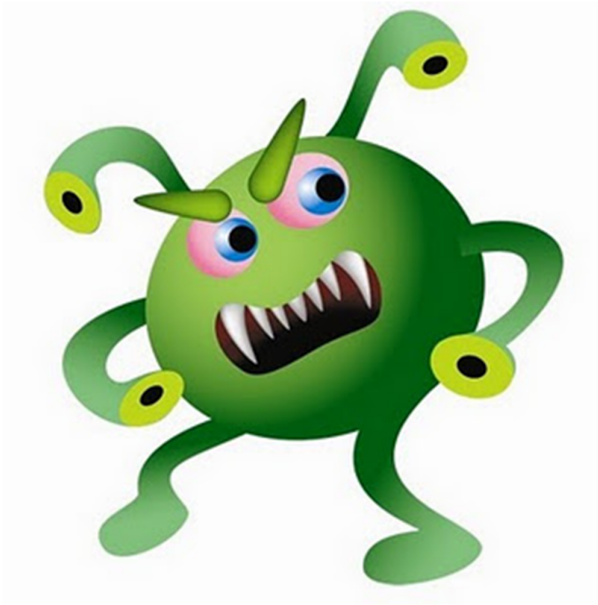
VIRUS



ABOUT VIRUS VALUE

Value တစ်ခုမှာရှိတဲ့ Data တစ်ခုကိုဖော်ပြတဲ့နေရာမှာ Data type အမျိုးအစား (၆)မျိုးအနက်က တစ်ခုခုနဲ့ဖော်ပြနိုင်ပါတယ်။ အဲ့ဒီ (၆) မျိုးကတော့ .....

1.REG_BINARY

Raw Binary Data, Hardware သတင်းတွေကို ကွန်ပျူတာမှ binary အဖြစ်သိမ်းပေမယ့်၊ Registery editor မှာ အကျဉ်းချုံးရန် Hexa Decimal နဲ့ပြပေးတယ်။

2.REG_DWORD
4 byte အရှည်ရှိတဲ့ ကိန်းဂဏန်းနဲ့ သိမ်း၊ Device Driver များ၊ Service နှင့်သက်ဆိုင်သော
ကန့်သတ်ချက်(parameter) များကိုဖော်ပြပေးတယ်။

3.REG_EXPAND_SZ
ကိန်းရှင် (variable) များ

4.REG_MULTI_SZ
multiple type, user များသိနိုင်သော Char နှင့် ဂဏန်းများရောနှောပုံ၊ နေရာလွတ်၊ ကော်မာနဲ့ အခြားအမှတ်တွေပါ။

5.REG_SZ
စာသားများပါဝင်ပြီး အလျားသတ်မှတ်ချက်ရှိသော အက္ခရာစဉ်ကိန်းတန်းတစ်ခု။

6.REG_FULL_RESOCE_DESCRIPTOR
Hardware တစ်ခုကို (Dirver တစ်ခု) Resource List ကိုသိမ်းဆည်းရန် ဒီဇိုင်းထုတ်ထားသော Nested Array တစ်ခုတို့ပဲ ဖြစ်ပါတယ်။

ဗိုင်းရပ်စ် ဆိုသည်မှာ (ပထမပိုင်း)

ဗိုင်းရပ်စ်ဆိုသည်မှာ လို့ခေါင်းစဉ်တပ်ထားတာ ကျွန်တော်လဲ သိသလောက်လေး ပြောပြပေးတာပါ။ ကကကွန် mail box မှာ ဗိုင်းစ်ရပ် အကြောင်းမေးလွန်းအား ကြီးလွန်း လို့ စာဖတ်ပြီး ပြောပြပေးတာပေါ့ဗျာ။
ကျွန်တော့်ဌာနက ဆရာကြီးတွေ၊ ကျွန်တော် ဗိုလ်ကြီးတွေ ဆီလဲ နဲနဲပါးပါး မေးမြန်းပြီး သိသလောက်ပြောပြ ပေးလိုက်တယ် General Knowledge ပေါ့ဗျာ..... ကဲ ဖတ်ပေးဦးဗျာ..... အကျိုးရှိမှာပါ...
လူတွေရော အားလုံးပါပဲ တစ်ခုခုဆို Virus လို့ပဲ သိပါတယ်။ တကယ်တော့ Virus အနွယ်ဝင် အမျိုးအစားများရှိနေပါတယ်။ အဲဒါတွေအကြောင်း ရှင်းလင်းပြထားတဲ့ မူလရေးသားသူ ဆရာမျိုးသူရ အားအထူး ကျေးဇူးတင်ရှိပါတယ်။

၁။ COMPUTER VIRUS

Computer virus ဆိုတာ သူ့ကိုသူ attach လုပ်ထားတဲ့ program (သို့) file တစ်ခုဖြစ်ပြီး ကွန်ပျူတာတစ်ခုကနေ တစ်ခုကို ပြန့်နှံ့ကူးစက်နိုင်ပါတယ်.. လူတွေမှာ Virus ကူးသလိုပဲ ပြန့်နှံ့ပြီးတော့ ကွန်ပျူတာရဲ့ System ကိုပုံမှန်အလုပ် မလုပ်အောင် နှောက်ယှက်မယ်၊ Windows ကို Error တွေများလာအောင် လုပ်မယ်၊ user data တွေကို ဖျက်ဆီးမယ်၊ Hardware တွေ Software တွေ အရေးကြီးတဲ့ File တွေကို ဖျက်ဆီးမယ်... စတာတွေကို လုပ်ဆောင်ပါတယ်..
ဒါပေမယ့် Virus အများစုဟာ executable fileတွေဖြစ်ကြပါတယ်.. ဥပမာ.. chrome.exe, system.bat , flashy.com စသဖြင့်ပေါ့ .. သူတို့ဟာ ကွန်ပျူတာထဲမှာ ရှိနေရင်တောင်မှ သင်ကိုယ်တိုင်မှ သွားမဖွင့်ရင်/ သွားမ run မိရင် ကွန်ပျူတာကို ဘာမှ မထိခိုက်နိုင်ပါဘူး... ဒါကြောင့် မှတ်ထားရမှာက လူ၏ လုပ်ဆောင်ချက်မပါဝင်ပဲ Computer Virus သည် မပျံ့နှံ့ မကူးစက်နိုင်ပါ...
Virus ပျံ့နှံ့နိုင်တဲ့ နည်းလမ်းတွေကတော့ အမျိုးမျိုးရှိပါတယ်...forward E-mail က attached file တွေ၊ memory stick(flash/thumb drives) တွေ၊ Full sharing ကနေ virus infected file ထည့်တာတွေ၊ သူငယ်ချင်း အချင်းချင်း မသိပဲနဲ့ Virus infected file ကို share လုပ်မိတာတွေ .. စသဖြင့်ပေါ့...ဗျာ

၂။ MALWARE

Malware ဆိုတာ အင်္ဂလိပ်စကား ၂ လုံး Malicious Software ကိုပေါင်းစပ်ပြီး ကွန်ပျူတာ ပညာရှင်တွေက အလွယ်ခေါ်ကြတဲ့ virus လို program တွေပါပဲ.. အဲဒီ Malware ကကွန်ပျူတာပိုင်ရှင်ရဲ့ ခွင့်ပြုချက်မရပဲ ၊ မသိစေပဲ single computer / server / computer network ထဲ ဝင်ပြီး ကွန်ပျူတာ System ပျက်ဆီးစေနိုင်အောင် ၊ အနှောက်အယှက်ဖြစ်အောင် ရေးလေ့ရှိကြပါတယ်.. Malware တစ်ခုမှာ Computer VIrus , worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software တွေပါဝင်လေ့ရှိပါတယ်..

၃။ WORM

worm ဆိုတာက virus နဲ့ဆင်တူအောင် ရေးထားကြတာပါပဲ.. virus တစ်ခုရဲ့ Sub-class လို့လည်းခေါ်လို့ရပါတယ်... သူကတော့ Virus လို လူကဖြန့်မှ ပျံ့တာမျိုးမဟုတ်ပဲ သူပါသူ Computer network ထဲမှာရှိတဲ့ အခြားကွန်ပျူတာတွေကို လူရဲ့လုပ်ဆောင်ချက် လုံးဝမပါပဲနဲ့ ပျံ့နှံ့စေတာဖြစ်ပါတယ်...သူပါသူ ဖြန့်နိုင်တဲ့ စွမ်းရည်ရှိတာပေါ့နော်...
အကြီးမားဆုံး အန္တရာယ်ကတော့ သူ က သူ့ပါသူ System file တစ်ခုလို အယောင်ဆောင်ပြီး သူ့ကိုယ်သူ သန်းပေါင်း ၁၀၀ လောက် copy ပွားနိုင်ပါတယ်၊ Hard disk ရဲ့ used space ကို များလာစေတယ်..Computer ရဲ့ System memory usage တွေ များလာစေတယ်.. network bandwidth တွေကိုတက်လာစေတယ်... Run ထားတဲ့ program တွေကို not responding ခဏခဏဖြစ်လာစေတယ်.. လူသိများတဲ့ worm ကတော့ Blaster worm ပါ.. ထွင်လိုက်တဲ့လူကတော့ ၂၀၀၃ ခုနှစ်တုန်းက အသက် ၁၈နှစ် အရွယ် Jeffrey Lee Parson ဖြစ်ပြီး ထောင် ၁၈ လ ကျသွားခဲ့ပါတယ်.. Blaster worm က windows စတက်တာနဲ့ Registry ကီး HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\ Run\windows auto update = msblast.exe မှာ နေရာယူပါတယ် ၊ msblast.exe ဆိုတာက တော့ နာမည်တူပေးထားတာပေါ့ Blaster worm က Computer System ထဲမှာ ရှိနေပြီဆိုတာနဲ့ Cracker တွေက ကွန်ပျူတာကို Remote လုပ်ပြီး ထိန်းချုပ်နိုင်အောင် ရေးထားပါတယ်..

ပိုင်းရပ်စ်ဆိုသည်မှာ (ဒုတိယပိုင်း)

၄။ TROJAN HORSE

Trojan horse ကို Trojan လို့လည်းခေါ်ပါတယ်..Trojan ဆိုတဲ့ မြင်းရုပ်ကြီးအကြောင်း ငယ်ငယ်က ကမ္ဘာ့သမိုင်းမှာသင်ဖူးကြမှာပေါ့.. Tri ဇာတ်ကားလည်း ကြည့်ဖူးကြမှာပါ... အဲဒီထဲကလိုပဲ အလုပ်လုပ်တယ်လို့ပြောလို့ရပါတယ်... ပုံမှန်အားဖြင့် အသုံးဝင်တဲ့ Software တွေမှာ ထည့်ထားတတ်ကြပါတယ်... ဥပမာပေါ့ဗျာ... Game တစ်ခုကို Install ပြီးဆော့နေပေမယ့် အခြားတစ်ဖက်မှာ Hacker တွေ Cracker တွေက ကွန်ပျူတာထဲကို ဝင်မွှေနေလို့ရအောင်လုပ်ပေးနေတယ်.. အဲဒီတော့ အဲဒီ Game ကို Trojan horse လို့ခေါ်တာပေါ့ .. တစ်ကယ်တော့ Game က တရားဝင်ထုတ်ထားတဲ့ Game ပဲ.. ဒါပေမယ့် Virus infected ဖြစ်နေတဲ့ Game လို့ပြောရလိုဖြစ်နေတာပေါ့..
နမူနာ Trojan Horse ကတော့ waterfalls.scr ဆိုတဲ့ free waterfall screen saver ပဲဖြစ်ပါတယ်..

Trojan horse တစ်ခုဟာ အောက်ပါအချက်များကို လုပ်ဆောင်ပေးနိုင်ပါတယ်...

* Remote Access
* Data Destruction
* Downloader/dropper
* Server Trojan(Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
* Disable security software
* Denial-of-service attack (DoS)

၅။ SPYWARE

သူကတော့ သူခိုးပေါ့နော်.. Spy တွေ ဘယ်လိုအလုပ်လုပ်သလဲဆိုတာသိကြမှာပါ.. သူလဲအဲလိုပါပဲ...
သူက ကွန်ပျူတာကို ထိခိုက်ဖျက်ဆီးချင်မှ ဖျက်ဆီးမယ်.. ဒါပေမယ့် ကွန်ပျူတာမှာသုံးနေတဲ့ user ရဲ့ အမျိုးမျိုးသော အချက်အလက်တွေ၊ အရေးကြီးတဲ့ Data တွေကို သူ့ရဲ့ Main server တစ်ခုခုကို နေ့စဉ် သတင်းပို့ပေးနေတယ်... Spyware တွေက များသောအားဖြင့် Web browser တွေကနေ ဂင်နိုင်ပါတယ်... ပြီးရင် သူက Browser home page ကိုပြောင်းထားတတ်ပါတယ်..သင့်ကို Error message တွေ အမျိုးမျိုးပြမယ်..(ဥပမာ- သင့်ကွန်ပျူတာမှာ problems တွေများနေပြီ..အဲဒါတွေပြင်ချင်ရင် အောက်ကခလုတ်ကို နှိပ်ပါ) စသဖြင့် ဆွဲဆောင်မယ်၊ သင်က link တစ်ခုကို click လိုက်ပေမယ့် သင်မဖွင့်ပဲနဲ့ အခြား Porn Site တွေ အလိုလိုပွင့်လာမယ် စသဖြင့်ပေါ့ဗျာ... တစ်ချို့ လူတွေက http cookie တွေကို Spyware တွေလို့ ထင်ကြပါတယ်.. တကယ်တော့မဟုတ်ပါဘူး ဒါပေမယ့် အဲဒီ cookie ထဲမှာ Spyware က track လုပ်နိုင်တဲ့ Data တွေပါလာတတ်တာကြောင့် Spyware Remover တော်တော်များများက Cookie တွေကို ဖျက်ပစ်ကြတာပါ.
Spyware ကို ကာကွယ်ချင်ရင်တော့ pop-ups ကျလာတဲ့ link တွေကို ရှောင်တာကောင်းပါတယ်... Free Spyware Remover တွေနဲ့လည်းကာကွယ်နိုင်ပါတယ်...

၆။ADWARE

Adware ဆိုတာကတော့ Advertising-supported software (သို့) software package တစ်ခုဖြစ်ပါတယ်....
သူကတော့ Screen မှာ Automatic ပေါ်လာအောင်ဖန်တီးထားပြီး Download အတင်းလုပ်ခိုင်းပါတယ်... :D
အချို့သော Adware များဟာ Spyware များဖြစ်တတ်ကြပါတယ်...

၇။CRIMEWARE

Crimeware ဆိုတာကတော့ Spyware, Adware, Malware အမျိုးအစားတွေထဲမှာပါပါတယ်..
သူ့ရဲ့ရည်ရွယ်ချက်ကတော့ financial crime တွေအတွက်ရည်ရွယ်ပြီးရေးကြတာများပါတယ်..
သူက user password တွေ၊ links တွေ၊ အချက်အလက်တွေ ကို မှတ်သားထားနိုင်ပြီး သူ့ကို Run ထားတဲ့လူက ပြန်ဖွင့်ကြည့်ပြီး user data တွေကို ခိုးယူနိုင်တာပေါ့.... ဥပမာပြောရရင်
ခုခေတ်စားနေတဲ့ key logger တို့ .. keystroke logging software တို့ဟာ Crimeware အမျိုးအစားတွေပဲဖြစ်ပါတယ်.