Security Alert

Mobile malware များကို ရှောင်ကြစို့

Smartphone malware က ထင်ထားသလောက် မကြီးမားသေးပါဘူး။ ဒါပေမဲ့ ကြီးထွားလာနေတာကိုတွေ့ရပါတယ်။ Malware တွေကို ရှောင်နိုင်ဖို့ အချက်လေးတွေ ဖော်ပြပေးချင်ပါတယ်။

အဖျက်အမောင့် software တွေက PC ကနေ cell phone တွေဆီကို ခုန်ကူးလာနေပါပြီ။ အခု malware ပြုလုပ်သူတွေက မြန်မြန်ရနိုင်မယ်ဆိုတဲ့ မျှော်လင့်ချက်နဲ့ phone တွေကို ပစ်မှတ်ထားလာကြပါပြီ။ ဥပမာပြောရရင် ကူးစက်ခဲ့တဲ့ DroidDream နဲ့ Plankton Android app တွေပါပဲ။ Android Market ထဲကို ဖြန့်ချိလိုက်တဲ့ infected app တစ်ခုက ဖော်ထုတ်မတွေ့ရှိခင်မှာ သုံးစွဲသူထောင်ပေါင်းများစွာကို ကူးစက်နိုင်ပါတယ်။

DroidDream ဖြစ်ရပ်မှာဆိုရင် လူထောင်ပေါင်းများစွာက Trojan horse ကူးစက်နေတဲ့ software ကို phone တွေဆီကို download လုပ်ခဲ့ကြပါတယ်။ အဲဒီ software က အသုံးပြုသူရဲ့ တည်နေရာနဲ့ phone နံပါတ်တွေကို remote server ဆီကို လှမ်းပို့ပေးပါတယ်။ အဲဒီနေ့မှာပဲ google က အဲဒီ app ကို Android Market ထဲကနေ ဖယ်ရှားခဲ့ပါပြီ။ ပြီးတော့ Phone တွေထဲက အဲဒီ app ကို အဝေးကနေ ဖယ်ရှားပစ်ပါတယ်။ ပြီးတော့ patch ကို update လုပ်ပြီး အဲဒီ Trojan horse လုပ်ဆောင်သွားတာတွေကို ပြင်ဆင်ပေးခဲ့ပါတယ်။

Android app တွေရဲ့ တည်ဆောက်ပုံအရ malware ရေးသူတွေက နာမည်ကြီး app တွေကို malware တွေပေါင်းစပ်ပြီး မတူညီတဲ့နာမည်သစ်တစ်ခုနဲ့ Android Market ထဲကို ပြန်ပြီး upload လုပ်နိုင်နေပါတယ်။ ဒါပေမဲ့ mobile malware တွေမှာ PC တွေရဲ့နှုန်းနဲ့ ကူးစက်မှုမျိုး မရှိသေးပါဘူး။ ပြီးတော့ တိုက်ခိုက်ခံရတဲ့ ပမာဏကလည်း သေးငယ်ပါတယ်။ ဒါ့အပြင် malware တွေပေါ်ပေါက်လာတဲ့ နာရီအတော်များများအတွင်းမှာပဲ သိရှိပြီး patch တွေထုတ်ပေးနိုင်ခဲ့ပါတယ်။ Symantec အဆိုအရတော့ အခုအချိန်မှာ သိပ်မကြီးထွားပေမယ့် အနာဂတ်မှာ ကြီးထွားလာမယ့် လက္ခဏာရှိနေပါတယ်။

စောင့်ကြည့်ရမယ့်ခြိမ်းခြောက်မှုများ

Malware ပြုလုပ်သူတွေက Android ကို ပိုကြိုက်ကြပါတယ်။ ဘာလို့လဲဆိုတော့ အသုံးပြုသူတွေ သူတို့စိတ်ကြိုက် app တွေကို အသုံးပြုခွင့်ပေးထားလို့ပါပဲ။ ဒါပေမဲ့ တခြား mobile gadget တွေကလည်း malware အန္တရာယ်ရှိနေတာပါပဲ။

Closed app စနစ်ဖြစ်တဲ့ Apple မှာတော့ app တွေကို App Store ကို မတင်ခင်မှာ အသေအချာစစ်ဆေးပါတယ်။ ဒါပေမဲ့ app ရဲ့ bit တိုင်းကို စစ်ဆေးပေးနိုင်တာ မဟုတ်ပါဘူး။

၂၀၁၀ခုနှစ် ဇူလိုင်မှာ Handy Light လို့ခေါ်တဲ့ app တစ်ခုက Apple ရဲ့ စစ်ဆေးမှုတွေကို ကျော်ဖြတ်နိုင်ခဲ့ပြီး App

Store ဆီကို ရောက်ရှိသွားခဲ့ပါတယ်။ အဲဒီ app က flashlight app နဲ့တူပေမယ့် အသုံးပြုသူတွေကို သူတို့ရဲ့ iPhone တွေကို cellular moderm အနေနဲ့ သုံးနိုင်စေတဲ့ unofficial tethering function တစ်ခု ကွယ်ဝှက်ပြီး ပါလာခဲ့ပါတယ်။ Handy Light က malware မဟုတ်ပါဘူး။ ဒါပေမဲ့ စိစစ်တဲ့စနစ်က အပြည့် အဝလုံခြုံမှုမရှိဘူးဆိုတာ ဖော်ပြနေပါတယ်။ အခု ထိတွေ့တဲ့ Mobile Malware အများစုကတော့ Android plaiform ပေါ်က infected app အသွင်မျိုးပဲရှိပါတယ်။ Phone ကို ကူးစက်ခံရဖို့ ဆိုရင် အသုံးပြုသူကိုယ်တိုင်က install လုပ်ရပါမယ်။ Malware ပြုလုပ်သူတွေက တခြား smartphone OS တွေကို စတင် ပစ်မှတ်ထားတာကြောင့် ဒီအခြေအနေက ပြောင်းသွားနိုင်ပါ တယ်။

နောက်ဆုံးမှာတော့ ဘယ်နေရာမှာနဲ့ ဘယ် app ကို သွင်းရမယ်ဆိုတာ အသုံးပြုသူရဲ့ ရွေးချယ်မှုမှန်ကန်ဖို့ အရေး ကြီးပါတယ်။ ဒီနှစ် ဇွန်လတုန်းက McAfee Lab က ထုတ်ခဲ့တဲ့ အစီရင်ခံစာ *(find.pcworld.com/72039)* အရ google ၊ ဒါမှ မဟုတ် Apple က ခွင့်ပြုမထားတဲ့ third-party app store တွေမှာရှိတဲ့ malware တွေက official market ထက်ပိုများ ပါတယ်။

ဘယ်လိုကာကွယ်ရမလဲ

အလုံခြုံဆုံးနည်းကတော့ ကိုယ်မကြားဖူးတဲ့ app တွေ ကို ရှောင်ပါ။ ပြီးတော့ app နဲ့ သူ့ရဲ့ publisher နဲ့ ပတ်သက် ပြီး download ခလုတ်မနှိပ်ခင်မှာ သေသေချာချာ စစ်ဆေးပါ။ app ကို install လုပ်တဲ့အခါမှာတော့ app က ကိုယ့်ရဲ့ device ကို access လုပ်နိုင်တဲ့ service တွေအတွက် permission တွေကို တွေ့ရပါမယ်။ ပြောရရင် alarm clock app တစ်ခုက ကိုယ့်ရဲ့ contact တွေဆီကို access မလုပ်သင့်ပါဘူး။ Permissions screen က တစ်ခုခု မသင်္ကာစရာဖြစ်ရင် app ကို download မလုပ်ပါနဲ့။

ကိုယ်က web ကို browse လုပ်နေတဲ့အခါမှာလည်း click နှိပ်တာကို သတိထားသင့်ပါတယ်။ ဇွန်လနှောင်းပိုင်း တုန်းက mobile security ကုမ္ပဏီတစ်ခုဟာ malicious ကြော်ငြာတွေက smartphone အသုံးပြုသူတွေကို ပစ်မှတ် ထားပြီး infected app တွေကို install လုပ်မိအောင် လုပ်ဆောင် ထားပါတယ်လို့ ဆိုပါတယ်။ Lookout Mobile Security လိုမျိုး mobile antivirus software တချို့မှာတော့ ဒီလို phishing attack တွေကို ကာကွယ်နိုင်တဲ့ feature ပါရှိပါတယ်။

တတ်နိုင်ရင် antivirus software ကို phone မှာ install လုပ်ပါ။ AVG ၊ McAfee နဲ့ Symantec တို့လို နာမည်ကြီး security ကုမ္ပဏီအများစုမှာ phone အတွက် mobile app ရှိပါတယ်။ Malware တွေကို စောင့်ကြပ်နိုင်တဲ့အပြင် အဲဒီ app ကို lock လုပ်ပြီး remote wipe လုပ်နိုင်တဲ့ feature တွေပါရှိပါတယ်။ ဒါကြောင့် phone တစ်ခုဝယ်ရင် တခြား app တွေမသွင်းခင်မှာ antivirus program တစ်ခု အရင်သွင်း သင့်ပါတယ်။

အခုအခြေအနေမှာတော့ smartphone malware တွေက ရှောင်ရလွယ်ပါတယ်။ ဒါပေမဲ့ အဲဒီ malware ရှိနေတယ် ဆိုတာ သတိပြုမိတာက ကိုယ့် data တွေ တခြားလူလက်ထဲ မရောက်အောင် ကာကွယ်နိုင်တဲ့ ပထမအဆင့်ပါပဲ။

အမည်မသိ internet အသုံးပြုမှုတွေကို တားဆီးမယ့် ဒိန်းမတ်နိုင်ငံ

ဒိန်းမတ် တရားရေးဌာနက အမည်မသိ internet အသုံးပြုမှုကို တားဆီးသုတ်သင်ဖို့ အဆိုတစ်ရပ် တင်သွင်းခဲ့ပါတယ်လို့ Computerworld Denmark ရဲ့ အဆိုအရ သိရပါတယ်။ ဒီအဆို အရ café နဲ့ library တို့လို open internet location တွေမှာ အသုံးပြုသူတွေရဲ့ identity တွေကို အတည်ပြုဖို့ လိုပါတယ်။ အဲဒီ open internet location တွေကရရှိတဲ့ data တွေကို ဒိန်းမတ်အစိုးရဆီကို အစီရင်ခံရမှာပါ။ ဒါက တိုင်းပြည်ရဲ့ အကြမ်းဖက်မှုတိုက်ဖျက်ရေးအတွက်လို့ ဆိုပါတယ်။

ဒီအဆို အတည်ဖြစ်သွားခဲ့ရင် ကုမ္ပဏီတွေက ဝန်ထမ်း တွေရဲ့ activity နဲ့ log in code တွေကိုပါ တင်ပြရပါမယ်။ ဒါကြောင့် စီးပွားရေးလုပ်ငန်းတွေရဲ့ လျှို့ဝှက်အချက်အလက် တွေက အစိုးရလက်ထဲကနေ ဖြတ်သွားရမှာပါ။ ဒီတော့ data collection storage နဲ့ transfer တွေနဲ့ပတ်သက်ပြီး လုံခြုံ ရေးစိုးရိမ်စရာတွေပါ တိုးလာပါပြီ။ ဒီလိုဆိုရင် ဒိန်းမတ်ရဲ့ internet အသုံးပြုမှုအပေါ် အစိုးရက စောင့်ကြည့်တဲ့ အဆင့် ဟာ အနောက်ဥရောပနိုင်ငံဆိုတာထက် အီရန်တို့၊ တရုတ် တို့လိုနိုင်ငံတွေနဲ့ ပိုမိုနီးစပ်သွားမှာပါ။ တရုတ်နိုင်ငံမှာတောင်မှ ဒီလိုပြင်းထန်တဲ့ ဥပဒေမျိုး မထုတ်သေးပါဘူး။

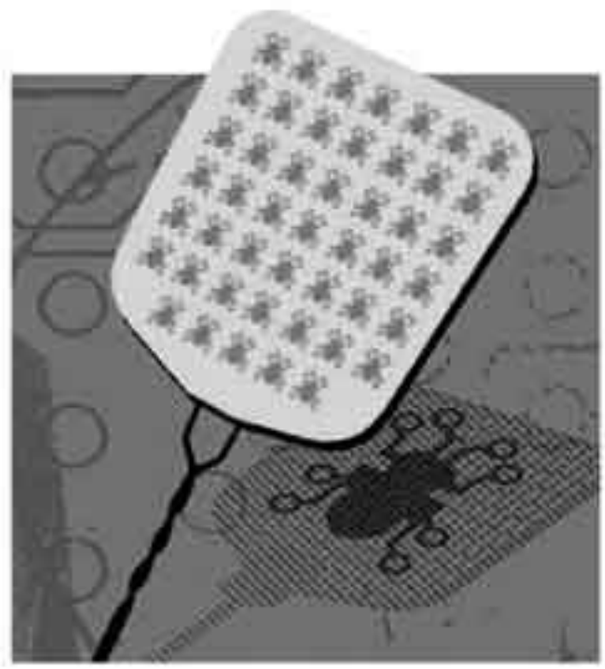
Bugs & Fixes

Adobe သုံးစွဲသူတွေရဲ့ identity တွေက စိုးရိမ်ရတဲ့ အခြေအနေဖြစ်နေပါတယ်။ Google ကတော့ သူ့ရဲ့ Chrome browser အတွက် update ၇ ခုကို ထုတ်ပေးခဲ့ပါတယ်။

Adobe က ColdFusion နဲ့ Live Cycle အပါအဝင် product တွေအတွက် ပြင်ဆင်မှုတွေကို ထုတ်ပေးခဲ့ပါတယ်။ Google ကလည်း အားနည်းချက်အများအပြားကို ပြင်ဆင်နိုင်ဖို့ Chrome ကို update လုပ်ခဲ့ပါတယ်။

Adobe ရဲ့ အပေါက်ပေါင်းများစွာ

Acrobat ၊ BlazeDS ၊ ColdFusion ၊ Flash Player ၊ Live Cycle ၊ Reader နဲ့ Shockwave player တွေမှာရှိတဲ့ ယိုပေါက်တွေအတွက် update ၆ ခု ထုတ်ပေးခဲ့ပါတယ်။ Adobe က Flash Player 10.3.181.16 နဲ့ အစောပိုင်း version တွေ (Windows ၊ Macintosh ၊ Linux နဲ့ Solaris တွေအတွက်) နဲ့ flash player 10.3.185.22 (For Android) တွေမှာရှိတဲ့ CVE-2011-2107 addresses ယိုပေါက်တွေကို important အဆင့် သတ်မှတ်ထားပါတယ်။



တကယ်လို့ ကိုယ်က malicious site တစ်ခုကို ရောက်ရှိသွားရင် attacker က ကိုယ့်ကို အလွယ်တကူ hack နိုင်ပါတယ်။ ပြင်ဆင်မှုတွေထဲမှာ 10.3.181.22 (Windows ၊ Macintosh ၊ Linux နဲ့ Solaris တွေအတွက်) ၊ ဒါမှမဟုတ် Android နဲ့ ActiveX အတွက် 10.3.185.23 version တွေကို update လုပ်ဖို့ ပါဝင်ပါတယ်။

ColdFusion 9.01 နဲ့အစောပိုင်း version တွေ(Windows ၊ Macintosh နဲ့ Unix တွေအတွက်) အတွက် အလားတူ ပြဿနာမျိုးကိုလည်း ပြင်ဆင်ပေးခဲ့ပါတယ်။ ပြီးတော့ Reader 10.0.1 နဲ့ အရင် version တွေ (Windows) နဲ့ Reader 10.0.3 နဲ့ အထက် (Mac) တွေမှာရှိတဲ့ critical flaw တွေကိုလည်း ပြင်ဆင်ပေးခဲ့ပါတယ်။

Shorkwave Player 11.5.9.620 နဲ့ အရင် version (windows နဲ့ Mac အတွက်) တွေမှာပါတဲ့ ယိုပေါက်တွေအတွက်လည်း ပြင်ဆင်မှုတွေထုတ်ပေးခဲ့ပါတယ်။ Adobe Reader user တွေကတော့ Reader X 10.1 ၊ ဒါမှမဟုတ် Reader 9.4.5 ၊ ဒါမှမဟုတ် 8.3 ကို update လုပ်သင့်ပါတယ်။ Shockwave Player အတွက်တော့ 11.6.0. 626 ကို update လုပ်သင့်ပါတယ်။

Chrome ရဲ့ ပြင်ဆင်ချက်

Google က ကိုယ့်ရဲ့ Chrome browser ကို version 12.0.742.112 နဲ့ Adobe Flash Player 10.3.181.34 တို့ကိုပါ update လုပ်ခဲ့ပါတယ်။ Update patch တွေထဲမှာမှ ၆ ခုကို high နဲ့ တစ်ခုကို medium အဆင့်သတ်မှတ်ထားပါတယ်။

Chrome update တွေမှာ memory corruption ၊ string handling ၊ HTML code နဲ့ တခြား အရာတွေအတွက် ပါဝင်ပါတယ်။ အခုလောလောဆယ်မှာတော့ bug နဲ့ ပတ်သက်ပြီး လျှို့ဝှက်ထားပါတယ်။ အသုံးပြုသူအများစု update လုပ်ပြီးတဲ့အချိန်မှာ ထုတ် ဖော်ပြောမှာပါ။ ဒါမှ attacker တွေ သတင်းအချက်အလက်တွေကို အသုံးမချနိုင်မှာဖြစ်ပါတယ်။

ပြင်ဆင်မှုတွေကိုရရှိဖို့ Chrome Web browser နောက်ဆုံး version ကို update လုပ်ပါ။ အသေးစိတ်သိချင်ရင်တော့ *(find.pcworld.com/72042)* ကို ကြည့်နိုင်ပါတယ်။ ■

Browsing ကို ခြေရာခံမှုကနေ ကာကွယ်ပေးမယ့် Tor network

ဒီအခမဲ့ ကွန်ရက်က internet ပေါ်မှာ လျှို့လျှို့ဝှက်ဝှက် နေချင်သူတွေအတွက် အရမ်းကို အဆင်ပြေစေပါတယ်။

ကိုယ်က internet ပေါ်မှာ လျှို့လျှို့ဝှက်ဝှက် ရှိနေတာမဟုတ်ပါဘူး။ ကိုယ့်မှာ နာမည်၊ အကြွေးဝယ် card နံပါတ်နဲ့ တခြား private data တွေကို web မှာ မဖော်ပြဘဲ safe surfing လုပ်တတ်တဲ့ အလေ့ရှိနေရင်တောင်မှ telecom ကုမ္ပဏီတွေနဲ့ search engine တွေက ကိုယ့်ရဲ့ လှုပ်ရှားမှုတွေကို log လုပ်နိုင်နေပါတယ်။ ကျွမ်းကျင်တဲ့ snooper တွေက ဒီ log တွေကနေပြီး IP address နဲ့ ကိုယ်ဘယ်မှာနေတယ်၊ ဘာကြိုက်တယ်ဆိုတာနဲ့ ဘယ်သူတွေနဲ့ ပြောဆိုခဲ့တယ်ဆိုတာ ဖော်ထုတ်နိုင်ပါတယ်။

Web ကို surfing လုပ်တဲ့အခါမှာ တကယ်လုံခြုံမှုရှိဖို့က website နဲ့ exchange လုပ်တဲ့ data တွေကို encrypt လုပ်ပြီး ဝင်လာတဲ့ data တွေကို mask လုပ်တာပါပဲ။ ဒီလိုလုပ်ဖို့ဆိုရင်တော့ Tor network ထဲကို ဝင်လာလိုက်ပါ။ ဒါက အကျိုးအမြတ်မယူတဲ့ Tor project အဖွဲ့နဲ့ internet ကို အခမဲ့ဖြစ်စေ၊ လုံခြုံစေအောင် ထိန်းထိမ်းနေတဲ့ စေတနာရှင်တွေရဲ့ ကမ္ဘာအနှံ့က ကွန်ရက်တွေ သုံးကာ တည်ဆောက်ထားတဲ့ အခမဲ့ server တစ်ခုပါပဲ။

ဒါက webpage တစ်ခုကို load လုပ်တဲ့အခါ ကိုယ့် browser က အဲဒီ page ပေါ်က data ကို request လုပ်ပြီး PC ဆီကို ပြန်လာပါတယ်။ Tor network ရဲ့ server တွေနဲ့ဆိုရင်တော့ ကိုယ့်ရဲ့ request က Tor Network ထဲကို relay လို့ခေါ်တဲ့ ဝင်ပေါက်ကနေ ဝင်သွားတာပါ။ Relay ဆိုတာကတော့ Tor software copy တစ်ခုကို run ထားတဲ့ server တွေပဲဖြစ်ပါတယ်။

ဒါက request တွေကို encrypt လုပ်ပြီး server relay တွေဆီက ကျပန်းအစီအစဉ်အတိုင်း ပို့ပေးပါတယ်။ ဒါက ကိုယ့်ရဲ့ လှုပ်ရှားမှုတွေကို စောင့်ကြည့်နေသူတွေကို ရှောင်ရှားတာ ပါပဲ။

ကိုယ့်ရဲ့လမ်းကြောင်းကို ဖျောက်ထားပါ

ကိုယ့်ရဲ့ request က node တွေကနေပြီး exit relay ကနေ ထွက်သွားပြီးရင် ကိုယ်ဝင်တဲ့ webpage ဆီရောက်သွားမှ decrypt ပြန်လုပ်လိုက်ပါတယ်။ အဲဒီ webpage server က log တွေမှာတောင်မှ အဲဒီ request လုပ်တဲ့ data နဲ့ ကိုယ့် နာမည် သက်ဆိုင်မှုရှိမှာ မဟုတ်ပါဘူး။ ကိုယ့်ရဲ့ တည်နေရာကို နောက်ယောင်ခံဖို့ဆိုရင် ပိုခက်သွားပါပြီ။

Tor က အခမဲ့ပါ။ Hacker တွေ၊ လုံခြုံရေးဂရုပြုသူတွေ အသုံးများပါတယ်။ Tor Network ထဲကို ဝင်ဖို့ Tor browser bundle *(find.pcworld.com/71973)* မှာ download ဆွဲပါ။ ကိုယ်က Tor network ကို သုံးမလား၊ မသုံးဘူးလားဆိုတာကို click တစ်ချက်နဲ့ ဆုံးဖြတ်နိုင်ပါတယ်။

ဒါပေမဲ့ Tor ကနေဝင်တာက အချိန်ကြာပါတယ်။ ကိုယ်က page အသစ်တစ်ခု request လုပ်တိုင်း node တွေ အများကြီးကနေ ဖြတ်သွားရတာကြောင့်ပါ။

ဒီလို ပိတ်ဆို့မှုတွေ သက်သာအောင် ကိုယ့်ရဲ့ ကိုယ်ပိုင် Tor relay တစ်ခုကို run ထားရပါမယ်။ ဒါက ထင်သလောက်လဲ ရှုပ်ထွေးမှု မရှိပါဘူး။ အဲဒီအတွက် ညွှန်ကြားချက်ကို *(find.pcworld.com/71974)* မှာ ကြည့်နိုင်ပါတယ်။ Server relay တစ်ခုကို volunteer လုပ်ပြီး internet ကို အခမဲ့ open ဖြစ်ဖို့ ကူညီနိုင်ပါတယ်။ PW

အောင်မြင့်နိုင်