ပြည်သူ့လွှတ်တော်ရုံး
သုတေသနဌာန

ရက်စွဲ။ ၂၀၁၆ ခုနှစ်၊ ဇူလိုင်လ ၂၂ ရက်

ဆိုက်ဘာတိုက်ခိုက်မှုများနှင့်
သတိပြုဆောင်ရွက်ရမည့်ဆိုက်ဘာလုံခြုံရေး

အကျဉ်းချုပ်

ယနေ့ခေတ်အချိန်အခါတွင် နည်းပညာများထွန်းကားလာသည်နှင့်အမျှ ဆိုက်ဘာတိုက်ခိုက်မှုများကို ကမ္ဘာ့နိုင်ငံများတွင် ရင်ဆိုင်ကြုံတွေ့နေရပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုများကြောင့် စီးပွားရေးလုပ်ငန်းများတွင်ဆုံးရှုံးနစ်နာရုံမျှသာမက နိုင်ငံတစ်နိုင်ငံ၏ ကာကွယ်ရေး၊ လုံခြုံရေး စသည့် အရေးကြီးသည့်ကဏ္ဍများတွင်ပါ နစ်နာဆုံးရှုံးမှုများစွာဖြစ်ပေါ်စေနိုင်ပါသည်။ နည်းပညာများသည် အဆင့်မြင့်ရှုပ်ထွေးလာသည်နှင့်အမျှ စုံစမ်းထောက်လှမ်းမှုများသည် ယခင်နှင့်မတူဘဲ ဆိုက်ဘာမှတစ်ဆင့် တိကျစွာထောက်လှမ်းနိုင်သောကြောင့် လူပုဂ္ဂိုလ်တစ်ဦးချင်းသာမက နိုင်ငံများ၏ နိုင်ငံရေး၊ စီးပွားရေး၊ လူမှုရေး၊ စစ်ရေးကဏ္ဍများတွင် သတင်းအချက်အလက်တို့၏ လုံခြုံမှုသည် အရေးအကြီးဆုံးဖြစ်လာပါသည်။ ဤစာတမ်းတိုတွင် ဆိုက်ဘာတိုက်ခိုက်မှုများကို ကြိုတင်ကာကွယ်မှုများပြုလုပ်နိုင်ရန် နိုင်ငံတကာတွင်လက်တွေ့အသုံးပြုနေသော ဆိုက်ဘာလုံခြုံရေးနည်းလမ်းများ၊ စံသတ်မှတ်ချက်များ၊ အသုံးပြုသည့်နည်းဗျူဟာများ၊ ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများ၊ ဆိုက်ဘာလုံခြုံရေး၊ ကမ္ဘာတစ်ဝန်းတွင် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများ၊ မြန်မာနိုင်ငံတွင်ပြင်ဆင်ဆောင်ရွက်နေမှုများကို ရေးသားဖော်ပြထားပါသည်။ သို့ဖြစ်ပါ ၍ ဤစာတမ်းပါ အကြောင်းအရာအချက်အလက်များသည် လွတ်တော်ကိုယ်စားလှယ်များအတွက် အထောက်အကူဖြစ်စေရန်ရည်ရွယ်၍ ရေးသားပြုစုတင်ပြထားပါသည်။

မာတိကာ

နိဒါန်း

၁။ ကမ္ဘာပေါ်တွင် ဆိုက်ဘာတိုက်ခိုက်မှုများမြင့်တက်လာသည့်အတွက် ခုခံကာကွယ်ရေး၊ ပြန်လည်တုံ့ပြန်နိုင်ရေးနည်းဗျူဟာများကိုလည်း တိုးမြှင့်လုပ်ဆောင်လာကြပါသည်။ ၂၀၁၅ခုနှစ်တွင် ဗြိတိန်အာမခံကုမ္ပဏီ Lloyd ၏ စီးပွားရေးလုပ်ငန်းများအပေါ် ဆိုက်ဘာတိုက်ခိုက်မှုများရှိခဲ့သောကြောင့် တစ်နှစ်လျှင်အမေရိကန်ဒေါ်လာ ၄၀၀ ဘီလီယံခန့် နစ်နာဆုံးရှုံးမှုများရှိခဲ့ပါသည်။ ဆိုက်ဘာလုံခြုံရေးသည် ကမ္ဘာ့အနာဂတ်လုံခြုံမှုအတွက် အလွန်အရေးပါသော အချက်တစ်ချက်ဖြစ်သောကြောင့် ကွန်ပျူတာကွန်ယက်များ၊ သတင်းအချက်အလက်များလုံခြုံမှုရှိစေရန်နှင့် ဆိုက်ဘာတိုက်ခိုက်မှုများမှကာကွယ်ရန် နိုင်ငံတကာတွင်ဆိုက်ဘာလုံခြုံရေး အစီအစဉ်များကို အထူးဂရုပြုလုပ်ဆောင်လာကြပါသည်။

ဆိုက်ဘာတိုက်ခိုက်မှု

၂။ ဆိုက်ဘာတိုက်ခိုက်မှုဆိုသည်မှာ သတင်းအချက်အလက်စနစ်များကို ကွန်ပျူတာများအသုံးပြု၍ တိုက်ခိုက်ခြင်းဖြစ်ပါသည်။ ကွန်ပျူတာစနစ်များ၊ နည်းပညာကို အသုံးပြုလုပ်ကိုင်ရသော စီးပွားရေးလုပ်ငန်းများကို ပျက်စီးဆုံးရှုံးစေရန်၊ စနစ်ချို့ယွင်းစေရန် နှောင့်ယှက်ခြင်းပင်ဖြစ်ပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုသည် ကွန်ပျူတာစနစ်များ၊ သတင်းအချက်အလက်များကို ပျက်စီးဆုံးရှုံးစေပြီး နောက်ဆက်တွဲအကျိုးရလဒ်အနေဖြင့် သတင်းအချက်အလက်ခိုးယူမှုများနှင့်လုံခြုံရေးအစီအမံများကို ဖောက်ထွင်းဝင်ရောက်ခြင်းကဲ့သို့ ဆိုက်ဘာမှုခင်းများကိုပါ ဆက်လက်ပေါ်ပေါက်လာစေပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုကို ကွန်ပျူတာကွန်ယက်စနစ်အား တိုက်ခိုက်မှုဟုလည်း ခေါ်ဆိုနိုင်ပါသည်။

ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများ

၃။ ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) လုံခြုံရေးဆိုင်ရာအချက်အလက်များအားခိုးယူခြင်း၊ လိမ်လည်ခြင်း၊ ဥပဒေချိုးဖောက်ခြင်း၊

(ခ) ဗိုင်းရပ်စ်မျိုးစုံဖြင့်တိုက်ခိုက်ခြင်း၊

(ဂ) ကွန်ပျူတာစနစ်များအား ဆက်လက်အသုံးပြု၍ မရရန်နှောင့်ယှက်ခြင်း၊

(ဃ) လျှို့ဝှက်နံပါတ်အားခိုးယူခြင်း၊ ချိုးဖောက်ဝင်ရောက်ခြင်း၊

(င) ကွန်ပျူတာစနစ်အတွင်း ထိုးဖောက်ဝင်ရောက်ခြင်း၊

(စ) websiteများအား ဖောက်ထွင်းဝင်ရောက်၍ ပြုပြင်ပြောင်းလဲခြင်း၊

(ဆ) ပုဂ္ဂလိကနှင့် အများသုံး web browser များအား ပိတ်ပင်ခြင်း၊

(ဇ) Distributed Denial of Service - DDoS တိုက်ခိုက်ခြင်း၊

(ဈ) မလျော်ကန်သောမက်ဆေ့ချ်များပေးပို့ခြင်း၊

(ည) အသိဉာဏ်ဆိုင်ရာမူပိုင်ခွင့်အားခိုးယူခြင်း သို့မဟုတ် ခွင့်ပြုချက်မရှိဘဲရယူသုံးစွဲခြင်း[1]

ဆိုက်ဘာတိုက်ခိုက်မှုလုပ်ဆောင်နေသောပုံစံများ

၄။ ဆိုက်ဘာတိုက်ခိုက်မှုလုပ်ဆောင်နေသောပုံစံများမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

- သက်ဆိုင်သူ၏ခွင့်ပြုချက်မရှိဘဲ မသမာသော လုပ်ဆောင်ချက်များပြုလုပ်ခြင်း၊
- မူလအသုံးပြုသူများ အသုံးမပြုနိုင်ရန်လုပ်ဆောင်ခြင်း၊
- အရေးကြီးစီးပွားရေးဆိုင်ရာ အချက်အလက်များကိုခိုးယူခြင်း၊
- အကြွေးဝယ်ကတ်များကိုခိုးယူခြင်း၊
- အင်တာနက်အသုံးပြု၍ မသမာမှုများပြုလုပ်ခြင်း၊
- အခြားသူများ၏ IP Address များကိုခိုးယူခြင်း၊
- အင်တာနက်၊ အီးမေးလ်အစရှိသည့်မီဒီယာများကိုအသုံးပြု၍ နှောက်ယှက်ခံလိုက်ခြင်း၊
- မီဒီယာများအသုံးပြု၍ မကောင်းသတင်းလွှင့်ခြင်း၊ ခြိမ်းခြောက်ခြင်း၊
- Bank Server တွင် သုံးစွဲသူများ၏ငွေစာရင်းများမှ မသိမသာငွေထုတ်ယူနိုင်သော software များထည့်သွင်းခြင်း၊[2]

---

[1] Techopedia၊ Definition - What does Cyberattack mean?၊ Techopedia၊ https://www.techopedia.com/definition/24748/cyberattack မှရရှိပါသည်။ (ကြည့်ရှုသည့်ရက် - မတ် ၈၊ ၂၀၁၆)

ဆိုက်ဘာတိုက်ခိုက်မှုတွင်သုံးသည့်စနစ်များ

၅။ ဥရောပလွှတ်တော် သုတေသနဝန်ဆောင်မှုလုပ်ငန်း၏ စာတမ်းအရ ဆိုက်ဘာတိုက်ခိုက်မှုတွင် အောက်ပါစနစ်များကို အသုံးပြုလေ့ရှိပါသည်-

(က) **Hacking**။ ဆော့ဖ်ဝဲများ၏ အားနည်းချက်များကို စွန့်စွန့်စားစားရှာဖွေ၍ တရားမဝင်ချဉ်းနင်းဝင်ရောက်ခြင်းစနစ်၊

(ခ) **Phishing**။ ပုဂ္ဂိုလ်ရေးဆိုင်ရာသတင်းအချက်အလက်များ ပေါက်ကြားစေရန် အင်တာနက်အသုံးပြုသူများကို လိမ်လည်လှည့်ဖျားခြင်း၊

(ဂ) **Malware**။ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ သတင်းအချက်အလက်များထုတ်လွှင့်ခြင်း၊ စုဆောင်းခြင်းများဆောင်ရွက်နိုင်သောဆော့ဖ်ဝဲ၊ ၎င်းတွင်သတင်းအချက်အလက်များခိုးယူခြင်း သို့မဟုတ် ချဉ်းနင်းဝင်ရောက်ရန်နည်းလမ်းများ ထောက်ပံ့ပေးခြင်း၊ အခြားသောကွန်ပျူတာပရိဂရမ်များကိုညစ်ညမ်းစေခြင်း၊ ပုံတူပွားနိုင်သောဗိုင်းရပ်စ်များစသည်တို့ဖြစ်ပါသည်။ ထိုနည်းလမ်းများကို အသုံးပြုခြင်းဖြင့် ကွန်ပျူတာတစ်ခုချင်းစီအား ပမာဏကြီးမားသော အတိုင်းအတာအထိ တိုက်ခိုက်မှုဖြစ်စေနိုင်ပါသည်။[3]

ဆိုက်ဘာလုံခြုံရေး

၆။ ဆိုက်ဘာလုံခြုံရေးဆိုသည်မှာ အင်တာနက်အသုံးပြုသည့်အဖွဲ့အစည်းများနှင့် အသုံးပြုသူများ၏ ပိုင်ဆိုင်မှုများကို ကာကွယ်ရန်အတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ tool များ၊ ချမှတ်ရန်လိုအပ်သောဆိုက်ဘာလုံခြုံရေးနည်းလမ်းများ၊ ညွှန်ကြားချက်များ၊ လုပ်ထုံးလုပ်နည်းများ၊ နည်းပညာများနှင့် လက်တွေ့ကျင့်သုံးရန်နည်းလမ်းကောင်းများ အသုံးပြုခြင်းကိုဆိုလိုပါသည်။

---

[2] ဇော်လှိုင်ထွန်း၊ Cyber လုံခြုံရေးအကြောင်းသိကောင်းစရာ၊ Myanmar Computer Emergency Response Team၊ http://www.mmcert.org.mm မှရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၂ ဇူလိုင်လ ၂၀၁၅)

[3] Piotr Bakowski၊ Briefing of European Parliamentary Research Service 12/11/2013၊ Cyber security in the European Union၊ www.Europarl.europa.eu/ မှရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၃ ဖေဖော်ဝါရီလ ၂၀၁၆)

၇။ ဆိုက်ဘာလုံခြုံရေးဆောင်ရွက်ရာတွင် အဓိကရည်ရွယ်ချက်များ၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံသတ်မှတ်ချက်များ၊ နိုင်ငံတကာစံသတ်မှတ်ချက်များနှင့်အင်တာနက်သုံးစွဲသူများလိုက်နာရမည့် အချက်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) **ဆိုက်ဘာလုံခြုံရေးလုပ်ဆောင်ရခြင်း၏အဓိကရည်ရွယ်ချက်။** ဆိုက်ဘာလုံခြုံရေးလုပ်ဆောင်ရခြင်း၏ အဓိကရည်ရွယ်ချက်များမှာ ဆိုက်ဘာအဖွဲ့အစည်းများနှင့် ၎င်းအဖွဲ့အစည်းများအတွင်း အသုံးပြုသူများ လျှို့ဝှက်အပ်သော သတင်းအချက်အလက်များနှင့်ပိုင်ဆိုင်မှုများကို လုံခြုံစိတ်ချစွာထိန်းသိမ်းနိုင်ရေး၊ မှန်ကန်စွာအသုံးပြုနိုင်ရေး၊ အပြန်အလှန်ယုံကြည်စွာဖလှယ်နိုင်ရေး၊ ဖြန့်ဝေနိုင်ရေး၊ ကွန်ယက်လုံခြုံရေးတို့ဖြစ်ပါသည်။

(ခ) **ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစံသတ်မှတ်ချက်များ။** ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစံသတ်မှတ်ချက်များမှာ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာတိုက်ခိုက်မှုများကို အတတ်နိုင်ဆုံးလျှော့ချရန်အတွက် ကမ္ဘာနှင့်အဝန်းလက်တွေ့အသုံးပြုနေသောဆိုက်ဘာလုံခြုံရေးနည်းလမ်းများနှင့် ဆိုက်ဘာလုံခြုံရေးသတ်မှတ်ချက်များကို ဆိုလိုပါသည်။ စံသတ်မှတ်ချက်များတွင် ယေဘုယျစံသတ်မှတ်ချက်များနှင့် ဆိုက်ဘာလုံခြုံရေးအကောင်အထည်ဖော်နိုင်ရန် အသေးစိတ်အချက်အလက်များ၊ အသုံးပြုမည့်နည်းဗျူဟာများပါဝင်ပါသည်။ စံသတ်မှတ်နိုင်ရန်အတွက် အခွင့်အာဏာရှိသော စံသတ်မှတ်ရေးအဖွဲ့အစည်းများ၏ ထောက်ခံချက်ရရှိမှသာလျှင် ဆိုက်ဘာလုံခြုံရေးစံအဖြစ် သတ်မှတ်နိုင်ပါသည်။

(ဂ) **နိုင်ငံတကာစံသတ်မှတ်ချက်များ။** ဆိုက်ဘာလုံခြုံရေးနှင့်ပတ်သက်သည့် နိုင်ငံတကာစံသတ်မှတ်ချက်များမှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(၁) စီးပွားရေးဆိုင်ရာသတင်းအချက်အလက်များအတွက် -ISO 27031(FCD)

(၂) ဆိုက်ဘာလုံခြုံရေးစီမံကိန်းများအတွက်- - ISO 27031(CD)

(၃) ကွန်ယက်ဆိုင်ရာလုံခြုံရေးစီမံကိန်းများအတွက် -ISO 27031(FDIS)

(၄) အသုံးချရမည့် လုပ်ငန်းဆိုင်ရာလုံခြုံရေးများအတွက် - ISO 27031(CD)

(၅) သတင်းအချက်အလက်ဆိုင်ရာစီမံခန့်ခွဲပေးခြင်းများအတွက်- O27031(FCD)

(၆) သတင်းအချက်အလက်လုံခြုံမှုစီမံခန့်ခွဲရေးဆိုင်ရာလမ်းညွှန်မှုများအတွက်-

ISOIECTR13335 (GMITS)

(ဃ) **အင်တာနက်သုံးစွဲသူများလိုက်နာရမည့်အချက်များ။** အင်တာနက်သုံးစွဲသူများ သတိပြုလိုက်နာရမည့်အချက်များမှာ မိမိသုံးစွဲသောကွန်ပျူတာကို နောက်ဆုံးပေါ်ဗိုင်းရပ်စ်ကာကွယ်ပေးသော ဆော့ဖ်ဝဲများကိုသာသုံးစွဲပြီး update လုပ်ပေးသင့်ပါသည်။ မိမိတို့၏သတင်းအချက်အလက်များ လုံခြုံစေရေးအတွက် သူတပါးအလွယ်တကူမခန့်မှန်းနိုင်သောလုံခြုံသော password များ ပေးသင့်ပါသည်။ ကွန်ပျူတာတွင်အခြား device များမသုံးစွဲမီ ထိုပစ္စည်းများဗိုင်းရပ်စ်ကင်းစင်စေရန်လည်း ဂရုစိုက်ရမည်ဖြစ်ပြီး ဗိုင်းရပ်စ်တွေ့ရှိခဲ့ပါက စနစ်ထိန်းချုပ်ကွပ်ကဲသူသို့ချက်ချင်းအကြောင်းကြားသင့်ပါသည်။ ဆိုက်ဘာလုံခြုံရေးထိခိုက်နိုင်သည့်ဖြစ်စဉ်များဖြစ်ပွားပါက ဆိုက်ဘာလုံခြုံရေးအဖွဲ့ကို ချက်ချင်းအကြောင်းကြားရပါမည်။ ကွန်ပျူတာသုံးစွဲပြီးပါက မိမိသုံးစွဲနေသော အကောင့်မှထွက်ပြီး ကွန်ပျူတာကိုပိတ်ခဲ့ရပါမည်။[4]

၈။ ဆိုက်ဘာတိုက်ခိုက်မှုများသည် များသောအားဖြင့် မခိုင်မာသော website များသို့ ဝင်ကြည့်ခြင်း၊ ဒေါင်းလုပ်ဆွဲခြင်းတို့မှတစ်ဆင့် ကွန်ပျူတာသို့ကူးစက်ပျံနှံ့ပါသည်။ ဗိုင်းရပ်စ်ကာကွယ်ရေးနှင့်အတူ ကောင်းမွန်သော၊ ခိုင်မာသောဆော့ဖ်ဝဲလုံခြုံရေးစနစ်များကို အသုံးပြုရပါ မည်။ Window 7၊ 8 တို့၏ ဆော့ဖ်ဝဲလုံခြုံရေးစနစ်များကောင်းမွန်သော်လည်း ပိုမိုခိုင်မာသည်ဟုထင်ရသော အခြားစနစ်များကိုလည်း အသုံးပြုနိုင်ပါသည်။

---

[4]ဇော်လှိုင်ထွန်း၊ Cyber လုံခြုံရေးအကြောင်းသိကောင်းစရာ၊ Myanmar Computer Emergency Response Team၊ http://www.mmcert.org.mm မှရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၅ ဖေဖော်ဝါရီလ ၂၀၁၆)

၁၀။ အကယ်၍ ကွန်ပျူတာများကို ကွန်ယက်ချိတ်ဆက်အသုံးပြုလျှင် အပျော်တမ်းသုံးစွဲသည့် အခြားမည်သည့်ကွန်ပျူတာနှင့်မျှ မချိတ်ဆက်သင့်ပါ။ ဆိုလိုသည်မှာ ဝန်ထမ်းများ၏ကိုယ်ပိုင် ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်းများအား ရုံးသုံးကွန်ပျူတာများတွင် ချိတ်ဆက်သုံးစွဲခြင်း မရှိစေရပါ ။ ကုမ္ပဏီ၏ IT ဌာနသည် ကွန်ယက်လုံခြုံရေးကို အမြဲစစ်ဆေးနေစေသင့်ပါသည်။ ကောင်းမွန်သောကွန်ယက်စနစ်ကို အသုံးပြုခြင်းအားဖြင့် ပုံမှန်မဟုတ်သည့်ထူးခြားဖြစ်စဉ်များရှိပါက အချိန်နှင့်တပြေးညီ သိရှိကာကွယ်နိုင်မည်ဖြစ်ပါသည်။[5]

မြန်မာနိုင်ငံတွင်ပြင်ဆင်ဆောင်ရွက်နေမှုများ

၉။ မြန်မာနိုင်ငံတွင် အစိုးရဝန်ကြီးဌာနများနှင့် ပြည်သူများ၏အင်တာနက်အသုံးပြုမှုများ အတွက်လုံခြုံမှုရှိစေရန် ဆက်သွယ်ရေးနှင့် သတင်းအချက်အလက်နည်းပညာဝန်ကြီးဌာနတွင် သတင်းအချက်အလက်နှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနကို ၁၅-၁-၂၀၁၅ နေ့တွင် ကျင်းပပြုလုပ်သော ပြည်ထောင်စုအစိုးရအဖွဲ့ အစည်းအဝေးအမှတ်စဉ် ၂/၂၀၁၅ တွင် အတည်ပြုခဲ့ပြီး ၁-၄-၂၀၁၅ ခုနှစ်တွင်၊ ဝန်ကြီးရုံး၏ အမိန့်ကြော်ငြာစာအမှတ် (၉/၂၀၁၅) ဖြင့် စတင်ဖွဲ့စည်းခဲ့ပါသည်။[6]

၁၀။ ဌာနဆိုင်ရာအသီးသီးမှ အကောင်အထည်ဖော်ဆောင်ရွက်ထားသည့် လုပ်ငန်းစဉ်များအား အကျိုးရှိရှိပေါင်းစပ်အသုံးပြုနိုင်ရေး၊ လုပ်ငန်းစဉ်အသစ်များအားလေ့လာ၍ စီမံကိန်းအသစ်များ ရေးဆွဲအကောင်အထည်ဖော်ဆောင်ရွက်ရေး၊ သတင်းအချက်အလက် ဆက်သွယ်ရေးနည်းပညာ၊ စံနှုန်းများသတ်မှတ်နိုင်ရေး၊ လိုအပ်သည့်ဥပဒေများ ပြဋ္ဌာန်းနိုင်ရေး၊ ပြဋ္ဌာန်းထားသည့် ဥပဒေနှင့်အညီ သတင်းအချက်အလက် ဆက်သွယ်ရေးနည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးလုပ်ငန်းများစနစ်တကျကြီးကြပ်၍ အကောင်အထည်ဖော် ဆောင်ရွက်နိုင်ရေးနှင့် အဖွဲ့အစည်း၊ ဌာနဆိုင်ရာအချင်းချင်းတို့အား ညှိနှိုင်းဆောင်ရွက် ပေးနိုင်ရေးအတွက်ရည်ရွယ်၍ ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနကို ဖွဲ့စည်းခဲ့ကြောင်းသိရှိရပါသည်။ ဝန်ကြီးဌာနများနှင့် ပြည်သူများအနေဖြင့် အီးမေးလ်နှင့် အင်တာနက်သုံးစွဲမှုများ ကျယ်ပြန့်လာသည့်အလျောက် ဆိုက်ဘာတိုက်ခိုက်မှုများ

---

[5] Anand Khanse aka HappyAndyK၊ Cyber Attacks – Definition, Types, Prevention၊ The Windows Club၊ ၂ ဒီဇင်ဘာလ ၂၀၁၄၊ http://www.thewindowsclub.com/cyber-attacks-definition-types-prevention မှရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၁၆ ဖေဖော်ဝါရီလ ၂၀၁၆)

[6] ဆက်သွယ်ရေးနှင့်သတင်းအချက်အလက်နည်းပညာဝန်ကြီးဌာန၊ about ITCSD၊ ဆက်သွယ်ရေးနှင့်သတင်းအချက်အလက်နည်းပညာဝန်ကြီးဌာန၊ http://www.mcit.gov.mm/content/about-itcs.html မှရရှိပါသည်။ (ကြည့်ရှုသည့်ရက် - ၂၄ ဖေဖော်ဝါရီလ ၂၀၁၆)

လည်း ကြုံတွေ့လာနိုင်သဖြင့် ကြိုတင်ကာကွယ်ခြင်း၊ သတိပေးဆောင်ရွက်ခြင်း၊ အသိပညာပေးခြင်းဖြင့် နိုင်ငံနှင့်ပြည်သူများလုံခြုံစိတ်ချစွာ အွန်လိုင်းစနစ်သုံးစွဲနိုင်ရန် ရည်ရွယ်ချက်ဖြင့် ဖွဲ့စည်းခဲ့ခြင်းဖြစ်ပါ သည်။ ဆိုက်ဘာလုံခြုံရေးနှင့်ပတ်သက်၍လက်ရှိအခြေအနေတွင် အာဆီယံဒေသခွဲအာရှ-ပစိဖိတ် ဒေသများနှင့်ချိတ်ဆက်ထားပြီးနောက်ပိုင်းတွင် အပြည်ပြည်ဆိုင်ရာအဖွဲ့အစည်းများနှင့်ပူးပေါင်း၍ သဘောတူညီချက်စာချုပ်များ ချုပ်ဆိုဆောင်ရွက်သွားမည်ဖြစ်ပြီး ဥပဒေအရအရေးယူခြင်းများ ဆောင်ရွက်နိုင်ရန် အီလက်ထရောနစ်နည်းဥပဒေနှင့် ဆိုက်ဘာဥပဒေများရေးဆွဲလျက်ရှိပါ သည်။[7]

၁၁။ Microsoft ကုမ္ပဏီသည် မြန်မာနိုင်ငံတွင် နည်းပညာဆိုင်ရာလုပ်ငန်းများ၊ အထူးသဖြင့် ဆိုက်ဘာလုံခြုံရေးနှင့်ပတ်သက်၍ ဆောင်ရွက်သွားမည်ဖြစ်ကြောင်းသိရှိရပါသည်။ ပိုမိုများပြားလာသော ဆိုက်ဘာရာဇဝတ်မှုများအားထိန်းချုပ်နိုင်ရန် ကျွမ်းကျင်ရှေ့နေများ၊ စုံစမ်းစစ်ဆေးရေးအဖွဲ့များ၊ မှုခင်းဆိုင်ရာသုံးသပ်သူများပါဝင်သော ဒစ်ဂျစ်တယ်ရာဇဝတ်မှုအဖွဲ့ (Digital Crimes Unit) တစ်ခုအားဖွဲ့စည်းပြီး ကမ္ဘာတစ်ဝန်းရှိပုဂ္ဂလိကကုမ္ပဏီများ၊ အစိုးရအဖွဲ့အစည်းများနှင့် ပူးပေါင်းဆောင်ရွက်လျက်ရှိပါသည်။[8]

ကမ္ဘာတစ်ဝန်းတွင်ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများ

၁၂။ ကမ္ဘာတစ်ဝန်းတွင် နည်းပညာအဆင့်အတန်း မြင့်မားလာသည်နှင့်အညီ ဆိုက်ဘာတိုက်ခိုက်မှုများသည်လည်း ပိုမိုများပြားလာလျက်ရှိပါသည်။[9] အမေရိကန်၊ ဥရောပနှင့် အာရှနိုင်ငံများ၏အစိုးရရုံးများ၊ ပုဂ္ဂလိကသတင်းမီဒီယာများ၊ အထင်ကရနိုင်ငံရေးသမားများကို တရုတ်နိုင်ငံတွင် အခြေပြုထားသည့် ကွန်ပျူတာများမှ ဆိုက်ဘာထိုးဖောက်တိုက်ခိုက်မှုများရှိနေကြောင်း မကြာခဏထုတ်ဖော်ပြောဆိုမှုများ ရှိနေပါသည်။[10]

---

[7] ကျော်ဇေယျ၊ မြန်မာနိုင်ငံတွင် ဆိုက်ဘာတိုက်ခိုက်မှုများကာကွယ်ရန် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနသစ်ဖွဲ့စည်း၊ အင်တာနက်ဂျာနယ်၊ အတွဲ ၁၆၊ အမှတ် ၂၁၊ တနလ်ာနေ့၊ ၈ ဇွန်လ ၂၀၁၅၊ စာမျက်နှာ ၆ မှ ရရှိပါသည်။

[8] အင်တာနက်ဂျာနယ်၊ Microsoft က မြန်မာနိုင်ငံမှာ ဘာတွေဆောင်ရွက်မလဲ၊ အင်တာနက်ဂျာနယ်၊ အတွဲ ၁၆၊ အမှတ် ၂၁၊ တနလ်ာနေ့၊ ၈ ဇွန်လ ၂၀၁၅၊ အချပ်ပိုမှ ရရှိပါသည်။

[9] စိုးထက်၊ ဆိုက်ဘာလုံခြုံရေးကုမ္ပဏီ Kaspersky Lab တိုက်ခိုက်ခံရ၊ အင်တာနက်ဂျာနယ်၊ အတွဲ ၁၆၊ အမှတ် ၂၂၊ တနလ်ာနေ့၊ ၁၅ ဇွန်လ ၂၀၁၅၊ စာမျက်နှာ ၆၈ မှ ရရှိပါသည်။

[10] မြန်မာ့သားကောင်း၊ နိုင်ငံတကာဆိုက်ဘာတိုက်ပွဲနှင့် မြန်မာစစ်တလင်း၊ မြန်မာ့သားကောင်း၊ ၂၂ သြဂုတ်လ ၂၀၁၃၊ http://www.myanmartharkaung.net/2013/08/blog-post_6603.html/ မှ ရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ဧပြီ ၂၅၊ ၂၀၁၆)

၁၃။ ၂၀၁၅ ခုနှစ်တွင် ဖြိတိန်အာမခံကုမ္ပဏီ Lloyd ၏ စီးပွားရေးလုပ်ငန်းများအပေါ် ဆိုက်ဘာတိုက်ခိုက်မှုများ ရှိခဲ့သောကြောင့် တစ်နှစ်လျှင်အမေရိကန်ဒေါ်လာ ၄၀၀ ဘီလီယံခန့် နစ်နာဆုံးရှုံးမှုများ ရှိခဲ့ပါသည်။[11]

၁၄။ ကမ္ဘာကျော် Anti-virus software ကုမ္ပဏီတစ်ခုဖြစ်သော Kaspersky Lab ၏ ကိုယ်ပိုင်စနစ်များကို မကြာမီကဟက်ကာများကတိုက်ခိုက်ခဲ့ကြပါသည်။ ထိုတိုက်ခိုက်မှုတွင် ယခင်ကမသိရှိခဲ့သော နည်းလမ်း ၃ ခုအထိပါဝင်ကြောင်းသိရှိရပါသည်။ [12] ၂၀၁၄ ခုနှစ်၊ ဧန်နဝါရီလ ၂၄ ရက်နေ့တွင် Syrian Electronic Army သည် CNN Facebook page နှင့် Twitter Account အပါအဝင် CNN မှ ပိုင်ဆိုင်သည့် account များကို တိုက်ခိုက်ခဲ့သည်။ တိုက်ခိုက်ခံရသည့် account များက ပြုလုပ်ခဲ့သည့် Tweet များတွင် အယ်လ်ကိုင်ဒါကို စီအိုင်အေက ထောက်ပံ့ပေးခဲ့ပုံနှင့် ဆီးရီးယန်းပြည်နယ်ကို အယ်လ်ကိုင်ဒါက ထိန်းချုပ်ထားသည်ဟူသော အိုစမာဘင်လာဒင်၏ ပြောကြားချက်သည် လိမ်လည်မှုများသာဖြစ်ကြောင်း အဓိပ္ပါယ်ရသည့် Tweet များ ပါဝင်ခဲ့သည်။ ထို့ပြင် CNN ၏ account ကို တိုက်ခိုက်ခဲ့ရခြင်းမှာ အလိမ်အညာများအတွက် လက်တုံ့ပြန်ခြင်းဖြစ်ကြောင်း Syrian Electronic Army က ပြောကြားခဲ့သည်။

၁၅။ ထို့အပြင် ၁၀-ဖ-၂၀၁၄ ခုနှစ်တွင် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုကြောင့် Twitter ဝန်ထမ်းများ၏ နာမည်များ၊ လိပ်စာများနှင့် social security နံပါတ်များသည် အင်တာနက်ပေါ်တွင် ပေါက်ကြားထွက်ပေါ်လာခဲ့ပါသည်။ ၁၁-ဖ-၂၀၁၄ တွင် ဗိုင်းရပ်စ်တစ်မျိုးကြောင့် Twitter သုံးစွဲသူ ၈၄၇၀၀ မှ တူညီသည့် message များကို Tweet ခဲ့ကြပြီးငင်း Tweet များမှ follower သန်းပေါင်းများစွာထံပျံ့နှံ့ခဲ့ပါသည်။ Lizard Squad ဟုခေါ်သော ဟက်ကာအဖွဲ့သည် Sony ၏ Play Station Network ကို DDoS တိုက်ခိုက်မှုဖြင့် တိုက်ခိုက်ခဲ့ပါသည်။ သို့ရာတွင်အချက်အလက်များပေါက်ကြားခဲ့ခြင်းမရှိကြောင်း Sony မှ ပြောကြားခဲ့ပါသည်။

---

[11] Politics ဂျာနယ်၊ ၂၀၁၉ ခုနှစ်တွင် ဆိုက်ဘာရာဇဝတ်မှုကြောင့်ဆုံးရှုံးရငွေ ဒေါ်လာ ၂ ထရီလီယံအထိရောက်ရှိမည်၊ Politics ဂျာနယ်၊ အမှတ် ၉၂၊ ဧန်နဝါရီ ၂၂၊ ၂၀၁၆၊ စာမျက်နှာ ၁၂ မှရရှိပါသည်။

[12] စိုးထက်၊ ဆိုက်ဘာလုံခြုံရေးကုမ္ပဏီ Kaspersky Lab တိုက်ခိုက်ခံရ၊ အင်တာနက်ဂျာနယ်၊ အတွဲ ၁၆၊ အမှတ် ၂၂၊ တနလင်္ဘာနေ့၊ ၁၅ ဇွန်လ ၂၀၁၅၊ စာမျက်နှာ ၆၈ မှ ရရှိပါသည်။

၁၆။ ထို့အပြင် eBay website သည် ၁၇-၉-၂၀၁၄ တွင် တိုက်ခိုက်ခံခဲ့ရပြီး ၎င်းဆိုက်ရှိ ထုတ်ကုန်စာရင်းကို click နှိပ်သူတိုင်းသည် eBay နှင့်ဆင်တူသည့် သုံးစွဲသူများ၏ အချက်အလက်များ ခိုးယူသော အခြားဆိုက်တစ်ခုသို့ အလိုအလျောက် ရောက်ရှိသွားခဲ့ပါသည်။ နာမည်ကျော် cloud sharing ဝန်ဆောင်မှုဖြစ်သော Dropbox သည် ၇-၁၀-၂၀၁၄ တွင် brute-force attack ကိုအသုံးပြုသည့် ဟက်ကာများ၏ တိုက်ခိုက်ခြင်းကို ခံခဲ့ရပါသည်။ ထို့ကြောင့် သုံးစွဲသူ ၇ သန်း၏ account များ ပေါက်ကြားခဲ့ရပါသည်။

၁၇။ ၂၉-၁၀-၂၀၁၄ တွင် မြောက်ကိုရီးယားရှိ ဟက်ကာများသည် တောင်ကိုရီးယားရှိ ဂိမ်းများ တွင်ကူးစက်နိုင်သည့် malware ကို ဖြန့်ချိခဲ့ပါသည်။ အဆိုပါ malware သည်ထုတ်ကုန် ၂၀၀၀ တွင် ကူးစက်ပျံနှံ့ခဲ့ပါသည်။ ထို့အပြင် ၂၄-၁၁-၂၀၁၄ တွင် Sony Pictures Entertainment ကို Guardians of Peace ဟုခေါ်သည့် ဟက်ကာအဖွဲ့က တိုက်ခိုက်ခဲ့ပါသည်။ ၎င်းတိုက်ခိုက်မှုကို မြောက်ကိုရီးယားမှဟက်ကာများက ဦးဆောင်သည်ဟု ယူဆခဲ့ကြပါသည်။ အဆိုပါဟက်ကာ အဖွဲ့သည် မြောက်ကိုရီးယားခေါင်းဆောင် ကင်ဂျုံအမ်ကိုလုပ်ကြံသည့် ဟာသဇာတ်ကားဖြစ်သော The Interview ကို ပြသခြင်းမပြုရန် တောင်းဆိုခဲ့ပါသည်။ ထို့အပြင်ဟက်ကာများသည် Sony ဆာဗာများမှ 100TB ပမာဏရှိသည့် အချက်အလက်များကိုရယူခဲ့ကြောင်း သိရှိခဲ့ပါသည်။[13]

၁၈။ ထို့အပြင်နည်းပညာထွန်းကားသောနိုင်ငံများဖြစ်သည့်အမေရိကန်နိုင်ငံ၊ မြောက်ကိုးရီးယား နိုင်ငံနှင့်တရုတ်နိုင်ငံတို့တွင်ပင် ဆိုက်ဘာတိုက်ခိုက်မှုများ ကြုံတွေ့နေရကြောင်းကို အောက်တွင် ဖော်ပြထားပါသည်-

(က) **အမေရိကန်နိုင်ငံ၏ ကွန်ပျူတာလုံခြုံရေးစနစ်တိုက်ခိုက်ခံရမှု။** အမေရိကန်နိုင်ငံတွင် ဆိုက်ဘာတိုက်ခိုက်မှုကြောင့် သုံးစွဲရသောစရိတ်သည် အမေရိကန်ဒေါ်လာ ၁၀၀ ဘီလီယံခန့်ရှိကြောင်း သိရှိရပါသည်။[14] တရုတ်ဟက်ကာတို့သည် အမေရိကန်နိုင်ငံ ဝန်ထမ်းရေးရာစီမံခန့်ခွဲမှုရုံး (Office of Personnel Management-OPM) ၏ ကွန်ပျူတာဖိုင်ပေါင်း ၁၀၀၀၀ အတွင်းသို့ ချဉ်းကပ်

[13] ဧူးနစ်(နည်းပညာ)၊ ၂၀၁၄ ခုနှစ်၏အကြီးကျယ်ဆုံးဆိုက်ဘာတိုက်ခိုက်မှုများ၊ ဧူးနစ်(နည်းပညာ)၊ ၁ ဧန်နဝါရီ ၂၀၁၄၊ http://www.zunite.org/2015/01/blog-post_11.html မှ ရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၁ ဧူလိုင်လ ၂၀၁၅)

[14] Politics ဂျာနယ်၊ ၂၀၁၉ ခုနှစ်တွင် ဆိုက်ဘာရာဇဝတ်မှုကြောင့်ဆုံးရှုံးရငွေ ဒေါ်လာ ၂ ထရီလီယံအထိရောက်ရှိမည်၊ Politics ဂျာနယ်၊ အမှတ် ၉၂၊ ဧန်နဝါရီ ၂၂၊ ၂၀၁၆၊ စာမျက်နှာ ၁၂ မှရရှိပါသည်။

ဝင်ရောက်ပြီး သတင်းအချက်အလက်များကို ခိုးယူခဲ့ကြောင်းသိရှိရပါသည်။ ထို တိုက်ခိုက်မှုကြောင့် ကွန်ပျူတာစနစ် ၂ ခုတွင် ဆိုးရွားစွာထိခိုက်ခဲ့ပါသည်။ OPM တွင် သန်းပေါင်းများစွာသော လက်ရှိတာဝန်ထမ်းဆောင်နေသူများနှင့် အငြိမ်းစား ယူသွားကြသော ဖက်ဒရယ်ဝန်ထမ်းများ၏ ရှင်းလင်းပြီးဖြစ်သည့် လုံခြုံရေး သတင်းများနှင့် မှတ်တမ်းမှတ်ရာများကို လုံခြုံစွာထိန်းသိမ်းထားရှိပါသည်။ ဟက်ကာများသည် အမေရိကန်နိုင်ငံသား ၄ သန်းတို့၏ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အသေး စိတ်အချက်အလက်များကိုခိုးယူခဲ့ကြပြီး ထိုမှတဆင့် အမေရိကန် ပြည်တွင်းအခွန် များဌာနကိုပါ ဆက်လက်တိုက်ခိုက်ခဲ့ပါသည်။ [15] အမေရိကန်ကာကွယ်ရေး အဆင့်မြင့်သုတေသနစီမံကိန်းအေဂျင်စီ (Defense Advanced Research Projects Agency-DARPA) က ၂၀၁၃ ခုနှစ်မှ ၂၀၁၇ ခုနှစ်အတွင်း ဆိုက်ဘာ ဘတ်ဂျက် ၁.၅၄ ဘီလီယံဒေါ်လာဖြင့် စစ်ရေးလိုအပ်ချက်နှင့် ကိုက်ညီအောင် ဆိုက်ဘာတိုက်ပွဲအတွက် အဓိကထားပြင်ဆင်လုပ်ဆောင်မည်ဟု The Malta Independent တွင် ဖော်ပြထားပါသည်။

(ခ) **မြောက်ကိုရီးယားနိုင်ငံအား ဆိုက်ဘာတိုက်ခိုက်ခံရမှုနှင့် တုန့်ပြန်နိုင်ရေးပြင်ဆင် ဆောင်ရွက်မှုများ။** အမေရိကန်နိုင်ငံက မြောက်ကိုရီးယားနိုင်ငံ၏ နျူကလီးယားလက်နက်ထုတ်လုပ်ရေးပရိဂရမ်အား ဆိုက်ဘာတိုက်ခိုက်မှုပြုလုပ်ခဲ့ သော်လည်း မအောင်မြင်ခဲ့ပေ။ ထိုသို့မအောင်မြင်ရခြင်းမှာ ကိုရီးယားဘာသာဖြင့် သီးခြားစီစဉ်ထားသည့် ကွန်ပျူတာဆက်သွယ်ရေးစနစ်ကြောင့် ဖြစ်ပါသည်။ လျှို့ဝှက်သတင်းရယူခြင်းနှင့် သီးခြားဆက်သွယ်ရေးစနစ်များ ဖန်တီးလုပ်ဆောင် ထားပြီး ဟက်ကာများထိုးဖောက်ဝင်ရောက်လာခြင်းကို တားဆီးပိတ်ပင်သည့် KwaryMyong စနစ်ကို အသုံးပြုထားပါသည်။ မြောက်ကိုရီးယားနိုင်ငံ၏ ဝင်ငွေ ၂၀ ရာခိုင်နှုန်းခန့်ကို အွန်လိုင်းစစ်ဆင်ရေးအတွက် သုံးစွဲလျက်ရှိပြီး ဆိုက်ဘာ စစ်ဆင်ရေးအေဂျင်စီတွင် လုပ်ကိုင်နေသူပေါင်း ၆၀၀၀ ခန့်ရှိကြောင်း၊ မြောက်ကို

[15] သိန်းဥာဏ်၊ တရုတ်ဟက်ကာတို့ အမေရိကန်ကွန်ပျူတာလုံခြုံရေးစနစ်သို့ ထိုးဖောက်ဝင်ရောက်တိုက်ခိုက်ပြီ၊ နိုင်ငံတကာသတင်းဂျာနယ်၊ အတွဲ ၂၊ အမှတ် ၄၆၊ ကြာသပတေးနေ့၊ ၁၁ ဇွန်လ ၂၀၁၅၊ စာမျက်နှာ ၁၀ မှ ရရှိပါသည်။

ရီးယားနိုင်ငံသည် Stuxnet ဗိုင်းရပ်စ်အပေါ်အခြေခံသည့် malware များကို တည်ဆောက်နေပြီဖြစ်ကြောင်း၊ ကွန်ပျူတာဗိုင်းရပ်စ်ကို ၂၀၁၀ ဇွန်လတွင် ရှာဖွေတွေ့ရှိခဲ့ကြောင်း၊ နိုင်ငံတစ်နိုင်ငံ၊ အဖွဲ့အစည်းတစ်ခုအတွင်းရှိ ကွန်ပျူတာနည်းစနစ်များနှင့် အခြေခံအဆောက်အဦများ၊ လုပ်ငန်းများကို ဖျက်ဆီးပစ်နိုင်စွမ်းရှိပြီး လူများကိုပင်သတ်နိုင်စွမ်းရှိကြောင်း မြောက်ကိုရီးယားနိုင်ငံ၏ Hamheung ကွန်ပျူတာနည်းပညာတက္ကသိုလ်တွင် နှစ်ပေါင်း ၂၀ ကြာ ကွန်ပျူတာသိပ္ပံဘာသာရပ်ကို သင်ကြားပို့ချပေးခဲ့သည့် ပါမောက္ခကင်ယောင်ကွမ်က ပြောကြားခဲ့ပါသည်။[16]

(ဂ) **ဆိုက်ဘာတိုက်ခိုက်မှုများ၏ထိပ်တန်းနိုင်ငံအဖြစ် တရုတ်နိုင်ငံဆက်လက်ရပ်တည်နေမှု။** အင်တာနက်တိုက်ခိုက်မှုအားလုံး၏ ထက်ဝက်နီးပါးခန့်သည် တရုတ်နိုင်ငံတွင်အခြေခံကြောင်း၊ အချို့တိုက်ခိုက်မှုများပင်လျှင် တရုတ်နိုင်ငံတွင် နေထိုင်သူများကပြုလုပ်ခြင်းဖြစ်ကြောင်း cloud ဝန်ဆောင်မှုကုမ္ပဏီ Akamai က နောက်ဆုံးထုတ်ပြန်ခဲ့သည့် အင်တာနက်အစီရင်ခံစာတွင်ဖော်ပြခဲ့သည်။ ၂၀၁၃ ခုနှစ် နောက်ဆုံးသုံးလပတ်အတွက် စစ်တမ်းကောက်ယူမှုအရ တရုတ်နိုင်ငံမှမြစ်ဖျားခံသည့် အင်တာနက်တိုက်ခိုက်မှုစုစုပေါင်း ၃၄ ရာခိုင်နှုန်းရှိကြောင်း၊ ထိုပမာဏသည် အခြားနိုင်ငံများထက် သာလွန်နေကြောင်း သိရှိရပါသည်။ Akamai သည် အင်တာနက်တိုက်ခိုက်မှုရင်းမြစ်ကို IP Address ဖြင့် ခွဲခြားဖော်ပြခဲ့သည်။ အခြားသောဆိုက်ဘာတိုက်ခိုက်မှု မြစ်ဖျားခံသည့်နိုင်ငံများတွင် အမေရိကန်က ၁၉ ရာခိုင်နှုန်း၊ ကနေဒါက ၁၀ ရာခိုင်နှုန်း၊ အင်ဒိုနီးရှားက ၅.၇ ရာခိုင်နှုန်းနှင့် တရုတ် (တိုင်ပေ) က ၃.၄ ရာခိုင်နှုန်း အသီးသီးရပ်တည်လျက်ရှိပါသည်။[17]

(ဃ) **ဂျပန်နိုင်ငံတွင်ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများ။** ဂျပန်နိုင်ငံအမျိုးသားအခွန်တော်ဆိုင်ရာ website တစ်ခု အွန်လိုင်းပေးချေမှုများကို လက်ခံခြင်းမပြုမီ နှောင့်

[16]သက်ဇော်၊ လူကိုပင်သတ်နိုင်စွမ်းရှိသည့် စစ်သည်ဟက်ကာတိုက်ခိုက်သူ ဖြဝဝဂ နီးပါးမြောက်ကိုရီးယားက လေ့ကျင့်သင်တန်းပေးထားပြီ၊ နိုင်ငံတကာသတင်းဂျာနယ်၊ အတွဲ ၂၊ အမှတ် ၄၅၊ ကြာသပတေးနေ့၊ ၄ ဇွန်လ ၂၀၁၅၊ စာမျက်နှာ ၄ မှ ရရှိပါသည်။

[17]နောင်နောင်၊ ဆိုက်ဘာတိုက်ခိုက်မှုများ၏ထိပ်တန်းအရင်းမြစ်အဖြစ် တရုတ်ဆက်လက်ရပ်တည်နေ၊ ရတနာပုံ၊ http://news.yatanarpon.com.mm/news/news-89819 မှ ရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ၁ ဇူလိုင်လ ၂၀၁၅)

ယှက်မှုများနှင့် ကြုံတွေ့ခဲ့ရပါသည်။ ယင်း website သည် ငွေလွှဲပို့ခြင်းဆိုင်ရာ လုပ်ဆောင်ချက်မှားယွင်းမှုများဖြစ်ပေါ်ခဲ့ပြီး အချို့စာမျက်နှာများကို လက်ခံရာတွင် အဆင်မပြေမှုများနှင့် ကြုံတွေ့ခဲ့ရပါသည်။ အေဂျင်စီမှအရာရှိများက အမည်မသိကွန်ပျူတာဟက်ကာအုပ်စုက အေဂျင်စီ website ကို ရည်ရွယ်ချက်ထား တိုက်ခိုက်နေခြင်းဖြစ်ကြောင်းဖော်ပြခဲ့ပါသည်။ ကွန်ပျူတာဟက်ကာအုပ်စုသည် ဝန်ဆောင်မှုငြင်းဆန်ခြင်းနည်းပညာ (DDoS) ကို အသုံးပြု၍ အရေးကြီးအချက်အလက်များခိုးယူမှုပြုလုပ်ရန် ကြိုးစားခြင်းဖြစ်နိုင်ကြောင်း၊ ယင်းနည်းပညာသည် website များကို အချက်အလက်ဖောင်းပွမှုများဖြစ်စေကာ နှောင့်နှေးကြန့်ကြာမှုများ ပေါ်ပေါက်စေနိုင်ကြောင်း သိရှိရပါသည်။[18] ထို့အပြင် ဂျပန်နိုင်ငံရှိ ကုမ္ပဏီနှင့်အဖွဲ့အစည်းပေါင်း ၁၀၀၀ ကျော်၏ ကွန်ပျူတာများဗိုင်းရပ်စ်တိုက်ခိုက်ခြင်းခံခဲ့ရကြောင်းသိရှိရပါသည်။ ယင်းဗိုင်းရပ်စ်သည်လွန်ခဲ့သောနှစ်က ဂျပန်နိုင်ငံ၏ပင်စင်ဌာနကို တိုက်ခိုက်ခဲ့သည့်ဗိုင်းရပ်စ်နှင့်ပုံစံတူဖြစ်ကြောင်း သိရှိရပါ သည်။ ယင်းတိုက်ခိုက်မှုကြောင့် အဆင့်မြင့်နည်းပညာနှင့် ကာကွယ်ရေးအချက်အလက်ပေါင်း အနည်းဆုံး ၂၀၀၀၀ ကျော် ပေါက်ကြားသွားခဲ့ပါသည်။ လွန်ခဲ့သောနှစ်တွင် အမ်ဒီဗွီဗိုင်းရပ်စ်သည် ဂျပန်ပင်စင်ဌာန၏ ကွန်ပျူတာ ၃၁ လုံး ကိုတိုက်ခိုက်ခဲ့ပြီး သတင်းအချက်အလက်ပေါင်း ၁.၂၅ သန်းပေါက်ကြားခဲ့ပါသည်။ တိုက်ခိုက်ခံရသော ကွန်ပျူတာများမှအချက်အလက်များကို ကွန်ပျူတာဖောက်ထွင်းဝင်ရောက်များက အလွယ်တကူခိုးယူမှုများ ပြုလုပ်ခဲ့ပါသည်။[19]

၁၉။ ရုရှား၊ အစ္စရေးနှင့်တရုတ်တို့တွင်လည်း ဆိုက်ဘာစစ်ပွဲအတွက် ပြင်ဆင်နေကြပါသည်။ တိုတောင်းလှသောအချိန်အတွင်းမှာပင် နည်းပညာသည် အံ့မခန်းတိုးတက်လာပြီး ၎င်းနည်းပညာဖြင့် လူတို့၏ကိုယ်ရေးအချက်အလက်များ၊ စီးပွားရေးကုမ္ပဏီကြီးများ၏ အစီအမံများ၊ အစိုးရတို့၏လျှို့ဝှက်ချက်များကို အဝေးမှရယူရန်ကြိုးစားလာကြသည်။ ကမ္ဘာအနှံ့ပျံ့နှံ့လာနေ

[18] မြန်မာ့အလင်းသတင်းစာ၊ ဂျပန်နိုင်ငံ အမျိုးသားအခွန်တော်ဆိုင်ရာဝက်ဘ်ဆိုက်တစ်ခု ဟက်ကာတိုက်ခိုက်ခြင်းခံရ၊ မြန်မာ့အလင်းသတင်းစာ၊ ကြာသပတေးနေ့၊ ဖေဖော်ဝါရီလ ၁၀၊ ၂၀၁၆၊ စာမျက်နှာ ၄ မှ ရရှိပါသည်။

[19] မြန်မာ့အလင်းသတင်းစာ၊ ဂျပန်နိုင်ငံမှ ကုမ္ပဏီ၊ အဖွဲ့အစည်း ၁၀၀၀ ကျော်၏ ကွန်ပျူတာများ ဗိုင်းရပ်စ်တိုက်ခိုက်ခံရ၍ သတင်းအချက်အလက်များ ပေါက်ကြား၊ မြန်မာ့အလင်းသတင်းစာ၊ အင်္ဂါနေ့ ၊ ဖေဖော်ဝါရီ ၉၊ ၂၀၁၆၊ စာမျက်နှာ ၄ မှ ရရှိပါသည်။

သည့် ဆိုက်ဘာတိုက်ခိုက်မှုများသည် အစိုးရများ၊ ကုမ္ပဏီများအကြား လျှို့ဝှက်ချက်များ ရယူနိုင်ရေးကို အဓိကထားလာကြသည်။ ထိုမှတစ်ဆင့် နိုင်ငံရေး၊ စီးပွားရေး လွှမ်းမိုးမှုများကို တည်ဆောက်နိုင်သောကြောင့်ဖြစ်ပါသည်။

၂၀။ ကမ္ဘာတစ်ဝန်းတွင်ဆိုက်ဘာတိုက်ခိုက်မှုများ၊ ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများ၊ ကာကွယ်ရေး၊ တုန့်ပြန်ရေးကိုပြင်ဆင်ဆောင်ရွက်လျှက်ရှိပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုတွင်ရင်းနှီးမြှုပ်နှံမှုများ ၂၀၀၆ ခုနှစ်ခန့်ကပင်စတင်ခဲ့ပြီး ယခုအခါနိုင်ငံပေါင်း ၁၄၀ ကျော်တွင် ဆိုက်ဘာလက်နက် ထုတ်လုပ်သည့် စီမံချက်များရှိနေကြောင်း လေ့လာမှုများအရသိရှိရပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုအတွက် ပြင်ဆင်နေသည့်နိုင်ငံများတွင် တရုတ်၊ အမေရိကန်၊ ဗြိတိန်၊ ပြင်သစ်၊ ကနေဒါ၊ အိန္ဒိယ၊ ဩစတြေးလျ၊ ရုရှားစသည့် နည်းပညာထွန်းကားသောနိုင်ငံများ အဓိကပါဝင်နေကြပါသည်။[20]

သုံးသပ်ချက်များ

၂၁။ အိုင်တီနည်းပညာကျယ်ပြန့်ထွန်းကားလာသည်နှင့်အညီ ဆိုက်ဘာတိုက်ခိုက်မှုများသည် စီးပွားရေးနှင့်နိုင်ငံရေးကို အကြီးအကျယ်ဒုက္ခပေးနိုင်ပြီး ယင်းဆိုက်ဘာရာဇဝတ်မှုများအား ကာကွယ်ရေးစရိတ်များလည်း ကြီးမားလာမည်ဖြစ်ကြောင်း သတိပေးမှုများထွက်ပေါ်လာခဲ့ပါသည်။ IBM Corp ၏ ဥက္ကဋ္ဌ Ginni Rometty က ကမ္ဘာပေါ်ရှိကုမ္ပဏီတိုင်းကို ဆိုက်ဘာရာဇဝတ်မှုများက အကြီးအကျယ်ခြိမ်းခြောက်လိမ့်မည်ဖြစ်ကြောင်း ပြောကြားခဲ့ပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုများသည် စီးပွားရေးလုပ်ငန်းများအပေါ် ဦးတည်ချက်ထားပြီး အချက်အလက်များဖျက်ဆီးခိုးယူခြင်းကြောင့် ၂၀၁၉ ခုနှစ်တွင် ကုန်ကျစရိတ်အမေရိကန်ဒေါ်လာ ၂.၁ ထရီလီယံအထိရောက်ရှိနိုင်ကြောင်း သုတေသနပြုလုပ်ချက်များအရ သိရှိရပါသည်။ ကမ္ဘာ့စီးပွားရေးဖိုရမ်ကလည်း ဆိုက်ဘာရာဇဝတ်မှုများသည် စီးပွားရေးလုပ်ငန်းများအပေါ်တွင် များစွာထိခိုက်မှုရှိနိုင်ကြောင်း သတိပေးပြောကြားခဲ့ပါသည်။[21]

---

[20] မြန်မာ့သားကောင်း၊ နိုင်ငံတကာဆိုက်ဘာတိုက်ပွဲနှင့် မြန်မာစစ်တလင်း၊ မြန်မာ့သားကောင်း၊ ၂၂ ဩဂုတ်လ ၂၀၁၃၊ http://www.myanmartharkaung.net/ 2013/08/blog-post_6603.html မှရရှိပါသည် (ကြည့်ရှုသည့်ရက် - ဧပြီ ၂၅၊ ၂၀၁၆)

[21] Politics ဂျာနယ်၊ ၂၀၁၉ ခုနှစ်တွင် ဆိုက်ဘာရာဇဝတ်မှုကြောင့်ဆုံးရှုံးရငွေ ဒေါ်လာ ၂ ထရီလီယံအထိရောက်ရှိမည်၊ Politics ဂျာနယ်၊ အမှတ် ၉၂၊ ဇန်နဝါရီ ၂၂၊ ၂၀၁၆၊ စာမျက်နှာ ၁၂ မှရရှိပါသည်။

နိဂုံး

၂၂။ ဆိုက်ဘာတိုက်ခိုက်မှုသည် နိုင်ငံတစ်နိုင်ငံ၏လုံခြုံမှုနှင့် တည်ငြိမ်အေးချမ်းမှုတို့အတွက် ကြီးမား သောအန္တရာယ်ဖြစ်ပါသည်။ ကွန်ပျူတာကွန်ယက်နှင့် သတင်းအချက်အလက်များ လုံခြုံမှုရှိစေရန်၊ နိုင်ငံနှင့်ပြည်သူများလုံခြုံစိတ်ချစွာ အင်တာနက်သုံးစွဲနိုင်ရန် ကြိုတင်ကာကွယ်ခြင်း၊ သတိပေးဆောင်ရွက်ခြင်း၊ အသိပညာပေးခြင်းနှင့် နည်းပညာပိုင်းဆိုင်ရာလုပ်ငန်းများတွင် ဆိုက်ဘာလုံခြုံရေးနှင့်ပတ်သက်၍ နိုင်ငံတကာတွင် မူဝါဒများချမှတ်ဆောင်ရွက်နေသည်ကို တွေ့ရှိရပါသည်။ တရားမဝင်ဖြန့်ချိသည့် ဆော့ဖ်ဝဲများသည် ကွန်ပျူတာဗိုင်းရပ်စ်များ ပါရှိလာနိုင်သည့်အတွက် တရားဝင်ထုတ်လုပ်ထားသည့်ဆော့ဖ်ဝဲများကိုသာ သုံးစွဲသင့်ပါသည်။ ဆိုက်ဘာလုံခြုံရေးဆောင်ရွက်ရာတွင် အစိုးရပိုင်းမှပါဝင်ပတ်သက်မှု၊ ဆိုက်ဘာလုံခြုံရေးဥပဒေစသည်တို့သည် အဓိကအရေးကြီးပါကြောင်း ရေးသားတင်ပြအပ်ပါသည်။

သုတေသနဌာန

ပြည်သူ့လွှတ်တော်ရုံး

သတိပြုရန်

ဤသတင်းအချက်အလက်သည် လွတ်တော်ကိုယ်စားလှယ်များအား ၎င်းတို့၏ လွတ်တော်ဆိုင်ရာ တာဝန်များကို ဆောင်ရွက်ရာတွင် အထောက်အကူပြုရန်အတွက် ဖြစ်ပါသည်။ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ ကိစ္စ တစ်စုံတစ်ခုအတွက် အသုံးပြုရန်မဟုတ်ပါ။ အချိန်နှင့်တပြေးညီ နောက်ဆုံးရသတင်းဖြစ်မည်ဟု သတ်မှတ် မထားသင့်ပါ။ ဤအချက်အလက်များအား တရားဝင် သို့မဟုတ် ပညာရှင်ဆိုင်ရာအကြံပေးချက်အဖြစ် မသတ်မှတ်သင့်ပါ။ အထူးအကြံပေးချက် သို့မဟုတ် သတင်းအချက်အလက်များလိုအပ်ပါက အရည် အသွေးပြည့်မီသော သင့်လျော်သည့် ကျွမ်းကျင်ပညာရှင်နှင့် ဆွေးနွေးတိုင်ပင်သင့်ပါသည်။ လွတ်တော် သုတေသနဝန်ဆောင်မှုသည် စာတမ်းတိုများတွင် ပါဝင်သောအကြောင်းအရာများနှင့် စပ်လျဉ်း၍ လွတ်တော် ကိုယ်စားလှယ်များ၊ လွတ်တော်ဝန်ထမ်းများနှင့် ဆွေးနွေးမှုများ ပြုလုပ်ပေးနိုင်ပါသည်။ အများပြည်သူနှင့် ဆွေးနွေးမှုများ ပြုလုပ်ခြင်းမရှိပါ။

သုတေသနလုပ်ငန်းဆိုင်ရာ စုံစမ်းမေးမြန်းမှုများပြုလုပ်ရန်
(သို့မဟုတ်) သုတေသနဌာနအား လာရောက်လေ့လာရန်
အောက်ပါလိပ်စာအတိုင်း ဆက်သွယ်နိုင်ပါသည်။

သုတေသနဌာန
ပြည်သူ့လွှတ်တော် C ဆောင် - ဒုတိယထပ်
တယ်လီဖုန်း - ၀၆၇ - ၅၉၁၂၈၄၊ ၀၆၇ - ၅၉၁၂၈၅

Research Dept; Email - pyithuhluttawresearch@gmail.com