Security Alert

Computer လုံခြုံရေး တင်းတင်းကျပ်ကျပ် စီမံပေး

Open-source tool တွေကို မှန်မှန်ကန်ကန် ပေါင်းစပ်အသုံးပြုပြီး ကိုယ့်ရဲ့ computer နဲ့ network ကို ကာကွယ်နိုင်တာကြောင့် အရေးကြီးအချက်အလက်တွေအတွက် သိပ်စိုးရိမ်ပူပန်နေစရာ မလိုတော့ပါဘူး။

လူအများစုအတွက်တော့ computer လုံခြုံရေး အကြောင်းနဲ့ ပတ်သက်လာရင် သွားဆရာဝန်ဆီ သွားရသလိုပါပဲ။ မသွားလို့ကလည်း မဖြစ်၊ နာမှာလည်းအသေကြောက်ဆိုတော့ ကြိုက်တာ၊ မကြိုက်တာ အသာထားလို့ မဖြစ်မနေ လုပ်ကို လုပ်ရတဲ့ အလုပ်တစ်ခုပါပဲ။ Computer လုံခြုံရေးနဲ့ပတ်သက်ရင်လည်း မလိုအပ်ဘဲ ငွေကုန်ကြေးကျများပြီး ဦးနှောက်ခြောက်ရတဲ့ အလုပ်ပိုတစ်ခုအဖြစ် ရှုမြင်ကြပါတယ်။ ဒါပေမဲ့ အိမ်မှာပဲ ဖြစ်ဖြစ်၊ ရုံးမှာပဲဖြစ်ဖြစ် ကိုယ့်ရဲ့ computer ကို လုံလုံခြုံခြုံ ထိန်းသိမ်းထားနိုင်တာဟာ ဘဏ်ထဲမှာထည့်ထားတဲ့ ကိုယ့်ရဲ့ ပိုင်ဆိုင်မှုတွေကို စောင့်ရှောက်နေတာနဲ့ အတူတူပဲလို့ ယူဆနိုင်ပါတယ်။ သတင်းကောင်းတစ်ခုကတော့ တစ်ကိုယ်ရေသုံး computer တွေနဲ့ အသေးစား network တွေအတွက် အခမဲ့ download ဆွဲချလို့ရတဲ့ open-source software တွေ အများကြီးရှိနေတာပဲဖြစ်ပါတယ်။

လုံခြုံရေးစည်းကို ကာကွယ်ပါ

Firewall ဆိုတာကတော့ network တွေအတွက် မရှိမဖြစ် လိုအပ်ချက်တစ်ခုပါ။ သူ့ကို သုံးလိုက်ခြင်းအားဖြင့် လုံခြုံရေးနယ်မြေတစ်ခု သတ်မှတ်လိုက်သလိုပါပဲ။ အသုံးမလိုတော့လို့ ဗီရိုထဲထည့်သိမ်းထားတဲ့ Pentium computer အဟောင်းလေးကို ဖုန်ခါလိုက်ရင် firewall အတွက် အသုံးပြုစရာ server တစ်လုံး ဖြစ်လာနိုင်ပါတယ်။

SmoothWall Express (smootwall.org) ဟာ Linux အပေါ်မှာ အခြေခံပြီး တည်ဆောက်ထားတဲ့ open-source firewall တစ်ခုဖြစ်ပါတယ်။ အဆင့်မြင့်မွမ်းမံမှုတွေနဲ့ ပြည့်စုံလုတဲ့ ဒီ software လေးဟာ Pentium အမျိုးအစား PC အစုတ်လေးပေါ်မှာ memory 128MB လောက်နဲ့ ကောင်းကောင်းအလုပ်လုပ်နိုင်ပါတယ်။ လွယ်ကူရှင်းလင်းတဲ့ design ကြောင့် Linux အကြောင်း လုံးဝမကြားဖူးတဲ့ သာမန် အိမ်သုံးသမားတွေတောင်မှ အေးအေးဆေးဆေး အသုံးပြုနိုင်မှာပါ။ ဒီနေ့ခေတ်ရဲ့ software တွေ သုံးလို့မရတော့တဲ့ ဒိတ်အောက် computer တစ်လုံးပေါ်မှာ install လုပ်ထားပြီး browser လေးထဲက သေသပ်ခန့်ညားလှတဲ့ web interface ကနေတစ်ဆင့် လိုအပ်တဲ့ configuration တွေ လုပ်နိုင်ပါတယ်။ Smoothwall Express ဟာ local network တွေ၊ wireless network တွေ သာမက web server တွေအတွက်သုံးတဲ့ DMZ network တွေမှာပါ အသုံးပြုနိုင်ပါတယ်။ Firewall တစ်ခုရဲ့ အခြေခံလုပ်ငန်းတွေဖြစ်တဲ့ port forwarding ၊ outbound filtering ၊

bad-IP-address blocking တွေအပြင် စီးပွားဖြစ် ထုတ်လုပ်ရောင်းချနေတဲ့ နာမည်ကြီး firewall တွေမှာသာပါတဲ့ quality-of-service (QoS) ၊ network traffic statistics တွေ အထိ ပါဝင်ပါတယ်။

လုံခြုံရေးသတိ အမြဲရှိပါ

Network လုံခြုံရေးအတွင်းစည်းထဲမှာ အပြန်အလှန်ဖြတ်သန်းသွားလာနေကြတဲ့ traffic တွေထဲမှာ သံသယဖြစ်စရာ တစ်စုံတစ်ခုတွေ့လေမလားလို့ အမြဲမပြတ် သတိထားကြည့်ရှုနေသင့်ပါတယ်။

ထိုးဖောက်ဝင်ရောက်မှုတွေကို ကာကွယ် တားဆီးနိုင်တဲ့ နည်းပညာမျိုးမှာတော့ Snort (snort.org) က အားကိုးရပါတယ်။ Antivirus မှာ အသုံးပြုတဲ့ virus software တွေရဲ့ လုပ်နည်းလုပ်ဟန်တွေကို မှတ်တမ်းတင်ထားတဲ့ လူဆိုးစာရင်းကို အခြေခံထားသလို သံသယဖြစ်ဖွယ် လုပ်ဆောင်ချက်တွေကို စောင့်ကြည့်ထောက်လှမ်းတဲ့ နည်းပညာကိုပါ ထည့်သွင်းပေါင်းစပ်ထားတဲ့ Snort ကို လူပေါင်း ၃၀၀,၀၀၀ အသုံးပြုနေကြပါပြီ။ ဒါဟာ ထိုးဖောက်ဝင်ရောက်မှုတွေကို ကာကွယ်တားဆီးတဲ့ နည်းပညာဖြစ်တဲ့ intrusion detection or intrusion prevention system (IDS/IPS) ကို အသုံးပြုနေကြတဲ့ အများဆုံး အရေအတွက်တစ်ခုဖြစ်ပြီး Linux ပေါ်မှာသာမက Windows ပေါ်မှာပါ သုံးလို့ရပါတယ်။

တိုက်ခိုက်မှုတွေ နည်းပညာမြင့်မားလာတဲ့အမျှ Snort ရဲ့ ကာကွယ်တားဆီးရေး နည်းပညာတွေကလည်း မြင့်မားလာရပါတယ်။ သုံးစွဲသူအရေအတွက် များပြားသလောက် အချင်းချင်းအပြန်အလှန် ပံ့ပိုးကူညီမှုတွေ ပြုလုပ်နေကြတာမို့ နည်းပညာတွေက အချိန်နဲ့ တပြေးညီဖြစ်နေရုံသာမက အကူအညီတွေကလည်း အလျှံပယ်ပါပဲ။ Snort ကို ဘယ်လို computer မျိုးပေါ်မှာမဆို အသုံးပြုနိုင်သလို Smoothwall firewall ပေါ်မှာပါ တစ်ခါတည်းတွဲပြီး အသုံးပြုနိုင်ပါတယ်။ Shoothwall မှာ ပါလာတဲ့ IDS က Snort ရဲ့ up to date rule တွေကို အသုံးပြုသွားမှာမို့ သီးခြား install လုပ်စရာ မလိုတော့ပါဘူး။

Computer ကို စောင့်ရှောက်ပါ

Firewall တွေ၊ IDS တွေ ဘယ်လောက်ပဲ အပြည့်အစုံတင်ထားပေမယ့် computer ပေါ်မှာတော့ antimalware ကိုလည်း မေ့ထားလို့ မရပါဘူး။ ပြီးခဲ့တဲ့နှစ်တုန်းက Microsoft ရဲ့ Security Essentials ထွက်လာခဲ့တဲ့အပြင် computer ၁၀ လုံးအထိ အခမဲ့သုံးစွဲခွင့်ပြုထားတာမို့ လုပ်ငန်းငယ်သမားတွေအတွက် အဆင်ပြေခဲ့ပါတယ်။ *(find.pcworld.com/71620)* တစ်ကိုယ်ရေတစ်ကာယ သုံးစွဲသူတွေအတွက်တော့ Microsoft Update Service မှာ ရရှိနိုင်ပါတယ်။ *(find.pcworld.com/71621)*

Online ပေါ်က credit card သူခိုးစျေးကွက် အဖမ်းခံရ

ဇြတိန်ရဲတပ်ဖွဲ့က လူ ၄ ဦးကို internet ပေါ်မှာ credit card သူခိုးစျေးဖွင့်မှုနဲ့ ထောင်ဒဏ်အသီးသီးချမှတ်လိုက်ပါတယ်။ အင်္ဂလိပ်ဘာသာစကားနဲ့ အရောင်းအဝယ်ပြုလုပ်နိုင်တဲ့ ဒီ website ဟာ အကြီးဆုံးဖြစ်ပြီး တစ်စုံတစ်ယောက်ရဲ့ computer ထဲကို ထိုးဖောက်ဝင်ရောက်ပြီး credit card နံပါတ်တွေကို ခိုးယူနိုင်တဲ့ software တွေလည်း ပံ့ပိုးပေးနေတယ်လို့ ဆိုပါတယ်။

တရားခံတွေဖွင့်ထားတဲ့ GhostMarket forum မှာ အသင်းဝင်ပေါင်း ၈,၀၀၀ ကျော်ရှိနေပြီး Zeus online banking malware လို online ကနေ bank account ခိုးနည်း၊ crystal meth လုပ်နည်း၊ ဗုံးလုပ်နည်းစတဲ့ တရားမဝင် နည်းပညာတွေကိုပါ ရောင်းချနေတယ်လို့ ရဲတပ်ဖွဲ့ကပြောပါတယ်။

အုပ်စုခေါင်းဆောင် Nicholas Webber ၁၉ နှစ်နဲ့ Gary Paul Kelly ၂၁ နှစ်တို့က ထောင်ဒဏ် ၅ နှစ်စီ အပြစ်ပေးခံရပြီး ကျန်တဲ့ ၂ ယောက်ကတော့ ၄ နှစ်တစ်ယောက်နဲ့ ၁၈ လ တစ်ယောက် အသီးသီး အပြစ်ဒဏ်ပေးခံခဲ့ရပါတယ်။ စွယ်စုံရဒုစရိုက် website ကြီးဖြစ်တဲ့ GhostMarket မှာ PIN နံပါတ်တွေ၊ PayPal account တွေနဲ့ password တွေ၊ လူမှုဖုံလုံရေးနံပါတ်တွေ၊ malware တွေ၊ အယောင်ဆောင်နည်းတွေ၊ botnet တွေ၊ ရဲတပ်ဖွဲ့ရဲ့ ခြေရာခံမှုကို ရှောင်တိမ်းနည်း tutorial

Password တွေလည်း လုံခြုံမှုအပြည့်ရှိပါစေ

ရုံးမှာ password policy ကောင်းကောင်းရှိပါသလား။ မရှိသေးဘူးဆိုရင်တော့ စဉ်းစားဖို့ အချိန်တန်ပါပြီ။ Password policy ရဲ့ လျှို့ဝှက်ချက်က စာရွက်ပေါ်မှာ ဘယ်လိုပဲ ကောင်းအောင်ရေးထားပေမယ့် လက်တွေ့ကျင့်သုံးမှုအားနည်းရင် အလကားပါပဲ။ သုံးစွဲသူတွေ အလွယ်တကူပေးထားတဲ့ password တွေဟာ network ကြီးတစ်ခုလုံးရဲ့ လုံခြုံရေးအတွက် ဘယ်လောက်အထိ ဆိုးဆိုးရွားရွား ထိခိုက်နေရတယ်ဆိုတာကို လက်တွေ့ လေ့လာကြည့်သင့်ပါတယ်။

Cracking tool တွေဖြစ်တဲ့ John the Ripper *(find.pcworld.com/71690)* နဲ့ Cain and Abel *(find.pcworld.com/71622)* တို့ဟာ အဘိဓာန်ကို အသုံးပြုတဲ့နည်း၊ brute force နည်းနဲ့ ၂ မျိုးပေါင်းနည်းတွေကို အသုံးပြုပြီး password တွေကို crack လုပ်ကြပါတယ်။

အဘိဓာန်ကို အသုံးပြုတဲ့နည်းဟာ အဘိဓာန်ထဲမှာပါသမျှ စကားလုံးအားလုံးကို database ထဲကနေ ဆွဲထုတ်ပြီး password ဟုတ်၊ မဟုတ် စစ်ဆေးပါတယ်။ Brute force နည်းကတော့ keyboard ပေါ်မှာပါတဲ့ အက္ခရာစာလုံးတိုင်းကို ဖြစ်နိုင်သမျှနည်းလမ်းတွေနဲ့ တွဲဖက် ပေါင်းစပ်ပြီး password ဟုတ်၊ မဟုတ် စစ်ဆေးပါတယ်။ ၂ မျိုးပေါင်းနည်းကတော့ အဘိဓာန်ထဲမှာပါတဲ့ စကားလုံးကို keyboard ပေါ်မှာပါတဲ့ အက္ခရာစာလုံးတွေနဲ့ တွဲဖက်ပေါင်းစပ်ပြီး password ဟုတ်၊ မဟုတ် စစ်ဆေးတဲ့အတွက်ကြောင့် "p@ssw0rd" လိုမျိုးကို အလွယ်တကူ ဖော်ထုတ်နိုင်ပါတယ်။ ဒီလိုမျိုး cracking tool တွေကို သုံးပြီး ကိုယ့် password ရဲ့ လုံခြုံမှုအဆင့်ကို ဆန်းစစ်ပြီး လိုအပ်သလို မြှင့်တင်နိုင်ပါတယ်။

အရေးပေါ်အခြေအနေအတွက် အသင့်ပြင်ထားပါ

Network နဲ့ computer တွေရဲ့ လုံခြုံရေးကို အစဉ်အမြဲထိန်းသိမ်းထားနိုင်ဖို့ ဘယ်နေရာမှာ အားနည်းချက် ရှိနေသလဲဆိုတာ သိနေဖို့လိုအပ်ပါတယ်။ အားနည်းချက်ရှာဖွေတဲ့ နည်းပညာတစ်ခုဖြစ်တဲ့ Open VAS *(find.pcworld.com/71624)* ဟာ open-source software တစ်ခုဖြစ်ပြီး နာမည်ကြီးလှတဲ့ Nessus 2 engine ပေါ်မှာ တည်ဆောက်ထားပါတယ်။ အိမ်သုံးတွေအတွက်ကတော့ Microsoft က အခမဲ့ဖြန့်ချိထားတဲ့ Baseline Security Analyzer *(find.pcworld.com/71625)* ကို အသုံးပြုပြီး Windows ပေါ်က အားနည်းချက်တွေနဲ့ လိုအပ်နေတဲ့ security update တွေကို ရှာဖွေစစ်ဆေး ပေးနိုင်ပါတယ်။ Open-source software တွေဟာ ရောင်းတန်းဝင်ပစ္စည်းတွေလို အပေါ်ယံရွေ့မှန်ကြဲထားတာမျိုးမရှိပေမယ့် အရမ်းအသုံးတည့်တယ်ဆိုတာကိုတော့ ဘယ်သူမှ မငြင်းနိုင်ပါဘူး။

တွေ အပြင် ဝင်ရောက်ထိုးဖောက်နိုင်တဲ့ server တွေ၊ website တွေရဲ့ စာရင်းတွေအထိ ပါဝင်တယ်လို့ ရဲတပ်ဖွဲ့က ဆိုပါတယ်။

Online ရာဇဝင်မှ စုံစမ်းထောက်လှမ်းခြင်း

အုပ်စုခေါင်းဆောင် Webber ဟာ GhostMarket forum ရဲ့ site administrator အဖြစ် လုပ်ဆောင်ခဲ့ပြီး အသင်းဝင်အသစ်တွေ လက်ခံရင်းနဲ့ forum ပေါ်မှာတင်သမျှကို edit လုပ်ပေးခဲ့ပါတယ်။ ရဲတပ်ဖွဲ့ရဲ့ online မှူခင်းတပ်ဖွဲ့က ၁၁ လကြာ စောင့်ကြည့်စုံစမ်းမှုတွေ ပြုလုပ်ပြီးတဲ့နောက်မှာ website ကို ပိတ်သိမ်းခဲ့ပါတယ်။ အဲဒီထဲမှာ cedit card နံပါတ်ပေါင်း ၁၃၀,၀၀၀ တွေ့ရှိခဲ့ပါတယ်။

အုပ်စုခေါင်းဆောင် နောက်တစ်ယောက်ဖြစ်တဲ့ Kelly ဟာ သူ့ computer ရဲ့ database ထဲက အချက်အလက်တွေနဲ့ GhostMarket forum ကိုတည်ဆောက်ဖို့ ကူညီပေးခဲ့တယ်လို့ ရဲတပ်ဖွဲ့က ဆိုပါတယ်။ သူတို့နှစ်ယောက်ဟာ ၂၀၀၉ ခုနှစ်တုန်းက လန်ဒန်မြို့ပေါ်ရှိ ကြယ်ငါးပွင့်အဆင့် ဟိုတယ်တစ်ခုရဲ့ အပျံစားအခန်းတွေမှာ ဖိမ်ခံပြီး ခိုးထားတဲ့ credit card တွေနဲ့ ငွေရှင်းတဲ့အခါမှာ အလိမ်ပေါ်သွားလို့ အဖမ်းခံခဲ့ရပါသေးတယ်။

အာမခံနဲ့ ထွက်လာပြီးနောက် Majorca ကို အောက်တိုဘာလလောက်မှာ ထွက်ပြေးခဲ့ပြီး နောက်တော့ ပြန်အဖမ်းခံခဲ့ရတာဖြစ်ပါတယ်။ GhostMarket အဖွဲ့ရဲ့ နောက်ဆက်တွဲ ငွေစာရင်းရှင်းတမ်းကိုတော့ ဆက်လက်လုပ်ဆောင်နေဆဲဖြစ်တယ်လို့သိရပါတယ်။

Smartphone data ခိုးယူခံရခြင်းအန္တရာယ်

သုတေသနပြုချက်တွေအရ smartphone တွေဟာ မသမာသူတွေရဲ့ အဓိကသားကောင်ဖြစ်နေတာကြောင့် ကိုယ့်ရဲ့ data တွေပါမသွားရအောင် ဘယ်လိုကာကွယ်ရမယ်ဆိုတာကို ဆွေးနွေးတင်ပြချင်ပါတယ်။

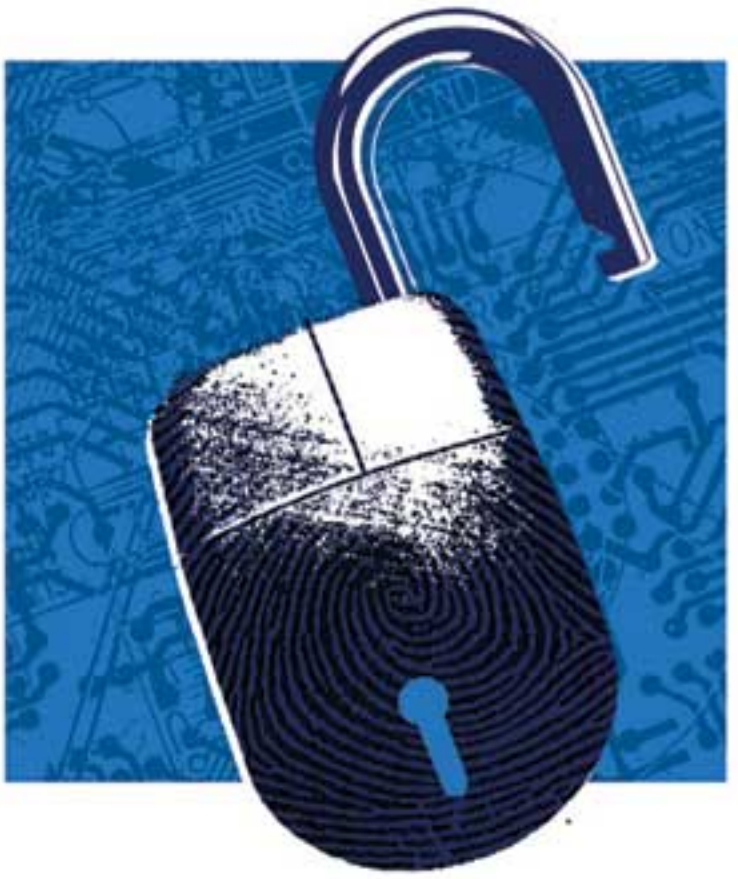
Computer နဲ့ internet ရဲ့ လုံခြုံရေးဆိုင်ရာ သတိပေးချက်တွေကိုတော့ ကြားဖူးနေကြပါတယ်။ ဒါပေမဲ့ smartphone ဆိုရင် ဘယ်လိုလုပ်ရပါ့မလဲ။ လုံခြုံရေးဆိုင်ရာ သုတေသီ Georgia Weidman က ဆွေးနွေးပွဲတစ်ခုမှာ သူ့ရဲ့ Android phone လေးထဲကို botnet လေးတစ်ခုဝင်သွားတာနဲ့ ရှိသမျှ data တွေ အကုန်ပါသွားနိုင်တယ်ဆိုတာကို သရုပ်ပြဆွေးနွေးခဲ့ပါတယ်။ မယုံနိုင်စရာကောင်းလောက်အောင် လွယ်ကူလွန်းလှတာမို့ smartphone သုံးစွဲသူတွေအနေနဲ့ ယုံကြည်စိတ်ချမှုမရှိတဲ့ website တွေကနေ softwre တွေဆွဲချ သုံးစွဲတာမျိုးကို လုံးဝရှောင်ကြဉ်သင့်တယ်လို့ ဆိုပါတယ်။

Smartphone ထဲကို botnet တစ်ကောင်ဝင်နိုင်ဖို့ သုံးစွဲသူကိုယ်တိုင်က file လေးတစ်ခု ဆွဲချဖို့လိုပါမယ်။ အဲဒီထဲမှာ bot လေးကို smartphone ရဲ့ operating system ထဲ ထည့်သွင်းတည်ဆောက်ပေးမယ့် program လေးပါဝင်ပါတယ်။ ဆွဲချမိတဲ့ file ကတော့ software ၊ သီချင်း၊ email attachment အမျိုးမျိုးဖြစ်နိုင်ပါတယ်။ Botnet လေး ဝင်သွားပြီးရင်တော့ မသမာသူ botmaster က data အဝင်အထွက်တွေကို ကြိုက်သလို ချယ်လှယ်နိုင်ရုံမက အထဲမှာ ရှိရှိသမျှအားလုံးကိုပါ အသာလေး 'မ' သွားနိုင်ပါတယ်။ ဒါပေမဲ့ သနားစရာ ပိုင်ရှင်ခမျာမှာတော့ ဘာဆိုဘာမှတောင် သိလိုက်ရမှာ မဟုတ်ပါဘူး။

အလားအလာရှိတဲ့ အန္တရာယ်ကောင် : SMS text messaging

မသမာသူ botmaster က တစ်ခုတစ်ယောက်ရဲ့ smartphone ထဲကို ဝင်သွားပြီဆိုရင် အရင်ဦးဆုံးလုပ်တဲ့ အလုပ်ကတော့ များနိုင်သမျှများများ မျိုးဆက်ပွားတော့တာပါပဲ။ အရင်တုန်းကတော့ smartphone နဲ့ internet အသုံးပြုပြီး botnet တွေကို email attachment တွေအဖြစ် ဖြန့်ဝေကြပါတယ်။ အခု တော့ SMS ကို အစားထိုးသုံးစွဲလာကြပါပြီလို့ သုတေသီ Weidman က ဆိုပါတယ်။ ဒီလို SMS ကို အသုံးပြုပြီး ဖြန့်ဝေရတာဟာ modem သုံးပြီး internet ကနေ ဖြန့်ရတာထက် battery အစားသက်သာပြီး ပိုပြီး သပ်သပ်ရပ်ရပ်နဲ့ အဆင့်အတန်းလည်းမြင့်တယ်လို့ သူကပြောပါတယ်။

Text message တွေနဲ့ အတူ botnet တွေကို smartphone ပိုင်ရှင်ရဲ့ သူငယ်ချင်းတွေဆီ ပေးပို့ရတာ တိုက်ခိုက်မှု စစ်မျက်နှာသစ် ဖွင့်လိုက်သလိုပါပဲ။လုံခြုံရေးနည်းပညာရှင်



တွေဖြစ်ကြတဲ့ Symantec နဲ့ Lookout တို့က Android နဲ့ iOS တို့အတွက် SMS ကနေတစ်ဆင့် ကူးစက်ခံရတဲ့ malware ကာကွယ်တားဆီးနိုင်မှုနှုန်းရေး လုပ်ငန်းစဉ်တွေကို လုပ်ဆောင်ခဲ့ပေမယ့်လည်း တိုက်ခိုက်မှုပုံစံပြောင်းလဲတာတွေက မြန်ဆန်လွန်းလို့ လိုက်မမီနိုင်အောင် ဖြစ်နေရပါတယ်။ ပိုဆိုးတာက security application အများစုဟာ smartphone ပေါ်မှာ တင်ထားတဲ့ software တွေကိုပဲ scan လုပ်နိုင်ပါတယ်။ Phone ရဲ့ operating system ထဲမှာ ဝင်ပုန်းနေတဲ့ botnet လို အရာမျိုး

ကိုတော့ ထောက်လှမ်းနိုင်စွမ်းမရှိပါဘူး။

Weidman ရဲ့ အဆိုအရတော့ Android ပေါ်မှာသာမက ဘယ်လို smartphone ပေါ်မှာမဆို ရှိနေတဲ့ data တွေ အခိုးမခံရအောင်၊ botnet တွေ အသွင်းမခံရအောင် ကာကွယ်နိုင်တဲ့ တစ်ခုတည်းသောနည်းလမ်းက computer တွေ၊ laptop တွေမှာ လိုက်နာရတဲ့ လုံခြုံရေးစည်းကမ်းအတိုင်း လိုက်နာကျင့်ကြံတာပဲဖြစ်ပါတယ်။ သံသယဖြစ်စရာကောင်းတဲ့ file တွေ၊ software တွေကို မသုံးဖို့၊ SMS တွေထဲမှာပါလာတဲ့ file တွေကို သူငယ်ချင်းဆီကဖြစ်နေရင်တောင်မှ သေချာအောင် စုံစမ်းပြီးမှ ဖွင့်ကြည့်ဖို့လိုပါတယ်။ ကိုယ့်ရဲ့ phone ထဲကို သွင်းလိုက်တဲ့ software တိုင်းမှာ အန္တရာယ်ကောင်တွေ ပါလာနိုင်တယ်ဆိုတာ အမြဲနှလုံးသွင်းထားဖို့လည်း လိုပါတယ်။

Bugs & Fixes

Google Chrome ရဲ့ အမှားပြင်ဆင်ချက်နဲ့အတူ Microsoft ရဲ့ Windows၊ IE နဲ့ Office ထဲက အမှားပြင်ဆင်ချက်ပေါင်း ၂၂ ခု ရှိခဲ့ပါတယ်။

Chrome browser ရဲ့ လုံခြုံရေးအတွက် အဓိကကျတဲ့ "Sandbox" ထဲမှာ အားနည်းချက်တွေရှိနေတဲ့အတွက် အမှားပြင်ဆင်ချက်တွေကို google က ထုတ်ပြန်လိုက်ပါတယ်။ တစ်ချိန်ထဲမှာပဲ Microsoft ကလည်း Windows ရဲ့ အမှားပြင်ဆင်ချက်တွေ တစ်လေ့ကြီးကို ထုတ်ပြန်လိုက်ပါတယ်။

Chrome အတွက် လုံခြုံရေးပိုင်းဆိုင်ရာ ပြင်ဆင်ချက်

နာမည်ကြီး Google Chrome မှာရှိနေတဲ့ လုံခြုံရေးပိုင်းဆိုင်ရာ အားနည်းချက် ၉ ခုကို google က ပြင်ဆင်ချက်တွေ ထုတ်ပြန်လိုက်ပါတယ်။ တွေ့ရှိခဲ့တဲ့ ၉ ခုထဲမှာ လုံခြုံရေး ထိခိုက်မှုအဆင့် သတ်မှတ်ချက်အဖြစ် တစ်ခုကို critical အဆင့်၊ ၂ ခုကို high အဆင့် နဲ့ ၆ ခုကို low အဆင့်သတ်မှတ်ခဲ့ပါတယ်။ အဲဒီထဲမှာ webpage တွေနဲ့ plug-in တွေကို malware တွေ ကူးစက်မခံရအောင် ကာကွယ်ပေးဖို့ အထူးစီမံထားတဲ့ Sandbox feature ထဲမှာရှိနေတဲ့ အားနည်းချက်လည်း ပါဝင်ပါတယ်။

ဒီပြင်ဆင်ချက်တွေကို install လုပ်ချင်ရင် Chrome ထဲကနေပြီး Option>>About Google Chrome ကို သွားလိုက်ရင် google server တွေဆီကို အလိုအလျောက် ချိတ်ဆက်ပြီးတော့ update ဖြစ်၊ မဖြစ်စစ်ဆေးပေး ပါလိမ့်မယ်။ မလုပ်ရသေးဘူးဆိုရင် update now ကို နှိပ်လိုက်ရုံပါပဲ။ အသေးစိတ် သိချင်ရင်တော့ *find. pcworld. com/71597* နဲ့ *find.pcworld. com/71598* မှာ ကြည့်နိုင်ပါတယ်။

Microsoft ရဲ့ အမှားပြင်ဆင်ချက် ၂၂ ခု

"Patch Tuesday" လို့ အမည်ပေးထားတဲ့ လစဉ် ထုတ်ပြန်နေကျ အမှားပြင်ဆင်ချက်တွေကို ဖေဖော်ဝါရီလတုန်းက လုံခြုံရေးပိုင်းဆိုင်ရာ ကြေညာချက် ၁၂ ခုနဲ့အတူ ထုတ်ပြန်ခဲ့ပါတယ်။ အဲဒီထဲမှာ Windows၊ Internet Explorer၊ Office

၊ Internet Information Service (IIS) မှာရှိနေတဲ့ လုံခြုံရေးပိုင်းဆိုင်ရာ အားနည်းချက် ၂၂ ခုအတွက် အမှားပြင်ဆင်ချက်တွေ ပါဝင်ပါတယ်။

လုံခြုံရေးပိုင်းဆိုင်ရာ ထိခိုက်မှု အဆင့်သတ်မှတ်ချက်ဖြစ်တဲ့ critical အဆင့် ၃ ခုနဲ့ important အဆင့် ၉ ခု ပါဝင်ပါတယ်။ ကြေညာချက် MS11-003 *(find.pcworld. com/71613)* ၊ MS11-006 (find.pcworld. com/71614) နဲ့ MS11-007 *(find. pcworld.com/71615)* တို့ကို critical အဆင့် သတ်မှတ်ထားပြီး Internet Explorer 6 ၊ 7 ၊ 8 နဲ့ Windows XP တို့မှာ ရှိနေတဲ့ အားနည်းချက်တွေဖြစ်ပါတယ်။

Critical အဆင့်သတ်မှတ်ထားတဲ့ အားနည်းချက်တွေရှိနေတဲ့ computer တွေကို မသမာသူတွေက online ကနေတစ်ဆင့် ထိုးဖောက်ဝင်ရောက်နိုင်ကြပါတယ်။ Internet စာမျက်နှာပေါ်က သမားရိုးကျ HTML file လေးကို ဝင်ကြည့်မိလိုက်တာမျိုး၊ ဓာတ်ပုံလေးတစ်ခု ကြည့်မိလိုက်တာမျိုး၊ font လေးတစ်ခု ဆွဲချပြီး အသုံးပြုလိုက်မိတာမျိုး စတဲ့ နေ့စဉ်ပုံမှန်လုပ်ကိုင်နေကျ အပြုအမူမျိုးတွေကနေတစ်ဆင့် computer ထဲကို program လေးတစ်ခု အလိုအလျောက်ဝင်ရောက်သွားပြီး မသမာသူတွေက online ကနေတစ်ဆင့် အလိုရှိသလို ထိန်းချုပ်မောင်းနှင်နိုင်စွမ်း ရရှိသွားနိုင်ပါတယ်။

Important အဆင့်ရှိတဲ့ အားနည်းချက်တွေရှိနေတဲ့ computer တွေကတော့ ပုံမှန် အလုပ်မလုပ်တော့တာမျိုး၊ online progaram တစ်ခုက လှမ်းသုံးခံရတာမျိုး၊ computer ထဲက အချက်အလက်တွေ နှိုက်ထုတ်ခံရတာမျိုး၊ သုံးစွဲခွင့် ပိတ်ပင်ခံရတာမျိုးတွေ ဖြစ်နိုင်ပါတယ်။ Computer လုံခြုံရေးပိုင်းဆိုင်ရာ သုတေသီတစ်ဦးဖြစ်တဲ့ Cupidon-3005 လို့ အမည်တပ်ထားသူတစ်ယောက်က မသမာသူတစ်ယောက်အနေနဲ့ ဘယ်နည်း၊ ဘယ်ပုံ ထိုးဖောက်ဝင်ရောက်နိုင်တယ်ဆိုတာကို ရှာဖွေဖော်ထုတ်ထားပါတယ်။ အသေးစိတ်ကိုတော့ *find. pcworld.com/7616* မှာ တင်ထားပါတယ်။

Microsoft က တော့ စုံစမ်းစစ်ဆေးနေပါတယ်လို့ပဲ တုံ့ပြန်ထားပြီး ဘာမှအကြောင်းမထူးသေးပါဘူး။ ကိုယ့်ရဲ့ computer ကို တိုက်ခိုက်မခံရဖို့တော့ Windows update ကိုသာ မှန်မှန်လုပ်ဖို့ပဲ လိုပါတယ်။ ဘယ်လိုဆွဲချရမယ်၊ ဘယ်နည်း၊ ဘယ်ပုံ လုပ်ရမယ်ဆိုတာတွေကိုတော့ *find. pcworld. com/71617* နဲ့ *find. pcworld.com.71618* မှာ အသေးစိတ် ဖော်ပြထားပါတယ်။

သန်းဝင်း BE (Electronics)

KMD ရဲ့ ပညာသင်ဆုများ

၂၀၁၁ တက္ကသိုလ်ဝင်တန်း စာမေးပွဲဖြေဆိုအောင်မြင်ပြီးတဲ့ ကျောင်းသား၊ ကျောင်းသူတွေအတွက် KMD မှ ဖွင့်လှစ်တဲ့ အင်္ဂလန်နိုင်ငံရဲ့ ပထမနှစ် computer diploma သင်တန်းကို တက်ရောက်ရင် scholarship တွေ ပေးသွားမှာဖြစ်တယ်လို့ သိရပါတယ်။ Scholarship အစီအစဉ်မှာ ၅ ဘာသာနဲ့ အထက် ဂုဏ်ထူးပါတဲ့ ကျောင်းသား၊ ကျောင်းသူတွေကို သင်တန်းကြေးကင်းလွတ်ခွင့် ၁၀၀ ရာခိုင်နှုန်းပေးသွားမှာဖြစ်ပြီး ၄ ဘာသာဂုဏ်ထူးပါတဲ့ ကျောင်းသား၊ ကျောင်းသူတွေကို သင်တန်းကြေးကင်းလွတ်ခွင့် ၄၀ ရာခိုင်နှုန်း၊ တစ်ဘာသာ၊ ဒါမှမဟုတ် ၂ ဘာသာဂုဏ်ထူးပါတဲ့ ကျောင်းသား၊ ကျောင်းသူတွေကို သင်တန်းကြေးကင်းလွတ်ခွင့် ၂၀ ရာခိုင်နှုန်း ပေးအပ်သွားမှာဖြစ်တယ်လို့ သိရှိရပါတယ်။

အဲဒီ ပထမနှစ် diploma သင်တန်းဟာ တစ်နှစ်ခန့်ကြာမြင့်မှာဖြစ်ပြီး ထူးထူးချွန်ချွန် အောင်မြင်ခဲ့ရင် ဒုတိယနှစ် diploma သင်တန်းကို တက်ရောက်ဖို့ သင်တန်းကြေး ကင်းလွတ်ခွင့် ၊ ဒုတိယနှစ်မှာ ထူးချွန်အောင်မြင်ခဲ့ရင် အင်္ဂလန်နိုင်ငံရဲ့ နောက်ဆုံးနှစ် computer ဘွဲ့သင်တန်းတက်ရောက်ဖို့ သင်တန်းကြေးကင်းလွတ်ခွင့်တွေ ရရှိဦးမှာ ဖြစ်တယ်လို့လည်း သိရပါတယ်။

ပထမနှစ် diploma ရရှိပြီးတဲ့သူဟာ Junior programmer ၊ Software engineer ၊ Database Design ၊ Web developer အဖြစ် ၊ ဒုတိယနှစ် diploma ရပြီးသူက Software engineer ၊ Project manager ၊ System analyst တစ်ယောက်အဖြစ် ၊ ဘွဲ့ရရှိပြီးရင် Database administrator ၊ Network engineer ၊ System Executive အဖြစ် အသက်မွေးဝမ်းကျောင်းပြုနိုင်မှာဖြစ်တယ်လို့သိရပါတယ်။

အသေးစိတ် သိချင်ရင်တော့ KMD Computer Centre၊ ဖုန်း - ၃၈၁၀၃၅ ၊ ၃၈၁၇၇၆ ၊ ၃၈၁၁၂၉ ၊ ၅၀၂၂၃၃ ၊ ၃၉၇၉၄၄ နဲ့ ၃၉၇၉၄၅ တို့ကို ဆက်သွယ်စုံစမ်းနိုင်တယ်လို့ သိရပါတယ်။