
M.E.H.N
အတွဲ ၁ ၊ အမှတ် ၃
ဩဂုတ်လ ၂၀၁၆ ခုနှစ်
One Year
Anniversary

# Contents

# ကျေးဇူးတင်လွှာ

MEHN ကို တစ်စိုက်မတ်မတ် အားပေးကြသော စာချစ်သူ ပရိသတ်များကို ဦးစွာပထမ ကျန်းမာ ချမ်းသာပါစေကြောင်း ဆုတောင်း မေတ္တာပို့သအပ်ပါတယ်။ MEHN မှ စာချစ်သူများအတွက် ဆိုက်ဘာ နည်းပညာနှင့် ပတ်သက်သော သတင်းများကို အချိန်နှင့် တပြေးညီ သိရှိနိုင်စေရန်အတွက် စဉ်ဆက်မပြတ် အားသွန်ခွန်စိုက် တင်ဆက်ပေးလျက်ရှိပါတယ်။ ဆိုက်ဘာသတင်းများအပြင် စာချစ်သူတို့အတွက် ဗဟုသုတတိုးပွားစေမည့် ဆောင်းပါးများ ၊ Software လမ်းညွှန်များ နှင့် Tutorials များ ကိုလည်း ဖော်ပြပေးလျက်ရှိပါတယ်။ တိုက်ခိုက်မှုများသည် နေ့စဉ်နှင့် အမျှ ဖြစ်ပွားလျက်ရှိပါတယ်။ တိုက်ခိုက်မည့် သူများကလည်း လက်တကမ်းတွင်ရှိပြီး တိုက်ခိုက်မည့် သားကောင်ကို အမြဲရှာဖွေနေလေ့ရှိပါတယ်။ ယနေ့ ခေတ်သည် Information Technology ဟု ခေါ်တွင်သော IT နည်းပညာ ခေတ်ဖြစ်သည်။ အချက်အလက်များသည်လည်း နေ့စဉ် လျှင်မြန်သော အဟုတ်များဖြင့် စီးဆင်းနေလျက်ရှိပါသည်။ ထို့အပြင် အချက်အလက်များဆိုသည်မှာ လူတိုင်းအတွက် အသက်တမျှ အရေးကြီးသော အကြောင်းအရာများဖြစ်သည်။ ထို ကိုယ်ရေးဆိုက်ရာ အချက်အလက်များ ပေါက်ကြားပါက ငွေကြေးထိခိုက်နစ်နာနိုင်ခြင်း ၊ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ ထိခိုက်နစ်နာနိုင်ခြင်း စသည့် ကြီးမားသော အန္တရာယ်များဖြင့် ရင်ဆိုင်ရမည် ဖြစ်သည်။ ထို့ကြောင့် အချက်အလက်များ ကာကွယ်ရေး လုပ်ငန်းစဉ်များသည် အမှန်တကယ် အလွန်ပင်အရေးကြီးသော ကိစ္စရပ်များဖြစ်သည်။ ကာကွယ်နည်းများကို သိရှိနိုင်ရန်အတွက် IT နည်းပညာများနှင့် ပတ်သက်သော စာပေများကို ဖတ်ရှု့လေ့လာသင့်ပေသည်။ MEHN အနေဖြင့် စာချစ်သူတို့၏ အကျိုးကို အစဉ်အမြဲ လိုလားပြီး တိုက်ခိုက်ခြင်း မခံရစေရန်အတွက် သတင်းဆောင်းပါးများတွင် ကာကွယ်နည်းများ ဆောင်ရန် ရှောင်ရန်များ စသည့် အချက်များကို အမြဲလေးပေးကာ ဂရုပြု ဖော်ပြပေးလျက်ရှိပါသည်။ MEHN သတင်းများကို ဖတ်ရှု့ခြင်းအားဖြင့် နည်းပညာ ဗဟုသုတများစွာရရှိပြီး တိုက်ခိုက်သူများ၏ တိုက်ခိုက်ခြင်းရန်မှ ရှောင်ရှားစေနိုင်မှာ ဖြစ်ပါတယ်။ MEHN ဝိုင်းတော်သားများအနေဖြင့် စာချစ်သူ ပရိသတ်ကြီးအတွက် ဆထက်ထမ်းပိုး ပိုမိုကြိုးစားပြီး နည်းပညာသတင်းများ ၊ ဆောင်းပါးများနှင့် Tutorials များကို တင်ဆက်ပေးသွားပါ့မယ်။ စာချစ်သူ ပရိသတ်များအားလုံး ကျန်မာ ချမ်းသာခြင်းဟူသော နှစ်ဖြာသော ချမ်းသာသုခတို့ဖြင့် ပြည့်စုံပြီး လိုအင်ဆန္ဒတွေ ပြည့်ဝပါစေကြောင်း ဆုမွန်ကောင်းတောင်း ပေးလိုက်ပါတယ်.....

ကျေးဇူးတင်စွာဖြင့်
21-9-2016
အယ်ဒီတာချုပ်
ကိုရီချင်

# အယ်ဒီတာ့စကား

စာချစ်သူ အားလုံး မင်္ဂလာအပေါင်းနဲ့ ပြည့်စုံပါစေလို့ ရှေးဦးစွာ ဆုတောင်းပေးပါတယ် ခင်ဗျာ...

ကျွန်တော်တို့ရဲ့ MEHN အဖွဲ့လေး စတင်ဖွဲ့စည်းပြီး စာချစ်သူတို့ထံသို့ နည်းပညာဆိုင်ရာ သတင်းများကို အကောင်းဆုံး တင်ဆက်ပေးခဲ့သည်မှာ အနုဆိုရင် တစ်နှစ်တင်းတင်း ပြည့်ခဲ့ပါပြီ။ ထိုသို့ အောင်မြင်စွာ ရပ်တည်လာနိုင်ခဲ့ခြင်းမှာ စာချစ်သူတို့၏ အားပေးထောက်ပံ့မှု၊ ကျွန်တော်တို့ MEHN အဖွဲ့လေး၏ အချိန်အား၊ ငွေအား၊ လူအား အကုန်အကျခံကာ ကြိုးစားအားထုတ်မှုတို့ကြောင့် ဆိုသည်မှာ ငြင်းနိုင်ဖွယ်ရာ မရှိပေ။ သို့ကြောင့်ပင် စာချစ်သူအားလုံးနှင့် MEHN အဖွဲ့သားအားလုံးအား ကျေးဇူးအထူးတင်ရှိကြောင်း ပြောကြားလိုပါတယ်။ နေ့စဉ်နှင့်အမျှ တိုးတက်ပြောင်းလဲနေသော နည်းပညာအသစ်အဆန်းများ၊ နိုင်ငံတကာဆိုက်ဘာလုံခြုံရေးနှင့် တိုက်ခိုက်မှုပုံစံများ၊ ကွန်ပျူတာ၊အိုင်တီဆိုင်ရာ Tutorial များကိုလည်း ဆက်လက် တင်ဆက်သွားအုံးမှာ ဖြစ်ပါတယ်။ စာချစ်သူတို့၏ အကြံပြုချက်၊ ဆွေးနွေးချက်များရှိပါကလည်း ပို့ပေးနိုင်ပါကြောင်း ပြောကြားရင် ကျွန်တော်တို့ရဲ့ နှစ်ပတ်လည်မြောက် သတင်းလေးများကို ဖတ်ရှုရင်း ဗဟုသုတများစွာ တိုးပွားကြပါစေ ခင်ဗျာ။

26-9-2016
အယ်ဒီတာ
ကိုသိန်း ( MEHN Team )

# MEHN ပိုင်းတော်သားများ၏ ရင်တွင်းဖြစ် စကားများ

Cyber သတင်းတွေ အကျိုးရှိစေတဲ့ ကျူတိုရီရယ်လေးတွေကို စာဖတ်သူတို့ရဲ့လက်ထဲကိုထည့်ပေးခဲ့တဲ့ MEHN ဟာအခုဆို ၁ နှစ်ပြည့်ခဲ့ပါပီ။ စာဖတ်သူတို့ရဲ့ အားပေးမှုကြောင့်သာ အခုထိ တည်ရှိနေနိုင်တာပါ။ နောင်ကိုလည်း စာဖတ်သူတို့အတွက် ကျွန်တော်တို့ဘက်မှ သတင်းများ ကျူတိုများကို ကြိုးစားပြီး ဖော်ပြပေးသွားဦးမှာ ဖြစ်ပါတယ်။ စာဖတ်သူတို့ကလည်း ဆက်လက်ပြီး အားပေးကြပါဦးလို့ ပန်ကြားရင်း MEHN ၁ နှစ်ပြည့်အတွက် အားလုံးရဲ့ ကိုယ်စား တောင်းဆိုလိုက်ပါတယ်။
"Happy Birthday MEHN"

22-9-2016
Algorithm

MEHN အဖွဲ့တစ်ခု ဖြစ်လာရတာ စုပေါင်းမှုအင်အားရဲ့ လမ်းစဘဲဖြစ်ပါတယ်။ စာဖတ်သူတွေ လေ့လာသူတွေရှိလို့လည်း ကျွန်တော်တို့ MEHN က နည်းပညာရပ်ဝန်းထဲမှာ ပညာတွေ မျှဝေခွင့်ရတာပါ။ ကျွန်တော်တို့လည်း သင်ယူလို့မကုန်တဲ့ IT နည်းပညာတွေကို လေ့လာပြီး ပြန်လည်မျှဝေခွင့် ရခဲ့လို့ MEHN အဖွဲ့အနေနဲ့ စာဖတ်သူတွေကို ဝမ်းသာစွာနဲ့ ကျေးဇူးတင်မိပါတယ်။ ယခုခေတ် အခြေအနေက IT နဲ့ပတ်သတ်ပြီး မလေ့လာဘူးဆိုရင် အချိန်ကြာလာတာနဲ့အမျှ ကိုယ်က ဘာမှမသိဘဲ ဖြစ်လာပါလိမ့်မယ်။ IT ပညာလေ့လာဖို့ ငယ်သူ ကြီးသူ မရှိပါဘူး။ သင်ယူရင် လူငယ် လူကြီး မရွေး အားလုံးတတ်မြောက်နိုင်ပါတယ်။ ကျယ်ဝန်းတဲ့ IT နယ်ပယ်မှာ လေ့လာမှုတွေ မလျော့ကျန်ရအောင် IT နှင့် သက်ဆိုင်သော အကြောင်းအရာတွေကို အမြဲတင်ဆက်ပေးနေတဲ့ MEHN Facebook Page သို့မဟုတ် Website ကို ဝင်ရောက်ဖတ်ရှုလေ့လာရင်း စာဖတ်သူအပေါင်း နည်းပညာအသိတွေ တိုးတက်ကြပါစေ။

22-9-2016
ပိုင်လင်

- မလောပါနဲ့
- လှေကားထစ်ကျော်မတတ်ပါနဲ့ ကျော်တတ်ပြီးရင်လည်း ပြန်ပြုတ်မကျစေဖို့ သေချာဂရုစိုက်ပါ
- ကိုယ်ကိုကိုယ် အထင်မကြီးပါနဲ့
- တစ်ဖက်သားကို အထင်မသေးပါနဲ့
- နည်းပညာလောကမှာ အသက်ငယ်တာ ကြီးတာက အဓိကမဟုတ်ပါဘူး လေ့လာမှုအားကသာ အဓိကပါ . .
- သူလေ့လာနေတဲ့ နည်းပညာနယ်ပယ်နဲ့ ကိုယ်လေ့လာနေတဲ့ နည်းပညာနယ်ပယ်ချင်း မပြိုင်ဆိုင်ပါနဲ့ ပညာရပ်တိုင်းက ဆက်စပ်နေပါတယ် . .
- ကမ္ဘာကြီးကျဉ်းတယ်ဆိုတာထက် IT လောကက ပိုပြီးကျဉ်းပါတယ်. .

- ရေသေလို့ မနေပါနဲ့
- ရေရှင်လို့ လေ့လာပါ . .

22-9-2016
bel0

အားလုံးပဲ မင်္ဂလာပေါင်းနဲ့ပြည့်စုံနိုင်ကြပါစေ.....။
ကျွန်တော် တို့ MEHN ရဲ့ မဂ္ဂဇင်း ကိုအားပေးကြသော စာချစ်သူများအားလုံး ကိုယ်စိတ် နှစ်ဖြာ ကျန်းမာ ချမ်းသာ ပါစေလို့ ကျွန်တော် Moesat မှ ရှေ့ဦး ပဏာမ မေတ္တာပို့ နှုတ်ခွန်းဆက်သပါရစေ။ ကျွန်တော်တို့ MEHN Facebook Page လေးကို စတင်တည်ထောင်လာတာ အခုဆိုရင် တစ်နှစ်ပြည့်ခဲ့ပါပြီ လစဉ်မဂ္ဂဇင်း ထုတ်ဝေပေးခဲ့တာ အခုဆို အမှတ်စဉ်(၃) ကို ရောက်ရှိခဲ့ပြီဖြစ်ပါတယ်။ ဒီလိုရပ်တည်နိုင်ခဲ့တာဟာ စာချစ်သူတို့ရဲ့ အားပေးမှုတွေက အဓိက အခန်းကပါဝင်တာကြောင့် ကျွန်တော်တို့ MEHN အဖွဲ့သားများကိုယ်စား ကျွန်တော်က ကျေးဇူးတင် စကားထပ်လောင်းဆိုပါရစေ။သတင်းတွေကိုလည်း စာချစ်သူတွေဆီ Up to Date ရောက်ရှိနိုင်အောင် အချိန်နဲ့အမျှ စာချစ်သူတို့ထံ ပို့ပေးသွားမှာပါ Page လေးကို Like လုပ်ထားဖို့မမေ့နဲ့နော်။ IT ပညာရပ်ကို စိတ်ဝင်စားတဲ့ ညီငယ်ညီမငယ်ကိုကိုမမ ဦးဦး ဒေါ်ဒေါ် များကို ကျွန်တော် Moesat က ဆရာ လုပ်ချင်မျိုးမဟုတ်ပဲ ကိုယ်တွေ့ကြုံခဲ့ရတာတွေကို Sharing လုပ်သည့် သဘောဖြင့် Message တစ်ခုပေးပါ ရစေ IT လောကကို စတင် ခြေချတော့မယ်ဆိုရင် ပထမဦးဆုံး မိမိသွားချင်သော လမ်းကြောင်းကို အတိအကျ ရွေးချယ်ပါ လမ်းကြောင်းသိပြီဆိုမှ ထိုလမ်းကြောင်းပေါ် ခြေတင်ပါ။ ဥပမာ - ကိုယ်ဟာ Network enginner ဖြစ်ချင်တာလား Web Developer ဖြစ်ချင်တာလား System Administrator/Enginner ဖြစ်ချင်တာလား စသဖြင့် ကိုယ်သွား ချင်တဲ့လမ်းကြောင်း သေချာ Planချပါ။ ပြီးတာနဲ့ တစ်ဆင့်ချင်း ဖြေးဖြေး မှန်မှန် သွားပါ နောက်လှည့်မကြည့်ပါနဲ့ အောက်ငုံ့မကြည့်ပါနဲ့ နောက်လှည့် ကြည့်တဲ့အခါ သံသရာလည်တတ်ပါတယ် အောက်ငုံ့ကြည်တဲ့အခါ စိတ်ကြီးဝင် ရပ်တန့်သွားတတ်ပါတယ် ဒါကြောင့် ခေါင်းမော့ရင်ကောပြီး ကိုယ်ဦးတည်ချက် မပျောက်ပျက်ဘဲ ဖြေးဖြေး မှန်မှန်လေးသွားပါ ရှေ့ဆရာကြီးတွေ စကားမှီငြမ်းပါ မကောင်းတာတွေ ပယ်ထုတ်ပါ ကောင်းတာတွေ သိမ်းထားပါ လူတိုင်း Perfect မရှိပါ။ ဒါကြောင့် ကောင်းတာလေးတွေ ရွေးချယ်တတ်ပါစေ။ လဲကျတိုင်း အားမလျော့ပါနဲ့ ပြန်လည်ထပါအရှုံးဟူသည် သေဆုံးထိတိုင် ရှိနေဦးမှာပါ။ ဒါကို ကျရှုံးချင်လို့ စိတ်ပျက်အားငယ်နေမယ့်အစား အားအင်သစ်တွေနဲ့ တဖန်နိုးထလိုက်ပါ။ မနက်ဖြန်တိုင်းက သင့်ကိုစောင့်မျှော်နေပါတယ် အိမ်မက်တွေ အကောင်အထည်ဖော်ပါ။ ငွေနောက်ကို မလိုက်ပါနဲ့ ပညာနောက်ကို ထပ်ချပ်မကွာလိုက်ပါ။ အောင်မြင်မှု မနက်ဖြန်တိုင်းက သင့်တွက်ဖြစ်နေမှာပါ။ ဒီစိတ်ဓာတ်နဲ့သွား တစ်နေ့ IT လောကမှာ နာမည်တစ်လုံး ရေးထိုးလာနိုင်လိမ့်မယ်ဆိုတာ ကျွန်တော်ရဲရဲကြီးအာမခံပါတယ်။ လုပ်ဆောင်ချက်တွေ အောင်မြင်ပါစေလို့ ဆုတောင်းပေးလိုက်ပါတယ်။ စာချစ်သူများအားလုံးကိုကျေးဇူးအထူးတင်လျက်

22-9-2016
Moesat

မင်္ဂလာပါ စာချစ်သူပရိတ်သတ်ကြီးရေ ကျွန်တော်တို့ Myanmar Ethical Hacking New (MEHN) ကို အစဉ်တစိုက် အားပေးခဲ့တဲ့အတွက် ကျေးဇူးအထူးဘဲ တင်ပါတယ်။ ခုဆိုရင် ကျွန်တော်တို့ MEHN TEAM ကြီးဟာ တစ်နှစ်ပြည့်ခဲ့ပြီဘဲ ဖြစ်ပါတယ်။ ကျွန်တော်တို့ စာချစ်သူပရိတ်သတ်ကြီး အတွက်ကော IT လောကထဲမှ လူငယ်တွေကော အားလုံးကို ကျွန်တော်တို့ နည်းပညာ ဗဟုသုတများ ဒီထက်မက ပိုပေးနိုင်အောင် အစဉ်အမြဲ ကြိုးစားလျက် ရှိပါတယ်။ ကျွန်တော်တို့ အားလုံးလည်း ပညာရပ်များကို ဖြည့်ဆည်းလျက်ရှိပါတယ်။ ကျွန်တော်တို့ Team ရဲ့ လိုအပ်ချက်လေးများ ရှိရင်လည်း စာချစ်သူပရိတ်သတ်ကြီးအနေဖြင့် ဂေဖန်အကြံပြုပေးကြပါလို့လည်း မေတ္တာရပ်ခံအပ်ပါတယ်ခင်ဗျာ။ ခုမှ IT လောကသို့ ဝင်မည့် ကျွန်တော်ရဲ့ ညီငယ် ညီမငယ်များကို ကျွန်တော်အနည်းငယ် အကြံပြုချင်ပါတယ်။ ကျွန်တော်တို့ တော်တော်များများက သူများတွေ Hacking ဆိုလိုက် Hacking သူများတွေ Network ဆိုလိုက် Network လိုက်ကျတာပါဘဲ။ တကယ်တော့ အခဲ့ဒါဟာ ကောင်းတဲ့အချက် တစ်ခုတော့ မဟုတ်ပါဘူး ကျွန်တော့် ညီငယ် ညီမငယ်များ အနေဖြင့် မိမိ ဘာကို ဂါသနာပါလဲ ဘာကို လုပ်ချင်လဲ ဆိုတာကို အဓိက ဆုံးဖြတ်ပါ။ ပြီးတော့ ကိုယ်သွားချင်းသော လိုင်းကို တစိုက်မတ်မတ် အရောက်သွားပါ။ စာအုပ်တစ်အုပ်ကို လက်ကိုင်ထားပြီးဖတ်ပါ တစ်အုပ်ပြီးမှ တစ်အုပ်ဖတ်ပါ။ ဆိုလိုချင်တာကတော့ အခြေခံပိုင်အောင် အခြေခံကစ သေချာလေ့လာပါလို့ မှာချင်တာပါ။ ကျွန်တော်တို့ စာအုပ်အများကြီးကို တပြိုင်ထဲ ဖတ်တဲ့သူဟာ ဘာနဲ့တူလဲဆိုတော့ မြင်းနှစ်ကောင်ကို တစ်ပြိုင်ထဲ ခွစီးနေသလိုပါဘဲ။ မြင်းနှစ်ကောင်ကို တစ်ပြိုင်ထဲခွစီးတဲ့ လူဟာ ပြုတ်ကျမယ်ဆိုတာ ကျွန်တော့် စာချစ်သူ ပရိတ်သတ်ကြီး သိလိမ့်မယ်လို့ ထင်ပါတယ်။ အခဲ့လိုပါဘဲ စာအုပ်အများကြီးကို တစ်ပြိုင်တည်းဖတ်တဲ့ လူဟာလဲ ကိုရောက်သင့်တဲ့ အနေအထားကို မရောက်ပဲ ဟိုလိုလို ဒီလိုလို နဲ့ ဟိုလိုဒီလိုကြီးဖြစ်ပြီး ပြည့်ဝတဲ့ IT ပညာရှင်တစ်ယောက် ဖြစ်ဖို့ရာ ခက်ခဲသွားမှာဘဲ ဖြစ်ပါတယ်။ နောက်ထပ် အကြံပေးချင်တာလေး တစ်ခုကတော့ ကျွန်တော်စာချစ်သူပရိတ်သတ်ကြီး ပညာရှာတဲ့နေရာမှာ ကိုယ်မသိတာကို မသိဘူး ပွင့်ပွင့်လင်းလင်းပြောပြီး တတ်သိနားလည်သော လူတွေကို မေးပါ။ တကယ်လို့ စာချစ်သူများရဲ့ သူငယ်ချင်းများကလည်း သူတို့မသိတာကို မေးလာခဲ့ရင်လည်း စာချစ်သူများသိရင် သေချာပြောပြပေးပါ။ သူများကိုလဲ အထင်မသေးပါနဲ့ ကိုယ့်ကိုကိုယ်လည်း အထင်မကြီးပါနဲ့ ကျွန်တော်တို့ လောကမှာ သူမသိတာကိုသိ ကိုမသိတာသူသိတာတွေလည်း ရှိပါတယ်။ ခုနကမေးတာ ဖြေပေးတာ ဆိုတာကတော့ အခဲ့လိုမေးပေး ဖြေပေးမှ ကျွန်တော်တို့ IT လောကကြီး တိုးတက်ပြီး သူများနိုင်ငံတွေထက် သာမှာဖြစ်ပါတယ်။ ကျွန်တော် နောက်ဆုံးအနေနဲ့ အကြံပြုချင်တာကတော့ မပျင်းပါနဲ့ ကြိုးစားပါ အောင်မြင်မှုက လက်တကမ်းမှပါ။ ပြီးတော့ ပညာရပ်တစ်ခုအတွက် ငါသိနေပြီ ဆိုပီးမမှတ်ပါနဲ့ လေ့လာပါ ဆက်လက်လေ့လာပါ လက်ဆင့်ကမ်းပါ။ ဆရာလုပ်ခြင်းတော့ မဟုတ်ပါဘူးခင်ဗျာ အကြံပေးခြင်းသာ ဖြစ်ပါတယ်။ ကျွန်တော်လဲ ဖြည့်ဆည်းဆဲ မပြည့်သေးတဲ့ အိုးလေးတစ်လုံးပါ။ ကျွန်တော့်တို့ MEHN လေးကို ဆက်လက်အားပေးပါအုံးလို့....အားလုံးကိုကျေးဇူးတင်ပါတယ်။ ဆရာသမားများနှင့် လူသာတိုင်းကို အစဉ်လေးစားလျက်....

22-9-2016
Thomas Linn

ကျွန်တော်တို့ MEHN ကို အမြဲအားပေးခဲ့ကြတဲ့အတွက် ကျေးဇူးတင်ပါတယ်လို့ ပထမဦးစွာ ပြောလိုပါတယ်ခင်ဗျ။ ဒီနေ့ (23-9-2016) ဟာ ကျွန်တော်တို့ MEHN ရဲ့ နှစ်ပတ်လည် နေ့လေး ဖြစ်သလို ကျွန်တော်တို့ MEHN မိသားစုလေး စတင်ဖြစ်ပေါ်လာရတဲ့ နေ့လေးပါ။ ကျွန်တော်တို့ MEHN က သတင်းလေးတွေကို အမြဲအားပေးကြလို့ အရမ်းဂမ်းသာမိပါတယ်။ ကျွန်တော်တို့ အစက ဒီလောကထဲ အဆင်ပြေပဲ့မလား။ နေရာလေး တနေရာစာရော

ရပ့ါမလား တွေးမိဘူးပါတယ်။ ခုတော့ ထိုက်သင့်သလောက်လေး ရောက်နေပြီလို့ မျှော်လင့်မိပါတယ်။ ကျွန်တော်တို့ အတွက်အားဆေးဟာ စာဖတ်သူတို့ရဲ့ Like လေးတွေပါပဲ။ ဒီ like လေးတွေကြောင့် ကျွန်တော်တို့ကို နောက်ထပ်ကြိုးစားချင် စိတ်လေးတွေ မွေးဖွားလာစေပါတယ်။ ကျွန်တော်တို့ဟာ စာဖတ်သူတွေကို နည်းပညာရဲ့ အံ့မခန်းတို့တက်မှုတွေ ဘာတွေလုပ်ဆောင်နိုင်လာတယ် ဆိုတာလေးကို တင်ဆက်ရုံလေးပါ။ အသိပညာ ဗဟုသုတ နည်းပါးခြင်းဟာ ဒုက္ခရောက်စေနိုင်တယ်ဆိုတဲ့ အသိလေးကို ထင်ဟပ်ပြသချင်တာပါ။ တကယ်လည်း ဒုက္ခရောက်နေကြပါတယ်။ ကျွန်တော်တို့ စာဖတ်သူတွေ အနေဖြင့် ကျွန်တော်တို့ ရေးသားသော စာလေးတွေကြောင့် ဒီဒုက္ခလေးတွေက ရှောင်နိုင်ရင် ပင်ပန်းရက်ချိုး နပ်ပါပြီ။ ကျွန်တော်တို့ ရေးသားတင်ပြမှုလေးတွေမှာ အမှားပါရင် ပြင်ပေးကြပါလို့ တိုက်တွန်းပါရစေဗျ။ ကျွန်တော်တို့ နိုင်ငံရဲ့ အိုင်တီလောကကိုလည်း အစဉ်တိုးတက် ဖွံ့ဖြိုးတိုးတက်အောင် ကူညီစောင့်ရှောက်ပေးကြပါလို့ မေတ္တာရပ်ခံပါရစေခင်ဗျ။ ကျေးဇူးတင်စွာဖြင့်....

22-9-2016
D3@D$"!"@R

# Youtube Video ရဲ့ နောက်ကွယ်တွင် ရှိသော အသံ Command မှတဆင့် Smartphone များကို Hack နိုင်ခြင်း


UC Berkeley and Georgetown University မှ သုတေသနပြုသူတွေ ဦးစီးဆောင်ရွက်မှုနဲ့ Youtube Video များ၏ နောက်ကွယ်တွင်ရှိသော Voice Command မှတဆင့် သင်၏ Smartphone ကို တိုက်ခိုက်နိုင်ပုံကို ပြသခဲ့ပါတယ်။ နည်းပညာရှင်းများမှ Youtube Video တွေရဲ့နောက်ကွယ်မှာ Voice command တွေကို ဝှက်ထားနိုင်တယ်လို့သိရပါတယ်။

ယခုနောက်ပိုင်းထွက်ရှိသည့် Smartphone များတွင်ပါဝင်သော စကားသံများကို ခွဲခြမ်းစိတ်ဖြာနိုင်သော စံနစ်ကြောင့် တိုက်ခိုက်ခံရနိုင်ခြင်း ဖြစ်ပါတယ်။ စမ်းသပ်ချက်များကို ဖုန်းအသံစံနစ်များဖြစ်သည့် Seri နှင့် Cortana မှာ စမ်းသပ်ပြီးပါပြီ။ နည်းပညာရှင်များ ရေးသားထားသော စာတမ်းတွင် တိုက်ခိုက်သူများသည် Youtube Video များအတွင်း Voice Command များကို မသိလိုက် မသိမသာ ပြောကြားပြီး တိုက်ခိုက်ခြင်း ဖြစ်သည်။ ဆိုလိုသည်မှာ Voice Command များကို တဆက်တည်း ပြောခြင်းမဟုတ်ဘဲ Video အတွင်း စကားပြောသယောင်နှင့် Voice Commands များ ပေးသွားခြင်း ဖြစ်သည်။

Youtube အသုံးပြုသူများအနေဖြင့် IT နည်းပညာပိုင်းဆိုင်ရာ နားလည်တတ်ကျွမ်းသူများရှိသလို နည်းပညာပိုင်းဆိုင်ရာ မသိသူများလည်း ပါဝင်နိုင်ပါသည်။ အများစုမှာ IT နည်းပညာပိုင်းဆိုင်ရာ အားနည်းသူများဖြစ်သည်။ သင်သည် တိုက်ခိုက်သူမှ ဖန်တီးထားသော Youtube Video File တစ်ခုကို ဖွင့်ကြည့်မိတယ်ဆိုကြပါစို့။ ဖုန်းကလည်း အနားမှာရှိနေမယ်။ တိုက်ခိုက်သူများသည် Video File အတွင်း Voice Commands များကို လှို့ဝှက် ထည့်သွင်းပြီး ပြောကြားသွားပါတယ်။ ထို အသံကို Smartphone ၏ Voice Command System မှ ကြားကာ Youtube Video မှ ပြောသည့်အတိုင်း လိုက်လုပ်သွားမည် ဆိုပါက တိုက်ခိုက်ခံရမည် ဖြစ်သည်။

နည်းပညာရှင်များသည် တိုက်ခိုက်သည့် နည်းလမ်း ၂ မျိုးဖြင့် စမ်းသပ်ထားပါသည်။ ထို နည်းလမ်း ၂ မျိုးကို Black Box Testing နှင့် White Box Testing ဟု ခေါ်ပါသည်။ Black Box Testing ဆိုသည်မှာ Voice Commands ကို လူကိုယ်တိုင်

ကြားနိုင်ပြီး နားလည်နိုင်သော နည်းလမ်းဖြစ်သည်။ ထို အသံကို Smartphone တွင်ပါဝင်သော အသံဖမ်းသည့် စံနစ်သည် ကြားသွားပါက Voice Commands အတိုင်း အလုပ်လုပ်သွားမည်ဖြစ်သည်။ Black Box Testing Voice Commands ကို ဖော်ပြပါ Links တွင် နားထောင်နိုင်ပါတယ်။

Black Box Testing : https://youtu.be/JQM1GqRGIus

White Box testing ဆိုသည်မှာ အသံကို ကြားရသော်လည်း လူကိုယ်တိုင်နားမလည် Smartphone တွင်ပါဝင်သော အသံဖမ်းသည့် စံနစ်သာ နားလည်နိုင်မည့် Voice Commands မျိုးဖြစ်သည်။ Smartphone ၏ အသံဖမ်းသည့်စံနစ်မှာ အသံကြိမ်နှုန်းများအပေါ်မူတည်ပြီး ခွဲခြမ်းစိတ်ဖြာသည့် နည်းစံနစ်ဖြစ်သည်။ ထို့ကြောင့် White Box testing တွင် Voice Commands များသည် မပီမသဖြစ်နေသော်လည်း ကြိမ်နှုန်းများ မှန်နေသည့်အတွက် ထို ကြိမ်နှုန်းကို Smartphone ၏ အသံဖမ်းသည့် စံနစ်က ဖမ်းယူနားလည်သွားပြီး Video File တွင် ပါဝင်သော Voice Command အတိုင်း လုပ်ဆောင်သွားမည် ဖြစ်သည်။ White Box Testing Voice Commands ကို ဖော်ပြပါ Links တွင် နားထောင်နိုင်ပါတယ်။

White Box Testing : https://youtu.be/wrNcBvkj2yk

အခြားသော Black Box နှင့် White Box Testing Voice Commands များကို လေ့လာချင်ပါက ဖော်ပြပါ Link တွင် ဝင်ရောက် လေ့လာနိုင်ပါတယ်။

Link : http://www.hiddenvoicecommands.com/

တိုက်ခိုက်နည်းများသည် နေ့စဉ်နှင့်အမျှ အသစ် အသစ်များ ထွက်ပေါ်လျက်ရှိပါတယ်။ စာရှု့သူများအနေဖြင့် နည်းပညာဗဟုသုတများ ရရှိစေပြီး တိုက်ခိုက်နည်းများကို သိရှိထားကာ ရှောင်ရှားနိုင်ကြပါစေကြောင်း အစီရင်ခံ ဖော်ပြလိုက်ရပါတယ်။

1-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ပိုင်လင် (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# Microsoft Office ကို ယှဉ်ပြိုင်မည့် LibreOffice


ဒီဇင်ဘာလ ၂၀၁၅ ခုနှစ်မှ စတင်ပြီး အီတလီ စစ်ဘက်ဆိုင်ရာ ရုံးလုပ်ငန်းများတွင် အသုံးပြုရန်အတွက် အီတလီအခြေစိုက် အမြတ်အစွန်းအတွက် မရည်ရွယ်သော Non-Profit ကုမ္ပဏီ တစ်ခုဖြစ်သော LibreItalia နှင့် သဘောတူညီမှုများ ပြုလုပ်ခဲ့သည်။ ထို ကုမ္ပဏီ၏ ရည်ရွယ်ချက်မှာ လူမှုရေးလုပ်ငန်းများ ၊ အစိုးရဘက်ဆိုင်ရာလုပ်ငန်းများ ၊ ပညာရေးဆိုင်ရာလုပ်ငန်းများ နှင့် ပြည်သူလူထုအကျိုးပြုခြင်းဆိုင်ရာ လုပ်ငန်းများကို အထောက်အကူပြုစေရန် အတွက် ဖြစ်သည်။

အီတလီ စစ်ဘက်ဆိုင်ရာ သတင်းတစ်ခုတွင် Open Source များကို အသုံးပြုခြင်းဖြင့် ယူရို 29 မီလီယံ ခန့် လျှော့ချနိုင်ဖွယ်ရှိကြောင်း ဆိုထားပါသည်။ ထို လျှော့ချနိုင်သည့် ငွေပမာဏသည် လာမည့်ဘဏ္ဍာရေး အခန်းကဏ္ဍတွင် များစွာ အကျိုးသက်ရောက်မှာ ဖြစ်တယ်လို့လည်း ရေးသားထားပါသည်။

အီတလီစစ်ဘက်ဆိုင်ရာ ရုံးများတွင် Microsoft Office များကို အသုံးပြုနေရာမှ အစားထိုး အနေဖြင့် Open Source LibreOffice ကို အသုံးပြုတော့မှာ ဖြစ်ပါတယ်။ ယခု ၀ယ်ယူထားသော Microsoft Office ၏ လိုင်စင်သက်တမ်း ကုန်ဆုံးသည့်အခါ LibreOffice ကို စတင် အသုံးပြုရန်အတွက် အီတလီ စစ်ဘက်ဆိုင်ရာ ဌာနများတွင် အကြောင်းကြားထားပြီးဖြစ်သည်။ 2017 ခုနှစ်တွင် အသုံးပြုသည့် အရေအတွက်ပေါင်း 75000 ခန့် ရှိမည်ဟုခန့်မှန်းထားပြီး ထိုအရေအတွက်မှာ အသုံးပြုသူအားလုံး၏ 70 ရာခိုင်နှုန်းရှိကြောင်း သတင်းတစ်ပုဒ်တွင် ဖော်ပြပါရှိပါတယ်။ 2020 ခုနှစ်မှာ နောက်ထပ် 25000 ခန့် ထပ်မံအသုံးပြုမှာ ဖြစ်ပါတယ်။

ယခုဆိုရင် Microsoft Office နှင့် ပြုလုပ်ထားသော စာရွက်စာတမ်းများကို LibreOffice ဖြင့် ပြန်လည် ပြုလုပ်ခြင်း လုပ်ငန်းစဉ်များကို ဆောင်ရွက်လျက်ရှိနေပါတယ်။ အရေအတွက် 5000 နီးပါးခန့် LibreOffice ၏ ထောက်ပံ့ပေးခြင်းဆိုင်ရာ Workstations များကိုလည်း တပ်ဆင်ပြီး ဖြစ်ပါတယ်။ LibreItalia မှ LibreOffice ကို ဌာနဆိုင်ရာ ၀န်ထမ်းများ ကျွမ်းကျင်စွာ အသုံးပြုတတ်စေရန် သင်ခန်းစာများကို ၊ ဗွီဒီယိုဖြင့် သရုပ်ပြသော လေ့ကျင့်ခန်းများကို ပြုလုပ်ပေးထားပါတယ်။

အီတလီတပ်မတော်မှ ဗိုလ်ချုပ်တစ်ဦးဖြစ်သူ Camillo Sileo မှ "ဒီ ပရောဂျက်က ကျွန်တော်တို့ စစ်ဘက်ဆိုင်ရာ ရုံးလုပ်ငန်းများအတွက် အများကြီး အထောက်အကူပြုမယ်လို့ မျှော်လင့်ပါတယ်။ အခုလည်း ရုံးဌာနအသီးသီးရှိ ဂန်ထမ်းများကို LibreOffice နှင့် ပတ်သက်ပြီး ကျွမ်းကျင်စွာ အသုံးပြုတတ်စေရန် ဆရာများနှင့် အတူ သင်ကြားစေပါတယ်" လို့ ပြောကြားခဲ့ပါတယ်။

အီတလီနိုင်ငံမှ ရုံးလုပ်ငန်းသုံး Microsoft Office ကိုသာ အစားထိုးသုံးစွဲသည်မဟုတ်လည်း များမကြာခင်မှာ Microsoft Windows OS များကို အစားထိုးနိုင်မည့် Zorin OS ဟုခေါ်သော Linux Distro ကိုပါ အစားထိုးရန် အစီအစဉ်များ ချမှတ်ထားပြီးဖြစ်သည်။ အကယ်၍သာ LibreOffice သည် ကွမ်ဟာကိုသာ ဖြန့်ကျက်နိုင်မည် ဆိုပါက Microsoft Office ကို အလဲထိုးနိုင်မည့် အခြေအနေမှာ ရှိနေပါသည်။ ထိုကြောင့် မည်သူကသာမည်လဲဆိုတာကို စောင့်ကြည့်ရမှာ ဖြစ်ပါတယ်။

2-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ကိုရီချင် (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# Facebook ကိုဝင်ရောက်သိမ်းပိုက်သွားနိုင်သော Google Chrome ရဲ့ Extension


Google Chrome ရဲ့ extension မှ တစ်ဆင့် Facebook အကောင့်ကိုဝင်ရောက်သိမ်းနှိုင်တယ်ဆိုတာကို ၁၉ နှစ်အရွယ်Danish ကျောင်းသားလေး Maxine Kjaer ကတွေ့ရှိခဲ့တာပါ။ Google မှ ထို extensionကို ဖယ်ရှားခံရပြီးတဲ့နောက်တွေ့ ရှိသွားတာပါ။ ဒီextensionက facebook post တွေကိုဖြန့်ဝေနိုင်အောင်လုပ်ဆောင်ထားတဲ့ extension တစ်ခုပါ။ Facebook အသုံးပြုသူတစ်ဦးက Chromeမှ ပေးတဲ့ link ကိုနှိပ်မိမယ်ဆိုလျှင် Chrome ပါဝင်တဲ့နည်းတွေနဲ့အတူ များပြားတဲ့လုပ်ဆောင်မှုတွေကသင့်Facebook အကောင့်ကိုhack ဖို့စနစ်လုပ်ဆောင်နေပါပြီ။

Google Chrome web store ကနေရရှိတဲextension တွေထဲမှာ Viral age နဲ့ Verify ဆိုတဲ့အကြောင်းအရာတွေနဲ့အတူuser ကိုတရားဝင်ဖြစ်အောင်လုပ်ဆောင်ပေးမယ်ဆိုတာလည်းပါဝင်နေတဲ့ အတွက် တရားဝင်extension ကဲ့သို့ လုပ်ဆောင်နေပါတယ် ။ သုတေသနပညာရှင်များတွေ့ရှိခဲ့တာကတော့ အားနည်းချက်ရှိတဲ့ extension ကို အသုံးပြုတဲ့ IP addresses မှတ်သားပြီး Digital Oceanမှာ တင်ထားတဲ့ C&C server ကနေ လှမ်းထိန်းချုပ်နေကြောင်း တွေ့ရှိခဲ့ပါတယ်။

Kjaer ရဲ့ ဒီနည်းပညာပေါ်ရှင်းပြထားတာကတော့ ဒီနည်းပညာအသစ်မှာဆိုရင် ကိုယ်မမျော်လင့်တဲ့အရာတွေ ပေါ်လာတတ်ပြီး အသုံးပြုသူရဲ့ Data တွေကိုပြောင်းလဲဖို့တိုက်တွန်းပါလိမ့်မယ်။ ဒီနည်းပညာမှာ file 3ခုပါဝင်ပြီး အဲ့ထဲမှာ အသုံးပြုသူ Browser ကထွက်သည့်တိုင်အောင် သူ့အချက်အလက်တွေမပျက်ဆီးဘဲရှိနေအုံးမှာပါ။

၁၈ ချက်ထက်မနည်းတဲ့ ပြည့်စုံတဲ့ အချက်အလက်တွေထဲမှာ User က မွေးနေ့ကဲ့သို့သော လိုအပ်ချက်တွေကို

တောင်းဆိုသည့်အတိုင်း ထည့်ပေးပြီး Loading လုပ်နေစဉ်အချိန်နဲ့ Done ဆိုပြီးပြီးဆုံးသွားတာနဲ့ အချက်အလက်များဟာ C & C server ကို ရောက်ရှိသွားနိုင်ပါတယ်။

Kjaer ပြောဆိုခြင်းမှသိရှိရပါတယ်။

C&C server ကနေ Browser ကိုဝင်ရောက်ထိန်းချုပ်ခြင်း

အခြေခံအားဖြင့် script တွေကို dowload လုပ်ခဲ့မယ်ဆိုရင် C&C server ကနေcontrol လုပ်ထိန်းချုပ်နိုင်မှာပါ။ တွက်ချက်မှုတွေအရ Chrome နည်းအသစ်ကိုကွန်ပြူတာမှာInstall လုပ်ခဲ့သူ 132,265 အထိ တိုက်ခိုက်မှုတွေ ခံနေရပါတယ်။ Maxine Kjaer ဟာ ဒီ extension ကို Chrome web store မှ ဖယ်ရှားဖို့ပြောကြားခဲ့သလို Blacklist လုပ်ဖို့ပါ ပြောကြားခဲ့ပါတယ်။ ဒီနည်းလမ်းကြောင့် ထို extension ကို အလိုလို ဖယ်ရှားပြီးသား ဖြစ်သွားမှာလည်း ဖြစ်ပါတယ်။

စာရှုသူတို့အနေနှင့် လည်း Google Chrome extension များကို သတိထားပြီး အသုံးပြုကြပါလို့ အကြံပြုပါတယ်။

4-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ပိုင်လင် (MEHN Team)

## ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်

# SSH ဆိုတာ ဘာလဲ

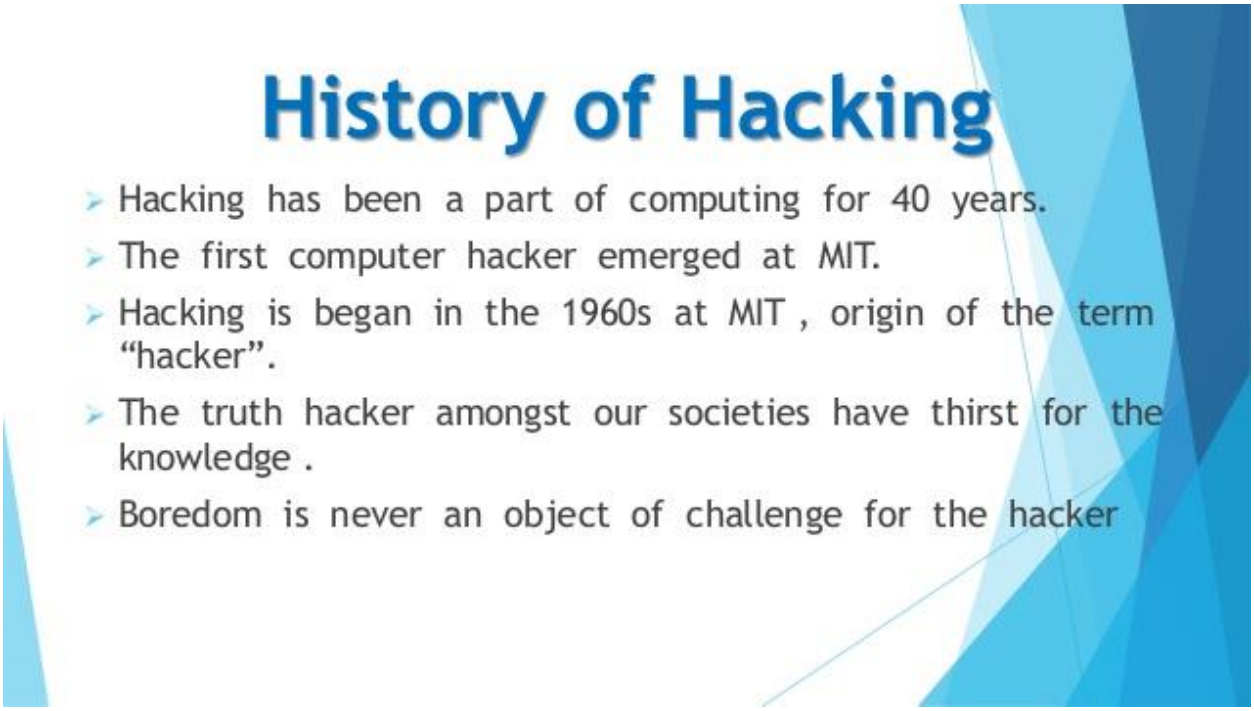

Secure Socket Shell လို့ခေါ်တဲ့ SSH ဟာဆိုရင်တော့ Administrator က network ပေါ်ကနေတခြားကွန်ပျူတာကို Remote Access လုပ်ရာမှာ လုံခြုံစိတ်ချရတဲ့ Protocol ပဲဖြစ်ပါတယ်။Secure Shell ဟာဆိုရင်တော့ လုံခြုံမှုမရှိတဲ့ Network ပေါ်ကနေ ကွန်ပျူတာ ၂လုံးအချက်အလက်များပိုဆောင်ရမှာလုံခြုံမှုရှိအောင်နဲ့Encryption တို့ကိုပြုလုပ်ပေးပါတယ်။

SSH ကိုတော့ Network Administrators တွေက systems တွေကို manage လုပ်ဖို့ , ကွန်ပြူတာတွေဝလုံးနဲ့ဝလုံး Remote လုပ်ဖို့ နဲ့ file တွေကို copy လုပ်ရာတို့တွင်ကျယ်ပြန့်စွာအသုံးပြုလာကြပါတယ်။SSH ကို cryptographic network protocol နဲ့ အသုံးဝင်တဲ့ Tools တစ်ပေါင်းထဲပါလာတဲ့ protocol တို့အနေနဲ့ပါအသုံးပြုလို့ရပါတယ်။

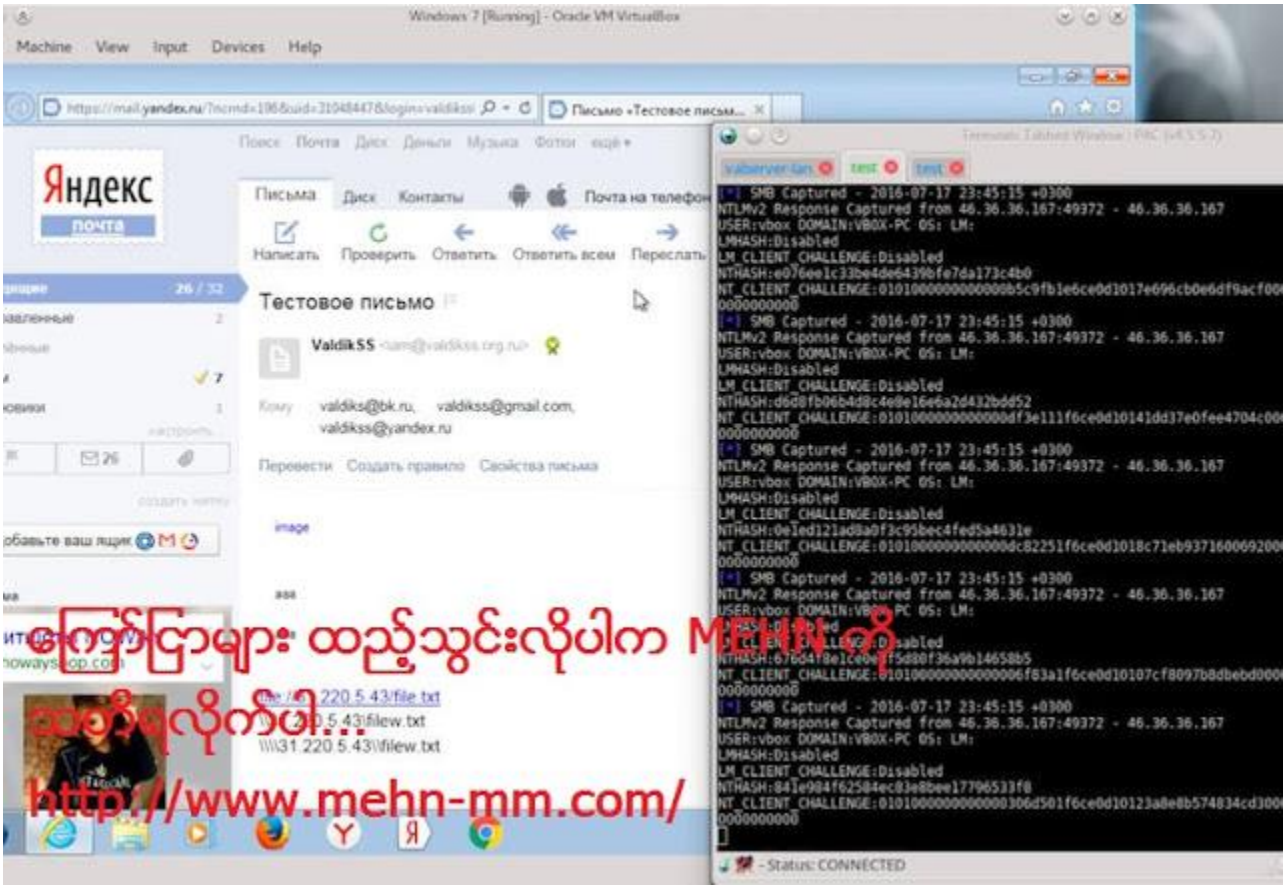
SSH ကို Client server model အနေနဲ့အသုံးပြုမယ်ဆိုရင်တော့ client application နဲ့ SSH Server တို့ကိုအသုံးပြုပြီး connect လုပ်ကြပါတယ်။Microsoft Windows ဘက်မှလွဲပြီး တခြား operation system တိုင်းမှာ default အနေနဲ့ပါဝင်ပါတယ်။Tunneling, Forwarding TCP ports နဲ့ secure file transfer (SCP) protocols တို့မှာ SSH က supports ပေးပါတယ်။SSH server ရဲ့ default listen TCP port ကတော့ 22 ပဲဖြစ်ပါတယ်။

8-8-2016
သတင်းစီစဉ်တင်ဆက်သူ:: Algorithm (MEHN Team)

ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်



# Microsoft မှ မပြင်သေးသော အားနည်းချက်တစ်ခု




Microsioft မှ window ရဲ့ အားနည်းချက်တွေ မပြင်ဆင်မှုဟာ ဟက်ကာတွေအား ကျွန်တော်တို့ရဲ့ username တွေ Password တွေ ခိုးယူနိုင်စေရန် ခွင့်ပြုမိနေသလို ဖြစ်နေပါတယ်။

ဒီအားနည်းချက်ဟာဆိုရင် အန္တရာယ်ရှိတဲ့ ဂက်ဆိုဒ်တွေကို Microsoft အကောင့်နဲ့ ဂင်မိလိုက်တာနဲ့ အသုံးပြုသူရဲ့ password တွေကို ရယူဖို့ ခွင့်ပြုစေခြင်းပဲ ဖြစ်ပါတယ်။ အဆိုပါ အားနည်းချက်ဟာဆိုရင်ဖြင့် တိုက်ခိုက်သူတွေကို အသုံးပြုသူ တစ်ဦးချင်းစီရဲ့ usernameနဲ့ password တွေကို ခိုးယူနိုင်စေမှာပဲ ဖြစ်ပါတယ်။

ဒါဟာ အလွန်ရိုးရှင်းပါတယ်။အသုံးပြုသူဟာ အန္တရာယ်ရှိတဲ့ ဂက်ခ်ဆိုက်ကို ဂင်ရောက်ကြည့် ရှူလိုက်ရုံပဲ ဖြစ်ပါတယ်။ ယခုအသစ်ထွက်ရှိလာတဲ့ အားနည်းချက်ဟာဆိုရင် User များရဲ့ မည်သူမည်ဂါဖြစ်တယ်ဆိုတာကအစ လွယ်ကူစွာ ခိုးယူနိုင်ပါတယ်။ ဒီအားနည်းချက်ဟာဆိုရင် အသက်၂၀သာ ရှိသေးတဲ့ Aaron Spangler မှ ၁၉၉၇ က တွေ့ရှိထားတဲ့

လူသိများတဲ့ အချက်ပဲ ဖြစ်ပါတယ်။ဒီအားနည်းချက်ကို Las Vegas မှာ ကျင်းပခဲ့တဲ့ ၂၀၁၅ ခုနှစ် Black Hat ရဲ့ နှစ်ပတ်လည် လုံခြုံ ရေးနဲ့ ဆိုင်တဲ့ ဟက်ကာများ အစည်းအဝေးမှာ ထပ်မံ သုတေသနပြုခဲ့ရတဲ့အချက်ပဲ ဖြစ်ပါတယ်။

ဒီအားနည်းချက်ဟာ window8 မှာ user တွေ microsoft account ဖြင့် login ဝင်လို့ မရခင် အထိ အရေးကြီးတဲ့ အချက်အဖြစ် မသတ်မှတ်ကြခဲ့ပါဘူး။ ဒီ microsoft account တွေဟာဆိုရင် Xbox,Hotmail, Outlook, Skype accounts နဲ့ တခြားသော အရာတွေကို ချိတ်ဆက်ထားမိခဲ့ ကြပါတယ်။ ဒီအားနည်းချက်မှ တဆင့်တိုက်ခိုက်မှုတွေဟာ တဖြည်းဖြည်း တိုးတက်များပြားလာပါတယ်။ဒီအချက်ဟာဆိုရင် တိုက်ခိုက်သူတွေကို Microsoft account အား အပြည့်အဝ ထိန်းချုပ်သွားစေနိုင်သည်အထိ အခွင့်အရေး ရရှိစေပါတယ်။

10-8-20116
သတင်း စီစဉ်တင်ဆက်သူ - D3@D$"i"@R (MEHN Team )

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# Drupal Web Application အား တိုက်ခိုက်နိုင်သော အားနည်းချက် ၃ ခု


Web Applications ပေါင်း များစွာရှိပါတယ်။ Website ဖန်တီးသူများအတွက် အလွယ်တကူ အသုံးပြုနိုင်ရန် Web Developers များမှ ဖန်တီးပေးထားခြင်းဖြစ်သည်။ Web Applications များကို တနည်းအားဖြင့် CMS (Content Management System) ဟုလည်း ခေါ်ပါတယ်။ CMS လို့ခေါ်ဆိုရခြင်းမှာ Applications များကို အသုံးပြုပြီး အသုံးပြုသူများအတွက် လွယ်ကူအဆင်ပြေသော Interfaces များဖန်တီးနိုင်ခြင်း ၊ တစ်ကြိမ်တည်း တစ်ပြိုင်တည်းတွင် အသုံးပြုသူအများအပြား အသုံးပြုနိုင်အောင် ဖန်တီးနိုင်ခြင်း ၊ အနေအထား အသွင်အပြင် စသည်တို့ကို လိုသလို ပြုပြင်နိုင်ခြင်း စသည့် လုပ်ဆောင်ချက်များကြောင့် CMS ဟု ခေါ်ဆိုခြင်း ဖြစ်သည်။

CMS ပေါင်း များစွာရှိပါတယ်။ Joomla , Drupal , WordPress , TYP03 , WebAsyst , Modx , Magento , ABO.CMS စသည်တို့အပြင် အခြားသော မြောက်များလှစွာသော CMS အမျိုးကွဲပေါင်းများစွာရှိပါသည်။ CMS အမျိုးအစားလိုက် အသုံးပြုထားသော Web Programming Languages များလည်း မတူညီကြပါဘူး။ ပါဝင်သော Modules များ Security Systems များစတာတွေလည်းမတူကြသလို အားနည်းချက် အားသာချက်များလည်း ရှိကြပါတယ်။ CMS များ အားလုံးတွင် အားနည်းချက် အားသာချက်များ ရှိသော်လည်း အဓိကမှာ အသုံးပြုသည့် Web Master အပေါ်တွင် မူတည်သည် Web Master ၏ ကျွမ်းကျင်မှုအလိုက် လုံခြုံရေးဆိုသည့် ကိစ္စရပ်များသည် အပြောင်းအလဲဖြစ်နေမည် ဖြစ်သည်။ ကျွမ်းကျင်သော Web Master များသည် Websites များနှင့် ပတ်သက်သော လုံခြုံရေးသတိ အမြဲရှိနေကြပြီး Web System များကို အမြဲတစ်စေ စစ်ဆေးကြည့်ရှု့ကာ အကာကွယ်များ ပြုလုပ်ထားမည် ဖြစ်သည်။

CMS ပေါင်းများစွာထဲမှ Drupal သည် လူသိများ ထင်ရှားကျော်ကြားလှသော Web Application တစ်ခုဖြစ်သည်။ Drupal ကို သန်းပေါင်းများစွာသော Web Developers များ ယနေ့အချိန်တွင် အသုံးပြုနေကြပြီဖြစ်သည်။ မကြာသေးမီကာလများက နည်းပညာရှင်များ တင်သွင်းခဲ့သော စာတမ်းတစ်စောင်တွင် Drupal Module တစ်ခုတွင် Remote Code Execution (RCE) ဟုခေါ်သော အားနည်းချက် ယိုပေါက်တစ်ခုရှိနေကြောင်း ရေးသားဖော်ပြခဲ့သည်။ ထိုအားနည်းချက် ယိုပေါက်ကြောင့် သန်းပေါင်းများစွာသော Websites များ အန္တရာယ်ဖြစ်နိုင်ကြောင်းကိုလည်း ထည့်သွင်းဖော်ပြခဲ့ကြပါတယ်။

RESTful Web Service

RESTful Web Service သည် Web Developer များထံသို့ အချက်အလက်များ ပြန်လည်ပေးပို့သည့် လုပ်ငန်းစဉ် ဖြစ်သည်။ တိုက်ခိုက်သူများသည် ထို ၎နည်းဆောင်မှုမှတဆင့် အချက်အလက်များကို ဖမ်းယူနိုင်ပါသည်။ RESTful Web Service အားနည်းချက် ယိုပေါက် ဖြစ်နေသော Drupal Version တွေကတော့ 7.x-2.x prior မှ 7.x-2.6 အထိ နှင့် 7.x-1.x prior မှ 7.x-1.7 အထိ ဖြစ်သည်။

Coder

Coder သည် Code များကို ခွဲခြမ်းစိတ်ဖြာ စစ်ဆေးပေးနိုင်သော လုပ်ငန်းစဉ် ဖြစ်သည်။ အားနည်းချက်မှာ Coder သည် အသုံးပြုသူသည် ခွင့်ပြုချက်ရရှိထားသူလား ခွင့်ပြုချက်မရရှိဘဲ ၎ငျောက်အသုံးပြုနေသူလားဆိုသည့်အချက်ကို မခွဲခြားနိုင်ခြင်းပင် ဖြစ်သည်။ တိုက်ခိုက်သူများသည် PHP Script ဖြင့် Coder အတွင်း ခွင့်ပြုချက်မရှိသော အကောင့်များကို ထည့်သွင်းပြီး ထိုးဖောက်သွားနိုင်ပါသည်။ Coder အားနည်းချက် ယိုပေါက် ဖြစ်နေသော Drupal Version တွေကတော့ 7.x-1.x prior မှ 7.x-1.3 အထိ နှင့် 7.x-2.x prior မှ 7.x-2.6 အထိ ဖြစ်သည်။

Webform Multiple File Upload

Webform Multiple File Upload သည် Websites သို့လာရောက်ကြသော အသုံးပြုသူများပေးပို့သည့် Files များကို စုဆောင်းသည့် လုပ်ငန်းစဉ်ဖြစ်သည်။ အားနည်းချက်မှာ အသုံးပြုသူများ ပေးပို့သည့် Forms များထဲတွင် တိုက်ခိုက်သူများမှ Remote Code Execution ဟုခေါ်သော တိုက်ခိုက်နည်းဖြင့် PHP Scripts များ အတွင်း Malicious Codes များထည့်သွင်းပြီး ဖောက်ထွင်းသွားနိုင်ပါသည်။ Webform Multiple File Upload အားနည်းချက် ယိုပေါက် ဖြစ်နေသော Drupal Version တွေကတော့ 7.x-1.x မှ 7.x-1.3 အထိ ဖြစ်သည်။

Web Security နည်းပညာရှင်များမှ Drupal ၏ နောက်ဆုံးထွက် Version များကို အသုံးပြုကြပါရန် တိုက်တွန်းနှိုးဆော်ထားပါတယ်။ စာချစ်သူတို့လည်း Drupal ကို အသုံးပြုနေတယ်ဆိုရင်တော့ နောက်ဆုံးထွက် Version ကို မြှင့်ထားဖို့ မမေ့ကြနဲ့ဦးနော်.....

11-8-2016
ကိုရီချင်

ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်

# DDoS တိုက်ပြီး ငွေရှာမယ့်အကြံ


အတွေးဆန်းတယ် ပြောရမလား အကြံထူးတယ် ပြောရမလားတော့ မသိဘူး။ ကော်လိုရာဒိုနဲ့ မီချီဂန်တက္ကသိုလ်က သုတေသီတွေပေါင်းပြီး DDoS ဝိုင်းတိုက်ပေးတဲ့သူတွေကို ဆုချနိုင်မဲ့ ဂုက်စာသွင်း ငွေကြေးစနစ်တစ်မျိုးကို တီထွင်ထားပါတယ်။ ကိုယ့်ကွန်ပျူတာကို DDoS တိုက်တဲ့နေရာမှာ ဝင်ပါစေပြီး DDoSCoin လို့ နာမည်ပေးထားတဲ့ ဒီငွေကြေးစနစ်နဲ့ ဆုငွေရယူနိုင်မှာပါ။ DDoSCoin ဟာလည်း ဂုက်စာသွင်းထားသော အချက်အလက်များဖြင့် ပြောသလိုလုပ်/မလုပ်ကို Bitcoin လိုပဲ စစ်ပါတယ်။ DDoS တိုက်တဲ့အချိန်မှာ ချိတ်ခဲ့တဲ့ TSL Connection ကို သက်သေအဖြစ် ယူတာပါ။

ခေတ်သစ် TSL ဗားရှင်းတွေမှာ ဆာဗာတစ်လုံးကို Handshake စလုပ်တဲ့အခါ ဆာဗာနဲ့ ကလိုင်းရင့် (Client) တွေဟာ Key အလွှာအပြောင်း လုပ်ကြပါတယ်။ ဒီ Key တွေကိုကြည့်ပြီး ဆာဗာ (Server) နဲ့ ချိတ်ဖူးထားတာ ဟုတ်/မဟုတ် စစ်လို့ရပါတယ်။ ဒီအချက်ကြောင့်ပဲ DDoSCoin ဆုကြေးကို လိုချင်တဲ့သူဟာ TSL Connection ပေးနိုင်တဲ့ ဆာဗာတွေကိုပဲ DDoS တိုက်နိုင်မှာ ဖြစ်ပါတယ်။ ဒါပေမဲ့ ထိပ်တန်းဝက်ဆိုက် (၁) သိန်းလောက်မှာ (၅၆) ရာခိုင်နှုန်းလောက်က TSL ကို ထောက်ပံ့နေကြပြီလို့ ဖန်တီးခဲ့သော သုတေသီနှစ်ဦးထဲက တစ်ဦးက ဆိုပါတယ်။

DDoSCoin မှာပါတဲ့ နောက်ထပ် လုပ်ဆောင်ချက်တစ်ခုကတော့ တိုက်ချင်တဲ့ပစ်မှတ်ကို သတ်မှတ်ပေးပြီး တခြားသူတွေကို ငွေချေတဲ့စနစ်ပါ။ PAY_TO_DDOS လို့ နာမည်ပေးထားပါတယ်။ ဒီလုပ်ဆောင်ချက်မှာ ဖြည့်ရတာ နှစ်ခုရှိပါတယ်။ တစ်ခုက DDoS တိုက်ချင်တဲ့ ဝက်ဆိုက်ရဲ့ ဒိုမိန်း (Domain) ပါ။ နောက်တစ်ခုက လိုချင်တဲ့ TSL Connection အရေအတွက်ပါ။ ဒီလို ငွေပေးချေမှုတွေကို DDoSCoin ရဲ့ Blockchain ထဲမှာ မှတ်ထားပေးပါတယ်။ ငွေရှာချင်တဲ့သူနေနဲ့ အဲဒီ Blockchain ထဲက ကြိုက်ရာတစ်ခု (တိုက်ချင်တဲ့ဒိုမိန်း) ကိုရွေး၊ DDoS တိုက်ပြီ: လိုချင်တဲ့ Connection အရေအတွက် ပြည့်တာနဲ့ ဆုငွေရယူနိုင်ပါတယ်။

သုတေသီနှစ်ယောက်ကတော့ DDoSCoin ဟာ Bitcoin အပြင် တခြားလူသုံးများတဲ့ အွန်လိုင်းငွေကြေးစနစ်တွေနဲ့လည်း လဲလှယ်နိုင်မှာပါလို့ ဆိုထားပါတယ်။ ဒီစနစ်မှာ ပြဿနာတစ်ခုရှိပါတယ်။ အဲဒါကတော့ Connection အရေအတွက်နဲ့

သတ်မှတ်ထားတဲ့အတွက် သတ်မှတ်တဲ့အရေအတွက်ပြည့်မှ ငွေချေတာပါ။ အကယ်လို့သာ ချိန်သားမကိုက်ဘဲ တစ်ယောက်တစ်ပေါက်လုပ်နေကြရင် အဲဒီ့အိုင်ပီတွေအကုန် အပိတ်ခံရမှာပါ။

နည်းပညာအရလည်း DDoS ဆိုတာ အများကြီး ဝိုင်းလုပ်ရတဲ့ ကိစ္စမျိုးပါ။ ဆုကြေးရဖို့လည်း ပါဝင်မဲ့သူတွေ အတိုင်းအတာတစ်ခုအထိ လိုမှာပါ။ ဒီအတွက်ကြောင့်ပဲ ပါဝင်ချင်တဲ့သူတွေကို ဘယ် Block ကို ရွေးမယ် (ဘယ်ဒိုမိန်းကို တိုက်မယ်) ဆိုတာကို ရွေးချယ်ခွင့် ပေးထားတာပါ။

PAY_TO_DDOS လုပ်ဆောင်ချက် ကို ဝက်ဆိုက်အက်ဒမင် (Website Admin) တွေသာမကပဲ တခြားသူတွေလည်း ရယူနိုင်ပါတယ်။ ဒီစနစ်ကို ထွင်ရတဲ့အကြောင်းကတော့ ဒိုမိန်းပိုင်ရှင်တွေ အနေဖြင့် ငွေနည်းနည်းသုံးရုံနဲ့ ကိုယ့်ဝက်ဆိုက်ရဲ့ ခံနိုင်အားကို စမ်းသပ်နိုင်ဖို့ပါပဲ။
ဒီစနစ်ဟာ စာတမ်းတင်ထားရုံသာ ရှိပါသေးတယ်။ လက်တွေ့အနေနဲ့ အကောင်အထည်မဖော်နိုင်သေးပါဘူး။ တကယ်လို့ အဲဒီလိုဝက်ဆိုက်ဖြစ်လာရင်လည်း ဥပဒေအရ အရေးယူတာ ခံရမှာပါ။ သူတို့ရဲ့ အခုဖွယ်စာတမ်းကို https://www.usenix.org/system/files/conference/woot16/woot16-paper-wustrow.pdf မှာ အသေးစိတ် ဖတ်ရှုနိုင်ပါသေးတယ်။

15-8-2016
သတင်းစီစဉ်တင်ဆက်သူ - Nub90d (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# ဝင်ငွေမှန်နေသည့် တရုတ်ဟက်ကာများ

တရုန်နိုင်ငံမှာ လုံခြုံရေးလုပ်ငန်း တစ်ခုဖြစ်သည့် ချီတာမိုဘိုင်း (Cheetah Mobile) မှ သုတေသီများ၏ အဆိုအရ ၂၀၁၄ ခုနှစ်က ပေါ်ထွက်ခဲ့သည့် Hummer အန်ဒရိုက်ထရိုဂျန် (Android Trojan) တစ်မျိုးသည် စမတ်ဖုန်း (Smart Phone) အသီးသီးသို့ လျင်လျင်မြန်မြန် ကူးစက်နေကြောင်း သိရသည်။ ၂၀၁၅ ခုနှစ်မှစ၍ ကူးစက်မှု အရှိန်ရလာသည့် အဆိုပါထရိုဂျန်သည် နေ့စဉ်ကူးစက်မှုနှုန်း (၁.၆) သန်းခန့် ရှိသည်။ ယခင်လများတွင် ပျံ့နှံ့မှုကျဆင်းလာသော်လည်း တစ်နေ့ကူးစက်နှုန်း (၁) သန်းဟူသော ပမာဏသည် နည်းပါးသည်ဟု မဆိုနိုင်သေးပေ။ ၂၀၁၆ ခုနှစ်အစပိုင်းတွင် တစ်နေ့ကူးစက်နှုန်း (၁၁၈၇၇၂၂) ဖြင့် အမြင့်ဆုံးသို့ ရောက်ရှိခဲ့ဖူးသည်။ အဆိုပါကိန်းဂဏန်းသည် ပြိုင်ဘက်ထရိုဂျန်တစ်ခုဖြစ်သော GhostPush ၏ နှုန်းထားဖြစ်သည့် (၆၉၁၀၇၉) ထက် နှစ်ဆနီးပါး သာလွန်သည်။

Hummer သည် Rooting Exploit ပါဝင်သည့် အန်ဒရိုက်မေးဂလ် ( Android Malware ) အမျိုးအစား ဖြစ်သောကြောင့် ကူးစက်ခံရသည်နှင့် အသုံးပြုသူ၏ ခွင့်ပြုချက်ကို ရယူခွင့်မလိုဘဲ အလိုရှိသည့်အတိုင်း ထိန်းချုပ်ကိုင်တွယ်သွားနိုင်စွမ်းရှိသည်။ ဖုန်း/တက်ဘလက် (Phone / Tablet) အတွင်းသို့ ထရိုဂျန် ရောက်ရှိသွားသည်နှင့် Adware များ ပေးပို့ခြင်း၊ အချက်အလက်များ ရယူခြင်း၊ မိုဘိုင်းသုံး ဆော့ဖ်ဝဲလ်များ ထည့်သွင်းခြင်းတို့ကို Hummer အား ထိန်းချုပ်သူများက ဆက်လက်လုပ်ဆောင်နိုင်ကြောင်း သိရသည်။

ကူးစက်ခံရသည့် အန်ဒရိုက်ပစ္စည်းတိုင်းအား ဆော့ဖ်ဝဲလ်တစ်ခုခန့် နေ့စဉ်ပေးပို့ကြောင်း ချီတာမိုဘိုင်းက ခန့်မှန်းထားသည်။ လက်ရှိတွင် နေ့စဉ်ကူးစက်သည့် ဖုန်း/တက်ဘလက် အရေအတွက်မှာ (၁) သန်းခန့်ရှိရာ Adware တစ်ခု ထည့်သွင်းပေးရန် ဆင့် (၅၀) ရရှိပါက အဆိုပါ Malware အား ဖြန့်ဖြူးသူများအနေဖြင့် ဒေါ်လာ (၅) သိန်းခန့် နေ့စဉ်ရရှိနိုင်ကြောင်း တွေ့ရသည်။ ဤပမာဏသည်သာ အမှန်တကယ်ဖြစ်ခဲ့ပါက လက်ရှိအသုံးများနေသည့် Ransomware များ၊ ငွေကြေးဆိုင်ရာ အချက်အလက်များ ခိုးယူသည့် ထရိုဂျန်များ၊ ကြော်ငြာလိမ်များဖြင့် ငွေရှာခြင်းထက် များစွာဝင်ငွေကောင်းနေသည်မှာ အမှန်ပင်ဖြစ်သည်။

Hummer အား ထိန်းချုပ်သည့် ဒိုမိန်းများအား ခြေရာခံသည့်အခါ ဒိုမိန်းများအား ရယူထားသည့် အီးမေးလ်အများစုမှာ တရုတ်နိုင်ငံမှ ဖြစ်ကြောင်း ချီတာမိုဘိုင်းမှ သုတေသီများက ထုတ်ဖော်နိုင်ခဲ့သည်။ ထို့အပြင် အဆိုပါထရိဂျန်သည်လည်း တရုတ်မြေအောက်စျေးကွက်မှ ထွက်ပေါ်လာခြင်းဖြစ်နိုင်ကြောင်း သုံးသပ်ထားသည်။

Hummer ကူးစက်ခံရသူ အများစုမှာ အိန္ဒိယ၊ အင်ဒိုနီးရှား၊ တူရကီ၊ တရုတ်နှင့် မက္ကဆီကိုတို့မှ အန်ဒရိုက်ပစ္စည်းများ ဖြစ်သည်။ အိန္ဒိယနိုင်ငံ တစ်ခုတည်းတွင်ပင် အကူးစက်ဆုံးဖြစ်သည့် အန်ဒရိုက် Malware တို့အနက် နံပါတ် (၂) နှင့် နံပါတ် (၃) နေရာတို့ကို Hummer မျိုးကွဲနှစ်ခုက နေရာယူထားသည်။

Hummer ထရိဂျန်၏ အန္တရာယ်ကြီးမှုပမာဏကို သိရှိနိုင်ရန် ချီတာမိုဘိုင်းမှ လက်တွေ့စစ်ဆေးချက်တစ်ခု ပြုလုပ်ခဲ့ရာ ကူးစက်သည့် ပစ္စည်းတစ်ခုသည် ကွန်ယက်ချိတ်ဆက်မှုပေါင်း (၁၀၀၀၀) ခန့်ပြုလုပ်ကာ နာရီအနည်းငယ်အတွင်း (၂) ဂစ်ဂါဘိုက်ဒေတာပမာဏသုံး၍ အန်ဒရိုက်ဆော့ဖ်ဝဲလ်ပေါင်း (၂၀၀) ကျော်ကို Install ပြုလုပ်ခဲ့ကြောင်း တွေ့ရသည်။

16-8-2016

သတင်းစီစဉ် တင်ဆက်သူ - Nub90d (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# အပြိုင်အဆိုင် Bug Bounty

Current Hitlist

| TARGET | MAXIMUM |
|---|---|
| iOS 9.3+ | $500000 |
| Google Chrome | $150000 |
| Microsoft EDGE | $125000 |
| Firefox | $80000 |
| Windows 10 LPE | $75000 |
| Adobe Reader | $60000 |
| Adobe Flash | $60000 |

More items are available. Please login to see the complete list.

Bug ဆိုတာကတော့ System တစ်ခု ရဲ့ ချို့ယွင်း အားနည်းချက်များလို့ အလွယ်တကူ မှတ်ယူနိုင်ပါတယ်။ အသေးစိတ်ကို ထပ်မံ ဖော်ပြရမယ်ဆိုရင်တော့ Bug ဆိုတာ System တစ်ခုတွင် ဖန်တီးသူ၏ သတိမမူမိသော လုပ်ဆောင်ချက်များမှ တဆင့်ဖြစ်ပေါ်လာသော အားနည်းချက် ယိုပေါက်များဖြစ်သည်။ Hacker များသည် ထိုအားနည်းချက် ယိုပေါက်များကို အမြဲရှာဖွေနေလေ့ရှိကာ တိုက်ခိုက်တတ်ကြပါသည်။

Bug Bounty ဆိုတာကတော့ Bug များကို ရှာဖွေသည့် အစီအစဉ်ဖြစ်သည်။ ထိုအစီအစဉ်တွင် မည်သူမဆို ပါဝင်ဆင်နွှဲနိုင်သည်။ Bug များကို ရှာဖွေသည့် သူများကိုတော့ Bug Bounty Hunter လို့ခေါ်တွင်ပါတယ်။

ယနေ့ခေတ်တွင် Bug Bounty အစီအစဉ်များစွာရှိပါတယ်။ Apple , Facebook , Youtube , Twitter , Pentagon စသည့် လူသိများသော Website များ Social Media များတွင် Bug Bounty အစီအစဉ်များကို များစွာ ပြုလုပ်ပေးလျက်ရှိပါတယ်။ Bug Bounty အစီအစဉ်တွင် ပါဝင်မည့် Bug Bounty Hunter များကိုလည်း ကမ္ဘာတဝှမ်း ဖိတ်ခေါ်ပြီး ပါဝင်ဆောင်ရွက်စေပါတယ်။ ဆုကြေးငွေများကလည်း မနည်းလှသော ပမာဏဖြစ်သည်။ ယခုဆိုလျှင် သူထက်ငါ အပြိုင်အဆိုင် Bug Bounty အစီအစဉ်များ ရေးဆွဲပြီး ဆုကြေးငွေများကိုလည်း တစ်စထက် တစ်စ တိုးမြှင့် ပေးလျက်ရှိပါတယ်။

Bug Bounty တွင် Zero Day Exploit ဆိုတာရှိပါတယ်။ Zero Day Exploit ဆိုတာကတော့ တစ်ခါမှ မရှာဖွေရသေးသော ပထမဦးဆုံးရှာဖွေ တွေ့ရှိသည့် Bug ဖြစ်ပါတယ်။ Facebook တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၁၀၀,၀၀ ၊ Apple တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၂၀၀,၀၀၀ ၊ Google တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၂၀၀,၀၀ ၊ Twitter တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၁၀၀,၀၀ ၊ Microsoft တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၁၀၀,၀၀ နှင့် Pentagon တွင် Zero Day Exploit အတွက် အမေရိကန် ဒေါ်လာ ၁၀၀,၀၀ စသည်ဖြင့် ဆုကြေးငွေပမာဏ အသီးသီးရှိကြပါတယ်။

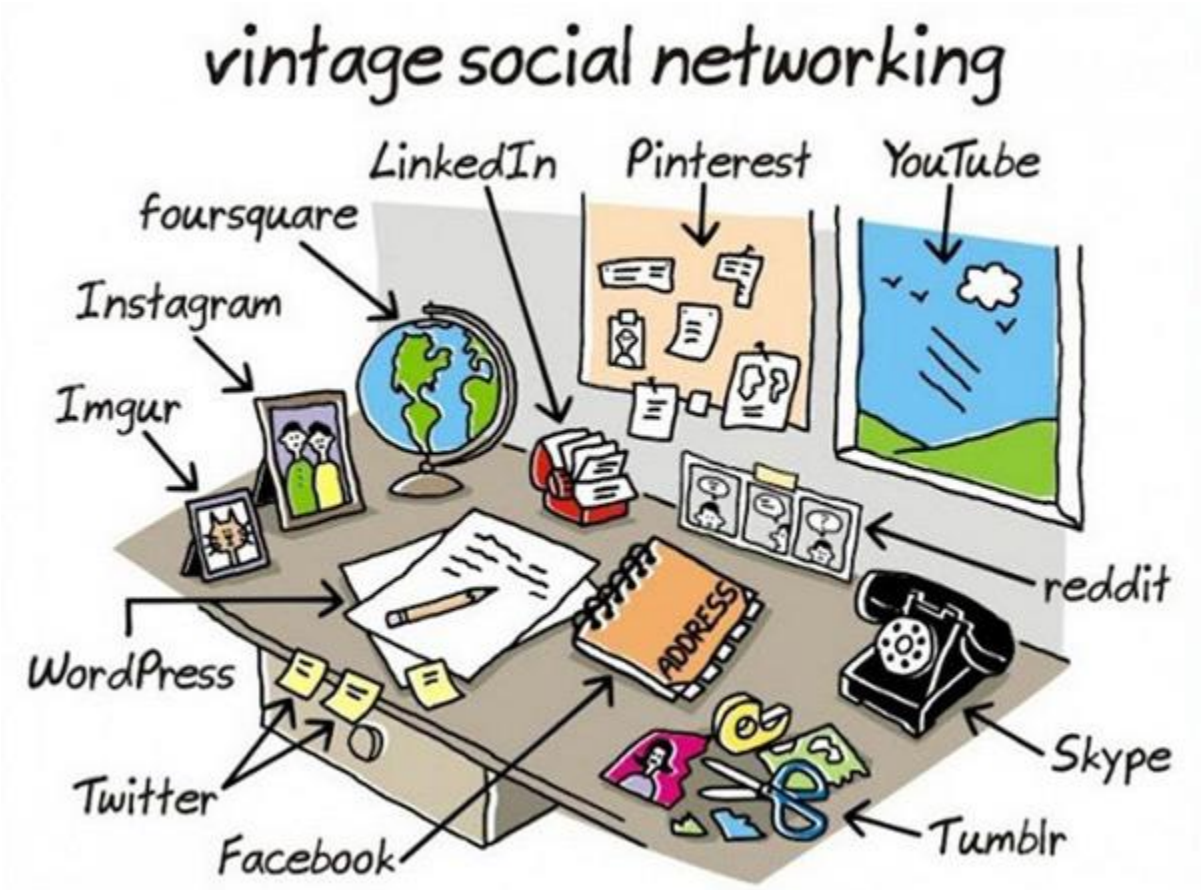
Exodus ကတော့ အခြားသူများထက် အဆများစွာ သာလွန်သော ဆုကြေးငွေပမာဏကို သတ်မှတ်ပေးလိုက်ပါတယ်။ ဒါကတော့ Bug Bounty အစီအစဉ်အတွက် ထူးခြားသော စိန်ခေါ်မှု့တစ်ရပ်ပါဘဲ။ Exodus သည် Zero Day Exploit များကို ရောင်းချခြင်း ၀ယ်ယူခြင်း စသည့် လုပ်ငန်းများကို လုပ်ကိုင်နေသော ကုမ္ပဏီ တစ်ခုဖြစ်သည်။ Bug Bounty အစီအစဉ်အတွက် ငွေကြေးပမာဏမှာ မျက်စိကျစရာဖြစ်ပါတယ်။ Bug Bounty Hunter များအနေဖြင့်လည်း မူရင်း သတ်မှတ်ထားသော ကုမ္ပဏီများမှာ Bug တွေကို ဖော်ပြမလား Exodus မှာ သွားရောင်းမလားဆိုရင် အများစုကတော့ Exodus မှာ သွားရောင်းကြပါလိမ့်မယ်။ ငွေကြေးပမာဏသည် မူရင်း ကုမ္ပဏီများတွင် ပေးသော ငွေကြေးပမာဏထက် အဆများစွာ သာလွန်သောကြောင့်ဖြစ်သည်။

Zero Day Exploit များကို အသုံးပြုပြီး တိုက်ခိုက်ခြင်းလုပ်ငန်းများကို ဆောင်ရွက်နိုင်ကာ ထို တိုက်ခိုက်ခြင်းလုပ်ငန်းများမှ ငွေကြေးမြောက်များစွာ ရရှိအောင် ဖန်တီးနိုင်ပါသည်။ ထို့ကြောင့် တိုက်ခိုက်သူများသည် Bug များကို အမြဲရှာဖွေနေလေ့ရှိသည်။ ထို့ကြောင့် Bug များသည် IT နယ်ပယ်တွင် မည်သည့် နေရာတွင်မဆို အရေးကြီးသော ယိုပေါက် အားနည်းချက်တစ်ခုဖြစ်သည်။ စာချစ်သူများအနေဖြင့် Bug များကို တွေ့ရှိပြီး ရောင်းချင်တယ်ဆိုရင်တော့ ပေးထားသော Link မှ တဆင့် Exodus ကို ဆက်သွယ် ရောင်းချနိုင်ပါကြောင်း အစီရင်ခံ ဖော်ပြလိုက်ရပါတယ် ခင်ဗျာ ...

https://rsp.exodusintel.com/

17-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ကိုရီချင် (MEHN Team)

ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်



# NSA ၏ Hacking အဖွဲ့ Hack ခံရ၊ ၎င်းတို့၏ Private Hacking Tools များ အွန်လိုင်းတွင် ထုတ်ဖော်ခံခဲ့ရ


US intelligence organization(NSA) နှင့် ပူးပေါင်းလုပ်ဆောင်နေသော Equation Group ဟု အမည်ရသည့် ဆိုက်ဘာတိုက်ခိုက်ရေးအဖွဲ့အား အမည်မဖော်လိုသည့် ဟက်ကာတစ်ယောက်(သို့မဟုတ်) ဟက်ကာတစ်ဖွဲ့မှ Hack ခဲ့ကြောင်း ပြောကြားခဲ့ပါတယ်။ ထိုသို့ Hack ခဲ့ပြီးနောက် Equation Group အသုံးပြုသော Malware, private exploits နှင့် အခြား Hacking tools များစွာကို ထုတ်ဖော်ခဲ့ပါတယ်။

ဒါဟာ ယုံကြည်ရခက်ခဲပေမယ့်လည်း အချို့သော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပညာရှင်များမှ ဖော်ထုတ်ထားသော အချက်အလက်များအား စစ်ဆေးပြီးနောက် ထို tools များသည် တရားဝင်ဖြစ်ကြောင်း တွေ့ရှိရပါတယ်။

ဇာတ်လမ်းက ဒီမှာတင်မရပ်သေးပါဘူး။ The Shadow Brokers လို့ ခေါ်တဲ့ အဖွဲ့မှ ဟက်ကာများဟာ ဆိုင်ဘာတိုက်ခိုက်မှုတွင် အကောင်းဆုံးစွမ်းဆောင်ပေးနိုင်သော weapons များနှင့် အချက်အလက်များကို Bitcoin ပေါင်း တစ်သန်း( US ဒေါ်လာပေါင် ၅၆၈ မီလီယံ) နှင့် အချိန်းအချက် ပြုလိုကြောင်းလည်း ပြောကြားခဲ့ပါတယ်။

Equation Group ဆိုတာလည်း လွန်ခဲ့သော ကာလများမှာ နံမည်ကြီးခဲ့သော Stuxnet တိုက်ခိုက်သူများနှင့် ဆက်ဆက်မှုနေတဲ့ အဖွဲ့ဖြစ်ပါတယ်။ ထိုအဖွဲ့အား US မှ အပြည့်အဝ ထောက်ပံ့ပေးနေသည်ဆိုသော်လည်း သက်သေပြစရာတော့ အခိုင်အလုံမပေးနိုင်ကြသေးဆဲ ဖြစ်ပါတယ်။

လွန်ခဲ့သော နှစ်ရက်ခန့်မှ The Shadow Brokers အဖွဲ့မှ Github နှင့် Tumblr တွင် Equation Group ၏ ဖိုင်များအား တင်ခဲ့ပါတယ်။ (ယခုအချိန်တွင် ပြန်ဖျက်သွားပြီး ဖြစ်ပါသည်)။ ဖိုင်များထဲတွင် အများဆုံးပါဝင်သည်မှာ Installation Scrips များ၊ command and control(C&C) Servers configuration ဖိုင်များနှင့် အမေရိကန်ထုတ်ဖြစ်သော Router, firewall များဖြစ်သည့် Cisco, Juniper, Fortinet တို့ကို ပစ်မှတ်ထားသည့် Exploit များပင် ဖြစ်လေသည်။ ထွက်ပေါ်လာသည့် ဖိုင်များအရ တရုတ်ကုမ္ပဏီတစ်ဖြစ်သော Topsec အားလည်း Equation Group မှ ပစ်မှတ်ထားနေကြောင်း တွေ့ရှိရပါတယ်။

အချို့သော ပညာရှင်များ ပြောဆိုနေသည်မှာလည်း ထိုဖော်ထုတ်ချက်များသည် သေချာစွာ သုတေသနပြုပြီး လုပ်ထားသော လိမ်ဆင်တစ်ခုသာဖြစ်ပြီး၊ Bitcoin ကိစ္စသည်လည်း ဘာမှမဟုတ်ကြောင်းနှင့် Media များမှ အာရုံကျလာစေရန် လုပ်ဆောင်ချက်တစ်ခုသာဖြစ်ကြောင်း ပြောကြားခဲ့ပါတယ်။

မည်သို့ပင်ဖြစ်စေ အမှန်သာ NSA ဟက်ခံခဲ့ရသည်ဆိုပါက ထိုတိုက်ခိုက်ခြင်းသည် ဆိုက်ဘာလောကအတွက် အလွန်မြင့်သော ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်မည်မှာ မလွဲပင်ဖြစ်ပါသည်။

18-8-2016
သတင်းစီစဉ်တင်ဆက်သူ :: ကိုသိန်း(MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# Public Network ကို ၁၁ မိနစ်အတွင်း ထိုးဖောက် ဝင်ရောက်ခဲ့သော အသက် ၇ နှစ်အရွယ် ပါရမီရှင်မလေး


နှစ်ရက်အတွင်း Public Wi-Fi Network မှ သတင်းအချက်အလက်များကို အသုံးပြုသူတွေ ဘယ်လောက်များများ ဖုန်းကနေ ရယူနိုင်သလဲဆိုတာ စုံစမ်းထုတ်ဖော် လေ့လာပြီး သည့် Conference တစ်ခုတွင် ၇ နှစ်အရွယ် ပါရီမီရှင်မလေးမှ တက်ရောက်နားထောင်ခဲ့ပြီးနောက် စိတ်ဝင်စားလာကာ Wifi Hotspot တစ်ခုကို စမ်းသပ် ထိုးဖောက် ခဲ့ပါတယ်။

ထို အသက် ၇ နှစ်အရွယ် ပါရမီရှင်မလေးမှ Online Video သင်ခန်းစာတွေကို ကြည့်ရှုပြီး Wi-Fi Hotspot ကို၁၀ မိနစ် ၅၄ စက္ကန့် အတွင်း ချိုးဖောက်နိုင်ခဲ့ပါတယ်။ Ethical Hacking Group များမှ လုံခြုံရေးပိုင်းဆိုင်ရာ ကျွမ်းကျင်သူများသည် Networks များ၏ အားနည်းချက်များကို အစဉ်တစိုက် ဖော်ပြပေးလျက်ရှိပါသည်။ ထို ဖော်ပြချက်များကို Video Files များဖြင့် ရှင်းလည်းထားချက်ပေါင်း များစွာလည်း ရှိပါသည်။ ထို Video Files များထဲတွင် ဖုန်းများအတွင်း ထိုးဖောက်ဝင်ရောက် ထားမှုများကို ပြသထားခြင်း ၊ Websites များအတွင်း ထိုးဖောက် ဝင်ရောက်မှုများကို ပြသထားခြင်း ၊ Networks များအတွင်း ထိုးဖောက် ဝင်ရောက်မှုများကို ပြသထားခြင်း စသည့် Video Files ပေါင်း များစွာ ပါဝင်ပါတယ်။ Video Files များတွင် အမှန်တယ် ထိုးဖောက်ဝင်ရောက်နိုင်သော နည်းလမ်းများကို ဖော်ပြပေးထားပါသည်။ ပါရမီရှင်မလေးမှ ထို Video Files များမှ သင်ခန်းစာများကို လေ့လာပြီ Public Network အား ထိုးဖောက် နိုင်ခဲ့ခြင်း ဖြစ်သည်။

Wifi နည်းလမ်းများ

Sniffing/Eavesdropping : Sniffing/Eavesdropping ဆိုသည်မှာ သားကောင်၏ အချက်အလက်များကို ဖမ်းယူခြင်း ခြေရာခံလိုက်ခြင်း ဖြစ်သည်။

Man In The Middle Attack : Man In The Middle Attack ကို အတိုကောက်အားဖြင့် MITMA ဟု ခေါ်ဆိုပါတယ်။ တိုက်ခိုက်သူသည် သားကောင်နှင့် Netwrok လမ်းကြောင်း ကြားအတွင်းသို့ ၀င်ရောက်လိုက်ပြီး သားကောင်နှင့် Network တို့အကြားတွင် အပြန်အလှန်ပေးပို့နေသည့် အချက်အလက်များကို ဖမ်းယူခြင်း ဖြစ်သည်။

DNS Cache Poisoning : DNS Cache Poisoning နည်းလမ်းတွင် တိုက်ခိုက်သူသည် DNS အတွင်း ရောက်ချင်သည့် လိပ်စာတစ်ခုကို အစားထိုးလိုက်ခြင်းဖြစ်သည်။ ဆိုလိုသည်မှာ မည်သည့် လိပ်စာကိုဘဲသွားသည်ဖြစ်စေ တိုက်ခိုက်သူ ဖန်တီးထားသည့် လိပ်စာကိုဘဲ လမ်းညွှန်စေရန် လုပ်ဆောင် လိုက်ခြင်း ဖြစ်သည်။

Rogue Access Points : Rogue Access Points ဆိုသည်မှာ Access Points အား Installation ပြုလုပ်ရာတွင် မှားယွင်းစွာ ပြုလုပ်မိသည့်အတွက် တိုက်ခိုက်သူများမှ တိုက်ခိုက်၍ ရနိုင်သွားခြင်း ဖြစ်သည်။

Unsecured Wifi Network : Unsecured Wifi Network ဆိုသည်မှာ Username and Passwords များ မပါရှိသော မလုံခြုံသော Wifi Networks များ ဖြစ်သည်။

WEP – Wired Equivalent Privacy : WEP သည် ပထမဆုံးသော Wireless Security လုပ်ငန်းစဉ်ဖြစ်သည်။

WPA – Wifi Proted Access : WEP ထက် ပိုမိုကောင်းမွန်သော Wireless Security လုပ်ငန်းစဉ် ဖြစ်သည်။ Temporal Key Integrity Protocol (TKIP) ကို အသုံးပြုထားပါသည်

WPA2-PSK - WPA2-PSK သည် WPA ကိုအဆင့်မြှင့်ထားသော Wireless Security လုပ်ငန်းစဉ် ဖြစ်သည်။ Pre Shared Key ကို အသုံးပြုထားပြီး အိမ်သုံး Wifi အမျိုးအစားဖြစ်သည်။

WPA2-AES – WPA2 ကိုဘဲ လုပ်ငန်းသုံးအတွက် ထုတ်လုပ်ထားခြင်းဖြစ်သည်။ Advanced Encryption Standard နည်းလမ်းဖြင့် ထုတ်လုပ်ထားခြင်း ဖြစ်သည်။

RADIUS – Remote Authentication Dial In User Service : RADIUS နည်းလမ်းသည် အသုံးပြုသူများအားလုံးအား ဗဟိုဦးစီးစံနစ်ဖြင့် ချုပ်ကိုင်ထားပြီး အသုံးပြုခွင့် ရှိသူများကိုသာ အသုံးပြုခွင့်ပေးထားသော နည်းလမ်းဖြစ်သည်။

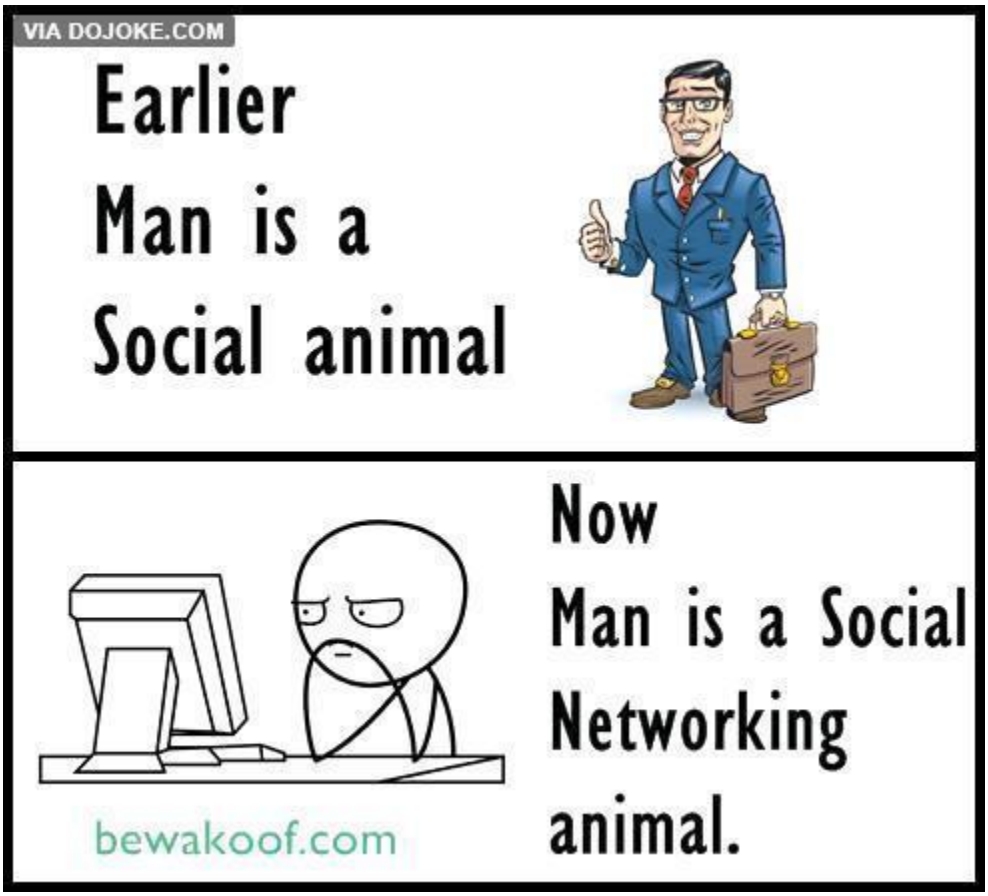
Channels : Channels ဆိုသည်မှာ Wireless အမျိုးအစားအပေါ်မူတည်ပြီး ကွဲပြားခြားနားသည့် ထုတ်လွှင့်မှု ပုံစံဖြစ်သည်။

Public Network များကို ထိုးဖောက်ရန်ဆိုသည်မှာ လွယ်ကူသည့်အလုပ်မဟုတ်ပေ။ သို့သော် Netwrok များ၏ အလုပ်လုပ်ပုံများကို ကောင်းမွန်စွာ သိရှိထားမည်ဆိုပါက ထိုးဖောက် တိုက်ခိုက်ရန်အတွက် များစွာ အထောက်အကူ ဖြစ်မှာ အမှန်ပင်ဖြစ်ပါတယ်။

22-8-2016

သတင်းစီစဉ် တင်ဆက်သူ - ပိုင်လင် (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**



# Android ဖုန်း ၉၀၀ မီလီယံ ကျော်၏ အားနည်းချက်များ


Android ဖုန်းများ၏ အားနည်းချက်ကို Qualcomm Chipsets အသုံးပြုထားသော ဖုန်းများတွင် ရှာဖွေတွေ့ရှိခဲ့ပြီး Android Smartphone တွေနဲ့ Tablet ၉၀၀ မီလီယံ ကျော်သည် တိုက်ခိုက်ခံနေရသည့် အခြေအနေတွင် ရှိနေပါတယ်လို့ ဖော်ပြခဲ့ပါတယ်။ Quardrooter အမည်ရသော လုံခြုံရေးပိုင်းဆိုင်ရာ နည်းပညာရှင်များသည် Android Mashmallow နှင့် Qualcomm Chipsets အသုံးပြုထားသော Android ဖုန်းများတွင် အားနည်းချက် ၄ ချက် ရှိနေကြောင်း ဖော်ထုတ်ခဲ့ပါတယ်။

ထို အားနည်းချက် ၄ ချက်မှာ -

1. CVE-2016-2503 ကို Qualcomm GPU driver တွင် တွေ့ရှိခဲ့ပြီး Google Android Security Bulletin မှ ဇူလိုင်လ ၂၀၁၆ ခုနှစ်တွင် ပြင်ဆင်ခဲ့ပါတယ်။
2. CVE-2016-2504 ကို Qualcomm GPU driver တွင် တွေ့ရှိခဲ့ပြီး Google Android ထိန်းချုပ်ရေးက ဩဂုတ်လ ၂၀၁၆ ခုနှစ်တွင် ပြင်ဆင်ခဲ့ပါတယ်။
3. CVE-2016-2059 ကို Qualcomm Kemel Module တွင် တွေ့ရှိခဲ့ပြီး ပြင်ဆင်နိုင်ခဲ့ပါတယ်။ သို့သော် ပြင်ဆင်နိုင်ထားပြီးဖြစ်သော Android ဖုန်းများ၏ အရေအတွက်ကို မသိရှိရသေးပေ။
4. CVE-2016-5340 ကို Qualcomm GPU Driver တွင် တွေ့ရှိခဲ့ပြီး ပြင်ဆင်နိုင်ခဲ့ပါတယ်။ သို့သော် ပြင်ဆင်နိုင်ထားပြီးဖြစ်သော Android ဖုန်းများ၏ အရေအတွက်ကို မသိရှိရသေးပေ။

Qualcomm ကတော့ ကမ္ဘာမှာ Designer LTE (Long Term Evolution) ကို ဦးဆောင်တဲ့အဖွဲ့ဖြစ်ပြီး LTE Modern စျေးကွက်မှာ 65% ပါဝင်ပါတယ်။ အကယ်၍ တိုက်ခိုက်သူများသည် မည်သည့် အားနည်းချက် တစ်ခုကို တိုက်ခိုက်သည်ဖြစ်စေ Android System တစ်ခုလုံးကို ထိန်းချုပ်နိုင်သွားမှာ ဖြစ်ပါတယ်။ တိုက်ခိုက်သူများသည် ထိုအားနည်းချက်များကို ထိုးဖောက်ပေးနိုင်သော Malware ပေါင်း မြောက်များစွာကိုလည်း ရေးသားထားပြီးဖြစ်ပါတယ်။ သားကောင်သည် တိုက်ခိုက်သူများ ဖန်တီးထားသော Malwares များကို Installation ပြုလုပ်မိသည်နှင့် တပြိုင်နက် ထိန်းချုပ်ခံရမှာ ဖြစ်ပါတယ်။

တိုက်ခိုက်ခံရနိုင်သော Android ဖုန်း များမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်။

- Samsung Galaxy S7 and Samsung S7 Edge
- Sony Xperia Z Ultra
- OnePlus One, OnePlus 2 and OnePlus 3
- Google Nexus 5X, Nexus 6 and Nexus 6P
- Blackphone 1 and Blackphone 2
- HTC One, HTC M9 and HTC 10
- LG G4, LG G5, and LG V10
- New Moto X by Motorola
- BlackBerry Priv

သင့်ဖုန်းရဲ့အားနည်းချက်ကိုဘယ်လိုစစ်ဆေးရင်ရမလဲ?

Android ဖုန်းများ၏ အားနည်းချက်များကို စစ်ဆေးနိုင်ရန်အတွက် Quadrooter မှ ထုတ်သော App ကို Installation ပြုလုပ်ထားရပါမယ်။

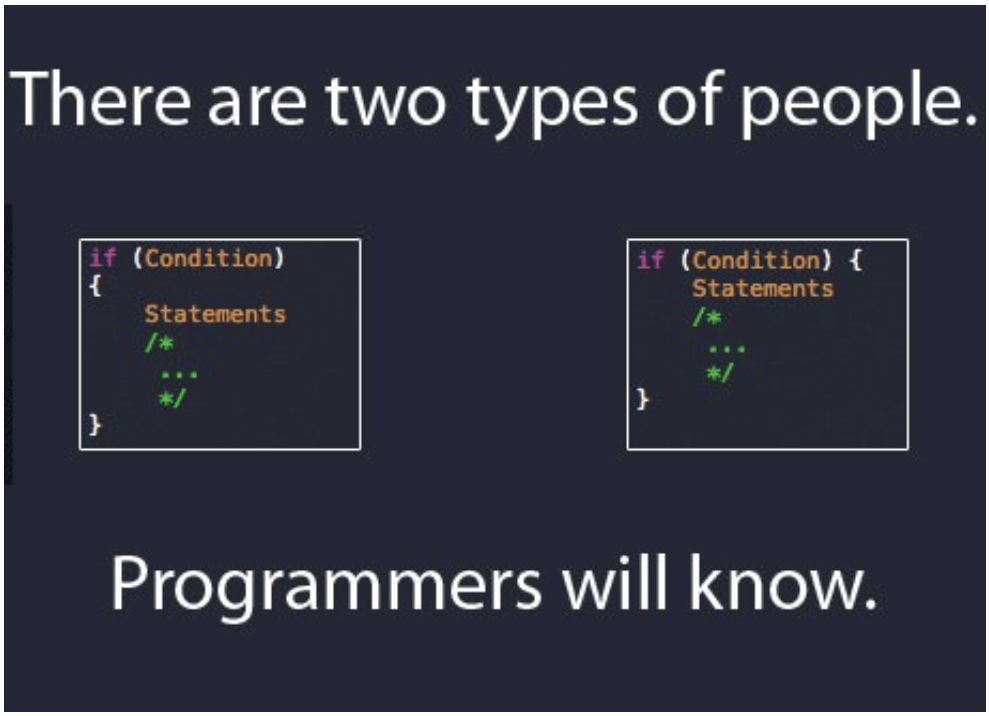
https://play.google.com/store/apps/details?id=com.checkpoint.quadrooter

လစဉ်ထုတ် Security Patch များကို မမြဲ ကြည့်ရှုနေပြီး ပြင်ဆင်ပေးထားရပါတယ်။

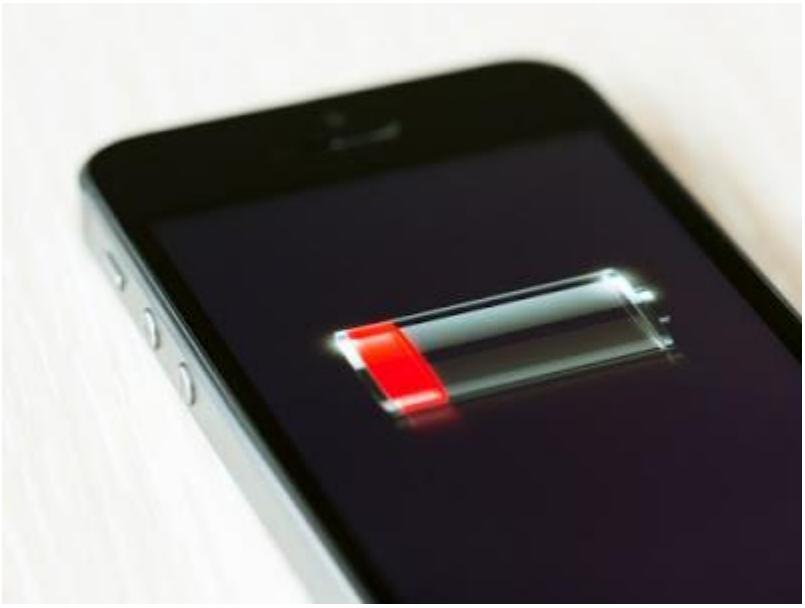
အမြဲ မပြတ် Android Version များကို မြှင့်တင်ထားရမည် ဖြစ်သည်။

23-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ပိုင်လင် (MEHN Team)

ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်



# Battery Status အချက်အလက် ပေးပို့မှုမှတဆင့် သင်၏ဖုန်းအား ထောက်လှမ်းနိုင်ခြင်း



HTML 5 Version အသစ်တွင် ဘက်ထရီအကြောင်းကို သိရှိစေနိုင်သော Function များစွာကို ထောက်ပံ့ပေးထားပါသည်။ ထို Function များမှတဆင့် ဖုန်းအသုံးပြုသူများ၏ ဘက်ထရီအား အခြေအနေများ (ဥပမာအားဖြင့် အားသွင်းရန်ကြာချိန် အားကုန်မည့်အချိန်များကို) Website များမှ သိစေနိုင်ပါသည်။ အကျိုးအမြတ်အားဖြင့် ဖုန်း၏ ဘက်ထရီ အားကုန်ခါနီးသောအခါ Website များသည် Low Power Version အခြေအနေဖြင့် အသုံးပြုသူများထံသို့ ဝန်ဆောင်မှု ပေးနိုင်ရန်ဖြစ်သည်။ ယမန်နှစ်က Security သုတေသနပညာရှင်များသည် ၎င်း HTML 5 Function များမှတဆင့် အသုံးပြုသူများ၏ အရေးကြီးသော အခြားအချက်အလက်များကိုပါ သိရှိစေနိုင်မည့် Code များကို ပေါင်းထည့်နိုင်ကြောင်း သတိပေးခဲ့သည်။ ယခုအချိန်တွင် ထိုသတိပေးချက်အား Princeton တက္ကသိုလ်မှ သက်သေပြလိုက်နိုင်ပြီဖြစ်သည်။

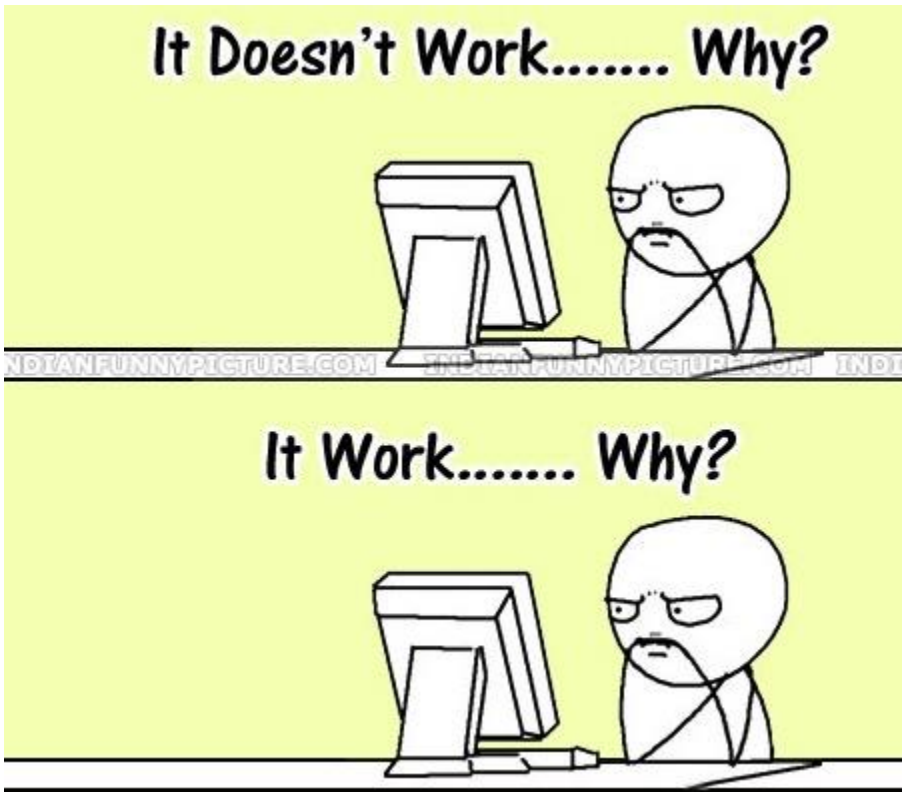
HTML 5 အားနည်းချက်များကြောင့် Battery အခြေအနေများကိုသာမက အခြားသော အချက်အလက်များကို Website များဆီသို့ ပေးပို့နိုင်ရန် ခိုင်းစေနိုင်သည်။ တိုက်ခိုက်မှု အောင်မြင်စေရန်အတွက်မှာ Attacker များအနေဖြင့် ၎င်းတို့၏ Website ဆီသို့ လာရောက်ကြည့်ရှုရန်သာ လိုအပ်ပါသည်။ အဆိုးဆုံးအချက်မှာ VPN ဖြစ်စေ AD Blocker တို့ကိုဖြစ်စေ သုံးသော်လည်း လုံခြုံမှုမရှိနိုင်ပါ။ Browser Cookie များ ဖျက်ပစ်သော်လည်း မရနိုင်ပါ။

ကာကွယ်ရန်နည်းလမ်းမှာ HTML 5 Feature များအား ပိတ်ပစ်ခြင်းပင် ဖြစ်သည်။ Firefox Browser တွင် အလွယ်တကူ ပိတ်နိုင်သော်လည်း အခြားသော Browser များတွင်မူ မပိတ်ပင်နိုင်သေးပေ။ ထို့ကြောင့် Browser ကုမ္ပဏီများသည် HTML 5 Feature များကို ပိတ်ပေးနိုင်မည့် Options များကို ထည့်သွင်းမည်ဟု သတင်းများ ထွက်ပေါ်လျက်ရှိကြောင်းသိရှိရပါသည်။

24-8-2016

သတင်းစီစဉ် တင်ဆက်သူ - Fr!d@y (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

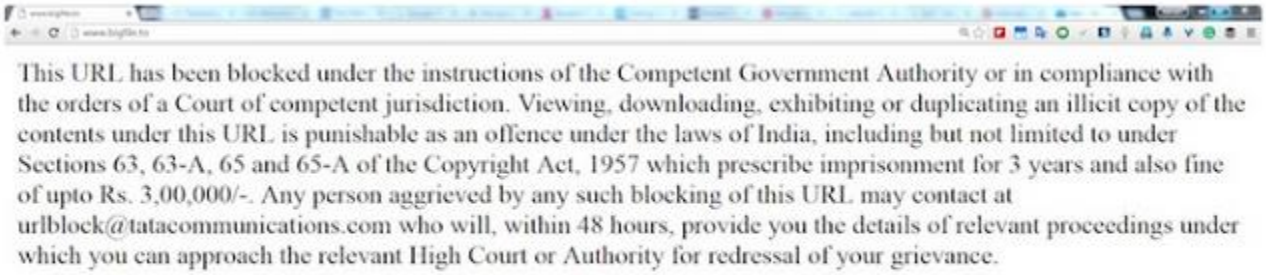


# Torrent ဆိုဒ် သုံးပါက ထောင်သုံးနှစ်ကျပြီး ဒဏ်ကြေးပေးရမည့် အိန္ဒယနိုင်ငံ


အိန္ဒယမှာ ထောင်ပေါင်းများစွာသော Torrent ဆိုဒ်များနှင့် အခြားသော ဖိုင် sharing ဆိုဒ်များကို banned ခဲ့ပြီးဖြစ်ပါတယ်။ ဒါပေမယ့် အိန္ဒယမှ အင်တာနက်သုံးစွဲသူများ မျက်လုံးပြူးသွားစေသော ကြော်ငြာချက်တစ်ကို တွေ့ခဲ့ရကြောင်း India Today ရဲ့ ဖော်ပြချက်အရ သိရှိရပါတယ်။

ထိုအကြောင်းအရာကတော့ ပိတ်ပင်ထားသော ပဘ်ဆိုဒ်များအား ပင်ရောက်ပါက ထောင်ဒဏ်သုံးနှစ်အပြင် ဒဏ်ကြေးသုံးသိန်းပေးဆောင်ရမည်ဆိုသည့်အကြောင်းပင်ဖြစ်ပါသည်။ ထိုဥပဒေတွင် သင်သည် တားမြစ်ထားသော ပဘ်ဆိုဒ်အား ပင်ရောက်ခြင်း၊ torrent file များအား download ချယူခြင်းတို့ ပြုလုပ်ပါက ပြစ်ဒဏ်ခံရမည်ဖြစ်ပါသည်။ ထို့အပြင် torrent ဖိုင်များ၊ pirated movies များအား ရယူခြင်းမရှိပဲ ထိုတားမြစ်ထားသော Site Link အား ပင်ရောက်ယုံဖြင့် အပြစ်ဒဏ်ကျခံရမည် ဖြစ်ပါသည်။

အိန္ဒယအစိုးရအနေဖြင့်လည်း torrent ဆိုဒ်များအား ပိတ်ပင်ရန်နည်းလမ်းအသစ်များအား အသုံးပြုထားပြီးဖြစ်ပါသည်။ အိန္ဒယအစိုးရ၏ တောင်းဆိုမှုအရ ISP(internet ပေးသည့် company) အများအနေဖြင့်လည်း ငွေကြေးအကုန်အကျများစွာဖြင့် ထို torrent ဆိုဒ်များအား ပိတ်ပင်နိုင်ရန် ပြုလုပ်ခဲ့ပါသည်။ အစိုးရအဖွဲ့အနေဖြင့် company အသေးများထက် အိန္ဒယ၏ ကြီးမားသော ဆက်သွယ်ရေး company များဖြစ်သည့် Airtel , Tata Communications တို့နှင့် ညှိနှိုင်းဆောင်ရွက်မှုများ ပြုလုပ်ခဲ့ပါသည်။




ထိုသို့ ပိတ်ပင်ခြင်းသည် torrent အား တရားဝင်အသုံးပြုနေသော လုပ်ငန်းရှင်များနှင့် အနုပညာရှင်များစွာ များစွာ သက်ရောက်မှုရှိခဲ့ပါသည်။ opensoure software များ၊ Linux Distro များမှာ ထို torrent ပေါ်တွင် အများဆုံး Distribute လုပ်ကြပါတယ်။ ယခုအချိန်အထိတော့ အိန္ဒယမှ ကြော်ငြာချက်အားပြင်ဆင်ခြင်း ရုတ်သိမ်းခြင်းများ မလုပ်သေးပါဘူး...သတင်းလွတ်လပ်ခွင့်ကို အလေးပေးအော်ဟစ်နေသော ယနေ့ခေတ်တွင် နောက်ထပ်မည်သို့ ဆက်လက်လုပ်ဆောင်မည်ဆိုသည်ကိုတော့ စောင့်ကြည့်ရမှာပဲ ဖြစ်ပါတယ်။

25-8-2016
သတင်း စီစဉ်တင်ဆက်သူ - ကိုသိန်း( MEHN Team )

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**

# Apple မှ အရေးပေါ် ကြေငြာချက် ထုတ်ပြန်


25-8-2016 ရက်နေ့တွင် Apple မှ IOS 9.3.5 နောက်ဆုံး Version ကို ထုတ်ပေးခဲ့ပါတယ်။ ထုတ်ပေးရသော အကြောင်းရင်းမှာ iPhones များနှင့် iPads များတွင် Zero-day Exploit များ တွေ့ရှိခဲ့ခြင်းကြောင့် ဖြစ်သည်။ Zero-day Exploit ဆိုသည်မှာ တစ်ခါဘူးမျှ မည်သူမျှ မဖော်ထုတ်ရသေးသည့် ယိုပေါက်အားနည်းချက်ဖြစ်သည်။ ထို Zero-day Exploit ကို UAE နိုင်ငံရှိ လူ့အခွင့်အရေး တက်ကြွလှုပ်ရှားနေသူ Ahmed Mansoor ၏ ဖုန်းတွင် စတင် တွေ့ရှိခဲ့ခြင်း ဖြစ်သည်။

ကမ္ဘာ့အကြီးဆုံး Exploit Software များကို ရေးသားနေသော NSO Group မှ အဆိုပါ Zero-day Exploit ကို ဖန်တီးခဲ့ခြင်းဖြစ်သည်။ ဖန်တီးရသည့် ရည်ရွယ်ချက်မှာ အတိုက်အခံများ ၊ သတင်းသမားများကို နောက်ယောင်ခံလိုက်နိုင်ရန်နှင့် အချက်အလက်များ ရယူနိုင်ရန်အတွက်ဖြစ်သည်။ ထို NSO Group သည် မြောက်များလှစွာသော ပြည်သူပြည်သားများ၏ ဖုန်းများအတွင်း Malware များထည့်သွင်းကာ လှို့ဝှက်ထောက်လှမ်းနေခဲ့သည်မှာ အချိန်အတော်ကြာခဲ့ပြီ ဖြစ်သည်။

Apple ၏ ယခု ဖြစ်ပေါ်နေသော Zero-day Exploit သည် တည်နေရာကို သိရှိနိုင်ခြင်း ၊ ဖုန်းထဲတွင် မှတ်သားထားသော ဖုန်းနံပါတ် လိပ်စာများကို သိရှိနိုင်ခြင်း ၊ စာပေးပို့သည့် စာများကို ဖတ်ရှုနိုင်ခြင်း ၊ ခေါ်ဆိုထားသော ဖုန်းနံပါတ် လိပ်စာများအား ကြည့်ရှုနိုင်ခြင်း ၊ စကားပြောခွက်ကို ထိန်းချုပ်နိုင်ခြင်း စသည့် တို့ကို လုပ်ဆောင်နိုင်ပါသည်။

ရာဇဝတ်မှုများ ဖမ်းဆီးနှိမ်နင်းရာတွင် ကူညီပါဝင် ဆောင်ရွက်လျက်ရှိသော Citizen Lab နှင့် Lookout တို့မှ Zero-day Exploit နှင့် ပတ်သက်သော အကြောင်းကြားစာများအား Apple သို့ ပေးပို့ခဲ့သည်။ ထို့ကြောင့် Apple မှ အကြောင်းကြားစာ ရပြီးပြီးခြင်း ၁၀ ရက်အတွင်းမှာပင် အားနည်းချက်ကို ပြင်ဆင်နိုင်ရန်အတွက် IOS 9.3.5 ကို အရေးပေါ်အခြေအနေ ကြေငြာပြီး ထုတ်ပေးခဲ့ခြင်း ဖြစ်သည်။

စတင် ဖြစ်ပွားပုံ

United Arab Emirates တွင် နေထိုင်သူ Ahmed Mansoor သည် လူ့အခွင့်အရေး တက်ကြွစွာ လုပ်ရှားမှု့များကြောင့် "Martin Ennals" ဆုကို ရရှိထားဖူးပြီး လူသိများ ထင်ရှားသူတစ်ဦးဖြစ်သည်။ ၂၀၁၆ ခုနှစ် ဩဂုတ်လ ၁၀ ရက်နေ့တွင် အမည်မသိ လိပ်စာတစ်ခုမှ စာတို သတင်းပေးပို့ချက် တစ်ခုကို သူ၏ iPhone မှတဆင့် လက်ခံရရှိခဲ့သည်။ Ahmed Mansoor သည် အစိုးရ၏ နောက်ယောင်လိုက်ခြင်းကို ခံရဖူးသည့် အတွေ့အကြုံရှိသည့်အတွက် သက်ာ်မကင်းဖြစ်ကာ ပေးပို့လာသော စာတို သတင်းပေးပို့ချက်ကို Citizen Lab ရှိ သုတေသနပညာရှင် Bill Marczak ထံသို့ ပေးပို့ခဲ့သည်။ ထို့နောက် Citizen Lab မှ ဆန်ဖရန်စစ္စကိုရှိ မိုဘိုင်းဖုန်း လုံခြုံရေးနည်းပညာ ကုမ္ပဏီ Lookout သို့ ဆက်သွယ်ပြီး အဆိုပါ စာတို သတင်းပေးပို့ချက်ကို စီစစ်ရန်အတွက် အကူအညီပေးပါရန် အကြံဉာဏ် တောင်းခံခဲ့သည်။

စာတို သတင်းပေးပို့ချက်အား စမ်းသပ် စစ်ဆေး သုတေသန ပြုလုပ်ပြီးသည့်နောက်တွင် သုတေသန ပညာရှင်များမှ IOS အား တိုက်ခိုက်နိုင်သော Malware ကို ရှာဖွေ တွေ့ရှိခဲ့သည်။ ထို Malware ကြောင့် ဖြစ်ပွားနိုင်သော အားနည်းချက် ၃ ခုကိုလည်း ရှာဖွေ တွေ့ရှိခဲ့သည်။ ထို အားနည်းချက် ၃ ခုမှာ -
CVE-2016-4657 : အခြားသော Coding များကို ထပ်ပေါင်းထည့်နိုင်ခြင်း
CVE-2016-4655 : အတွင်းပိုင်းရှိ Memory အား လိုအပ်သလို ကိုင်တွယ်ခွင့် ရရှိနိုင်ခြင်း
CVE-2016-4656 : အတွင်းပိုင်းရှိ Coding များကို Admin အဆင့် ကိုင်တွယ်ခွင့်ရပြီး လိုအပ်သလို ပြုပြင်နိုင်ခြင်း

စသည်တို့ ဖြစ်ပွားစေနိုင်ပါသည်။

အကယ်၍ Ahmed Mansoor သာ ပေးပို့လာသော စာတို သတင်းပါ Link အား နှိပ်မိလိုက်မည်ဆိုပါက ဖုန်းတစ်ခုလုံး ထိန်းချုပ်ခံရပြီး အချက်အလက်များကို ရယူခြင်း ခံရမည် ဖြစ်သည်။ Citizen Lab မှ "တိုက်ခိုက်သူတွေက Ahmed Mansoor ရဲ့ ဖုန်းကို ထိန်းချုပ်လိုကြပြီး ဖုန်းကင်မရာ ၊ စကားပြောခွက် စသည်တို့မှ တဆင့် အဆက်အသွယ်ပြုလုပ်သော ဆက်သွယ်ချက်များကို မှတ်သားထားနိုင်ရန်အတွက် ကြိုးပမ်းကြခြင်း ဖြစ်ပါတယ်။ ထို့အပြင် ဖုန်းခေါ်ဆိုထားမှု့တွေ ၊ ဖုန်းနံပါတ် လိပ်စာတွေ ၊ စာပေးပို့ထားသော စာတိုတွေ စတာတွေကိုလည်း လိုချင်နေကြပါတယ်" လို့ ထုတ်ဖော်ပြောကြားခဲ့ပါတယ်။

Lookout ၏ ထုတ်ပြန်ကြေငြာချက်ထဲတွင်

အသုံးပြုသူများမှ ပေးပို့လာသော စာတို သတင်းပါ Link ကို ဖွင့်မိပါက Zero-day Exploit သည် Memory ၏ လုပ်ငန်းဆောင်တာများကို ဖောက်ပြန်စေပြီး Web Browser ကို အားနည်းချက်ဖြစ်ပေါ်စေကာ ထို အားနည်းချက်မှ တဆင့် တိုက်ခိုက်သူများမှ တိုက်ခိုက်နိုင်စေရန် ဖန်တီးပေးခြင်း

အတွင်းပိုင်းအဆင့် ပြင်ဆင်နိုင်သော လုပ်ငန်းဆောင်တာများဖြစ်သော Jailbreak လုပ်ငန်းစဉ်ကို လုပ်ဆောင်နိုင်ပြီး အသုံးပြုသူမသိစေဘဲ အခြားသော Malware များကိုပါ Installation လုပ်သွားနိုင်ခြင်း

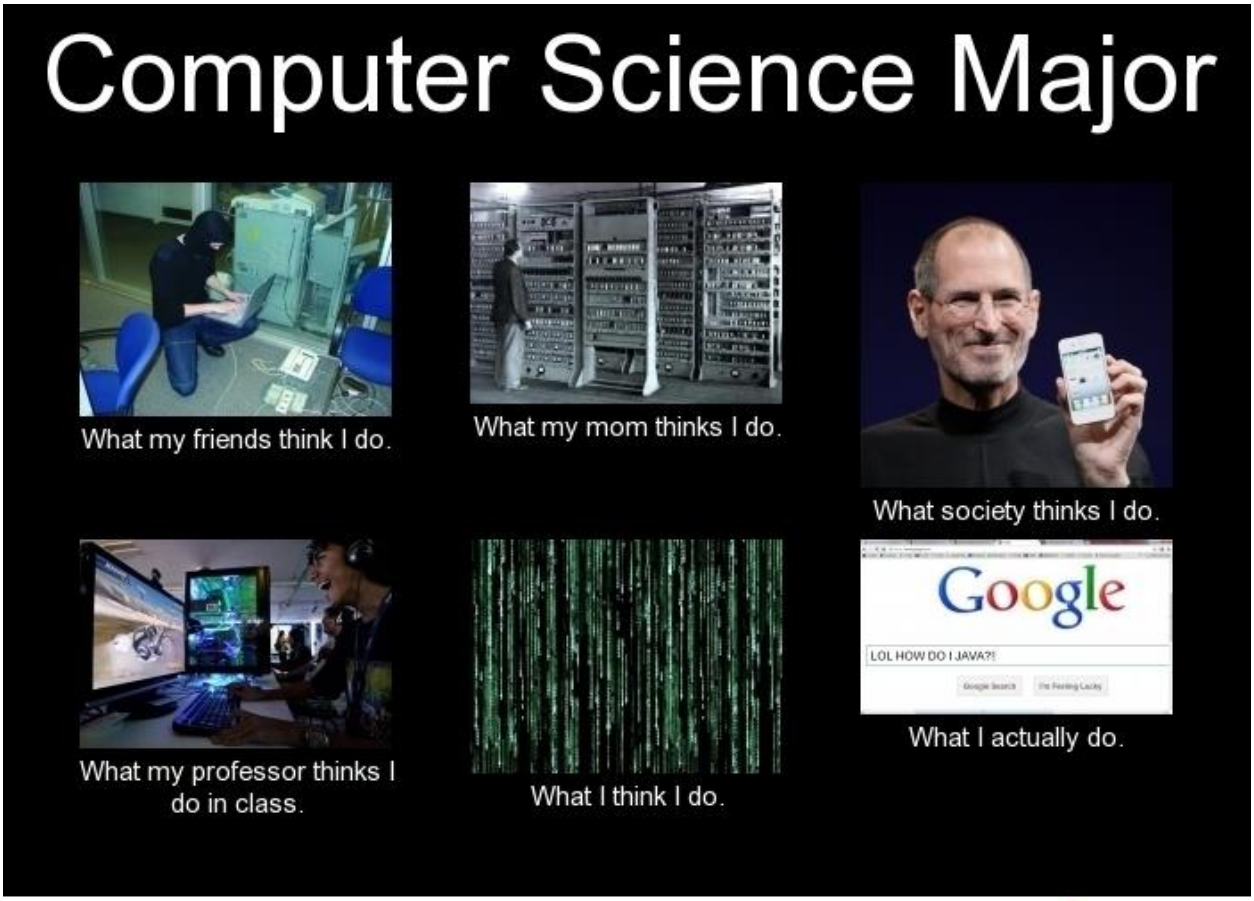
စသည့် တို့ကို ဖော်ပြထားပါတယ်။

Apple မှ ယခု ဖြစ်ပေါ်နေသော Zero-day Exploit သည် အသုံးပြုသူများအတွက် အလွန်ပင် အန္တရာယ်ကြီးကြောင်း ဖော်ပြထားပြီး အရေးပေါ် အခြေအနေတရပ်အဖြစ် ကြေငြာထားကာ Apple မှ နောက်ဆုံးထုတ်ပေးထားသော IOS Version 9.3.5 ကို Installation ပြုလုပ်ကြပါရန် နှိုးဆော်ထားပါသည်။

တိုက်ခိုက်သူများသည် နေရာတိုင်းတွင် ရှိပြီး အချိန်မရွေး တိုက်ခိုက်နိုင်ပါတယ်။ ထိုသို့ တိုက်ခိုက်ခြင်း မခံရအောင် နည်းပညာဗဟုသုတများ ရှာမှီးထားသင့်ပေသည်။ ယခု အားနည်းချက်သည် စာတို Link မှ တဆင့် တိုက်ခိုက်သွားခြင်းဖြစ်သည်။ ထို့ကြောင့် စာချစ်သူများအနေဖြင့် မည်သည့် နေရာမှ ဖြစ်စေ ယုတ်စွအဆုံး ကိုယ်နှင့် ရင်းနှီးခင်မင် ကျွမ်းဝင်သော မိတ်ဆွေ သူငယ်ချင်း အပေါင်းအသင်းများမှ မသိသော Link များကို Social Network မှတဆင့် ဖြစ်စေ Email မှတဆင့် ဖြစ်စေ ဖုန်း မှတဆင့် ဖြစ်စေ ပေးပို့လာပါက ဖွင့်မကြည့်မိစေရန် အလွန်ရေးကြီးပါသည်။ Malware များပါသော Link များကို ဖွင့်ကြည့်မိပါက တိုက်ခိုက်ခံရမည် ဖြစ်ပါကြောင်း ဖော်ပြလိုက်ရပါတယ် ခင်ဗျာ....

26-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - ကိုရီချင် (MEHN Team)

**ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်**



# အွန်လိုင်းပေါ်က ကွတ်ထိယမုဆိုးများ


အသက်မပြည့်သေးတဲ့ မိန်းကလေးတွေအပါအဝင် အမျိုးသမီးပုံ (၂၀၀၀) လောက်ကို တင်ထားတဲ့ ဩစတေးလျနိုင်ငံက ဝက်ဆိုက်တစ်ခုကို တွေ့ထားပါတယ်။ အဲဒီဆိုက်မှာ မှတ်ပုံတင်ထားတဲ့ သူတွေအနေနဲ့ တရားမဝင်ပုံတွေ အလဲအလှယ်လုပ်လို့ ရပါတယ်။ ပြီးတော့ တင်ပေးလိုက်တဲ့ ကောင်မလေးရဲ့ ကိုယ်ရေးအချက်အလက်တွေဖြစ်တဲ့ နာမည်အပြည့်အစုံ၊ လိပ်စာ၊ ကျောင်းနေသေးရင် တက်နေတဲ့ကျောင်းနဲ့ ဖုန်းနံပါတ်တွေကို ဖြည့်ပေးနိုင်တဲ့သူကို "အောင်မြင်တဲ့မုဆိုး" အဖြစ် သတ်မှတ်ပေးပြီး တရားမဝင် ဓာတ်ပုံတွေကို ဆုအနေနဲ့ ချီးမြှင့်ပါတယ်။

ဩစတေးလျမီဒီယာတစ်ခုဖြစ်တဲ့ News ကတော့ ဒီဝက်ဆိုက်စဖွင့်ခဲ့တဲ့ ၂၀၁၅ ဒီဇင်ဘာကစပြီး ဩစတေးလျကျောင်း (တက္ကသိုလ်၊ ကောလိပ်) ပေါင်း (၇၀) လောက်က ဆယ်ကျော်သက်အမျိုးအမီးတွေကို ပစ်မှတ်ထားခဲ့တာလို့ ဆိုထားပါတယ်။ ဝက်ဆိုက်မှာ မှတ်ပုံတင်တဲ့ လူငယ်တွေ အမျိုးသားတွေအနေနဲ့ ကျောင်း၊ ဒါမှမဟုတ် ရပ်ကွက်တစ်ခုခုက ပစ်မှတ်အနေနဲ့ သတ်မှတ်လိုက်တဲ့ အမျိုးသမီးပုံကို တင်ပေးရပါတယ်။ ပြီးရင် ဝက်ဆိုက်ထဲက မုဆိုးလုပ်ချင်တဲ့ တစ်ယောက်ယောက်က သူ့အချက်အလက်တွေပြည့်စုံအောင် သတင်းလိုက်စုပေးရတာပါ။ News သတင်းစာရဲ့ အဆိုအရတော့ တစ်ချို့ဆိုရင် သူငယ်ချင်းအုပ်စုတစ်ခုလုံးကိုတောင် ပစ်မှတ်အနေနဲ့ တင်ထားတာမျိုး ရှိတယ်လို့ ပြောပါတယ်။

သတင်းလိုက်စုပေးတဲ့သူက စုသလို၊ comment တွေနဲ့ အားပေးတဲ့သူတွေကိုလည်း တွေ့ရပါတယ်။ "သားကြီး ကြိုးစားထား ..." "မရရအောင် လိုက်ကွာ ..." ဆိုတာမျိုးတွေပေါ့။ အကယ်လို့ မုဆိုးတစ်ယောက်ယောက်က သတင်းအချက်အလက် ပြည့်ပြည့်စုံစုံရခဲ့ရင်တော့ အဲဒီကောင်မလေးရဲ့ ဝတ်လစ်စားလစ်ပုံတွေကို ဆုအဖြစ် ပေးအပ်ပါတယ်။

တစ်ခါတစ်လေတော့လည်း အဲဒီ့အမျိုးသမီး:ကို စိတ်ဝင်စားလို့ အချက်အလက်တွေလိုချင်လို့ သတင်းစုံစမ်းတာမျိုးလည်း ဖြစ်နိုင်ပါတယ်။ ဒီလိုအခြေအနေမျိုးဆိုရင်တော့ ဆုက တခြားလဲလှယ်စရာ တစ်မျိုးမျိုး ဖြစ်လာမှာပါ။ ဆိုကြပါစို့ ... ကောင်လေးတစ်ယောက်က ဓာတ်ပုံတစ်ပုံတင်ပြီး ဒီကောင်မလေးရဲ့ ဖုန်းနံပါတ်နဲ့ လိပ်စာပေးရင် ဘယ်လောက်ပေးမယ်ဆိုပြီး တင်တာမျိုးပေါ့။ လတ်တလောမှာတော့ အမျိုးသမီး (၃၀၀) လောက်ရဲ့ အချက်အလက်နဲ့ မိမွေးတိုင်းဖမွေးတိုင်းပုံတွေကို အောင်အောင်မြင်မြင်လဲလှယ်နိုင်ခဲ့တာ တွေ့ရပါတယ်။

ကျောင်းသူတော်တော်များများနဲ့ အမျိုးသမီး:တော်တော်များများဟာ ဒီလိုဝက်ဆိုက်ရှိတာ မသိကြပါဘူး။ သူတို့တင်လိုက်တဲ့ ဓာတ်ပုံတစ်ပုံဟာ ဒီဝက်ဆိုက်ပေါ်ရောက်သွားရင် အလိုလိုနေရင်း သားကောင်အဖြစ်ကို ရောက်သွားနိုင်ပါတယ်။ တစ်ချို့ကောင်လေးတွေကတော့ သူတို့သူငယ်ချင်းတွေဓာတ်ပုံနဲ့ ငွေရှာနေကြပြီးတော့၊ တစ်ချို့ကောင်လေးတွေကတော့ သူတို့သူငယ်ချင်းပုံတွေကို ပြန်ဖယ်ခိုင်းနေတာ တွေ့ရပါတယ်။ ကိုယ့်ဓာတ်ပုံကို လာပြန်ဖယ်ခိုင်းတဲ့ ကောင်မလေးတွေလည်း ရှိပါတယ်။ ဒါမျိုးဆိုရင် "ထိပ်တန်းစာရင်း" ထဲ ထည့်ပြီး လာဖယ်ခိုင်းတဲ့သူကို အပြစ်ပေးတာမျိုး လုပ်ပါတယ်။

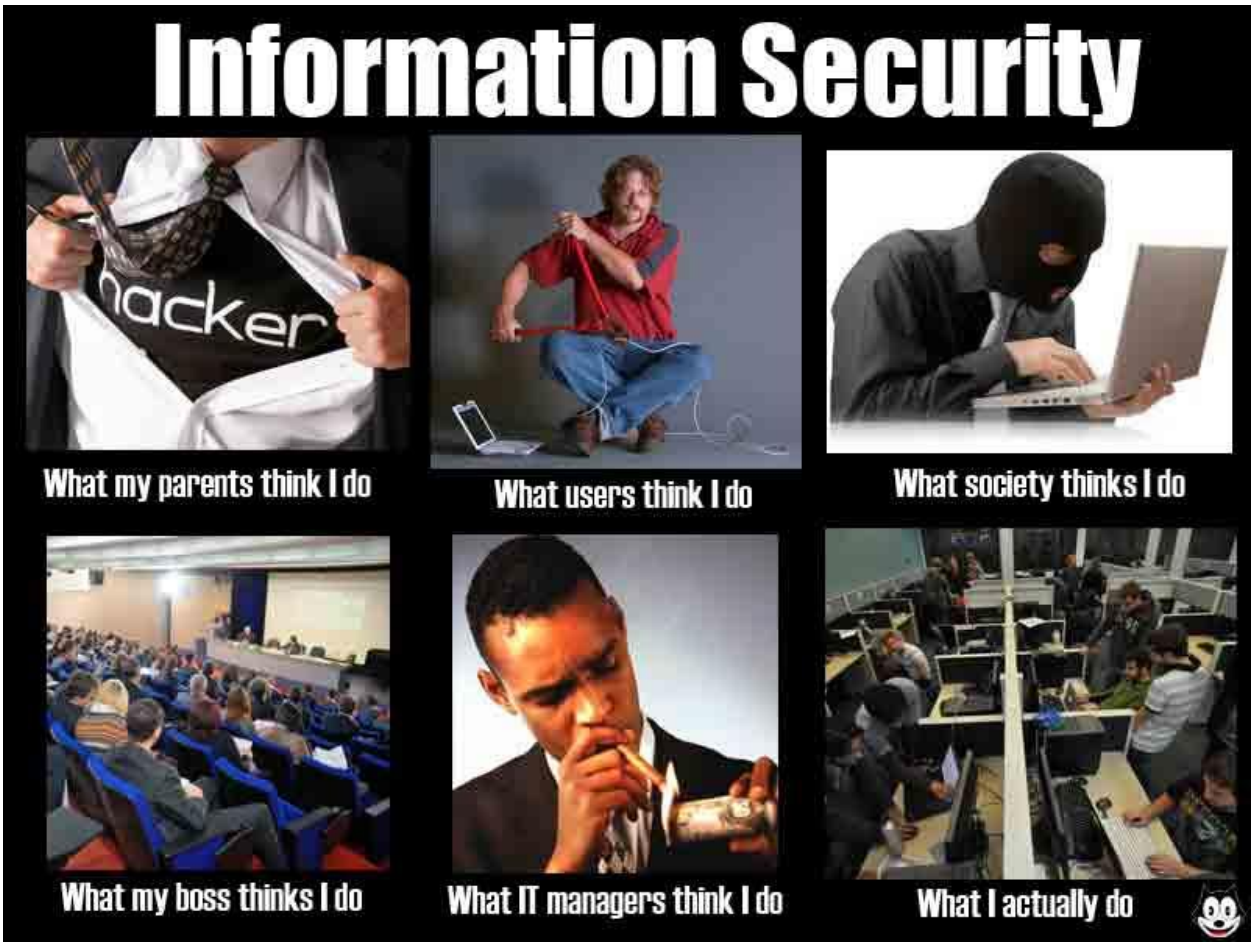
ဒီလို ကိုယ်ရေးအချက်အလက်တွေဖော်ထုတ်တဲ့ပြစ်မှုမျိုးဟာ ဩစတေးလျမှာဆို အမြင့်ဆုံးပြစ်ဒဏ်အနေနဲ့ ထောင် (၁၅) နှစ်အထိ ကျနိုင်ပါတယ်။ ဓာတ်ပုံကို တရားမဝင်အသုံးချတဲ့ ပုံတင်သူအနေနဲ့ကတော့ ထောင် (၅) နှစ်လောက် ကျနိုင်ပါတယ်။ မှတ်ပုံတင်ထားတဲ့ လူငယ်အများစုကတော့ ဗီဝီအန်နဲ့ သုံးကြတာတွေ့ရပေမဲ့ သေသေချာချာလိုက်ရင် ရပါတယ်။

ဒီဝက်ဆိုက်အကြောင်း ရဲကိုသတင်းပေးတဲ့သူတွေ အများကြီးရှိပါတယ်။ ဒါပေမဲ့ ဩစတေးလျဖက်ဒရယ်ရဲအဖွဲ့ကတော့ ဒီဆိုက်ကို တစ်ခြားနိုင်ငံတစ်ခုမှာ Hosting ထားထားလို့ ဖြုတ်ချရခက်နေတာပါလို့ အကြောင်းပြချက် ပေးပါတယ်။ နိုင်ငံတကာရဲတပ်ဖွဲ့နဲ့ ညှိနှိုင်းပြီး ထိရောက်တဲ့ပြစ်ဒဏ်ချနိုင်အောင် စီစဉ်သွားမှာပါလို့ သတင်းထုတ်ထားပါတယ်။ တကယ်တမ်းဆို ဆိုက်ကို ဖြုတ်မချနိုင်ရင်တောင် မှတ်ပုံတင်တဲ့သူတွေကို အပြစ်တစ်ခုခုပေးတာမျိုး လုပ်လို့ရပါတယ်။

ကိုယ်ရေးအချက်အလက်ဆိုတာ ကိုယ့်အကြောင်းပဲဖြစ်လို့ မသိသာပေမဲ့ မသမာတဲ့စိတ်ထားရှိတဲ့သူတွေအတွက် အရမ်းအရေးပါတဲ့အရာပါ။ လိပ်စာကတစ်ဆင့် သွားလေ့သွားထရှိတာတွေကို နောက်ယောင်ခံတာမျိုး၊ ဖုန်းနံပါတ်ကတစ်ဆင့် လိင်အသားပေးဝက်ဆိုက်တွေမှာ လိင်လုပ်သားအနေနဲ့ တင်ပြီး အရှက်ခွဲမယ်လို့ ခြိမ်းခြောက်တာမျိုးတွေ လုပ်လို့ရပါတယ်။ မြန်မာနိုင်ငံမှာလည်း ဒီကိစ္စတွေနဲ့ သိပ်မစိမ်းတော့ပါဘူး။ ဒါကြောင့် မြန်မာအမျိုးသမီးတွေအနေနဲ့ သတင်းအချက်အလက်လုံခြုံရေးကို သတိမူဖို့လိုကြောင်း အသိပေးလိုက်ရပါတယ်။

29-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - Nub90d (MEHN Team)

ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်



# တရုတ်နိုင်ငံသည် ဟက်ကင်းပြုလုပ်နိုင်မှုမှ ကာကွယ်နိုင်မည့် ဂြိုလ်တုတစ်ခုအား စမ်းသပ်လွှတ်တင်ထားခြင်း


Quantum နည်းပညာသည် စမ်းသပ်သုတေသနပြု လေ့လာနေဆဲဖြစ်သော နည်းပညာတစ်ခုဖြစ်သည်။ နည်းပညာစွမ်းပကားလည်း လွန်စွာမြင့်မားသည်။ NASA နှင့် Google တို့တွင် Quantum နည်းပညာ အသုံးပြု တည်ဆောက်ထားသော Super Computer များရှိကြသည်။ အဆိုပါ Super Computer များအတွက် အသုံးပြုသော OS ကိုလည်း တီထွင်ထုတ်လုပ်ထားရှိပြီးဖြစ်သည်။ Quantum နည်းပညာကို အနာဂတ် နည်းပညာပိုင်းတွင် ကျယ်ပြန့်စွာ နေရာယူလာမည်ဖြစ်သော နည်းပညာတစ်ခုအဖြစ် ပညာရှင်များက မျှော်လင့်ထားကြသည်။ Communication Security အပိုင်းတွင်လည်း Quantum နည်းပညာသည် မည်သည့် ကြားဖြတ်ဖမ်းယူမှုကိုမဆို ကာကွယ်ပေးနိုင်သောကြောင့် Security လွန်စွာမြင့်မားသည်ဟု ဆိုနိုင်သည်။ အဘယ်ကြောင့်ဆိုသော် Photon အမှုန်များကြားတွင် သတင်းအချက်အလက်များကို Encode ပြုလုပ်ပြီး ဆက်သွယ်မှု ပြုလုပ်သောကြောင့် ကြားဖြတ်ဝင်ရောက်ဖမ်းယူခြင်း ပြုလုပ်ပါက သတင်းအချက်အလက်များသည် အလိုအလျောက် ပျက်စီးသွားမည်ဖြစ်သည်။ ဥပမာအားဖြင့် လူနှစ်ယောက်သည် Encryption ပြုလုပ်ထားသော Message တစ်စောင်ဖြင့် ဆက်သွယ်မှုပြုလုပ်နေစဉ် ... တခြားသော လူတစ်ယောက် ဝင်လာသည်နှင့်တပြိုင်နက် Message သည် ဖတ်၍မရနိုင်သော အခြေအနေသို့ အလိုအလျောက် ပြောင်းလဲသွားမည်ဖြစ်သည်။

ယနေ့ခတ်သည် အီလက်ထရောနစ် နည်းပညာဖြင့် စောင့်ကြည့်ထောက်လှမ်းနေမှုများနှင့် ဆိုက်ဘာတိုက်ခိုက်မှုပေါင်းများစွာ ပေါ်ထွန်းနေသော ခေတ်တစ်ခေတ် ဖြစ်သည်။ ထို့ကြောင့် နိုင်ငံတကာ ပညာရှင်များအနေဖြင့် မည်သည့် ထိုးဖောက်တိုက်ခိုက်မှုကိုမဆို ကောင်းမွန်စွာ ကာကွယ်ပေးနိုင်မည့် စနစ်များကို အမြဲတစေ သုတေသနပြု စမ်းသပ်တီထွင်လျက်ရှိသည်။ ထို့ကြောင့် Quantum နည်းပညာသည် လုံခြုံမှုပိုင်းဆိုင်ရာ စနစ်များအတွက် ပညာရှင်များ အာရုံစိုက်လာသော အရာတစ်ခုဖြစ်လာသည်။

တာတိုဆက်သွယ်ရေးအပိုင်းတွင်လည်း Security သုတေသန ပညာရှင်များသည် Quantum နည်းပညာကို အသုံးပြုကာ လုံခြုံမှုအပြည့်ရှိကြောင်း စမ်းသပ်အတည်ပြုပြီး ဖြစ်သည်။ တာဝေးဆက်သွယ်မှုအပိုင်းတွင်မူ မစမ်းသပ်ရသေးချေ။ ယခုအချိန်တွင် Quantum နည်းပညာသုံး တာဝေးဆက်သွယ်မှု လုံခြုံရေးစနစ်အား တရုတ်နိုင်ငံသည် စမ်းသပ်ရန်အတွက် အစပျိုးလိုက်နိုင်ပြီဖြစ်သည်။ ၂၀၁၆ ဩဂုတ်လ ၁၅ ရက်နေ့က Quantum Mechanic Theory ၏ အခြေခံဥပဒေသများကို စမ်းသပ်လေ့လာရန်အတွက် ရည်ရွယ်ပြီး ကမ္ဘာ့ပထမဆုံးသော Quantum Communication Satellite (Quantum ဆက်သွယ်ရေး နည်းပညာသုံး ဂြိုလ်တု) တစ်ခုကို အာကာသဆီသို့ ကမ္ဘာ့ပတ်လမ်းကြောင်းတစ်ခုအတိုင်း လွှတ်တင်ထားလိုက်ပြီဖြစ်သည်။

ဂြိုလ်တုသည် အလေးချိန်အားဖြင့် ၆၀၀ ကီလိုဂရမ်ရှိသည်။ ဂိုဘီကန္တာရရှိ Jiuquan ဂြိုလ်တုလွှတ်တင်ရေး အခြေစိုက်စခန်းတွင် ဩဂုတ်လ ၁၅ ရက်နေ့က လွှတ်တင်ခဲ့ခြင်း ဖြစ်ပြီး ဂြိုလ်တု၏ တာဝန်ချိန်သက်တမ်းမှာ ၂ နှစ်သာ ဖြစ်ကြောင်းသိရှိရသည်။ ကမ္ဘာမြေပြင်အထက် ၁၂၀၀ ကီလိုမီတာ (၇၄၆ မိုင်) အကွာတွင် လွှတ်တင်ထားပြီး မြေပြင်ဆက်သွယ်ရေး အခြေစိုက်စခန်းများသည် တရုတ်နှင့် ဥရောပနိုင်ငံများတွင် ထားရှိသည်။ မြေပြင်ဆက်သွယ်ရေး စခန်းများအချင်းချင်း ချိတ်ဆက်မှုတွင် လုံခြုံမှု ရှိ / မရှိ စမ်းသပ်နိုင်ရန်အတွက် ဖြစ်သည်။

တရုတ်နိုင်ငံသည် အနာဂတ်တွင် Quantum Technology ၏ အရေးပါလာမှုအပေါ် ယုံကြည်လျက်ရှိသည်။ လာမည့် ၅နှစ်အတွင်း နိုင်ငံတော်စီးပွားရေး ဖွံ့ဖြိုးတိုးတက်မှုအတွက် မဟာဗျူဟာရေးဆွဲရာတွင် Quantum Technology အား ထည့်သွင်းရေးဆွဲထားသည်။ အမေရိကန်နိုင်ငံသည် Quantum နည်းပညာအတွက် တစ်နှစ်လျှင် ဒေါ်လာသန်း ၂၀၀ ထည့်သွင်းပေးထားသည်။ တရုတ်နိုင်ငံသည် Quantum နည်းပညာအတွက် ၂၀၀၅ ခုနှစ်မှစ၍ နှစ်စဉ် ဒေါ်လာ သန်း ၁၉၀၀ ထိ ရင်းနှီးမြုပ်နှံထားသည်။ ၂၀၁၅ ခုနှစ်တွင်မူ ဒေါ်လာသန်းပေါင်း ၁၁၀,၀၀၀ ထိ တိုးချဲ့ရင်းနှီးမြုပ်နှံထားသည်။

အကယ်၍ ဂြိုလ်တုသည် ၎င်း၏ Mission ဖြစ်သော မြေပြင်ဆက်သွယ်မှုစခန်းနှစ်ခု၏ ဆက်သွယ်မှုစနစ်တွင် လုံခြုံမှုလုံးဝစိတ်ချရမည် ဆိုလျှင် Encryption နှင့် Cryptography နည်းပညာနှစ်ခု၏ ကြီးမားသော အောင်မြင်မှု တစ်ခုကို မှတ်တိုင်ထူနိုင်မည်ဖြစ်သည်။

ဂြိုလ်တု Project ကို ဦးဆောင်သူ သိပ္ပံပညာရှင် Pan Jianwei သည် ဆင်ဟွာ သတင်းဌာနသို့ အောက်ပါအတိုင်း ပြောကြားခဲ့သည်။

"အခုလွှတ်တင်လိုက်တဲ့ ဂြိုလ်တုဟာ တရုတ်နိုင်ငံရဲ့ အခန်းကဏ္ဍကို ပြောင်းလဲစေမှာ အမှန်ပါပဲ။ အရင်တုန်းက တရုတ်နိုင်ငံဟာ တခြားနည်းပညာရဲ့ နောက်လိုက်အဖြစ် အသုံးပြုနေရတဲ့ နိုင်ငံကနေ နည်းပညာအသစ်တစ်ခုကို စွန့်ဦးတီထွင် မိတ်ဆက်ပေးမယ့် နိုင်ငံသစ်တစ်ခု ဖြစ်လာပါလိမ့်မယ်။ တကယ်လို့သာ ကျနော်တို့ စမ်းသပ်မှု အောင်မြင်ပြီး အာကာသ ပတ်လမ်းအတွင်းမှာလည်း Quantum နည်းပညာသုံး ဂြိုလ်တုတွေကို များများ လွှတ်တင်နိုင်ခဲ့မယ်ဆိုရင် တရုတ်နိုင်ငံဟာ လာမယ့် ၂၀၃၀ မှာ ကမ္ဘာလုံးဆိုင်ရာ Quantum နည်းပညာသုံး ဂြိုလ်တုဆက်သွယ်ရေး ကွန်ယက်တစ်ခုကို ပထမဆုံးတည်ထောင်ခဲ့တဲ့ နိုင်ငံတစ်ခုဖြစ်လာပါလိမ့်မယ် "

ပန်သည် အဆိုပါဂြိုလ်တု၏ Payload တွင်အောက်ပါအပိုင်း ၅ ပိုင်းတို့တပ်ဆင်ထားသည်။

၁။ Quantum Key Communicator (Quantum Key ချိတ်ဆက်မှုစနစ်)
၂။ Quantum Entanglement Emitter(Quantum photon ထုတ်လွှင့်မှုစနစ်)
၃။ Quantum Entanglement Source (Quantum photon ပင်မအရင်းအမြစ်)
၄။ Quantum Experiment Controller (Quantum နည်းပညာ ထိန်းချုပ်မှုစနစ်)
၅။ Processor
၆။ Laser Communicator (လေဆာချိတ်ဆက်မှုစနစ်)

အဆိုပါ Payload များကို ဘေကျင်းရှိ တရုတ်သိပ္ပံအကယ်ဒမီ (National Space Science Center NSSC) မှ တာဝန်ထမ်းဆောင်နိုင်မှု သက်တမ်း ၂ နှစ်အထိ ဒီဇိုင်းပြုလုပ်ထားကြောင်း သိရှိရသည်။

30-8-2016
သတင်းစီစဉ် တင်ဆက်သူ - Fr!d@y (MEHN Team)

## ကြော်ငြာများထည့်သွင်းလိုပါက MEHN Facebook စာမျက်နှာမှတဆင့် ဆက်သွယ်နိုင်ပါသည်