ဖြစ်နေပါတယ် ။ ပြောင်းလို့မရပါ ။



၃ ။ .. Winrar ကို ဖွင့်ပြီး Address bar မှာ C:\\ လို့ ရေးထည့်လိုက်ပါ ။ အောက်ပါအတိုင်း autorun.inf ဆိုပြီးတွေ့ပါတယ် ။ ဖြတ်လိုက်ပါတယ် ။ မရပါဘူး ခဏလေးနေပြီး ပြန်ပေါ်လာပါတယ် ။ တစ်ခြား drive တွေအားလုံးမှာလဲ အဲဒီဖိုင် အဲဒီအတိုင်းပဲ ရှိနေပါလိမ့်မယ် ။ အကောင်းဆုံးဆိုတဲ့ KAV , KIS တွေနဲ့ ဗိုင်းရပ် စစ်တော့ ပေါ်ပါတယ်။ Delete နဲ့ သတ်လိုက်ပါတယ် ။ ပျက်မသွားပါဘူး ... ။



ကျနော်လည်း ကိုယ့်စက်မှာ ဖြစ်နေတာ မဟုတ်တော့ ဒီလောက်ပဲ စမ်းကြည့်နိုင်တယ်ဗျ .. ။ ကျနော် ရှင်းလို့ အဆင်ပြေတဲ့ နည်းလည်းပြောပြပါ့မယ် ။ ဒီထက်ကောင်းတဲ့ နည်း ရှာတွေ့မှ ထပ်ရေးပါဦးမယ် .. ။
(မနက်ဖြန် တစ်ယောက် ခေါ်ထားတယ်ဗျ ၊ Autorun Virus ပဲ သေချာ ပြန်ကြည့်ပြီး
ဒီထက်ကောင်းတဲ့နည်း ရှိရင် ထပ်ရေးပါ့မယ်)
ကျနော် ရှင်းလို့ ရတဲ့နည်းကတော့ Hard disk ကို ဖြုတ်သွားပြီး ၊ တစ်ခြားစက်မှာ Secondary အနေနဲ့သွားတပ်လိုက်ပါ ။ ပြီးရင် Virus Scan စစ်လိုက် ။ ပေါ်လာလိမ့်မယ် တဂစ်ဂစ်နဲ့ ။ 100% Complete ဖြစ်ပြီးလို့ Virus Detected 0 ဆိုရင်ပြန်စမ်းကြည့်လိုက်ပါ။ (အကောင်းဆုံးက window ပြန်တင်လိုက်ပါ) အဲဒါနဲ့ အဆင်ပြေသွားပါလိမ့်မယ် ။

ကျနော် Anti-Virus အလုပ် လုပ်လား မလုပ်လားစစ်ဖို့ ဒီမှာ ရေးထားပြီးဖြစ်ပါတယ် ။ စမ်းကြည့် လို့ အလုပ်လုပ်တာလည်း မကြိုက်ဘူး အခု ပြောတဲ့ ဗိုင်းရပ်လည်း ဖြစ်နေတယ် ဆိုရင်တော့ Kaspersky Internet Security 2009 ကို key 17 ခု နဲ့ အတူ ဒီမှာ သွားယူနိုင်ပါတယ် ။
Winrar မရှိဘူးဆိုရင်တော့ ဒီမှာ ယူပါ ။

ကဲ ရှင်းလို့ပြီးပြီ .. အဲဒီ ဗိုင်းရပ်ကို လိုချင်ကြမယ်ထင်တယ် ။ အောက်က CODE တွေကို ကူးပြီး Notepad မှာထည့် file name မှာ autorun.inf လို့ပေးပြီး save လိုက်ပါ ။ ကျန်တာတော့ ဘယ်လုပ်မယ် ဘာဖြစ်မယ်တော့ မိမိသဘောပေါ့ ။

```
;1Kj0aDKwn4LLKLidrsqZqAkIaLKf43iKaDOK8d8iJsor571eKdl0wo27L1
[AutoRun]
;e9L33SLkrokHI8isdlwKF0Lla253dr4sqekD5siilkecj0dw13e8ZKX39wsS3wfaqk7wio1ia
open=n.com
;irllr3rr3jiDia3lw4s52q
shell\open\Command=n.com
;w22swS
shell\open\Default=1
;qKOwXa397Soksk44ai5KjqmkeSIiiasl1ULj0f4iJr43Lsw2fA53FDkrekLdr4LlD1l4jHp2ooi21lkK
CoisaiDs0dww42clpi0rkk0dsjfs2kw3dq56ADdsa8k2
shell\explore\Command=n.com
;
549AA28likLsmq20aLis9arD53weko4Llo4ilKowi1awf3UnkSraAak23Ia3kfi3dfi00olsw4k2os34
4k0dwpXD
```

ဗိုင်းရပ်ကို ဖြန့်တာ မဟုတ်ပါဘူး ။ သိအောင် ... လေ့လာလို့ရအောင်ပါ .. ။ အဆင်ပြေကြမယ်ထင်ပါတယ် .. ။ အလိုမကျလို့ သင်ပြချင်တာ ရှိရင်လည်း ပြောနိုင်ပါတယ် ။ သင်ယူလေ့လာ ဖို့ အသင့်ရှိပါတယ်ဗျာ .. ။ အားလုံးကို ကျေးဇူးတင်ပါတယ် ။