Smartphone တွေဆီ ဦးလှည့်လာတဲ့ ရာဇဝတ်မှုကျူးလွန်သူများ

Phone ဝယ်ယူသူတွေက smartphone ကို ပိုပြီး အာရုံကျလာသလို ရာဇဝတ်မှု ကျူးလွန်သူတွေက လည်း smartphone တွေကို ပိုပြီးပစ်မှတ်ထားလာ ပါတယ်။ အဲဒီလိုဆိုပေမယ့် သူတို့က PC တွေကိုလည်း လက်မလွှတ်သေးပါဘူး။ »

ရာဇဝတ်မှုကျူးလွန်သူတွေက ကိုယ်ရေးအချက်အလက်တွေ၊ ဘဏ် account နံပါတ်တွေ၊ အကြွေးဝယ် card account နံပါတ်တွေ ခိုးယူဖို့၊ လိမ်လည်မှုတွေကျူးလွန်ဖို့ PC တွေကို နှစ်သြိုက်ကြတာပဲဖြစ်ပါတယ်။ ဒီလို တိုက်ခိုက်မှုအများစုက Microsoft ရဲ့ ဆယ်စုနှစ်တစ်ခု သက်တမ်းရှိ Windows XP လည်ပတ်ရေးစနစ်မှာ ဖြစ်ပွားတာ ဖြစ်ပါတယ်။ အခုတော့ Windows XP နေရာကို ပိုမို လုံခြုံမှုရှိတဲ့ Windows 7 က နေရာဝင်ယူလာပါပြီ။ ဒါကြောင့် hacker တွေကလည်း ပစ်မှတ်နေရာအသစ်ကို ရှာဖွေကြတော့မှာ ဖြစ်ပါတယ်။

ယခု ၂၀၁၁ ခုနှစ်မှာတော့ smartphone အလုံးရေ ၄၁၂ သန်း ရောင်းချရမယ်လို့ ရည်မှန်းထားပါတယ်။ ဒါဆိုရင် ပထမဆုံးအနေနဲ့ smartphone ရောင်းချမှုက PC ရောင်းချမှုကို ကျော်တက်သွားပါလိမ့်မယ်။ ဒါကြောင့် smartphone တွေဆီကို ဦးတည်မယ့် ရာဇဝတ်မှုကျူးလွန်မှုတွေလည်း များလာတော့မှာ ဖြစ်ပါတယ်။ Mobile လုံခြုံရေးကုမ္ပဏီ Lookout ရဲ့ အဆိုအရ သူများအကျိုး ပျက်စီးရာပျက်စီးကြောင်းဖန်တီးတဲ့ ဖျက်ဆီးရေး software ဖြစ်တဲ့ malware နဲ့ သူလျှို software ဖြစ်တဲ့ sypware ကို သူတို့စစ်ဆေးခဲ့တဲ့ phone အလုံးရေ ၁၀၀ အနက် ၉ လုံးမှာ တွေ့ရတယ်လို့ သိရပါတယ်။ အဲဒီနှုန်းက ၂၀၀၉ ခုနှစ် ဒီဇင်ဘာလတုန်းကတွေ့ရှိခဲ့တဲ့ phone အလုံးရေ ၁၀၀ မှာ ၄ လုံး တွေ့ရှိတဲ့နှုန်းထက် ၂ ဆကျော် ဖြစ်နေပါတယ်။

တကယ်တော့ အကာအကွယ်ဖြစ်စေဖို့ လက်တွေ့ထိရောက်နိုင်တဲ့ လုပ်ဆောင်ဖို့အသင့်ဆုံးအချက်က smartphone ကို PC တစ်လုံးလို သဘောထားတာပဲဖြစ်ပါတယ်။ ဖြစ်ရပ်အများစုမှာ ဖြစ်တတ်တာက လိမ်လည်တဲ့ mobile application ၊ ဒါမှမဟုတ် ဖျက်လိုဖျက်စီးလုပ်တဲ့ mobile application တွေ ဖြစ်ပါတယ်။ အဲဒီလို ဖြစ်ရပ် အမျိုးအစားပေါင်းက ၅၀၀ ကျော်ရှိတယ်လို့ လုံခြုံရေးကုမ္ပဏီတစ်ခုက ပြောပါတယ်။ ဒီဖြစ်ရပ်တွေဟာ အသုံးပြုသူကို တစ်ခုခုစေခိုင်းတဲ့နည်းကို အသုံးပြုကြပါတယ်။ ဥပမာ – program တစ်ခုကို လက်ခံဖို့၊ ဒါမှမဟုတ် install လုပ်ဖို့ click နှိပ်ခိုင်းတာမျိုး ဖြစ်ပါတယ်။ ဒါကြောင့် ပြဿနာအများစုကို သတိကလေး တစ်ချက်နဲ့ ရှောင်ရှားနိုင်ပါတယ်။ ဒါပေမဲ့ အနာဂတ်မှာ စက်က အလိုအလျောက် ဆောင်ရွက်တဲ့ တိုက်ခိုက်မှုတွေ ရှိလာနိုင်တယ်လို့ ပညာရှင်တွေက သတိပေးထားပါတယ်။

တိုက်ခိုက်မှု အဖြစ်ပွားဆုံးက ဥရောပအရှေ့ပိုင်းနဲ့ တရုတ်ပြည်တို့ ဖြစ်ပါတယ်။ တိုက်ခိုက်မှုများပြားတဲ့ ရာခိုင်နှုန်းလို့ ပြောနိုင်တဲ့ ၈၈ ရာခိုင်နှုန်းမှာ Nokia ရဲ့ Symbian သုံး phone တွေမှာ ဖြစ်ပွားတာဖြစ်ပါတယ်။ Symbian ဟာ ကမ္ဘာ့လူသုံးအများဆုံး smartphone platform ဖြစ်ပြီး လာမယ့် နှစ်အနည်းငယ်အတွင်း Microsoft ရဲ့ Windows Phone စနစ်နဲ့ အစားထိုးသွားမယ်လို့ Nokia က ဖေဖော်ဝါရီလတုန်းက ပြောကြားသွားခဲ့ပါတယ်။

၂၀၀၄ ခုနှစ်နဲ့ ၂၀၀၅ ခုနှစ်မှာ ဖြစ်ပွားတဲ့ Cabir နဲ့ Commwarrior လို တိုက်ခိုက်မှုတွေဟာ ဆိုးဆိုးဝါးဝါး ဖျက်စီးမှုမရှိပါခဲ့ဘူး။ ဒါပေမဲ့ ၂၀၀၉ ခုနှစ်ကစပြီး တိုက်ခိုက်မှုတွေ ဆိုးဝါးပြင်းထန်လာပါတယ်။ ၂၀၁၀ ပြည့်နှစ်၊ စက်တင်ဘာလ

PCWorldMyanmar

တုန်းက hacker တွေဟာ Symbian phone တွေမှာ ဖျက်ဆီးရေး software တွေ ထည့်သွင်းကာ စပိန်နိုင်ငံ ဘဏ်တစ်ခုက ငွေတွေခိုးယူဖို့ အားထုတ်ခဲ့ဖူးပါတယ်။ ZeuS ဖျက်ဆီးရေး software ကပ်ငြိနေတဲ့ နေအိမ်တွေက PC တွေကို အသုံးချပြီး အဲဒီလို အားထုတ်ခဲ့တာ ဖြစ်ပါတယ်။ ZeuS ဖျက်ဆီးရေး software ဟာ ဘဏ်က ငွေကြေးလွှဲပြောင်းမှုတွေ ဆောင်ရွက်ပေးပို့တဲ့ လုံခြုံရေးသင်္ကေတ စကားဝှက်တွေကို ရာဇဝတ်မှုကျူးလွန်သူတွေက သိရှိကာ ရာဇဝတ်မှုကျူးလွန်နိုင်စေတာ ဖြစ်ပါတယ်။

အမေရိကန်ပြည်ထောင်စုမှာ ခေတ်စားနေတဲ့ phone တွေဟာလည်း အဲဒီတိုက်ခိုက်မှုတွေကနေ ပြေးလို့မလွတ်ပါဘူး။ Google ရဲ့ Android ၊ Research In Motion ရဲ့ BlackBerry ၊ Apple ရဲ့ iPhone ၊ Microsoft ရဲ့ Windows Mobile လည်ပတ်ရေး software တွေကို တိုက်ခိုက်ခံရမှုတွေ တွေ့နေရတာကြောင့် ရှေ့နှစ်တွေဆိုရင် အဲဒီထက် ဆိုးဝါးနိုင်တယ်လို့ ပြောလို့ရပါတယ်။

အချို့ပညာရှင်တွေက Android ဟာ ဖျက်ဆီးရေး software တွေရဲ့ မျက်စိကျစရာဖြစ်နိုင်တယ်လို့ ပြောကြပါတယ်။ အကြောင်းရင်းကတော့ ဘယ်သူမဆို internet တစ်နေရာရာကနေပြီး application တစ်ခုဖန်တီးကာ ဖြန့်ချိနိုင်တာကြောင့် ဖြစ်ပါတယ်။ Google ကတော့ လုံခြုံရေးရည်ရွယ်ချက်နဲ့ application တွေကို ဟန့်တားတဲ့ နည်းပညာ အတားအဆီးတွေ ပြုလုပ်ထားပါတယ်။ ဥပမာ – application တွေကို တစ်ခုနဲ့တစ်ခု လွှမ်းမိုးမှုမရှိတာ၊ အသုံးပြုသူ ခွင့်ပြုချက်မရှိဘဲ phone ရဲ့ လုပ်ဆောင်ချက်တွေကို ပြုပြင်ပြောင်းလဲမှု မပြုနိုင်တာလို အကန့်အသတ်ရှိတဲ့ အခြေအနေမှာ လည်ပတ်သုံးစွဲပါတယ်။ ဖျက်ဆီးရေးလှုပ်ရှားမှုတွေကို ကာကွယ်ထားတဲ့ စည်းကမ်းဥပဒေတွေ ဖောက်ဖျက်ရင် google က အဲဒီ application ကို သူ့ရဲ့ တရားဝင် Android စျေးကွက်ကနေ ဖယ်ရှားပါတယ်။

တိုက်ခိုက်မှုတွေက mobile application တွေ၊ download လုပ်မှုတွေကတစ်ဆင့် ဖြစ်ပေါ်တတ်တာကြောင့် application တွေ download မလုပ်ခင် အထူးဂရုတစိုက် စဉ်းစားသင့် ပါတယ်။ ယုံကြည်ရတဲ့ website တွေက application တွေကိုသာ install လုပ်သင့်ပြီး ဖျက်ဆီးရေး software တွေ ဟုတ်၊ မဟုတ် သေချာအောင် ဆန်းစစ်သင့်ပါတယ်။

Smartphone ဆိုတာက ကိုယ့်လက်ထဲမှာကိုင်ထားတဲ့ computer အသေးစားကလေးပဲ ဖြစ်ပါတယ်။ ဒါကြောင့် ကိုယ်က computer တွေ တွေ့ကြုံနိုင်တဲ့ Trojan horse တွေ၊ virus

တွေနဲ့ တွေ့ကြုံနိုင်ပါတယ်လို့ လုံခြုံရေးကိစ္စတွေ စမ်းသပ်လုပ်ဆောင်နေတဲ့ ကုမ္ပဏီတစ်ခုက ပြောပါတယ်။

အန္တရာယ်ကို မမေ့မလျော့ရှိသူတွေကတော့ လုံခြုံရေးထုတ်ကုန်ကို အသုံးပြုမှာဖြစ်ပါတယ်။ iPhone platform ကလွဲပြီး ကျန် phone တွေအတွက် အခမဲ့ထုတ်ကုန်တွေ၊ ငွေကြေးတန်ဖိုးသင့်တင့်တဲ့ထုတ်ကုန်တွေ စျေးကွက်မှာရနိုင်နေပါပြီ။ အဲဒါတွေကို F-Secure ၊ Symantec ၊ Kaspersky တို့လို လုံခြုံရေးကုမ္ပဏီကြီးတွေ၊ Lookout နဲ့ DroidSecurity လို ဖြန့်ချိရေးကုမ္ပဏီတွေမှာ ဝယ်ယူနိုင်ပါတယ်။

Mobile phone software တွေအပေါ် ထိန်းချုပ်မှုအားကောင်းရင် တိုက်ခိုက်မှုနည်းတတ်ပါတယ်။ ဥပမာ – Apple က ထိန်းချုပ်မှုအားကောင်းတာကြောင့် ပြဿနာ အများစုအတွက် စိတ်ပူစရာသိပ်မလိုပါဘူး။ iPhone တွေပေါ်မှာ တွေ့ရှိခဲ့တဲ့ ဖျက်ဆီးရေး software တစ်ခုသာ ရှိပါတယ်။ အဲဒီ software က Apple ရဲ့ ခွင့်ပြုထားမှုမရှိတဲ့ software တွေကို ဆောင်ရွက်နိုင်အောင် ပြုပြင်ထားတဲ့ phone တွေကို တိုက်ခိုက်ခဲ့တာ ဖြစ်ပါတယ်။

လုံခြုံရေးရည်ရွယ်ချက်နဲ့ Microsoft က ၂၀၁၀ ပြည့်နှစ်၊ အောက်တိုဘာလက သူ့ရဲ့ phone သစ် Windows Phone 7 အတွက် စနစ်တစ်ခု ပြောင်းလဲကျင့်သုံးခဲ့ပါတယ်။ သူက application ရောင်းချမှုကို သူ့ရဲ့ ကိုယ်ပိုင်စျေးကွက်မှာသာ

ကန့်သတ်ထားပြီး application တီထွင်သူတွေအတွက် လုံခြုံရေးနဲ့ privacy လိုက်နာရေး လိုအပ်ချက်တွေကို ထုတ်ပြန်ထားပါတယ်။ Application အသစ်ပေါ်တိုင်း လုံခြုံရေးစစ်ဆေးချက်ပြုလုပ်တယ်လို့လည်း Microsoft က ပြောပါတယ်။

Cellphone တွေကို ငွေတောင်းခံတဲ့ တိုက်ခိုက်မှုတွေက ရာဇဝတ်မှုကျူးလွန်သူတွေအတွက် ငွေဖြစ်အလွယ်ဆုံး နည်းလမ်းဖြစ်တယ်လို့ လုံခြုံရေးကုမ္ပဏီ F-Secure က ပြောပါတယ်။ Hacker တွေက ဒါကို ဘယ်လောက် အဓိကထားဆောင်ရွက်နေတယ်ဆိုတာကို facebook ပေါ်က လိမ်လည်မှုတွေကိုကြည့်ရင် သိနိုင်ပါတယ်။ Facebook ပေါ်က နည်းမျိုးစုံသုံး လိမ်လည်မှုတွေက online စစ်တမ်းပြုလုပ်တယ်လို့ဆိုကာ အချက်အလက်တွေဖြည့်ခိုင်းပြီး cellphone နံပါတ်တွေ တောင်းယူပါတယ်။ အဲဒီနောက်မှာ လစဉ်ဝန်ဆောင်ခတွေ တောင်းယူတော့တာပါပဲ။ ဒါကြောင့် ထူးထူးဆန်းဆန်း စရိတ်စက တောင်းခံလွှာတွေ ပါ၊ မပါ ငွေတောင်းခံလွှာတွေကို ပုံမှန်စစ်ဆေးဖို့ လိုပါတယ်။

BlackBerry တွေက တိုက်ခိုက်ခံရခဲပါတယ်။ အဲဒီအပြင် ဖျက်ဆီးရေး software ဖန်တီးသူတွေရဲ့ နေရပ်ဖြစ်တဲ့ ရုရှားနဲ့ တရုတ်တို့လို နိုင်ငံတွေမှာ BlackBerry ကိုင်ဆောင်မှုတွေ များသေးပါပါဘူး။ BlackBerry တွေမှာ ဖြစ်တတ်တာက FlexiSPY လို သူလျှို software ပြဿနာ ဖြစ်ပါတယ်။ အဲဒီသူလျှို software တွေကို တစ်စုံတစ်ယောက်က (အထူးသဖြင့် သဝန်တိုသူခင်ပွန်း၊ ဒါမှမဟုတ် ဇနီး) တိတ်တဆိတ် ထည့်သွင်းပြီး phone ပိုင်ရှင် ခြေစကြံဖြန့်ရာကို နောက်ယောင်ခံတာ၊ phone ခေါ်ဆိုမှုတွေ နားထောင်တာ၊ စာသားပေးပို့မှုတွေနဲ့ email တွေကို ဖတ်ရှုတာတွေ ပြုလုပ်ပါတယ်။

ကိုယ်က microphone ကို အဝေးထိန်းစနစ်နဲ့ ဖွင့်နိုင်၊ phone နဲ့ ပြောဆိုနေတာတွေကို နားထောင်နိုင်တယ်လို့ လုံခြုံရေးကုမ္ပဏီတစ်ခုက ပြောပါတယ်။ မလိမ့်တပတ်နဲ့ ကိုယ်ရေးအချက်အလက်တွေ တောင်းခံတာကလည်း smartphone အမျိုးအစားအားလုံးမှာ အဖြစ်များနေတဲ့ ပြဿနာဖြစ်ပါတယ်။ PC တွေမှာလည်း ရိုးနေပြီဖြစ်တဲ့ ဒီလို တိုက်ခိုက်မှုတွေက ဘဏ်လို ယုံကြည်စိတ်ချရတဲ့နေရာကနေ တောင်းခံသလိုလိုနဲ့ ကိုယ်ရေးအချက်အလက်တွေ တောင်းခံတာဖြစ်ပါတယ်။

PC သုံးစွဲသူတွေထက် mobile phone သုံးစွဲသူတွေကို အဲဒီအလိမ်အညာတွေ အထိခံရဖို့ ဖြစ်နိုင်ခြေ ၃ ဆ ပိုတယ်လို့ မကြာမီကလေ့လာခဲ့တဲ့ လုံခြုံရေးကုမ္ပဏီ Trusteer က ပြောပါတယ်။ ဖြစ်နိုင်ချေများတဲ့ အကြောင်းက mobile phone တွေဟာ တစ်ချိန်လုံးဖွင့်ထားပြီး ဖန်သားပြင် အသေးကလေးက လိမ်ညာမှုတွေကို ထောက်လှမ်းဖို့ ခက်ခဲစေလို့ဖြစ်တယ်လို့ သိရပါတယ်။ ဒါကြောင့် mail တွေထဲက web link ကို click နှိပ်တာမျိုး မပြုလုပ်ဖို့လည်း သတိပေးထားပါတယ်။

လျှို့ဝှက် သတင်းအချက်အလက်တွေကိုလည်း လူအများသုံး Wi-Fi ကွန်ရက်ကတစ်ဆင့် သင်္ကေတစကားဝှက်နဲ့ ပိတ်ထားတာမရှိဘဲ ပေးပို့ရင် အခိုးခံရနိုင်ပါတယ်။ ဒါကြောင့် လေဆိပ်၊ ဒါမှမဟုတ် internet cafe ကွန်ရက်က တစ်ဆင့် ပေးပို့တာမျိုးမပြုလုပ်သင့်ပါဘူး။

Smartphone နဲ့အတူ သူ့ထဲက အချက်အလက်တွေ ပျောက်ဆုံးတာဟာလည်း smartphone ပိုင်ရှင်တွေအဖို့ အဖြစ်တတ်ဆုံး အန္တရယ်ပါပဲ။ ဒါကြောင့် phone ကို ကိုယ်ပိုင်သင်္ကေတ၊ အမှတ်အသားတစ်ခုနဲ့ ပိတ်ထားသင့်ပါတယ်။ ပျောက်သွားတဲ့ phone ကို ရှာဖွေပေးနိုင်တဲ့ software ၊ အချက်အလက်တွေကို ဖျက်စီးပစ်နိုင်တဲ့ software ကို ထည့်သွင်းထားနိုင်ရင် ပိုကောင်းပါတယ်။

Apple ၊ Microsoft နဲ့ RIM တို့က သူတို့ phone တွေအတွက် အခမဲ့ application တွေ ဖြန့်ချိပေးလျက်ရှိကာ Android နဲ့ တခြား phone တွေကလည်း F-Secure နဲ့ Lookout လို တတိယအုပ်စုတွေကနေပြီး အလားတူ application တွေကို ရရှိနိုင်ပါတယ်။

စောလျ