"Emotet အကြောင်း သိကောင်းစရာများ"

■■■■■■■■■■■■■■■■■■■■■■■

.

၁။ Emotet ဆိုတာဘာလဲ။

Emotet ဟာ အဖျက်အမှောင့် Trojan နဲ့ ဆိုက်ဘာရာဇဝတ်မှုလုပ်ငန်းတစ်မျိုး ဖြစ်ပါတယ်။ သူ့ကို Geodo နဲ့ Mealybug လို့ လူသိများပါတယ်။ ပထမဆုံး စတင်တွေ့ရှိခဲ့တာကတော့ ၂၀၁၄ ခုနှစ်၊ မေလလောက်မှာဖြစ်ပြီး ဂျာမနီနဲ့ ဩစတြီးယားဘဏ်တွေကို ပစ်မှတ်ထားတိုက်ခိုက်ခဲ့တာကို တွေ့ရှိခဲ့ရပါတယ်။ Emotet ရဲ့ အစောပိုင်းဗားရှင်းတွေဟာ ဘဏ်တွေကိုတိုက်ခိုက်ဖို့ Module တွေသာပါတဲ့အတွက် သူ့ကို Banking Trojan လို့ခေါ်ပါတယ်။

.

၂။ Emotet က ဘာတွေလုပ်ဆောင်သလဲ။

အစောပိုင်းထွက်ရှိတဲ့ Emotet မှာ Bank တွေကိုတိုက်ခိုက်ဖို့ Module သာပါပေမယ့် နောက်ပိုင်းဗားရှင်းတွေမှာတော့ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာ (C2 Server)ကနေ အခြားသော Module တွေကို Download လုပ်ယူမယ့် Main Module၊ Spam မေးလ်တွေ ထပ်ပို့မယ့် Spam Module၊ Web Browser တွေနဲ့ Mail Client တွေဆီကနေ Login လုပ်တဲ့ Credential တွေ ခိုးယူမယ့် Module၊ ကွန်ရက်ထဲမှာရှိတဲ့ အခြားသောကွန်ပျူတာတွေကို တိုက်ခိုက်မယ့် Spreader Module၊ တိုက်ခိုက်ခံရတဲ့ ကွန်ပျူတာကနေ အီးမေးလ် Content တွေကို ခိုးယူမယ့် Module၊ တိုက်ခိုက်ခံရတဲ့ အီးမေးလ်လိပ်စာပိုင်ရှင်နဲ့ ဆက်နွယ်ပတ်သက်တဲ့အီးမေးလ်အကောင့်တွေကို ခိုးယူမယ့် Module၊ တိုက်ခိုက်ခံရတဲ့ ကွန်ပျူတာကနေ DDoS တိုက်ခိုက်မယ့် DDoS Module တွေ ပါဝင်ပါတယ်။

.

၃။ Emotet က ဘယ်လိုနည်းနဲ့ တိုက်ခိုက်သလဲ။

Emotet ပါတဲ့အီးမေးလ်တွေမှာ Invoice နံပါတ်နဲ့သော်လည်းကောင်း၊ လက်ခံရရှိသူရဲ့ နာမည်နဲ့သော်လည်းကောင်း Subject မှာခေါင်းစဉ်တပ်ပြီး ပေးပို့ကြပါတယ်။ အဖွဲ့အစည်းတစ်ခုခုကို ပစ်မှတ်ထားတိုက်ခိုက်တဲ့မေးလ်တွေမှာတော့ သက်ဆိုင်ရာနိုင်ငံရဲ့ ဘာသာစကားကို အသုံးပြုပြီး ပေးပို့လေ့ရှိပါတယ်။ အဲဒီအီးမေးလ်တွေမှာ Microsoft Word ဖိုင် (သို့မဟုတ်) PDF ဖိုင်တွေ

ပါလာတတ်ပြီး ဒီဖိုင်တွေကို ဖွင့်မိရာကနေ တိုက်ခိုက်ခံရတာ ဖြစ်ပါတယ်။ ခုနောက်ပိုင်းမှာတော့ PDF ဖိုင်တွေအနေနဲ့ ပေးပို့တာ မရှိတော့ပါဘူး။

.

၄။ Microsfot Word ဖိုင်ဖွင့်မိရုံနဲ့ တိုက်ခိုက်ခံရနိုင်ပါသလား။

Microsoft Word ဖိုင်ကို ဖွင့်ကြည့်ရုံသက်သက်နဲ့တော့ တိုက်ခိုက်မခံရနိုင်ပါဘူး။ Word ဖိုင်ကို ဖွင့်ကြည့်တဲ့အခါ ပုံ(၁)မှာမြင်ရတဲ့အတိုင်း Security Warning က "Enable Content" ကို နှိပ်မိလို့ ဖိုင်ထဲမှာပါတဲ့ အဖျက်အမှောင့် VB Script တွေကို အလုပ်လုပ်သွားလို့သာ တိုက်ခိုက်ခံရတာ ဖြစ်ပါတယ်။

.

၅။ တိုက်ခိုက်ခံရရင် ဘာဆက်လုပ်ရမလဲ။

တိုက်ခိုက်ခံရရင်တော့ တိုက်ခိုက်မှုကို အမြန်ဆုံး ထိန်းချုပ်နိုင်ဖို့ လိုပါတယ်။ Word ဖိုင်ထဲမှာပါတဲ့ VB Script တွေဟာ ဟက်ကာတွေရဲ့ဆာဗာ(၅)ခုကို ချိတ်ဆက်ပြီး အဲဒီကနေ နောက်ထပ် Trojan တွေကို Download လုပ်ပါတယ်။ Trojan တွေဟာ Polymorphic ကုဒ်တွေနဲ့ ဖွဲ့စည်းထားတာကြောင့် ဒီ Trojan တွေကို Antivirus တော်တော်များများက တန်းမသိပါဘူး။ Emotet တိုက်ခိုက်ခံရတဲ့ကွန်ပျူတာတွေမှာ Trojan တွေကို နေ့စဉ်လဲလှယ်သလို ချိတ်ဆက်တဲ့ဆာဗာတွေကလည်း နေ့စဉ်နဲ့အမျှ ပြောင်းလဲနေပါတယ်။ Trojan တွေရဲ့ နာမည်တွေဟာလည်း အမြဲပြောင်းလဲနေကြသလို Drop ချတဲ့ Folder တွေက ပြောင်းလဲနေတာကြောင့် Antivirus တွေက စုံစမ်းထောက်လှမ်းနိုင်ဖို့ ခက်သလို Manual ဖယ်ရှားနိုင်ဖို့လည်း ခက်ခဲနိုင်ပါတယ်။

.

၆။ တိုက်ခိုက်ခံထားရကြောင်း ဘယ်လိုသိရှိနိုင်သလဲ။

ကွန်ပျူတာရဲ့ Schedule Task တွေမှာ၊ Registry ရဲ့ Autorun တန်ဖိုးတွေမှာ ကိုယ်သုံးနေကြမဟုတ်တဲ့ Application တွေ ရောက်ရှိနေပြီဆိုရင်၊ Application နာမည်တွေ အမြဲတမ်းပြောင်းလဲနေရင် ဒါဆိုရင်တော့ Emotet ရဲ့ တိုက်ခိုက်ခြင်းကို ခံနေရပြီ ဖြစ်ပါတယ်။ Scedule Task နဲ့ Registry ကနေ ဒီ setting တွေကိုဖယ်ရှားပြီး ကွန်ပျူတာထဲကလည်း ဒီဖိုင်တွေကို ဖယ်ရှားနိုင်မယ်ဆိုရင် Emotet ရဲ့ တိုက်ခိုက်ခြင်းကို ကျော်လွှားနိုင်မှာ ဖြစ်ပါတယ်။

.

၇။ Emotet တိုက်ခိုက်မခံရအောင် ဘယ်လိုကာကွယ်နိုင်မလဲ။

Emotet ဟာ အီးမေးလ်လမ်းကြောင်းကတဆင့်သာ ပေးပို့တာဖြစ်ပါတယ်။ အီးမေးလ်မှာပါတဲ့ မသက်ာဖွယ်ရာ Word ဖိုင်ကိုသာ ဖွင့်မကြည့်ဖြစ်ခဲ့ရင် တိုက်ခိုက်ခံရမှာ မဟုတ်ပါဘူး။ ပုံ(၂)မှာ ပြထားသလို Microsoft Word ရဲ့ Word Option--> Trust Center မှာ "Disable all macros without notification" သာရွေးထားခဲ့မယ်ဆိုရင် Emotet Trojan ရဲ့ တိုက်ခိုက်ခြင်းကို ခံရတော့မှာ မဟုတ်ပါဘူး။

.

၈။ Emotet တိုက်ခိုက်ခံရရင် နောက်ဆက်တွဲဆိုးကျိုးက ဘာတွေဖြစ်နိုင်သလဲ။

Emotet တိုက်ခိုက်ခံရရင် Browser ထဲမှာ သိမ်းထားတဲ့ Login Password တွေ အကုန်ပါသွားပြီး ဒီ Password တွေကိုအသုံးပြုပြီး တစ်ချိန်ချိန်မှာ အဖျက်အမှောင့်ကိစ္စတွေ လုပ်ဆောင်နိုင်ပါတယ်။ Email Client တွေရဲ့ Password တွေ၊ ကိုယ့်ရဲ့ Mail Contact List တွေနဲ့ Mail Body ထဲမှာပါတဲ့အကြောင်းအရာတွေကို ခိုးယူတာကြောင့် နောက်ပိုင်း Emotet Campaign တွေမှာ ပုံ(၃)မှာပြထားသလို ကိုယ့်မေးလ်လိပ်စာနာမည်ကို အလွဲသုံးစားပြုလုပ်ပြီး ကိုယ့်မိတ်ဆွေတွေထံ Emotet Trojan ပါတဲ့မေးလ်တွေ ပေးပို့တာကြောင့် ဒီမေးလ်တွေကိုဖွင့်ဖတ်မိပြီး Attachment ကိုဖွင့်မိတဲ့သူတွေဟာ Emotet ရဲ့ တိုက်ခိုက်ခြင်းကို ခံရမှာဖြစ်တဲ့အပြင် ကိုယ့်ရဲ့ဂုဏ်သတင်း၊ ကိုယ့်အဖွဲ့အစည်းရဲ့ ဂုဏ်သတင်းကို ထိခိုက်ကျဆင်းစေမှာ ဖြစ်ပါတယ်။ အီးမေးလ်ပို့တဲ့အခါမှာ ကိုယ်လိပ်မူပေးပို့ချင်တဲ့သူ (To) နေရာမှာ အီးမေးလ်လိပ်စာတွေအများကြီး ထည့်သွင်းမယ့်အစား တတ်နိုင်သမျှ အီးမေးလ်နည်းအောင်လုပ်ပြီး ကျန်တဲ့လိပ်စာတွေကို Blind Carbon Copy (BCC) အနေနဲ့ ပို့ခြင်းအားဖြင့် Emotet က အီးမေးလ်လိပ်စာအများအပြားကို ပေးပို့ခြင်းက လျော့ပါးသက်သာစေပါတယ်။

.

၉။ သံသယဖြစ်ဖွယ်မေးလ်လို့ ဘယ်လိုသတ်မှတ်လို့ရမလဲ။

အီးမေးလ်လက်ခံရရှိတဲ့အခါမှာ ဒီအီးမေးလ်ပေးပို့တဲ့သူကို ကိုယ်ကမသိရှိခဲ့ရင်၊ ဒါမှမဟုတ် အီးမေးလ်ထဲမှာပါတဲ့ အကြောင်းအရာတွေဟာ ကိုယ်နားမလည်တဲ့အကြောင်းအရာတွေ ဖြစ်နေခဲ့ရင်၊ ဒီအီးမေးလ်ကို ဘာကြောင့်လက်ခံရရှိတာလဲဆိုတာကို စဉ်းစားမသိရှိခဲ့ရင် ဒီလိုအီးမေးလ်မျိုးတွေကို

သံသယဖြစ်ဖွယ်မေးလ်အဖြစ် သတ်မှတ်ရပါမယ်။ ဒီလိုသံသယမေးလ်ကို အခြားသောမသက်ဆိုင်တဲ့သူတွေကို Forward ပေးပို့ခြင်း၊ ဖျက်ပစ်ခြင်းတို့ မပြုလုပ်ဘဲ အီးမေးလ်ကို Analysis ပြုလုပ်ဖို့ ထိန်းသိမ်းထားရပါမယ်။

.

၁၀။ မသက်ဖွယ်အီးမေးလ်ကို လက်ခံရရှိခဲ့ရင် ဘယ်လိုလုပ်ဆောင်သင့်သလဲ။

မသက်ဖွယ်ရာ အီးမေးလ်ကို လက်ခံရရှိခဲ့တယ်ဆိုရင် ကိုယ့်အဖွဲ့စည်းမှာရှိတဲ့ IT Team ကို အရင်ဆုံးဆက်သွယ်ဆောင်ရွက်ပြီး လိုအပ်တဲ့ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာဆောင်ရွက်မှုတွေကို လုပ်ဆောင်ရပါမယ်။ ကိုယ့်အဖွဲ့အစည်းကို ပစ်မှတ်ထားတိုက်ခိုက်နေတယ်လို့ သံသယရှိခဲ့တယ်ဆိုရင်၊ ဆိုက်ဘာတိုက်ခိုက်မှုခံခဲ့ရရင်တော့ သက်ဆိုင်ရာ IT Team ကနေတဆင့် အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာနရဲ့ ဖုန်းနံပါတ်ဖြစ်တဲ့ ၀၆၇-၃၄၂၂၇၂ ကိုဖြစ်စေ၊ အီးမေးလ်တွေဖြစ်တဲ့ incident@ncsc.gov.mm နဲ့ infoteam@mmcert.org.mm တို့ကိုဖြစ်စေ သတင်းပေးပို့တိုင်ကြားနိုင်ပါတယ်။

.

Reference

==========

https://en.wikipedia[.]org/wiki/Emotet

https://www.malwarebytes[.]com/emotet/

https://www.proofpoint[.]com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

https://www.proofpoint[.]com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return

https://www.fortinet[.]com/blog/threat-research/deep-dive-into-emotet-malware

https://www.jpcert.or[.]jp/english/at/2019/at190044.html