ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများနှင့်သက်ဆိုင်သော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံလုပ်ထုံးလုပ်နည်းများ

မိတ်ဆက်

၁။ ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်၊ အစိုးရရုံးဌာနများသည် သတင်းအချက်အလက် နည်းပညာများကို အသုံးပြု၍ e-Government လုပ်ငန်းစဉ်များအား အရှိန်အဟုန်မြင့် အကောင် အထည်ဖော်ဆောင်ရွက်လျက် ရှိပါသည်။ မြန်မာနိုင်ငံတွင် သတင်းအချက်အလက်နည်းပညာ (ICT) ဖွံ့ဖြိုးတိုးတက်မှုနှင့်အတူ ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာခြိမ်းခြောက်ခံရမှုများ (Cyber Security and Threat)၊ ဆိုက်ဘာအကြမ်းဖက်တိုက်ခိုက်မှု (Cyber Terrorist Attack) များဖြစ်ပေါ်လျက်ရှိပြီး အစိုးရရုံးဌာနများ၏ အရေးကြီးသောသတင်းအချက်အလက်များအား လုံခြုံစိတ်ချစွာ အသုံးပြုနိုင် ရေးနှင့် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများအား ကာကွယ်လျှော့ချနိုင်ရေးသည် အလွန်ပင်အရေးပါလှ ပါသည်။

ရည်ရွယ်ချက်

၂။ ဤစံလုပ်ထုံးလုပ်နည်း၏ ရည်ရွယ်ချက်မှာ အစိုးရရုံးဌာနအသီးသီးရှိ လုပ်ငန်းသုံးကွန်ပျူတာ များအား ဆိုက်ဘာတိုက်ခိုက်ခံရမှုမှ ကာကွယ်နိုင်ရန်နှင့် လျှော့ချနိုင်ရန်၊ အရေးကြီးသော သတင်းအချက်အလက်များအား လုံခြုံစိတ်ချစွာ အသုံးပြုနိုင်ရန်အတွက် လိုက်နာရမည့် လုပ်ငန်း စဉ်များနှင့် စံလုပ်ထုံးလုပ်နည်းများကို ရေးသားပြုစုခြင်း ဖြစ်ပါသည်။

ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံလုပ်ထုံးလုပ်နည်းများ

၃။ အစိုးရရုံးဌာနအသီးသီးတွင် အသုံးပြုလျက်ရှိသော ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများ၌ ဆိုက်ဘာ တိုက်ခိုက်ခံရမှုကြောင့် သတင်းအချက်အလက်များ ပျက်စီးဆုံးရှုံးခြင်း၊ ခိုးယူခံရခြင်းနှင့် ဖွင့်ချခံရ ခြင်းများမှ ကာကွယ်နိုင်ရန် လိုက်နာကျင့်သုံးရမည့် စံသတ်မှတ်ချက်များမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

(က) User Account လုံခြုံရေး

(ခ) User Account ၏ စကားဝှက်လုံခြုံရေး

(ဂ) အသုံးပြုနေသော Port များနှင့် Service များ လုံခြုံရေး

(ဃ) ကွန်ပျူတာစနစ် (Operating System) နှင့် ဆော့ဖ်ဝဲလ်များ၏ လုံခြုံရေး

(င) ဒေတာများ Backup ထားရှိမှု

(စ) External Storage Device များ၏ လုံခြုံရေး

(ဆ) အင်တာနက်သုံးစွဲမှု လုံခြုံရေး

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

(ဈ) အီးမေးလ်လုံခြုံရေး

(ည) စက်ပစ္စည်းများကို ကာကွယ်ခြင်း

(ဋ) လူမှုကွန်ရက်ကို သတိပြုသုံးစွဲခြင်း

(ဌ) ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာပေးသင်တန်းပို့ချခြင်း

User Account လုံခြုံရေး

၄။ ရုံးသုံးကွန်ပျူတာများတွင် အရင်းအမြစ်များသုံးစွဲခြင်း (Application များသုံးစွဲခြင်းနှင့် ဒေတာများအား ရယူသုံးစွဲခြင်း)အတွက် တစ်ဦးချင်းစီအတွက် ကိုယ်ပိုင်အကောင့်များဖြင့် သုံးစွဲရမည်။ User Account များကို ဖန်တီးရာတွင် Administrator Account၊ Standard Account နှင့် Guest Account ဟူ၍ (၃)မျိုးဖန်တီးနိုင်ပြီး Account အမျိုးအစားတစ်ခုချင်းစီအလိုက် အရင်းအမြစ်များကို အသုံးပြုခွင့် ကန့်သတ်နိုင်ပါသည်။

၅။ Administrator အကောင့်သည် ကွန်ပျူတာအတွင်းရှိ အရင်းအမြစ်များကို စီမံခန့်ခွဲပိုင်ခွင့် အပြည့်အဝ ရရှိထားသောကြောင့် Application များကို တပ်ဆင်ခြင်း (Installation)၊ ဖယ်ရှားခြင်း (Uninstallation) နှင့် ကွန်ပျူတာစနစ် (Operating System)အား ပြုပြင်ပြောင်းလဲခြင်းတို့အတွက် လုပ်ပိုင်ခွင့်အပြည့်အဝရရှိပြီး အခြားသော အသုံးပြုသူ Account များအား ဖန်တီးခြင်း၊ ဖယ်ရှားခြင်း တို့ကို ပြုလုပ်နိုင်သည့်အတွက် ရုံးသုံးကွန်ပျူတာများ၌ Administrator Account အား အသုံးပြုခြင်းအစား လုပ်ပိုင်ခွင့်ကန့်သတ်ထားသော Standard Account ဖြင့်သာ စကားဝှက်ခံ၍ ပြောင်းလဲသုံးစွဲရမည်။ Guest Account အသုံးပြုသူများအနေဖြင့် ကွန်ပျူတာအတွင်းရှိ အရင်းအမြစ်များကို အနိမ့်ဆုံးခွင့်ပြုချက်ဖြင့်သာ ဝင်ရောက်သုံးစွဲခွင့်ရှိသော်လည်း ဆိုက်ဘာတိုက်ခိုက်သူများက ၎င်း Account ကိုအသုံးပြု၍ Administrator Account အဖြစ် လုပ်ပိုင်ခွင့်တိုးယူခြင်း (Privilege Escalation) ပြုလုပ်နိုင်သည့်အတွက် Guest Account အား အသုံးပြုခြင်းမရှိလျှင် ပိတ်ပင်ထားသင့်ပါသည်။

User Account ၏ စကားဝှက်လုံခြုံရေး

၆။ User Account များနှင့်ပတ်သက်သော စကားဝှက်များသည် ခိုင်မာမှုရှိရန်နှင့် လုံခြုံမှုရှိရန် အလွန်အရေးကြီးပါသည်။ ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများအား ဆိုက်ဘာတိုက်ခိုက်မှုများမှ ကာကွယ်လျှော့ချနိုင်ရန်အတွက် စကားဝှက်ဆိုင်ရာမူဝါဒ (Password Policy) ချမှတ်ဆောင်ရွက်ရန် လိုအပ်ပြီး စကားဝှက်ဆိုင်ရာမူဝါဒတွင် အောက်ပါအချက်များ ပါရှိရမည်-

(က) စကားဝှက်များတွင် ကွန်ပျူတာအားအသုံးပြုသူ၏အမည်၊ ဌာနအမည်၊ မွေးသက္ကရာဇ်၊ မှတ်ပုံတင်အမှတ်စသည့် အချက်အလက်များ မပါရှိရ။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

(ခ) စကားဝှက်ကို အင်္ဂလိပ်အက္ခရာစာလုံးကြီး (A, B, စသည်)၊ စာလုံးသေး (a, b, စသည်)၊ ဂဏန်းများနှင့် အထူးသင်္ကေတများ (#, $, စသည်)တို့ကို ပေါင်းစပ်၍ ပေးရမည်။ (ဥပမာ - 'qAlmk(iHm`V-2X)

(ဂ) ယခင်အသုံးပြုပြီးသော စကားဝှက်များကို ပြန်လည်အသုံးပြုခြင်းအား ရှောင်ကြဉ်ရမည်။

(ဃ) စကားဝှက်ကို သတ်မှတ်ရာတွင် စာလုံးရေ ၁၂ လုံးနှင့် ၁၆ လုံးကြား ဖြစ်ရမည်။

(င) အဘိဓာန်တွင်ရှိသော စကားလုံးများအား စကားဝှက်အဖြစ်အသုံးပြုခြင်း မပြုရ။ သို့သော် စကားလုံး ၄ လုံး၊ ဂဏန်းများနှင့် အထူးအက္ခရာတစ်လုံးအား ပေါင်းစပ်၍မူ သုံးနိုင်သည်။ (ဥပမာ - BigFr0gLeapsM00n!)

(စ) စကားဝှက်များကို စာရွက်စာတမ်းများတွင် ရေးမှတ်ခြင်း၊ ကွန်ပျူတာတွင် Plain Text ဖိုင်အနေဖြင့် သိမ်းဆည်းခြင်းမှ ရှောင်ကြဉ်ပါ။ စာရွက်တွင်ရေးပါက လုံခြုံသောနေရာတွင်ထားပါ။

(ဆ) ရှုပ်ထွေးသော စကားဝှက်များကို စီမံခန့်ခွဲရန်အတွက် LastPass၊ Dashlane၊ 1Password၊ Bitwarden နှင့် KeePass ကဲ့သို့သော Password Manager ဆော့ဖ်ဝဲလ်များ သုံးစွဲနိုင်သည်။ Keylogger/Spyware/Remote Access Trojan (RAT) များ၏ အန္တရာယ်ကို ရှောင်ရှား နိုင်ရန်အတွက် Microsoft Word ဖိုင်တွင် စကားဝှက်ခံ၍ သိမ်းခြင်းနည်းလမ်းကိုလည်း ရှောင်ကြဉ်ရမည်။ Password Manager တွင် သိမ်းဆည်း၍ မရနိုင်သော အချက်အလက်များကိုသာ Encrypt လုပ်ထားသော Word ဖိုင်တွင် သိမ်းဆည်းထားသင့်ပြီး မိမိသာနားလည်နိုင်သော သင်္ကေတဖြင့် မှတ်သားရန်လိုသည်။

(ဇ) ကွန်ပျူတာများ (သို့မဟုတ်) Router ကဲ့သို့သော စက်ပစ္စည်းများတွင် တပါတည်း ပါရှိသော စကားဝှက်များကို အသုံးမပြုဘဲ စကားဝှက်အားပြောင်းလဲသုံးစွဲရမည်။

(ဈ) အကောင့်အသီးသီးအတွက် မတူညီသော စကားဝှက်ကိုသာ အသုံးပြုရမည်။

(ည) စကားဝှက်များကို ကျပန်းပေးနိုင်လေလေ၊ ဟက်ကာများက ဖော်ရန် ခက်လေလေ ဖြစ်ပါသည်။ Password Manager ဆော့ဖ်ဝဲလ်များကို သုံး၍ ကျပန်းစကားဝှက်များ ဖန်တီးနိုင်သည်။

(ဋ) စကားဝှက်များအား အခြားသူများနှင့် မျှဝေသုံးစွဲခြင်း မပြုလုပ်ရ။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

(င) စကားဝှက်များအား အခြားသူများအား ပြောကြားခြင်း၊ အသုံးပြုခွင့်ပေးခြင်း၊ အီးမေးလ်၊ စာတိုနှင့် အခြားသောအီလက်ထရောနစ်ဆက်သွယ်မှုပုံစံများတွင် ထည့်သွင်းပေးပို့ခြင်း မပြုလုပ်ရ။

(ဉ) ကီးဘုတ်လက်ကွက်ပုံစံဖြစ်သော "qwerty"၊ "123456"၊ "asdfgh" တို့ကိုရှောင်ပါ။

သုံးစွဲနေသောစကားဝှက်များကို မည်မျှအကြာတွင် ပြောင်းသင့်သနည်း။

၇။ စကားဝှက်ကို အကြိမ်မည်မျှပြောင်းလဲရမည်နှင့် ပတ်သက်၍ သမားရိုးကျ အကြံပြုချက်များက ရက် ၃၀၊ ရက် ၆၀ သို့မဟုတ် ရက် ၉၀ တိုင်း စကားဝှက်ကို ပြောင်းရန် အကြံပြုကြသည်။ သို့သော် လမ်းညွှန်ချက်အသစ်များက သတ်မှတ်ထားသောအချိန်ကာလထက် သီးခြားအခြေအနေများ ပေါ်မူတည်၍ စကားဝှက်ပြောင်းရန် အကြံပြုသည်။ ၎င်းအကြံပြုချက်များမှာ အောက်ပါအတိုင်းဖြစ်သည်-

(က) မိမိအသုံးပြုသောဝန်ဆောင်မှု တိုက်ခိုက်ခံရပြီးချိန်တွင် စကားဝှက်ကို ပြောင်းလဲရမည်။

(ခ) မိမိအကောင့်နှင့်ပတ်သက်၍ သံသယဖြစ်ဖွယ် အပြုအမူများ တွေ့ရှိလျှင် စကားဝှက်ကို ပြောင်းလဲရမည်။

(ဂ) အခြားသူများနှင့် အကောင့်ကို မျှဝေမသုံးသောအခါ ၎င်းတို့မသုံးတော့လျှင် စကားဝှက်ကို ပြောင်းလဲရမည်။

(ဃ) အများပြည်သူအသုံးပြုသော ကွန်ပျူတာများ၌ သုံးစွဲပြီးနောက်တွင် စကားဝှက်ကို ပြောင်းလဲရမည်။

(င) ငွေကြေးဆိုင်ရာ အကောင့်များကဲ့သို့ အလွန်အရေးကြီးသော အကောင့်များအတွက်မူ မည်သည့်အကြောင်းပြ ချက်မျှ မရှိလျှင်ပင် ၃ လ နှင့် ၆ လ အကြား စကားဝှက်ကို မဖြစ်မနေ ပြောင်းလဲသင့်သည်။

(စ) စကားဝှက်ကို မကြာခဏပြောင်းလဲခြင်းက အားနည်းသောစကားဝှက်များ ပေးမိစေနိုင်သည်။ မကြာခဏ ပြောင်းလဲခြင်းက စကားဝှက်များကို ချရေးရန် အကြောင်းရင်းဖြစ်စေသည်။

(ဆ) Password Manger များသုံးစွဲပါက ခိုင်မာသော၊ မတူညီသော စကားဝှက်များကို ဖန်တီးပေးနိုင်သည်။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

အသုံးပြုနေသော Port များနှင့် Service များ လုံခြုံရေး

၈။ ရုံးဌာနများတွင်ကွန်ရက်များချိတ်ဆက်အသုံးပြုနိုင်ရန်နှင့် အင်တာနက်ချိတ်ဆက်ရန်အတွက် Transmission Control Protocol (TCP)နှင့် User Datagram Protocol (UDP) Port များကို သုံး၍ ချိတ်ဆက်အသုံးပြုရသည်။ Port များသည် ကွန်ပျူတာအချင်းချင်း ချိတ်ဆက်ခြင်း၊ အင်တာနက်မှ Website များနှင့် ဆာဗာများသို့ ဝင်ရောက်ရာတွင် ဝင်ခွင့်ပြုသည့် တံခါးသဖွယ်အလုပ်လုပ်သော ကြောင့် Port များ၏လုံခြုံရေးသည် အလွန်အရေးကြီးပါသည်။ Port အမျိုးအစား ၂ မျိုးရှိပြီး ကွန်ပျူတာအချင်းချင်း (သို့မဟုတ်)ကွန်ပျူတာမှ အခြားစက်ပစ္စည်းများနှင့် ချိတ်ဆက်အသုံးပြုရသော Physical Port များနှင့် အင်တာနက်မှ ဒေတာရယူပေးပို့ခြင်း၊ ကွန်ပျူတာစနစ်များ၏ Service (ဝန်ဆောင်မှုများ)ပြုလုပ်ရာတွင် အသုံးပြုသော Logical Port များဖြစ်သည်။ Physical Port များ လုံခြုံစေရေးအတွက် ဌာနတွင်းရှိ စက်ပစ္စည်းများ၊ စနစ်များ၊ ဝန်ဆောင်မှုများနှင့် သတင်းအချက်အလက်ရယူသုံးစွဲခွင့်ကို ကန့်သတ်ထားရှိပြီး Physical Security နှင့်ပတ်သက်သော မူဝါဒများ ချမှတ်ထားရမည်။ Logical Port များ၏ လုံခြုံရေးအတွက်မူ မလိုအပ်သော၊ အသုံးမပြုသော Port များနှင့် Service များကို ပိတ်ထားရမည်။ Logical Port များသည် အရေအတွက်အားဖြင့် ၆၅၅၃၆ ခု ရှိပြီး ၎င်းတို့မှာ အသုံးများသော Port များ (1-1023)၊ မှတ်ပုံတင်ထားသော Port များ (1024-49151) နှင့် Dynamic/Private Port များ (49152-65535) တို့ဖြစ်သည်။

၉။ ဆိုက်ဘာတိုက်ခိုက်သူများသည် ဌာနတွင်းရှိ ကွန်ပျူတာများ စက်ပစ္စည်းများတွင် မည်သည့် ဝန်ဆောင်မှုများအသုံးပြုထားသည်၊ မည်သည့် Port များဖွင့်ထားသည်ကို ဆိုက်ဘာလုံခြုံရေးအားနည်းချက်များစစ်ဆေးသည့်ဆော့ဖ်ဝဲလ် (Vulnerability Scanners) များဖြင့် စစ်ဆေးကြပြီး ၎င်းတို့ အများဆုံး ပစ်မှတ်ထားတိုက်ခိုက်ကြသော Port များမှာ Port 21 (File Transfer Protocol)၊ Port 22 (Secure Shell)၊ Port 445 (Server Message Block) နှင့် Port 3389 (Remote Desktop Protocol) တို့ဖြစ်သည်။

၁၀။ ဖိုင်များကို ရွှေ့ပြောင်းရာတွင် အသုံးပြုသော File Transfer Protocol (FTP) သည် စကားဝှက်များကို ဝှက်စာစနစ်အသုံးပြု၍ ပေးပို့ခြင်းမရှိဘဲ ရိုးရိုးစာသားအနေဖြင့်သာ ပေးပို့သည့်အတွက် ကြားဖြတ်ဖမ်းယူနိုင်သည့်ဆော့ဖ်ဝဲလ် (Packet Sniffer) များက အသုံးပြုသူအမည်နှင့် စကားဝှက်များကို အလွယ်တကူဖမ်းယူရရှိနိုင်ပါသည်။ ကွန်ပျူတာတစ်လုံးမှ တစ်လုံးသို့ အဝေးမှ ဝင်ရောက်နိုင်ရန်အတွက် အသုံးပြုသော Secure Shell Protocol (SSH) တွင် အသုံးပြုသူအမည်နှင့် စကားဝှက်တို့သည် ခန့်မှန်းရလွယ်ကူနေပါက ကွန်ပျူတာစနစ်အတွင်းသို့ တိုက်ခိုက်သူများက အလွယ်တကူဝင်ရောက်နိုင်မည်ဖြစ်ပါသည်။ ဖိုင်များနှင့် ပရင်တာအသုံးပြုခြင်းကို မျှဝေသည့် Windows စနစ်တွင် တစ်ပါတည်းပါရှိသည့် Server Message Block Protocol (SMB) ကို အသုံးပြုပါက Update ပြုလုပ်ထားခြင်းမရှိသော Microsoft Windows Server 2003/2008/

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

Windows XP/Windows 7 တို့တွင် EternalBlue Exploit ဖြင့် အလိုအလျောက်တိုက်ခိုက်ခြင်း ခံရနိုင်ပြီး မည်သည့် Windows စနစ်တွင်မဆို စကားဝှက်ကို အလွယ်တကူပေးထားပါက တိုက်ခိုက်သူများက စနစ်အတွင်းသို့ အလွယ်တကူဝင်ရောက်နိုင်ပြီး ဖိုင်များအား ဖတ်ခြင်း၊ ပြင်ခြင်းနှင့် ဖျက်ဆီးခြင်းများကို ပြုလုပ်နိုင်ပါသည်။ Windows စနစ်တွင် ပါရှိသော Remote Desktop Protocol (RDP) ကို ဖွင့်ထားပါက တိုက်ခိုက်သူများက Bluekeep ကဲ့သို့သော RDP ၏ လုံခြုံရေးအားနည်းချက်ကို တိုက်ခိုက်သော Exploit များဖြင့် တိုက်ခိုက်၍ ကွန်ပျူတာစနစ်များ အတွင်းသို့ဝင်ရောက်နိုင်ပါသည်။ ထို့ကြောင့် ရုံးလုပ်ငန်းသုံးကွန်ပျူတာများတွင် အသုံးမပြုသည့် Port များနှင့် Service များကို ပိတ်ထားခြင်း၊ Service များကို အသုံးပြုရာတွင် အလိုအလျောက် ပါရှိပြီးဖြစ်သည့် စကားဝှက်များကို အသုံးပြုခြင်းမှရှောင်ကြဉ်ခြင်းတို့ကို ဆောင်ရွက်ရမည်။

ကွန်ပျူတာစနစ် (Operating System) နှင့် ဆော့ဖ်ဝဲလ်များ၏ လုံခြုံရေး

၁၁။ လုပ်ငန်းသုံးကွန်ပျူတာများတွင် တပ်ဆင်သုံးစွဲမည့် ကွန်ပျူတာစနစ်(Operating System) နှင့် ဆော့ဖ်ဝဲလ်များ၏လုံခြုံရေးအားနည်းချက်များကြောင့် Ransomware တိုက်ခိုက်ခံရမှုများနှင့် အခြားသောဆိုက်ဘာတိုက်ခိုက်မှုများ ဖြစ်ပွားစေနိုင်သောကြောင့် ၎င်းတို့၏လုံခြုံရေးသည် အထူး အရေးပါလှပါသည်။ လိုင်စင်မပါရှိသော ကွန်ပျူတာစနစ်များ၊ ဆော့ဖ်ဝဲလ်များအား အသုံးပြုခြင်း၊ အခမဲ့ရရှိသောဆော့ဖ်ဝဲလ်များကို မယုံကြည်ရသည့် Website များနှင့် အရင်းအမြစ်များ (ဥပမာ- Torrent များနှင့် P2P ဆော့ဖ်ဝဲလ်များ)မှ ရယူသုံးစွဲခြင်း၊ ကွန်ပျူတာစနစ်များနှင့် ဆော့ဖ်ဝဲလ်များကို ပုံမှန် Update မပြုလုပ်ခြင်းတို့ကြောင့် ဆိုက်ဘာလုံခြုံရေးအားနည်းချက်များ ဖြစ်ပေါ်ကာ အဖျက် အမှောက်ဆော့ဖ်ဝဲလ် (Malware) များ၏ တိုက်ခိုက်မှုကို ခံရနိုင်ပါသည်။ ထို့ကြောင့် လုပ်ငန်းသုံး ကွန်ပျူတာများတွင် ဌာန၏ IT ပိုင်းဆိုင်ရာတာဝန်ခံများ၏ ခွင့်ပြုချက်မရှိဘဲ မလိုအပ်သော ဆော့ဖ်ဝဲလ်များ၊ ဂိမ်းများကို Download လုပ်၍ တင်ခြင်း၊ ရုံးလုပ်ငန်းနှင့် မသက်ဆိုင်သော Website များသို့ဝင်ရောက်ကြည့်ရှုခြင်းတို့ကို ရှောင်ကြဉ်ရမည်။ အလားတူ ကွန်ရက်စောင့်ကြည့်သော ဆော့ဖ်ဝဲလ်များ၊ စကားဝှက်ခန့်မှန်းသောဆော့ဖ်ဝဲလ်များကို ဌာနကွန်ပျူတာစနစ်အတွင်း တပ်ဆင် အသုံးပြုခြင်း၊ ကွန်ပျူတာဗိုင်းရပ်စ်များ ဖန်တီးခြင်း၊ ပေးပို့ခြင်း၊ ပျံ့နှံ့စေခြင်းနှင့် ခွင့်ပြုချက်မရဘဲ ဌာန၏ကွန်ပျူတာကွန်ရက်အား ထောက်လှမ်းခြင်း၊ ဖောက်ထွင်းဝင်ရောက်ခြင်းအား ရှောင်ကြဉ်ရမည်။ အဖျက်အမှောက်ဆော့ဖ်ဝဲလ်အမျိုးအစားများနှင့် ၎င်းတို့၏အလုပ်လုပ်ပုံများမှာ အောက်ပါ အတိုင်းဖြစ်ပါသည်-

(က) **Ransomware**။ Ransomware ဆိုသည်မှာ ကွန်ပျူတာတွင်းရှိဖိုင်များကို ဖွင့်မရအောင်ပြုလုပ်၍ ဖိုင်များကို ပြန်လည်ရရှိလိုပါက ငွေပေးချေမှုပြုလုပ်ရသော ပရိုဂရမ်တစ်မျိုးဖြစ်သည်။ တောင်းခံသော ငွေအမျိုးအစားမှာ များသောအားဖြင့် Crypto ငွေကြေးဖြစ်သော BitCoin ဖြစ်ပြီး ပေးချေရသော ငွေပမာဏမှာ ဒေါ်လာ ၃၀၀ မှ

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

ဒေါ်လာသန်း ၅၀ အထိဖြစ်နိုင်သည်။ အချို့သော Ransomware များသည် လူအားလုံးကို ပစ်မှတ်ထားတိုက်ခိုက်ပြီး အချို့သော Ransomware များသည် နာမည်ကြီးကုမ္ပဏီများ၊ အစိုးရအဖွဲ့အစည်းများကိုသာ ပစ်မှတ်ထားတိုက်ခိုက်သည်။ (၁၈-၇-၂၀၂၁)ရက်နေ့တွင် Telecom Argentina ကို REvil Ransomware တိုက်ခိုက်ခဲ့သောဖြစ်စဉ်၌ ကွန်ပျူတာအလုံးရေ (၁၈၀၀၀)ကျော် တိုက်ခိုက်ခံခဲ့ရပြီး ဖိုင်များကို ပြန်ရရန် ဒေါ်လာ ၇.၅ သန်း တောင်းခံခဲ့သည်။

(ခ) **Cryptominers**။ Crypto ငွေကြေးရရှိရန်အတွက် သူတစ်ပါး၏ ကွန်ပျူတာကို တိုက်ခိုက်ကာ ၎င်းကွန်ပျူတာ၏ CPU/GPU ကိုသုံးစွဲ၍ ငွေရှာသည့်ပရိုဂရမ် ဖြစ်သည်။

(ဂ) **Botnet**။ ကွန်ပျူတာများကို တိုက်ခိုက်ပြီး တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာများက ဆိုက်ဘာတိုက်ခိုက်မှုများကို ကျူးလွန်စေရန် ညွှန်ကြားချက်ပေးသော ပရိုဂရမ်ဖြစ်သည်။ ၂၀၁၆ ခုနှစ်တွင်ဖြစ်ပွားခဲ့သော Dyn ဆာဗာ DDoS တိုက်ခိုက်ခံရပြီး ၂ နာရီကြာ ဝန်ဆောင်မှုရပ်တန့်ခဲ့ရမှုသည် Botnet ဆယ်သန်း၏ တပြိုင်နက် တိုက်ခိုက်မှုကြောင့် ဖြစ်သည်။

(ဃ) **Infostealers**။ တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာများမှ စကားဝှက်နှင့် အဖိုးတန် အချက်အလက်များကို တိတ်တဆိတ်ခိုးယူနေသည့် ပရိုဂရမ် ဖြစ်သည်။ Trojan နှင့် Spyware အမျိုးအစား Malware များသည် Infostealer များ ဖြစ်သည်။ PlugX Remote Access Trojan သည် သတင်းအချက်အလက်များကို ခိုးယူရန် တီထွင်ထားသော Malware တစ်မျိုးဖြစ်ပြီး အင်တာနက်မချိတ်ထားသော ကွန်ပျူတာများမှ အချက်အလက်များကိုပင် ခိုးယူရန် ဒီဇိုင်းပြုရေးသားထားသည်။

(င) **Zero-Day Exploit**။ ကွန်ပျူတာ၊ ကွန်ရက်စနစ်များအတွင်းသို့ ထိုးဖောက်ဝင်ရန် အတွက် မည်သူမျှမသိရှိသေးသော ဆိုက်ဘာလုံခြုံရေးအားနည်းချက်ကို အသုံးချ၍ တိုက်ခိုက်သည့် ပရိုဂရမ် (သို့မဟုတ်) ကုဒ် ဖြစ်သည်။

(စ) **Virus**။ ကွန်ပျူတာစနစ်အတွင်းတွင် အခြားသောဖိုင်များကို ကူးစက်ပြန့်ပွားစေရန် ရည်ရွယ်၍ ရေးသားထားသော ပရိုဂရမ်ဖြစ်သည်။

(ဆ) **Worm**။ ကွန်ပျူတာစနစ်များ၏ လုံခြုံရေးအားနည်းချက်ကို တိုက်ခိုက်သော ကွန်ရက်မှတစ်ဆင့် ကူးစက်ပြန့်ပွားနိုင်သည့် အဖျက်အမှောက်ပရိုဂရမ်ဖြစ်သည်။ Stuxnet နှင့် WannaCry တို့သည် Worm အမျိုးအစားများဖြစ်ပြီး Worm သည် Malware များတွက် ကူးစက်မှု အမြန်ဆုံးဖြစ်သည်။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

ဒေတာများ Backup ထားရှိမှု

၁၂။ သတင်းအချက်အလက်များ၊ အရင်းအမြစ်များနှင့် ဝန်ဆောင်မှုများအား ဆိုက်ဘာတိုက်ခိုက်သူများရန်မှ ကာကွယ်နိုင်ရန်အတွက် ကြိုတင်ပြင်ဆင်မှုများပြုလုပ်ရန် လိုအပ်သကဲ့သို့ မတော်တဆမှုကြောင့်သော်လည်းကောင်း၊ သဘာဝဘေးအန္တရာယ်ကျရောက်ခြင်းကြောင့်သော်လည်းကောင်း ဒေတာများ ပျက်စီးဆုံးရှုံးခဲ့ပါက မိမိတို့၏လုပ်ငန်းများ၊ ဝန်ဆောင်မှုများအား လျင်မြန်စွာဖြင့် ပြန်လည်ဆောင်ရွက်နိုင်စေရန်အတွက် ဒေတာများ Backup ထားရှိခြင်းသည် အလွန်အရေးပါလှပါသည်။ Backup ပြုလုပ်ခြင်းသည် ဒေတာများကို လိုအပ်လာလျှင် ပြန်လည်အသုံးပြုနိုင်ရန်အတွက် သိမ်းဆည်းထားခြင်းဖြစ်ပြီး ထိရောက်သော Backup စနစ်အတွက် မူရင်းအပါအဝင် မိတ္တူ (၂)မျိုး ထားရှိခြင်းဖြစ်ပါသည်။ မိတ္တူပွားရာတွင် External Hard Drive၊ Removable Drive နှင့် Cloud Storage များအနက်မှ မတူညီသောစနစ် (၂)မျိုးကို အသုံးပြု၍ သိမ်းဆည်းရမည်။

၁၃။ ထိရောက်သောဒေတာသိမ်းဆည်းခြင်းဖြစ်ရန်အတွက် အရေးကြီးသည့်ဒေတာများကို ကြိုတင်သတ်မှတ်ခြင်း၊ သိမ်းဆည်းမည့်နေရာသတ်မှတ်ခြင်း၊ သိမ်းဆည်းနိုင်သည့်ဒေတာပမာဏကို ကြိုတင်သတ်မှတ်ထားခြင်းတို့ကို ပြုလုပ်ရမည်။ Backup အမျိုးအစားများကို အောက်ပါအတိုင်း သတ်မှတ်နိုင်ပါသည်-

(က) **အပြည့်အစုံသိမ်းဆည်းခြင်း (Full Backup)**။ Full Backup သည် ဒေတာအားလုံးကို သိမ်းဆည်းခြင်းဖြစ်ပြီး ပြန်လည်အသုံးပြုသောအခါတွင် အခြား Backup အမျိုးအစားထက် ပို၍ပြည့်စုံသော်လည်း Backup ပြုလုပ်ရန် လိုအပ်သောအချိန်မှာ အခြားအမျိုးအစားများထက် ပိုကြာသည်။

(ခ) **ပေါင်းထည့်သိမ်းဆည်းခြင်း (Incremental Backup)**။ နောက်ဆုံးသိမ်းဆည်းထားခဲ့သည့်ဒေတာများမှစ၍ စတင်သိမ်းဆည်းခြင်းဖြစ်ပြီး Backup ပြုလုပ်ရန် အမြန်ဆုံးဖြစ်သည်။

(ဂ) **ကွဲပြားခြားနားချက်ကိုသာသိမ်းဆည်းခြင်း (Differential Backup)**။ နောက်ဆုံးအပြည့်သိမ်းဆည်းထားသော ဒေတာများနှင့် တိုက်စစ်၍ မတူညီသောဒေတာများကိုသာ သိမ်းဆည်းခြင်းဖြစ်သည်။ Backup ပြုလုပ်သောအချိန်မှာ Incremental Backup ထက် ပို၍ကြာသည်။

၁၄။ ဒေတာများ Backup ပြုလုပ်ခြင်းနှင့်ပတ်သက်၍ အရေးကြီးသည့်အချက်မှာ သိမ်းဆည်းထားသောဒေတာများအား ပြန်လည်အသုံးပြုနိုင်ခြင်း ရှိ၊ မရှိ စစ်ဆေးခြင်းဖြစ်သည်။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

External Storage Device များ၏ လုံခြုံရေး

၁၅။ ပြင်ပသိုလှောင်ရေးပစ္စည်းများ (External Storage Device) များဖြစ်သည့် External Hard Disk နှင့် Flash Disk တို့ကို လုပ်ငန်းသုံးကွန်ပျူတာများတွင် ချိတ်ဆက်အသုံးပြုခြင်းမှတဆင့် ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်ပွားကာ သတင်းအချက်အလက်များခိုးယူခံရခြင်း၊ ဖျက်ဆီးခံရခြင်းများ ဖြစ်ပေါ်နိုင်သဖြင့် အောက်ပါအချက်များအတိုင်း လိုက်နာရမည်-

(က) External Storage Device များအား ဆိုက်ဘာလုံခြုံရေးအကာအကွယ်ဖြစ်သည့် Antivirus နှင့် Endpoint Security ဆော့ဖ်ဝဲလ်များရှိသည့် ကွန်ပျူတာများတွင်သာ ချိတ်ဆက်အသုံးပြုရမည်။

(ခ) External Storage Device တွင်ပါရှိသော Shortcut Link များနှင့် ပရိုဂရမ်များကို နှိပ်၍ ဖွင့်ကြည့်ခြင်းမျိုး မလုပ်ရ။

(ဂ) အရေးကြီးသောဖိုင်များကို External Storage Device တွင် သိမ်းဆည်းဖူးပါက အခြားသူများသို့ ငှားရမ်းခြင်း၊ ပျောက်ဆုံးခြင်းများ မဖြစ်စေရ။ အရေးကြီးသော ဒေတာများ External Storage Device တွင် ယာယီသိမ်းဆည်းပြီးတိုင်း Device အား Format ပြုလုပ်ရမည်။ Device တွင် အရေးကြီးဒေတာများအား အမြဲတမ်းသိမ်းဆည်း လိုပါက Disk အား Encrypt ပြုလုပ်ပြီး သုံးစွဲရမည်။

(ဃ) ပြပွဲများမှပေးဝေသော (သို့မဟုတ်) ကောက်ယူရရှိသော External Storage Device များကို Malware များ ရှိ၊ မရှိ သေချာစွာ စိစစ်ပြီးမှသာ သုံးစွဲရမည်။

(င) ကွန်ပျူတာတွင် External Storage Device များကို အလိုအလျောက် အလုပ်လုပ်စေ နိုင်သော Autoplay လုပ်ဆောင်ချက်များကို ပိတ်ထားရမည်။

(စ) ရုံးလုပ်ငန်းသုံး Storage Device များနှင့် ကိုယ်ရေးကိုယ်တာသုံး Storage Device များကို ရောနှောမသုံးစွဲဘဲ သီးခြားစီခွဲ၍ အသုံးပြုရမည်။

အင်တာနက်သုံးစွဲမှု လုံခြုံရေး

၁၆။ ဆိုက်ဘာတိုက်ခိုက်ခံရမှုအများစုသည် အင်တာနက်၊ အီးမေးလ်၊ Website နှင့် လူမှုကွန်ရက် များကို မှန်ကန်စွာ အသုံးမပြုသောကြောင့်ဖြစ်သဖြင့် အင်တာနက်သုံးစွဲရာတွင် လုံခြုံစိတ်ချစွာ ရှိရေးအတွက် အောက်ပါအချက်များအား လိုက်နာရမည်-

(က) Update ပြုလုပ်ထားခြင်း မရှိသည့် Web Browser များကို အသုံးမပြုရ။

(ခ) Website များကို ဝင်ရောက်ကြည့်ရှုရာတွင် Secure Socket Layer (SSL) အသုံးပြု ထားသော https:// ဖြင့်စသော Website များကိုသာ ဝင်ရောက်ကြည့်ရှုရမည်။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

(ဂ) Website များသို့ ဝင်ရောက်ရာတွင် မတူညီသောအကောင့်များနှင့် မတူညီသော စကားဝှက်ကိုထားရှိရမည်။

(ဃ) စကားဝှက်များကို Web Browser များတွင် သိမ်းဆည်းခြင်း မပြုရ။ သိမ်းဆည်းလိုလျှင် Password Manager တစ်ခုခုကို သုံးစွဲရမည်။ Web Browser များတွင် မလိုအပ်သော Add-on များ တပ်ဆင်သုံးစွဲခြင်း မပြုရ။

(င) Web ၌ရှာဖွေရာတွင် မိမိ၏ တည်နေရာနှင့် လှုပ်ရှားမှုများကို ခြေရာခံခြင်းမှ ရှောင်ရှားနိုင်ရန်အတွက် Web Browser တွင် Privacy Badger ကဲ့သို့သော Add-on ကို အသုံးပြုရမည်။ မိမိ၏ အွန်လိုင်းတွင်ဆောင်ရွက်ခဲ့သော ဒစ်ဂျစ်တယ်ခြေရာများကို မိမိဆန္ဒမပါဘဲ ဒစ်ဂျစ်တယ်ပလက်ဖောင်းများ၊ Website များက မှတ်တမ်းတင်ခြင်း၊ ခြေရာခံခြင်းများ ဆောင်ရွက်နေသည်ကို သတိပြုပါ။

(စ) ကြော်ငြာများမှတဆင့် အဖျက်အမှောက် Website များသို့ မရောက်သွားစေရေးအတွက် Adware Add-on ကို တပ်ဆင်အသုံးပြုရမည်။

(ဆ) ဆိုရှယ်မီဒီယာ၊ Website များနှင့် အီးမေးလ်များ အသုံးပြုရန် ဝင်ရောက်ရာတွင် Two Factors Authentication (သို့မဟုတ်) Multi-factor Authentication စနစ် အသုံးပြုပါ။

(ဇ) Virtual Private Network (VPN) များအသုံးပြုလျှင် ဆိုက်ဘာတိုက်ခိုက်မှုများအား ခြေရာခံ၍ မရနိုင်သောကြောင့် Public Wifi များတွင် ချိတ်ဆက်အသုံးပြုချိန်မှအပ ရုံးကွန်ရက်အတွင်း အင်တာနက်အသုံးပြုခဲ့ပါက VPN အားချိတ်ဆက်အသုံးမပြုရ။ Global Protect ကဲ့သို့ မိမိ၏ရုံးမှ သုံးစွဲခွင့်ပြုသော VPN များအပ မိမိ၏သဘောဖြင့် Download လုပ်၍ သုံးစွဲနေသော VPN များကို သုံးစွဲခြင်း မပြုရ။ VPN များသည် မိမိနှင့် VPN Service Provider ကြား မသမာသူများမှ ကြားဖြတ်ဖမ်းယူခြင်း မပြုနိုင်အောင် တီထွင်ထားသော ဆော့ဖ်ဝဲလ်များသာဖြစ်ပြီး မိမိ၏လှုပ်ရှားမှုများအားလုံးကို VPN Service Provider များက သိရှိနိုင်သလို အခမဲ့ရရှိသည့် အချို့သော VPN ဆော့ဖ်ဝဲလ်များသည် မိမိ၏ စကားဝှက်များကိုပါ ခိုးယူနိုင်ကြောင်း သတိပြုပါ။

(ဈ) Phishing တိုက်ခိုက်မှုနှင့်အဖျက်အမှောက် Website များ၏ သဘောကို နားလည်ထားရမည်။

Phishing တိုက်ခိုက်မှု

၁၇။ Phishing (လှည့်ဖြားခြင်း) ဆိုသည်မှာ အီလက်ထရွန်းနစ်ဆက်သွယ်မှုနည်းလမ်း (အီးမေးလ်၊ SMS၊ ဖုန်း စသည်) တစ်ခုခုကို အသုံးပြု၍ သုံးစွဲသူများကို လိမ်လည်လှည့်ဖြားခြင်း ဖြစ်ပါသည်။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

Phishing တိုက်ခိုက်မှုများသည် သုံးစွဲသူများ၏ အမည်များ၊ စကားဝှက်များ၊ ခရက်ဒစ်ကဒ်နှင့် ပတ်သက်သော အချက်အလက်များ၊ ကွန်ရက်နှင့်ပတ်သက်သောအချက်အလက်များကဲ့သို့ အရေးကြီးသော၊ လျှို့ဝှက်သော အချက်အလက်များကို ခိုးယူရန် ကြိုးပမ်းပါသည်။ ဖုန်းမှဖြစ်စေ၊ အီးမေးလ်မှဖြစ်စေ တရားဝင်အဖွဲ့အစည်း (သို့မဟုတ်) ပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက် အယောင်ဆောင်၍ အန္တရာယ်ရှိသော Link သို့မဟုတ် ဖိုင်များ နှိပ်စေခြင်း၊ လျှို့ဝှက်သောအချက်အလက်များကို ပြောစေခြင်းများ ပြုလုပ်စေရန် Social Engineering (လူမှုလှည့်ဖြားခြင်း) နည်းလမ်းကို အသုံးပြုကြပါသည်။ ပိုမိုယုံကြည်စိတ်ချရစေရန်အတွက် တိုက်ခိုက်ခံထားရသောအီးမေးလ်အကောင့်များအသုံးပြု၍ဖြစ်စေ၊ Domain Record များ၏ အားနည်းချက်များကို အသုံးပြု၍ဖြစ်စေ အယောင်ဆောင်အီးမေးလ်များမှတစ်ဆင့်လည်း အဖျက်အမှောက်လင့်များ၊ ဖိုင်များကို ပေးပို့နိုင်သည်။ လူတို့၏ လောဘစိတ်၊ သိလိုစိတ်နှင့် စိုးရိမ်ပူပန်စိတ်တို့ကို အခွင့်ကောင်းယူ၍ အီးမေးလ်တွင်ပါဝင်သော Link များနှင့် Attachment ဖိုင်များကို ဖွင့်စေရန်အတွက် ဆွဲဆောင်မှုရှိသော အကြောင်းအရာများ ရေးသားပေးပို့တတ်ကြသည်။

၁၈။ Phishing တိုက်ခိုက်မှုအမျိုးအစားများအား အောက်ပါအတိုင်း ဖြစ်ပါသည်-

(က) **အထူးပစ်မှတ်ထား လှည့်ဖြားခြင်း (Spear Phishing)**။ လူပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက် (သို့မဟုတ်) အဖွဲ့အစည်းတစ်ခုအား ပစ်မှတ်ထားကာ လှည့်ဖြားတိုက်ခိုက်ခြင်း ဖြစ်သည်။

(ခ) **ထိပ်တန်းအရာရှိများကို လှည့်ဖြားခြင်း (Whaling)**။ ငွေကြေးဆိုင်ရာ အထူးလုပ်ပိုင်ခွင့်ရှိသော ထိပ်တန်းအရာရှိကြီးများကို ပစ်မှတ်ထားကာ လှည့်ဖြားတိုက်ခိုက်ခြင်း ဖြစ်သည်။

(ဂ) **SMS မှတစ်ဆင့် လှည့်ဖြားခြင်း (Smishing)**။ SMS များကို အသုံးပြု၍ လိမ်လည်လှည့်ဖြားခြင်း ဖြစ်သည်။

(ဃ) **ဖုန်းဆက်၍ လှည့်ဖြားခြင်း (Vishing)**။ ဖုန်းခေါ်ဆိုမှုများမှတစ်ဆင့် လိမ်လည်လှည့်ဖြားခြင်း ဖြစ်သည်။

အီးမေးလ်လုံခြုံရေး

၁၉။ ဖိုင်များ၊ Link များနှင့်ပတ်သက်၍ ယုံကြည်စိတ်ချရသော ပေးပို့သူထံမှ ပေးပို့လာသော ဖိုင်များကိုသာ ဖွင့်ပါ။ သံသယဖြစ်ဖွယ် အကြောင်းအရာများ၊ မထင်မှတ်ထားသော တောင်းဆိုမှုများ ပါ၊ မပါ သေချာစွာ စစ်ဆေးပါ။ Spam နှင့် Phishing များကို စစ်ထုတ်ပေးသော အီးမေးလ်ဝန်ဆောင်မှုများကို အသုံးပြုပါ။

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

၂၀။ မသင်္ကာဖွယ်အီးမေးလ်ဆိုသည်မှာ အီးမေးလ်တစ်ခုကို မိမိ မသိရှိသော သူစိမ်းတစ်ယောက်ထံမှ လက်ခံရရှိခြင်း၊ အီးမေးလ်ကို မည်သည့်အကြောင်းကြောင့် လက်ခံရရှိသည်ကို မသိရှိခြင်း၊ အီးမေးလ်တွင် Link များ/Attachment ဖိုင်များ (အထူးသဖြင့် ZIP ဖိုင်များနှင့် ၎င်းဖိုင်ထဲတွင် .exe ဖိုင်များနှင့် .lnk ဖိုင်များ ပါရှိခြင်း)၊ အမည်မသိ Domain များ အသုံးပြု၍ ပေးပို့ခြင်း၊ Attachment ဖိုင်အမည်များတွင် ဖတ်၍မရသော စာလုံးများပါရှိခြင်း တို့ဖြစ်သည်။ မသင်္ကာဖွယ်အီးမေးလ်အား လက်ခံရရှိပါက အောက်ပါအတိုင်း လိုက်နာသင့်ပါသည်-

(က) အီးမေးလ်အား အခြားသူထံသို့ ပေးပို့ခြင်းအား ရှောင်ကြဉ်ခြင်း၊

(ခ) အီးမေးလ်အား Forensics ပြုလုပ်နိုင်ရန်အတွက် ဖျက်ပစ်ခြင်းမှ ရှောင်ကြဉ်ခြင်း၊

(ဂ) အီးမေးလ်ပေးပို့သူအား သိရှိပါက ၎င်းပုဂ္ဂိုလ်မှ အီးမေးလ်ပေးပို့ခြင်း ဟုတ်၊ မဟုတ် မေးမြန်းခြင်း၊

(ဃ) အီးမေးလ်တွင် ပါဝင်သော Attachment အား သက်သေထိန်းသိမ်းနိုင်ရန်အတွက် Antivirus များဖြင့် စစ်ဆေးခြင်းမှ ရှောင်ကြဉ်ခြင်း၊

(င) အီးမေးလ်အား Download လုပ်၍ Text Editor တစ်ခုခုဖြင့်ဖွင့်ကာ ပေးပို့သော Domain အား စစ်ဆေးခြင်း။

စက်ပစ္စည်းများကို ကာကွယ်ခြင်း

၂၁။ စက်ပစ္စည်းလုံခြုံရေးအတွက် ကွန်ပျူတာများ အသုံးမပြုချိန်တွင် Screen ကို Lock ချထားခြင်းသည် မသမာသူများမှ မိမိ၏ စက်ပစ္စည်းများကိုင်တွယ်ခြင်းမှ ကာကွယ်နိုင်ပါသည်။ ကွန်ပျူတာများ ပျောက်ဆုံးသည့်အခါ အရေးကြီးသည့် အချက်အလက်များ ခိုးယူခြင်း ခံနေရသဖြင့် “Find My Device”၊ “Remote Wipe” စသော လုပ်ဆောင်ချက်များကို အသုံးပြုသင့်ပါသည်။ သို့သော် ခိုးယူသူမှ OS (Linux/Windows) အသစ်ကို အသုံးပြုချိန်၌ အဆိုပါ လုပ်ဆောင်ချက်များ အလုပ်လုပ်မည် မဟုတ်ပါ။ ကွန်ပျူတာများတွင်မူ Disk Encryption လုပ်ဆောင်ချက်ဖြစ်သော “BitLocker” ကို အသုံးပြုခြင်းဖြင့် အချက်အလက် ခိုးယူခြင်းမှ ကာကွယ်နိုင်ပါသည်။ Firewall ဆော့ဖ်ဝဲလ်များကို အသုံးပြုခြင်းဖြင့် ခွင့်ပြုချက်မရှိဘဲ မိမိ၏စက်ပစ္စည်းကို ရယူသုံးစွဲရန် ကြိုးပမ်းနေသော ကွန်ပျူတာများကို သိရှိနိုင်သလို ၎င်းတို့၏ရန်ကိုလည်း ကာကွယ်နိုင်ပါသည်။

လူမှုကွန်ရက်ကို သတိပြုသုံးစွဲခြင်း

၂၂။ လူမှုကွန်ရက်အများစုသည် မိမိ၏ ပို့စ်များကို မည်သူအား ပေးမြင်စေမည်၊ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို မည်သူ့အား ပြသမည်၊ မည်သူ့ထံ ရယူသုံးစွဲခွင့်ပေးမည် စသည့် အချက်များကို ချိန်ညှိနိုင်ရန်အတွက် Setting များထားရှိပါသည်။ အဆိုပါ Setting များကို ပုံမှန် စစ်ဆေးသုံးသပ်ရန် လိုအပ်ပါသည်။ အိမ်လိပ်စာများ၊ ဖုန်းနံပါတ်များ၊ အလုပ်ခွင်၊ မွေးနေ့ စသည့်

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

အချက်အလက်များသည် မသမာသူထံ ရောက်သွားပါက ထိုအချက်အလက်များကို အလွဲအသုံးပြုနိုင်ပါသည်။ မိမိအား အွန်လိုင်းတွင် “Firend Request” လုပ်သူနှင့် “Follow” လုပ်သူတိုင်းတို့သည် ကောင်းသောရည်ရွယ်ချက်ဖြင့် ဟုတ်ချင်မှ ဟုတ်ပါလိမ့်မည်။ အချို့သည် ပရိုဖိုင်အတုများ၊ Bot များ (အထူးသဖြင့် Twitter)နှင့် မကောင်းကြံလိုသော ပုဂ္ဂိုလ်များလည်း ဖြစ်နိုင်ပါသည်။ ပထဝီအနေအထားနှင့်ပတ်သက်သော အချက်အလက်များ (Geotag) အား ဝေမျှခြင်းကို ရှောင်ကြဉ်ရမည်။ အွန်လိုင်းတွင် မိမိတင်သမျှ ပို့စ်များနှင့် ဓာတ်ပုံများသည် မိမိ၏ဒစ်ဂျစ်တယ်မှတ်တမ်းများ ဖြစ်ပါသည်။ ဒေတာများကို ဖျက်ခဲ့လျှင်ပင် အခြားသောသူများက Screenshot ရိုက်ခြင်း၊ အွန်လိုင်းတွင် Cache အနေဖြင့်၊ Web Archive အနေဖြင့် ကျန်ရှိနိုင်ကြောင်း သတိပြုပါ။

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာပေးသင်တန်းပို့ချခြင်း

၂၃။ ဝန်ထမ်းများအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အသိပညာပေးသင်တန်းများ ဖွင့်လှစ်ပို့ချနိုင်ခြင်းဖြင့် သတင်းအချက်အလက်များ ဖျက်ဆီးခံရမှု၊ ခိုးယူခံရမှုနှင့် ပေါက်ကြားမှုများ လျော့ပါးစေရန်အတွက် ဝန်ထမ်းများက မိမိတို့တွင် တာဝန်ရှိကြောင်း နားလည်စေခြင်း၊ ကွန်ရက်မှတဆင့်ဖြစ်စေ၊ Web Browser များမှတဆင့်ဖြစ်စေ၊ အီးမေးလ်မှတဆင့်ဖြစ်စေ ဖြစ်ပွားသော ဆိုက်ဘာတိုက်ခိုက်မှုများကို နားလည်စေခြင်း၊ Social Engineering နည်းလမ်းနှင့် Phishing နည်းလမ်းများမှတစ်ဆင့် လှည့်ဖြားတိုက်ခိုက်မှုများကို နားလည်စေခြင်း၊ စက်ပစ္စည်းလုံခြုံရေး၏ အရေးပါမှုကို နားလည်စေခြင်း၊ ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်ပွားပါက တုံ့ပြန်လုပ်ဆောင်ရမည့် အစီအစဉ်များကို နားလည်စေခြင်း စသည့်အကျိုးကျေးဇူးများကို ရရှိစေသည့်အတွက် ဝန်ထမ်းတိုင်းအား ဆိုက်ဘာလုံခြုံရေး အသိပညာပေးသင်တန်းကို နှစ်စဉ် ပို့ချပေးသွားရမည်။

နိဂုံး

၂၄။ ဖော်ပြပါ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံလုပ်ထုံးလုပ်နည်းများကို လိုက်နာကျင့်သုံးခြင်းဖြင့် သက်ဆိုင်ရာ ပြည်ထောင်စုအစိုးရအဖွဲ့အစည်းများနှင့် ဝန်ကြီးဌာနများအသီးသီးရှိ လုပ်ငန်းသုံးကွန်ပျူတာများအား ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများမှ ကာကွယ်လျော့ချနိုင်ပြီး အရေးကြီးသော သတင်းအချက်အလက်များအား လုံခြုံစိတ်ချစွာ အသုံးပြုနိုင်မည်ဖြစ်သည်။ ထို့ပြင် သတင်းအချက်အလက်နည်းပညာအခြေခံသည့် e-Government လုပ်ငန်းစဉ်များအား အရှိန်အဟုန်မြှင့်အကောင်အထည်ဖော်ဆောင်ရွက်ရာ၌ ပြည်ထောင်စုအစိုးရအဖွဲ့အစည်းများနှင့် ဝန်ကြီးဌာနအသီးသီးတွင် ကွန်ပျူတာလုံခြုံရေးဆိုင်ရာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ (Computer Security Incident Response Team - CSIRT) များဖွဲ့စည်းပြီး ဆိုက်ဘာတိုက်ခိုက်မှုများဖြစ်ပေါ်လာပါက အချိန်နှင့်တပြေးညီ တုံ့ပြန်ဆောင်ရွက်ခြင်း၊ မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ (mmCERT/cc) ထံ သတင်းပို့တိုင်ကြားခြင်း၊ ဆိုက်ဘာတိုက်ခိုက်မှု သတင်းအချက်အလက်များမျှဝေခြင်းနှင့် ဆိုက်ဘာတိုက်ခိုက်မှုများကို ပူးပေါင်းကိုင်တွယ်ဖြေရှင်းခြင်းများ ပြုလုပ်ဆောင်ရွက်

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc

ခြင်းဖြင့် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုကြောင့် ဆုံးရှုံးနစ်နာရမှုများလည်း လျော့ပါးစေနိုင်မည်ဖြစ်ပါသည်။

မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့

ကိုးကားစာရင်း

၁။ Physical Security Policy (EC-Council - Certified Network Defender)

၂။ Host Security (EC-Council - Certified Network Defender)

၃။ Data Backup Policy (EC-Council - Certified Network Defender)

၄။ Personal Device Usage Policy (EC-Council - Certified Network Defender)

၅။ Software and Application Policy (EC-Council - Certified Network Defender)

၆။ Software Installation Policy (Sans Institute)

၇။ Password Construction Guidlines (Sans Institute)

၈။ Password Protection Policy (Sans Institute)

၉။ အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့်အချက်များ (Version 1.0) - mmCERT/cc

Copyright © Oct 28 2023, Myanmar Computer Emergency Response Team, mmCERT/cc