## 1. Runtime Analysis: Second Step of Malware Analysis

Malware Analysis ရဲ့ ဒုတိယ အဆင့်ဖြစ်တဲ့ Runtime Analysis အကြောင်းကို ဒီဆောင်းပါးမှာ အဓိကထားပြောသွားမှာဖြစ်ပါတယ်။ Runtime Analysis ကို စတင်လေ့လာမယ်ဆိုရင် သင်ရဲ့ computer မှာအရင်ဆုံး ကြိုတင်ပြင်ဆင်မှုတွေ လုပ်ထားရပါမယ်။ တစ်နည်းအားဖြင့်တော့ လိုအပ်တဲ့ configuration တွေလုပ်သင့်ပါတယ်။ ပထမဆုံး malware run မယ့် infected အဖြစ်ခံရမယ့် computer ကို အရင်ဆုံး ဆုံးဖြတ်သင့်ပါတယ်။ အကြံပေးရမယ်ဆိုရင် malware ကို သင့်ရဲ့ Host computer မှာ တိုက်ရိုက် run တာမျိုး မလုပ်စေချင်ပါဘူး။ သင့် computer တွင် Virtualization Software ဖြစ်သော VMware Workstation, VirtualBox စသည်တို့ကို သုံးပြီး အဲဒီ Virtualization Software ပေါ်တွင် တင်ထားသော Operating System အပေါ်တွင်သာ malware ကို စမ်းသပ်သင့်ပါတယ်။ သင့် computer ကို network ချိတ်ထားခြင်းရှိမရှိ ကိုလည်း သတိထား စစ်ဆေးရပါမယ်။ အကယ်၍ သင့် computer က network နဲ့ ချိတ်ထားခဲ့ပါက malware(.exe) ကို စမ်းသပ်တဲ့အခါ ချိတ်ထားတဲ့ network အတွင်းမှာ ရှိသော အခြား computer တွေအပေါ်မှာ မလိုလားအပ်သော ပြဿနာတွေ ဖြစ်သွားနိုင်ပါတယ်။

Runtime Analysis ဆိုတာက malware ကို execute လုပ်ပြီး malware ရဲ့လုပ်ဆောင်ပုံ (behavior) တွေကို စောင့်ကြည့် လေ့လာတာဖြစ်ပါတယ်။ malware ရဲ့လုပ်ဆောင်ပုံ တွေကို စောင့်ကြည့်တယ် ဆိုတာကတော့ malware run တဲ့အခါ မိမိရဲ့ computer မှာ ဘယ် process တွေကို create လုပ်လဲ၊ terminate လုပ်လဲ ဆိုတာတွေ၊ Registry entry တွေမှာ ဘယ်လို အပြောင်းအလဲ တွေရှိလဲ ဆိုတာတွေ နှင့် external network connection တွေရှိမရှိ စတာတွေကို လေ့လာတာဖြစ်ပါတယ်။ Malware ရဲ့ behavior အကုန်လုံးကိုဖော်ထုတ်နိုင် ဖို့ကတော့ အခက်အခဲ ရှိနိုင်ပါတယ်။

Runtime Analysis လုပ်ရာမှာ လိုအပ်တဲ့ tools တွေနှင့် ၄င်း tools တွေရဲ့ လုပ်ဆောင်နိုင်ပုံတွေကို ယှဉ်တွဲဖော်ပြလိုက်ပါတယ်။

1. Process Explorer — Display information about Process, File and Registry
2. Regshot — Display information about File and Registry
3. Wireshark — Display information about Network
4. Netcat — Display information about Network
5. Process Monitor — Display information about Process, File and Registry
6. Fundelete — Display information about File
7. Autoruns — Display information about Registry
8. Strams/ADSSpy — Display information about File

ဖော်ပြပါ Tools တွေအပြင် တခြားအသုံးဝင်သော tools တွေကိုလည်း ရှာဖွေပြီး စမ်းသပ်နိုင်ပါတယ်။

Runtime Analysis လုပ်ရာတွင် tools တွေကို procedure အတိုင်း သုံးပါက ပိုပြီး ထိရောက်စေပါတယ်။ Malware ကို execute မလုပ်ခင် Process Explorer, Regshot, Wireshark နှင့် Process Monitor တို့ကို အရင် run ထားရပါမယ်။ ပြီးမှ Malware ကို execute လုပ်ရပါမယ်။ ဒါမှသာ malware ရဲ့ လုပ်ဆောင်ပုံတွေကို tools တွေမှာမြင်ရမှာဖြစ်ပါတယ်။ ၄င်း tools တွေက ဖော်ပြတဲ့ information တွေမှတစ်ဆင့် malware ရဲ့ လုပ်ဆောင်ပုံတွေကို လေ့လာနိုင်ပါတယ်။