Malware Analysis အကြောင်းတစ်စေ့တစ်စောင်း

Malware ကိုတစ်နည်းအားဖြင့် Malicious Software လို့ခေါ်ကြပါတယ်။ Malware ဟာ Computer Virus ထက်ကို ပိုပြီးတော့ ကျယ်ပြန့်ပါတယ် ။ Malware ကို ယေဘုယျအားဖြင့် Virus, Worm,Trojan, Horse, Rootkit, Bot, DoSTool, Exploit kit, Spyware စသည်ဖြင့် အမျိုးမျိုး သတ်မှတ်ကြပါတယ်။

Malware အကြောင်းကို စိတ်ဝင်စားလို့ လေ့လာမယ်ဆိုရင် အောက်ပါအတိုင်း နည်းလမ်း(၃)သွယ်ဖြင့် အသေးစိတ် လေ့လာနိုင်ပါတယ်။ ပထမနည်းလမ်းကတော့ Surface Analysis ၊ ဒုတိယ နည်းလမ်းကတော့ Runtime Analysis နှင့် တတိယ နည်းလမ်းကတော့ Static Analysis တို့ဖြစ်ပါတယ်။

Surface Analysis ကို လေ့လာမယ်ဆိုရင် အဆင့်(၄)ဆင့်ဖြင့် လေ့လာနိုင်ပါတယ်။ပထမအဆင့်မှာ Preparation တွေလုပ်ရပါမယ်။ဒုတိယ အဆင့်အနေနဲ့ Feature Analysis တွေလုပ်ရပါမယ်။တတိယအဆင့် အနေနဲ့ Packet Analysis လုပ်ရပါမယ်။နောက်ဆုံးအဆင့် အနေနဲ့ ရလာတဲ့ Results တွေကို Comparative Analysis လုပ်ရပါမယ်။

Runtime Analysis ဟာ malware တွေကို execute လုပ်ပြီး သူ၏ Behavior ကိုဆက်ပြီးတော့ လုပ်ဆောင်ပါတယ်။ Static Analysis ဟာ Coding တွေကိုကြည့်ပြီး malware တွေဟာဆက်ပြီးတော့ အလုပ်လုပ်ပါတယ်။

Malware ရဲ့အဓိက ရည်ရွယ်ချက်များကတော့ ထိခိုက်နစ်နာစေသောရည်ရွယ်ချက်ဖြင့် Crashing a system လိုပုံစံမျိုး၊ Dos ပုံစံမျိုးစသည်ဖြင့် အသုံးပြုသူတွေ စိတ်အနှောက်အယှက် ဖြစ်အောင် လုပ်ဆောင်ကြပါတယ် ။ နောက်ပြီးတော့ Havoc via DDos, Sending Spam, Visiting affiliate site, Stalking, Self-assertion လိုမျိုး malware တွေဖန်တီးပြီးတော့ User တွေကိုတိုက်ခိုက်ကြပါတယ်။

Malware တွေဟာ မိမိ၏ စက်အတွင်းကို Download လုပ်ခြင်းများ, File Installation လုပ်ခြင်းများ, system folder ထဲကို Copy ကူးခြင်းများ၊ Software ရဲ့အားနည်းချက်များ၊ OS များ၊ Browser များ၊ USBများ၊ Network ချိတ်ဆက်ခြင်းများ၊ Mail များ၊ Peer To Peer ချိတ်ဆက်ခြင်းများ စသည့် အကြောင်းအမျိုးမျိုးဖြင့် malware များဟာ မိမိ၏စက်အတွင်းကို ဝက်ရောက် လာနိုင်ပါတယ်။

Security Features တွေဖြစ်သော Window Firewall များ၊ Window Update ပြုလုပ်ခြင်းစသည့် တို့ကို Disable လုပ်ပြီး malware တွေဟာမိမိ၏ စက်အတွင်းကို ဝင်ရောက်လာနိုင်ပါတယ်။ ပြီးတော့ Anti-Virus Software၊ Analysis tools များကို ရှောင်ရှားပြီးတော့လည်း malware များဟာ မိမိ၏ စက်အတွင်းကို ဝင်ရောက် လာနိုင်ပါတယ်။

Registry entries, key logging, packet capture တွေလိုမျိုး malware တွေဟာ Information တွေကိုလည်း ခိုးယူနိုင်ပါတယ်။ ပြီးတော့ Bot Program လိုမျိုး C&C Server နှင့် ချိတ်ဆက်ပြီး execute commands နဲ့ အလုပ်လုပ်ပါတယ်။ ပြီးတော့သူချိတ်ဆက်ထားတဲ့ စက်တွေကို ချက်ချင်းဖြန့်ဝေပြီး ထိခိုက်အောင် လုပ်ဆောင်ပါတယ်။

CSIRTs အဖွဲ့ အစည်းများ၊ Anti-virus/Anti-spyware Company များ၊ software developers များ၊ Security tool developers များ၊ Security service providers များ၊ Governments များ၊ Law enforcement များ၊ Private enterprises များ၊ Organizations များ စသည့် အဖွဲ့ အစည်းများဟာ malware အကြောင်းကို မသိမဖြစ်သိထားရပါမယ်။

Incident များကိုဖြေရှင်းခြင်း၊ ချို့ယွင်းချက်များကိုစစ်ဆေးခြင်း ၊ Attack ဖြေရှင်ခြင်း၊ Threat evaluation၊ Penetration tests၊ Computer forensics၊ Signature creation စသည်တို့ကို လုပ်ဆောင်မယ့် သူတွေဟာ Malware အကြောင်းကို သိထားမှသာ လုပ်ဆောင်နိုင်မှာပါ။

Malware ကို စိတ်ဝင်စားလို့ လေ့လာမယ်ဆိုရင် အောက်ပါအတိုင်း အဆင့်ဆင့် လေ့လာနိုင်ပါတယ်။ပထမ အဆင့်အနေနဲ့ Vendor's Information ကိုရယူရပါမယ်။ဒုတိယ အဆင့်အနေနဲ့ Malware Collection ကိုလုပ်ရပါမယ်။တတိယ အဆင့်အနေနဲ့ Surface Analysis လုပ်ပါမယ်။ စတုတ္ထအဆင့်အနေနဲ့ Runtime Analysis လုပ်ရပါမယ်။နောက်ဆုံးအဆင့်အနေနဲ့ Static Analysis လုပ်ရပါမယ်။

ဒီ Article လေးဟာ Malware ၏အခြေခံ အကြောင်းအရာတွေပါ။ စိတ်ဝင်စားလို့ ဆက်လက် လေ့လာရအောင် Malware အကြောင်းကို ဆက်လက်ဖော်ပြပါအုံးမယ်။