Security Alert

Email account hijack လုပ်ခြင်းမခံရဖို့ ဘယ်လို ကာကွယ်ကြမလဲ

> ကိုယ့်ချစ်သူက ကိုယ့်ဆီဖုန်းဆက်ပြီး ဘာကြောင့် enhancement နဲ့ ပတ်သက်ပြီး email တွေ ဆက်တိုက် ပို့နေတာလဲလို့ မေးမြန်းတဲ့အပြင် ကိုယ့်လုပ်ဖော် ကိုင်ဖက်တွေကလည်း သူတို့ဆီကြောင်ကြာတွေ ပို့နေတာ မရပ်သေး ဘူးလားလို့ မေးလာတယ် ဆိုပါတော့။ အဲဒါတွေကို ကိုယ်က ပို့နေတာရော ဟုတ်ရဲ့လား။

စာရေးသူရဲ့ သုငယ်ချင်းတစ်ယောက်က သူ့ဆီကနေပြီး မရှိတဲ့ email လိပ်စာတစ်ခုဆီကို ပို့လိုက်လို့ပြန်ရောက်လာတဲ့ email တွေကို လက်ခံရရှိခဲ့ပါတယ်။ ဒါပေမဲ့ ဒီ email account က သူအသုံးနည်းတဲ့ account ဖြစ်ပြီး သူအဲဒီ spam mail တွေကို ဘယ်သူဆီကိုမှ မပို့ဘူးလို့ဆိုပါတယ်။

အစတော့ သူက spammer တွေ သူ့ accountကို hijack လုပ်ထားတယ်ထင်ပြီး password ကို reset လုပ်ပါတယ်။ ဒါပေမဲ့ ဒီ message ဆွေက ဝင်လာနေတုန်းပါပဲ။

ဒါကဘာကြောင့် ဖြစ်ရတာလဲ။ သူ့ဆီကပို့လိုက်တဲ့ message တွေ ရောဟုတ်ရဲ့လား၊ ဒါမှမဟုတ် ပို့တဲ့သူတွေက သူ့ email address ကို spoofed return address အနေနဲ့ email header ထဲထည့်ပေးလိုက်သလား။ ဒါကို ရပ်တန့်ဖို့ ဘာလုပ်နိုင်သလဲ။ သူ့ချွေးချယ်လိုက်တာက တော့ email account အဟောင်းကိုဖျက်ပြီး အသစ်တစ်ခုဖွင့်လိုက်တာပါပဲ။

Comromised or Spoofed

ကိုယ်က ဒီအခြေအနေနဲ့ ကြုံရရင်ပထမဆုံးကြည့်သင့်တာက ကိုယ့်ရဲ့ email account ဒါမှမဟုတ် ကိုယ့် PC ကတစ်နည်းနည်းနဲ့ malware ကူးစက်မှုခံထားရသလားဆိုတာကြည့်ပါ။ အဖြစ်နိုင်ဆုံးတရားခံက spoofed email header ပါပဲ။ ဒါက spammar တွေက email header ထဲက from address ကိုပြောင်းပြီး ကိုယ်ဆီကနေ spam email တွေ ပို့သလို လုပ်တာပါပဲ။

Spammer တွေက ဒီလိုလုပ်ပြီး spam filter တွေကို လှည့်ဖျားတာပါ။ ဒါကြောင့် ဒီ junk message တွေက spam မဟုတ်သလို ဖြစ်သွားပါတယ်။ လူတွေက မသိတဲ့သူထက် သိတဲ့လူတွေဆီက email တွေကို ပိုပြီး ဖွင့်ကြလို့ပါပဲ။ Fidelis Security Systems ရဲ့ ဒါရိုက်တာတစ်ယောက်ဖြစ်တဲ့ Will Irace ရဲ့ အဆိုအရ ဒီ email ဆွေက အတော်ဆလးပဲ့နဲ့နေပါပြီ။ ကိုယ်ကသံသယရှိလို့ password ပြောင်းပေမယ့် ဆက်ဖြစ်နေရင် spammer တွေက email address တွေ spoof လုပ်ထားတာ ကျိန်းသေပါပြီ။

McAfee Cloud & Content Security ရဲ့ အကြီးတန်းဒါရိုက်တာတစ်ယောက်ဖြစ်သူ Melissa Sierra က account အများစုက compromise လုပ်ခံရတာထက် spoofe လုပ်ခံရတာများပြီး ပိုင်ရှင်က အဲဒီ account ကို မသုံးဘူးဆိုရင် ပိုဖြစ်နိုင်ပါတယ်လို့ ပြောပါတယ်။ သူက ထပ်ပြီးတော့ သုံးလက်စဆိုရင်ဆော့ rootkit တို့ phishing attack တို့လို malware ကြောင့် ဖြစ်နိုင်ပါတယ်။

Resolving a Spoofed Email Account

Bounced-email alert တွေရဲ့ message header တွေထဲမှာ အသေးစိတ် အချက်အလက်တွေပါရှိလို့ ပို့တဲ့မူလပင်ရင်းကိုရှာဖွေနိုင်ပါတယ်။ အများအားဖြင့် သူတို့က PC ရဲ့ botnet ဒါမှမဟုတ် တခြားတစ်နည်းနည်းနဲ့ ကူးစက်ခံရထားတဲ့ source ကနေ လာတာဖြစ်တာကြောင့် မူရင်းဖြစ်ချိသူကို ရှာတွေ့ဖို့ဆိုတာမလွယ်ပါဘူး။

တကယ်လို့ ကိုယ်က header ထဲမှာ spam ပို့လိုက်တဲ့ IP address ကိုတွေ့ရင် ဒီ message က ဘယ်ကလာလဲဆိုတာ ဆုံးဖြတ်နိုင်ပါတယ်။ အဲဒီနောက် ISP ကို အဲဒီ IP ကို ကိုယ့်အတွက် block လုပ်ဖို့ပြောနိုင်ပါ

တယ်။ ဒါက spoof အတွက်တော့ ယာယီအတွက်ပဲဖြစ်ပါတယ်။တကယ်လို့ spoofed email ဆိုရင် spammer က မတူညီတဲ့ IP တနေ ထပ်ပို့မှာ ဆိုတော့ ISP က ကိုယ့်ကို အကူအညီပေးနိုင်မှာမဟုတ်ပါဘူး။

အဲဒီ account ကို မသုံးဘူးဆိုရင် ဖျက်လိုက်တာက အထိရောက်ဆုံးပါပဲ။ တကယ်လို့ သုံးနေတဲ့ account ဆိုရင်တော့ ဒီလိုဖျက်ပစ်ဖို့ အဆင်မပြေနိုင်ပါဘူး။

Keeping a Law Email Profile

ကိုယ်က spoofing စဖြစ်ခဲ့သွားရင် လုပ်နိုင်တာသိပ်မရှိတော့ပါဘူး။ ဒီလို လုပ်ဖို့ spammer တွေက ကိုယ့်ရဲ့ email account လိပ်စာဆယ်ခုကို အရင်ဆုံး စုဆောင်းပါတယ်။ Irace ကတော့ ရယ်စရာအနေနဲ့ Online မှာ စိတ်ဝင်စားတာတွေ ဘာမှမလုပ်ပါနဲ့ ကိုယ့်ရဲ့ email လိပ်စာကိုလည်း ဘယ်သူကိုမှမပေးပါနဲ့လို့ ပြောထားပါတယ်။

Siem ကတော့ တချို့သောအလေ့အကျင့်လေးတွေက ကိုယ့် email account ကို လူသိနည်းစေပါတယ်။ ဥပမာ ကိုယ့်ရဲ့ ပင်ရင်း account ကိုကိုယ်သိတဲ့ သူတွေနဲ့ပဲသုံးပါ။ ကိုယ်သိတဲ့သူထဲက တစ်ယောက် ယောက်ကူးစက်ခံရရင် spammer က ကိုယ့်လိပ်စာကို သိသွားနိုင်ပေမယ့် risk ကတော့ ပိုပြီးနည်းသွားပါတယ်။

ပြီးတော့ public online forum တွေမှာ အခြားအရေးမကြီးတဲ့ email account ကိုသုံးပါ။ ဒီအချက်တွေက အန္တရာယ်ကိုလျော့ကျစေပဲရှိပြီး spammer တွေက ကိုယ့် email လိပ်စာကို spoofed message header အနေနဲ့သုံးတာကို အပြည့်အဝတားဆီးနိုင်တဲ့ နည်းလမ်းတော့ မရှိသေးမရှိပါဘူး။

Drive ထဲက data များကို ငွေမကုန်ဘဲ လုံခြုံစွာနဲ့ ဖျက်ပစ်နိုင်ဖို့

ကိုယ့်ရဲ့ flash drive ၊ hard-disk ၊ solid-state drive ဒါမှမဟုတ် hybrid hard drive ထဲက data အဟောင်းတွေကိုငွေမကုန်ပဲ လုံးဝကုန်စင်သွားအောင် ဖျက်ပစ်နိုင်ပါတယ်။

ဒီနေရာမှာ ကိုယ့်ရဲ့ harddisk ၊ SSD နဲ့ USB flash drive တွေကို ကိုယ် မစွန့်ပစ်ခင်သေသေချာချာ data တွေဖျက်ပေးနိုင်တဲ့ အခမဲ့ tool တွေကို မော်ပြသွားပါမယ်။ မတူညီတဲ့ drive တွေက မတူညီတဲ့ storage method တွေကို run ထားတဲ့အတွက်ကြောင့် တစ်မျိုးစီအတွက် tool တစ်မျိုးစီလိုနိုင်ပါတယ်။

နေ့ခင်း ကိုယ် delete လုပ်နေတဲ့ data တွေက ကိုယ့်ရဲ့ drive ပေါ်ကနေ တကယ် ပျက်သွားတာ မဟုတ်ပါဘူး။ Data ကို ညွှန်းတဲ့ အညွှန်းလေးကိုပဲ ဖျက်လိုက်တာပါ။ ဒီလို data တွေကို အပြီးအပိုင် ဖျက်ပစ်ဖို့အတွက်တော့ 0 နဲ့ 1 တွေကို အဲဒီ data ပေါ်ရေးပေးနိုင်တဲ့ app လိုပါတယ်။

Laptop drive ထဲက data တွေ ရှင်းဖို့ မကြိုးစားခင်မှာ AC adapter တပ်ထားပါ။ မဟုတ်ရင် drive ကို wipe လုပ်နေတုန်း battery အားကုန်သွားရင် hard drive သုံးမရ ဖြစ်သွားနိုင်ပါတယ်။

သံလိုက်အားခြေပြ harddisk တွေအတွက်တော့ အခမဲ့ရတဲ့ secure wipe software DBAN *(find.pcworld.com/71984)* ကိုစမ်းသပ်သုံးစွဲပါ။ ဒါက sector တိုင်းကို မဖျက်ခင်မှာ random data တွေနဲ့ အကြိမ်များစွာ လိုက်ဖြည့်လိုက်ပါတယ်။ ဒါဆမဲ့ flash memory တွေကိုတော့ တစ်ခါတစ် ရံအပြည့်အဝမဖျက်နိုင်လို့ DBAN ကို hybrid harddisk/SSD တွေမှာ မသုံးသင့်ပါဘူး။

Well and Truly Erase

ကိုယ့်မှာ hybrid hard drive ဒါမှမဟုတ် SSD ရှိရင် CMRR ရဲ့ အခမဲ့ Secure Erase Utility *(find.pcworld.com/72853)* ကိုစမ်းသပ်ကြည့်ပါ။ ဒီ app က Serial ATA (SATA) နဲ့ Parllel ATA (PATA) drive တွေရဲ့ firmware ထဲမှာ secure erase run လိုက်ပါတယ်။ ဒါကြောင့် အဓိပ္ပာယ်မရှိတဲ့ data တွေကို memory အကုန်လုံးမှာ လိုက်ဖြည့်ပေးပြီး ဖျက်ပေးမှာပါ။

ဒီ tool ကိုသုံးပြီး hardware ကိုဖျက်ဖို့ HDDerase.exe ကို CD ဒါမှမဟုတ် USB ထဲကူးပြီး CD/USB ကနေ boot တက်ပါ။ ပြီးတော့ hdderase လို့ command prompt မှာ ရိုက်ပြီး enter ခေါက်ပါ။ ကိုယ့် hard drive ရဲ့ sector ကိုင်းကို စိတ်ချရအောင် ဖျက်ပေးသွားမှာပါ။ ဒီလိုလုပ်တာက နာရီပေါင်းများစွာတော့ ကြာနိုင်ပါတယ်။

တခြားသူတွေ ကိုယ့် USB stick ထဲက data တွေပြန်မယူနိုင်စေဖို့ အခမဲ့ Roadkil's Disk Wipe utility *(find.pcworld.com/72854)* ကို download လုပ်ပါ။ ပြီးတော့ run ပြီး ကိုယ် ဖျက်ချင်တဲ့ USB drive ကို ရွေးပြီး random data နဲ့ ဖြည့် ဒလား wipe ပဲ လုပ်ရဲလား ဆိုတာရွေးပါ။ Pass တယ်နစ်ကြိမ် လုပ်မလဲဆို တာရွေးပါ။ ၃ ကြိမ်ဆိုရင် စိတ်ချရပါတယ်။

ပြီးတော့ စဖျက်လို့ရပါပြီ။ ကိုယ့် data ကို ဖျက်ဖို့အကောင်းဆုံးကတော့ drive ကို ဖျက်ဆီးပစ်တာဖြစ်မေ့ယ့် အဲဒီလိုမလုပ်နိုင်ရင်တော့ အခုအော်ပြဆဲးလိုက်တဲ့ နည်းလမ်းတွေက ဒုတိယအကောင်းဆုံး ဖြေရှင်းနည်းတွေပါပဲ။

West Hero