# Surface Analysis: First Step of Malware Analysis

Malicious Software (Malware) Analysis ဆိုတာ malware နဲ့ပတ်သက်ပြီး ရနိုင်တဲ့ information တွေကို စုဆောင်းခြင်း၊ အဲဒီ malware ကို execute လုပ်ပြီးတဲ့နောက် မိမိရဲ့ computer မှာ ဘယ်လိုမျိုးတွေပြောင်းလဲ လုပ်ဆောင်သွားသလဲဆိုတာ နှင့် malware ရဲ့ coding ကိုကြည့်ပြီးသူ့ရဲ့ လုပ်ဆောင်ပုံတွေကို အနီးစပ်ဆုံး ခန့်မှန်း လေ့လာတာဖြစ်ပါတယ်။

Malware ကို စတင်လေ့လာမယ်ဆိုရင် ယေဘူယျအားဖြင့် နည်းလမ်း(၃)ခုနှင့် လေ့လာနိုင်ပါသည်။ ပထမနည်းလမ်းကတော့ Surface Analysis ၊ ဒုတိယ နည်းလမ်းကတော့ Runtime Analysis နှင့် တတိယ နည်းလမ်းကတော့ Static Analysis တို့ဖြစ်ပါတယ်။ ဒီဆောင်းပါးမှာတော့ ပထမနည်းလမ်းဖြစ်တဲ့ Surface Analysis အကြောင်းကို အဓိကထားပြော သွားမှာဖြစ်ပါတယ်။

Surface analysis လုပ်ခြင်းက ရိုးရှင်းလွယ်ကူပေမယ့် ရလာတဲ့ information တွေကတော့ malware analysis လုပ်ငန်းစဉ်တွင် အလွန်ကို အသုံးဝင်ပါတယ်။

Surface analysis လုပ်ရာတွင်

1. Preparation
2. Feature Analysis
3. Pack Analysis
4. Comparative Analysis ဆိုပြီးအဆင့် (၄)ဆင့်ဖြင့် လုပ်ဆောင်နိုင်ပါသည်။

## 1. Preparation

Preparation ဆိုတာကတော့ အရင်ဆုံး malware program ကို စမ်းမယ့် သင့် computer တွင် surface analysis လုပ်ရာတွင် လိုအပ်သော tools (software) တွေကို စုဆောင်းထားခြင်း၊ ကြိုတင် install လုပ်ထားခြင်းတို့ ဖြစ်ပါသည်။

## 2. Feature Analysis

Feature Analysis ဆိုတာက

- File attribute — file name, file size နှင့် file type တို့ကို လေ့လာခြင်း။
- Hash value — Cryptographic hash function ကို အသုံးပြုပြီး ရလာတဲ့ Hash value ကို analyze လုပ်ခြင်း။
- Strings — malware file ထဲတွင် ပါသော အဓိပ္ပါယ်ရှိတဲ့ Strings များကို လေ့လာခြင်း တို့ဖြစ်ပါတယ်။

**Tools**: HashTab, digest.exe, TrID, BinText and strings.exe

## 3. Pack Analysis

Pack Analysis အကြောင်းမပြောခင် အရင်ဆုံး Packing အကြောင်းကို ဆွေးနွေးပါမယ်။ Executable file တွေကို Packing လုပ်ခြင်းအားဖြင့် file size ကို သိသိသာသာ ချုံ့ပေးပါတယ်။ Internet မှ download ချတဲ့အခါမှာလည်း download time ကိုလည်း လျော့နည်းစေပါတယ်။ ဒါ့အပြင် executable file ရဲ့ resources နှင့် code တွေကို disassemble လုပ်ခြင်း၊ decompile လုပ်ခြင်းတို့မှလည်း ကာကွယ်ပေးနိုင်ပါတယ်။

Pack Analysis ဆိုတာ malware file က pack ဒါမှမဟုတ် unpack လုပ်ထားသလားကို analyze လုပ်ခြင်းဖြစ်ပါတယ်။ အကယ်၍ pack လုပ်ထားပါက သင့်တော်ရာ Unpacking Tools တွေနဲ့ unpack လုပ်ပြီး analysis လုပ်ရာတွင် အသုံးဝင်သော information တွေကို ရနိုင်ပါတယ်။

**Tool**: CFF Explorer, PEiD and Stud_PE

## 4. Comparative Analysis

Comparative Analysis ဆိုတာကတော့ Surface Analysis ရဲ့ အရင် အဆင့်တွေမှာ လေ့လာလို့ ရလာတဲ့ result တွေကို အခြားသူတွေပြောထားတဲ့ resulte တွေ၊ vendor's website တွေမှာပြောထားတဲ့ result တွေနှင့် anti-viurus ဖြင့် scan လုပ်ပြီး ရလာတဲ့ result တွေကို နှိုင်းယှဉ်သုံးသပ်တာဖြစ်ပါတယ်။ အဲဒီလို နှိုင်းယှဉ်ခြင်းအားဖြင့် analysis လုပ်ရာတွင် ထိရောက်မှုရှိစေပါတယ်။