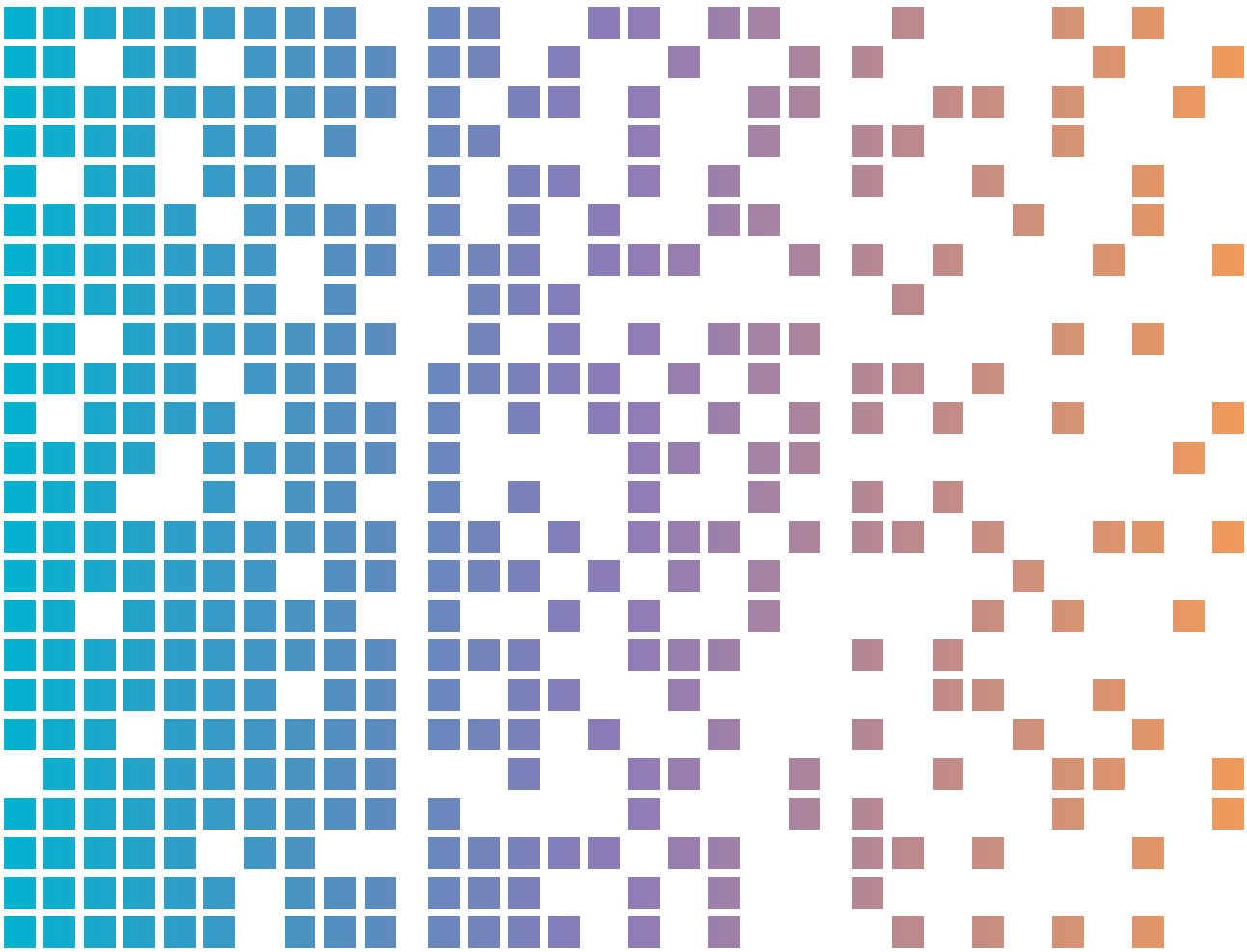
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

တိတ်တဆိတ်ခိုးယူခြင်း - ဆိုင်ဘာရာဇာဝတ်သားများသည် အချက်အလက်ခိုးယူသည့် မသမာသော malware များကို အသုံးပြုကာ လုပ်ငန်းဆိုင်ရာ ကွန်ရက်များကို တိုက်ခိုက်မှုများ လုပ်ပါသည်။



အကြောင်းအရာ ရှုပ်ထွေးမှု
အတန်အသင့်

မာတိကာ

စကားစပ်

အချက်အလက်များ ခိုးယူသည့် မသမာသော malware များသည် ယုံကြည်ရသည့် အသုံးပြုသူ၏ အထောက်အထားများနှင့် စနစ်၏ အချက်အလက်များကို ခိုးယူပြီး ဆိုင်ဘာရာဇာဝတ်သားများ အနေဖြင့် အလွဲသုံးစားလုပ်ရန်နှင့် အများအားဖြင့် ငွေရေးကြေးရေး အကျိုးအမြတ် ရရှိရန်အတွက် အသုံးပြုသည့် ဆော့ဖ်ဝဲ ဖြစ်ပါသည်။ ဤစတြေးလျအပါအဝင် ကမ္ဘာတဝှမ်းမှ အဖွဲ့အစည်းတချို့နှင့် ကဏ္ဍစုံအား တိုက်ခိုက်ရာတွင် အချက်အလက်ခိုးယူသည့် ဆော့ဖ်ဝဲများ အသုံးပြုထားကြောင်း တွေ့ရှိထားပါသည်။ ဤစာစောင်သည် စာဖတ်သူများအတွက် အချက်အလက်ခိုးယူသည့် malware နှင့် ပတ်သက်သော ဆိုင်ဘာလုံခြုံရေးဆိုင်ရာ လမ်းညွှန်ချက်များ ပါဝင်သကဲ့သို့ အဖွဲ့အစည်းများနှင့် ၎င်းတို့၏ အမှုထမ်းများအတွက် ထိခြိမ်းခြောက်မှု၏ လှုပ်ရှားမှုနှင့် အန္တရာယ်လျှော့ချနိုင်ရေးအတွက် လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။

အဓိက ပို့ဝိုင့်များ

- အချက်အလက်များခိုးယူသည့် malware ကို info stealer ဟုလည်း ခေါ်ပြီး ၎င်းသည် တိုက်ခိုက်ခံရသူ၏ စက်ပစ္စည်းမှ အချက်အလက်များကို ခိုးယူရန်အတွက် လုပ်ဆောင်ထားသည့် malware ဖြစ်ပါသည်။ ထိုအထဲတွင် အကောင့်၏ နာမည်များ၊ လျှို့ဝှက်ကုဒ် password များ၊ ခရက်ဒစ်ကဒ် အချက်အလက်များ၊ cryptocurrency wallet များ၊ ဖိုင်များနှင့် cookies၊ user history နှင့် ဖောင်ကို အလိုအလျောက်ဖြည့်ပေးသည့် အချက်အလက်များ စသည့် browser အချက်အလက်များကို ခိုးယူနိုင်ပါသည်။
- ဆိုင်ဘာရာဇာဝတ်သားများသည် အခိုး ခံရသော လုပ်ငန်းအကောင့်များနှင့် ဆက်စပ်မှုရှိသော user credentials ကို ဝယ်ယူပြီး ထိုအချက်များကို အသုံးပြုကာ တိုက်ခိုက်ခံရသူ၏ လုပ်ငန်းရှင် စက်ပစ္စည်းထဲသို့ ကနဦးဝင်ရောက်ချက်များ ပြုလုပ်ခြင်းအပြင် ၎င်းလုပ်ငန်းနှင့် ဆက်စပ်သည့်သူများ နှင့် စီးပွားရေးလုပ်ငန်း၏ စနစ်များထဲသို့ ဝင်ရောက်နိုင်ပါသည်။ ထိုကဲ့သို့ တိုက်ခိုက်ခံရသည့် အဖွဲ့အစည်းများအတွက် ဆက်စပ်သည့် နောက်ဆက်တွဲ သက်ရောက်မှုထဲတွင် ငွေညှစ်တောင်းခံသည့် ဆော့ဖ်ဝဲများ၊ ခြိမ်းခြောက်၍ ငွေညှစ်ခြင်းနှင့် လုပ်ငန်းသုံး အီးမေးလ်များ ချိုးဖောက်ခံရခြင်းအပြင် မူပိုင်ခွင့်ရှိသည့် အရာများ အခိုးခံရနိုင်ခြင်းတို့ ပါဝင်ပါသည်။
- ဆက်သွယ်ညှိနှိုင်းရေးမှူးရုံး၏ ဩစတြေးလျ ဆိုင်ဘာလုံခြုံရေးစင်တာ (ASD's ACSC) အနေဖြင့် တွေ့ရှိရသည်မှာ တိုက်ခိုက်မှု ခံရသည့် ကိုယ်ပိုင် စက်ပစ္စည်းကို အသုံးပြုကာ လုပ်ငန်း၏ အရင်းအမြစ်ကို ရယူသည့် အမှုထမ်း များကြောင့် လုပ်ငန်း၏ ကွန်ရက် ချိုးဖောက်တိုက်ခိုက်ခံရမှု ဖြစ်ပေါ်ခဲ့ကြောင်း တွေ့ရှိရပါသည်။ တစ်ခုတည်းမကသော အနေအထားတွင် တွေ့ရသည်မှာ ဆိုင်ဘာ ရာဇာဝတ်သားများသည် အခိုး ခံရသည့် တရားဝင် user credential များကို အသုံးပြုကာ လုပ်ငန်း၏ ကွန်ရက်ထဲ ကနဦး ဝင်ရောက်ခွင့် ရရှိကြောင်း တွေ့ရှိရပါသည်။ အဆင့်မြင့်သော user အကောင့်များကို ဆိုင်ဘာရာဇာဝတ်သားများ ရရှိသည့်အခါတွင် တိုက်ခိုက်ချိုးဖောက်ခံရမှု အတိုင်းအတာ ပိုမိုကြီးမားကြောင်းလည်း စုံစမ်းစစ်ဆေးမှုအရ တွေ့ရပါသည်။
- အမှုထမ်းများ၊ contractor များ၊ service provider သို့မဟုတ် လုပ်ငန်းများကို မိမိ၏ ကွန်ရက်အား အဝေးမှ ဝင်ခွင့်ပြုသည့် အဖွဲ့အစည်းများအနေဖြင့် - Bring Your Own Device (BYOD) hardware အပါအဝင်- အချက်အလက်ခိုးယူနိုင်မှုကို သတိပြုပြီး ၎င်းတို့၏ ရန်မှ မိမိကိုယ်ကို ကာကွယ်မှုလုပ်ရန် စဉ်းစားသင့် ပါသည်။ ဆိုင်ဘာရာဇ ဝတ်သားများသည် အချက်အလက်ခိုးယူသည့် ဆော့ဖ်ဝဲများ အသုံးပြုကာ နည်းလမ်းပေါင်းစုံဖြင့် တိုက်ခိုက်ခံရသူ၏ စက်ပစ္စည်းထဲ ဝင်ရောက်ရန်ကြိုးစားပြီး ထိုအထဲတွင် မှန်ကန်သည့်အရာကဲ့သို့ ဟန်ဆောင်သည့် phishing အီးမေးလ်များ၊ pirated software download များ၊ search engine optimisation (SEO) နည်းလမ်းများ၊ မသမာသည့် ကြော်ငြာများ သို့မဟုတ် မသမာသည့် လင့်ခ်များကို ဆိုရှယ်မီဒီယာ ပလက်ဖောင်းများပေါ်တွင် တင်ထားခြင်းတို့ ပါဝင်ပါသည်။ အထွေထွေအားဖြင့် အသုံးပြုသူ၏ အပြုအမူနှင့် လုံခြုံရေးထိန်းချုပ်မှု အားနည်းခြင်းတို့ကြောင့် အလုပ်အတွက်သာမက ကိုယ်ရေးကိုယ်တာအတွက် အသုံးပြုသည့် စက်ပစ္စည်းများသည် ထိုနည်းလမ်းဖြင့် တိုက်ခိုက်ခံရနိုင်ခြေ များပါသည်။
- အချက်အလက်ခိုးယူသည့် ဆော့ဝဲသည် ဆိုင်ဘာ ရာဇဝတ်သားများ ဆိုင်ဘာတိုက်ခိုက်မှုလုပ်ပြီး ငွေရေးကြေးရေး အမြတ်များစေမည့် မျက်စိကျလောက်သည့် ပုံစံကို လုပ်ပေးလေ့ရှိပြီး အထူးသဖြင့် သက်တမ်းနည်းသည့် ဆိုင်ဘာ ရာဇဝတ်သားများနှင့် နည်းပညာအကန့်အသတ် ရှိသူများအတွက် လုပ်ဆောင်ပေးထားပါသည်။ တချို့ဆိုင်ဘာရာဇာဝတ်သားများသည် အချက်အလက်ခိုးယူသည့် ပစ္စည်းများကို Malware-as-a-Service (MaaS) စတိုင် အစီအစဉ်များအဖြစ် ရောင်းချပြီး ထိုပစ္စည်းများအတွက် အသုံးပြုခကို လစဉ်ကြေးတောင်းခံမှု လုပ်ပါသည်။

နောက်ခံအကြောင်း

အချက်အလက်များ ခိုးယူသည့်စက်ပစ္စည်းများကို ဆိုင်ဘာရာဇဝတ်သားများ အသုံးပြုခြင်းသည် ဩစတြေးလျအတွင်းမှ အဖွဲ့အစည်းများ၏ လုံခြုံရေးနှင့် ကောင်းမွန်စွာတည်ရှိရေးအတွက် ခြိမ်းခြောက်မှု တစ်ခု ဖြစ်ပါသည်။ အချက်အလက်များ ခိုးယူမှုသည် ဆိုင်ဘာလုံခြုံရေး ချိုးဖောက်မှု ကြီးကြီးမားမား မဖြင်ခင် ဖြစ်တတ်သည့် လူပ်ရှားမှုများဖြစ်ပြီး ၎င်းတို့ကို ဆိုင်ဘာရာဇဝတ်သားများက တရားဝင် ဝင်ရောက်ခွင့်ရသည့် user credential များ စုဆောင်းရေးအတွက် အသုံးပြုခြင်း ဖြစ်ပါသည်။ ထို user credential များသည် လုပ်ငန်း၏ စနစ်များနှင့် ဒေတာများထဲ ကနဦးဝင်ရောက်ပြီး အလွဲသုံးစားမှုများ လုပ်ပါသည်၊ အထူးသဖြင့် အင်တာနက်ဖြင့် အဝေးမှ ဝန်ဆောင်မှုပေးခြင်းနှင့် အဆင့်မြင့်သော အရာများ အတွက် ဝင်ရောက်ခွင့်ရှိသည့် previlegedအကောင့်များထဲ ဝင်ရောက်ခြင်း ဖြစ်ပါသည်။

သတိပြုရန် - ရာဇဝတ်သားများအနေဖြင့် အခိုးခံရသည့် user credential အစစ်များကို ဝယ်ယူနိုင်ရန်အတွက် ကနဦးဝင်ရောက်နိုင်အောင် လုပ်ဆောင်ပေးသည့် ကြားနေပွဲစားများသည် ဆိုင်ဘာရာဇဝတ်မှု ဂေဟစနစ်တွင် အထူး ကဏ္ဍတွင် ပါဝင်ပါသည်။ ၎င်းပွဲစားများသည် ရာဇဝတ်သားများ မျက်စိကျလောက်သည့် အရည်အသွေး ကောင်းသည့် လုပ်ငန်းသုံး user credential များကို လေလံတင်ရောင်းချလေ့ရှိပြီး ဆိုင်ဘာ ရာဇဝတ်သားများက ထိုအချက်အလက်များကို ဝယ်ယူကာ အဖွဲ့အစည်းများ၏ ကွန်ရက်ထဲသို့ ဝင်ရောက်ပြီး အလွဲသုံးစားမှုများ လုပ်ရန်အတွက် အသုံးပြုလေ့ရှိသည်။

အခိုးခံရသည့် user credential အစစ်အမှန်များသည် ဆိုင်ဘာရာဇဝတ်သားများအတွက် အင်မတန် အဖိုးတန်ပြီး အကြောင်းရင်းမှာ ထိုအချက်များဖြင့် လုပ်ငန်းများ၏ ကွန်ရက်များနှင့် စနစ်ထဲသို့ ကနဦးဝင်ရောက်ခွင့် ရရှိစေသည့်အတွက် ဖြစ်ပါသည်။ အခိုးခံရသည့် user credential အစစ်များကို အသုံးပြုသည့် အခါ ဆိုင်ဘာရာဇဝတ်သားများအနေဖြင့် သာမာန် နည်းဗျူဟာနှင့် နည်းပညာများကို အဆင့်ကျော်လုပ်နိုင်ပြီး ထိုအထဲတွင် -

- ပစ်မှတ်ကို မှတ်သားခြင်းနှင့် ပစ်မှတ်ထားသည့်အရာကို လေ့လာနိုင်ခြင်း
- ပစ်မှတ်ထားသည့် ကွန်ရက်၏ အားနည်းချက်များကို တစ်စခြင်းစီ ဖယ်ထုတ်နိုင်ခြင်း
- ကနဦးဝင်ရောက်သည့်အဆင့်တွင် ၎င်းလုပ်ငန်းများကို လုပ်ကိုင်ပေးမည့် vector များကို တိုးချဲ့နိုင်ပြီး ထိုအထဲတွင် -
  - phishing အစစ်ကဲ့သို့ ဟန်ဆောင်ထားသည့်အရာများ
  - ဆော့ဖ်ဝဲ၏ အားနည်းချက်များကို အလွဲသုံးစားလုပ်ခြင်း
  - RemoteDesktop Protocol (RDP) သို့မဟုတ် virtual privatenetwork (VPN) ဝန်ဆောင်မှုကဲ့သို့ အဝေးမှ လုပ်ဆောင်နိုင်သည့် ဝန်ဆောင်မှုများကို ပစ်မှတ်ထားခြင်း
  - (လျှို့ဝှက်ကုဒ် password ကို ခန့်မှန်းခြင်း) user credential များ ရရှိရေးအတွက် အတင်းအဓမ္မနည်းဖြင့် တိုက်ခိုက်မှု လုပ်ဆောင်ခြင်းတို့ ပါဝင်ပါသည်။

ထိုကဲ့သို့ တစ်ဆင့်ခြင်းလုပ်ဆောင်ရာတွင် အချိန်၏ ရင်းနှီးမြှုပ်နှံမှုနှင့် နည်းပညာစွမ်းရည်များ လိုအပ်သည့်အတွက် တချို့ ဆိုင်ဘာရာဇဝတ်သားများအတွက် မဟန့်အတား ဖြစ်စေနိုင်ပါသည်။ အထူးသဖြင့် လုပ်ငန်း၏ ကွန်ရက်လုံခြုံရေးကို မထိုးဖောက်နိုင်သည့် ဆိုင်ဘာရာဇဝတ်သားများအတွက် အချက်အလက်ခိုးယူသည့် ကူးစက်မှုနည်းလမ်းက အကျိုးရှိနိုင်ပြီး ထိုကူးစက်မှုများသည် မသမာသူများ လိုချင်နေသည့် လုပ်ငန်းကွန်ရက်၏ user credential များကို လျင်မြင်စွာနှင့် အလွယ်တကူ ရရှိစေနိုင်သည့်အတွက် ဖြစ်ပါသည်။

အဝေးမှ အလုပ်လုပ်ကိုင်သည့်အခါ တချို့အမှုထမ်းများသည် ကိုယ်ရေးကိုယ်တာအတွက်သာမက အလုပ်အတွက်ပါ ကိုယ်ပိုင် စက်ပစ္စည်းဖြင့် အင်တာနက် browser များကို အသုံးပြုတတ်ပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ရာတွင် အမှုထမ်းများသည် ၎င်းတို့အသုံးပြုသည့် user credential များကို web browsersတွင် လျှို့ဝှက်ကုဒ် password သိုလှောင်ထားခြင်း သို့မဟုတ် တိုးချဲ့ခြင်းများ သို့မဟုတ် web browser ၏ အလိုအလျောက်ဖောင်ဖြည့်ပေးခြင်းမျိုးကို အသုံးပြုနိုင်ပါသည်။ အချက်အလက်ခိုးယူမှုသည် web browser တွင် သိမ်းထားသည့် password များ၊ authentication cookies နှင့် အခြား ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို ပစ်မှတ်ထားနိုင်ပါသည်။

လုပ်ငန်းသုံး စက်ပစ္စည်းမဟုတ်သည့် ကိုယ်ပိုင် စက်ပစ္စည်းများတွင် လုပ်ငန်းတွင် အသုံးပြုသည့် လုံခြုံရေးမူဝါဒများမရှိသည့်အတွက် ထိုကိုယ်ပိုင် စက်ပစ္စည်းများသည် အဖွဲ့အစည်းအတွက် လုံခြုံရေး အန္တရာယ်များ ဖြစ်စေနိုင်ပါသည်။ ဥပမာ အမှုထမ်းများသည် တရားဝင် ဆော့ဖ်ဝဲများကို ဒေါင်းလုဒ်လုပ်ခြင်းနှင့် အန္တရာယ်ဖြစ်နိုင်ခြေများသည့် ဆိုက်ထဲ ဝင်ကြည့်ခြင်းများ ပြုလုပ်ပါက ဆိုင်ဘာတိုက်ခိုက်မှုရန်နှင့် malware ကူးစက်မှုများ ဖြစ်နိုင်ခြေပိုများနိုင်ပါသည်။

ငွေရေးကြေးရေး အမြတ်အစွန်းအတွက် အချက်အလက်ခိုးယူသည့် malware များ၊ ဖြန့်ဖြူးသူများနှင့် ကနဦးဝင်ရောက်ချက်ကို ရောင်းစားသည့် ပွဲစားများနှင့် ransomware တို့၏ ပူးပေါင်းမှုသည် ဆိုင်ဘာရာဇဝတ်မှု ဂေဟစနစ်တွင် အဓိက အစိတ်အပိုင်းတွင် ပါဝင်ပါသည်။ ဆိုင်ဘာရာဇဝတ်သားများ ပစ်မှတ်ထားသ ည့် တိုက်ခိုက်မှု အဆင့်ဆင့်တွင် အထူးပြုမှုနှင့် စွမ်းရည်များ ပိုမို တိုးတက်လာသည်နှင့်အမျှ ဆိုင်ဘာရာဇဝတ် ဂေဟစနစ်လည်း ပိုမို ထိရောက်စွာ လုပ်ကိုင်နိုင်မှု ရှိလာပြီး ထိုစွမ်းရည်များကို အခြား ရာဇဝတ်သားအတွက် ဝန်ဆောင်မှုကဲ့သို့ ရောင်းချမှု လုပ်ပါသည်။

ခြိမ်းခြောက်ခြင်းဆိုင်ရာ လုပ်ရှားမှု

ASD ၏ ACSC သည် ကမ္ဘာတလွှားတွင် ပိုမိုဖြစ်ပေါ်လာနေသည့် အချက်အလက်ခိုးယူခြင်း လှုပ်ရှားမှုများကို ခြေရာခံခြင်းနှင့် စောင့်ကြည့်မှုများ ပြုလုပ်နေပြီး ထိုကဲ့သို့ အချက်အလက်ခိုးယူခြင်းများသည် ဩစတြေးလျအတွက်လည်း ခြိမ်းခြောက်မှုတစ်ခု ဖြစ်ပါသည်။ ကဏ္ဍဆိုင်ရာ အစီရင်ခံစာတွင် ဖော်ပြချက်အရ ၂၀၂၃ ခုနှစ်အတွင်း ဆိုင်ဘာရာဇဝတ်မှု မျိုးစုံ ရှိသည့်ကြားထဲ အချက်အလက်ခိုးယူသည့်နည်းသည် ပေါ်ပြူလာ အဖြစ်ဆုံးဖြစ်ကြောင်း ဖော်ပြထားပါသည်။ တရားမဝင် dark web စျေးကွက်တွင် အခိုးခံရသည့် ဒေတာအချက်အလက်များစွာကို ရောင်းချခြင်းနှင့် ကနဦးဝင်ရောက်ခြင်းဆိုင်ရာ ပွဲစားများ၏ လုပ်ရပ်က ထိုကဲ့သို့ လုပ်ရပ်ကို ပိုမို အရှိန်မြင့်စေသည်ကို တွေ့ရပြီး ၂၀၂၄ ခုနှစ်အထိ အရှိန်ကောင်းစွာ ဖြစ်ပေါ်ဆဲ ဖြစ်ပါသည်။

အချက်အလက်များ ခိုးယူသည့် ဂေဟစနစ်

အဆင့် ၁ - မသမာသည့် malware ကို ရယူခြင်း

အချက်အလက်ခိုးယူသည့် ဆော့ဖ်ဝဲများသည် ဆိုင်ဘာရာဇဝတ်သားများ၏ စျေးကွက်တွင် MaaS သို့မဟုတ် Stealer-as-a-Service ကဲ့သို့ ရောင်းချခြင်း သို့မဟုတ် အရင်းအမြစ်ကုဒ်များအဖြစ် ရောင်းချခြင်းများ ပြုလုပ်ကြပါသည်။ MaaS ဆိုသည်မှာ malware ထုတ်လုပ်သူများမှ ၎င်းတို့၏ မသမာသည့် ဆော့ဖ်ဝဲများကို အသုံးပြုရန် ဝယ်ယူသည့် လူတစ်ဦးတစ်ယောက်ခြင်းစီအား web-based ပလက်ဖောင်းမှတဆင့် ရောင်းချပေးသည့် စီးပွားရေး ပုံစံဖြစ်ပြီး Software-as-a-Service ရောင်းချမှုနှင့် ဆင်တူပါသည်။ ဤ MaaS ပုံစံသည် လူအများအား ဆိုင်ဘာရာဇဝတ်သား ဖြစ်လာရန် ပိုမိုလွယ်ကူစေပြီး အကြောင်းရင်းမှာ ထိုကဲ့သို့သော မသမာသည့် malware များကို ဖြန့်ဝေရန်နှင့် အချက်အလက်များ ခိုးယူပြီး ဆိုင်ဘာတိုက်ခိုက်မှုများ လုပ်ရန်အတွက် နည်းပညာအရည်အချင်း များများစားစား မလိုအပ်အောင် လုပ်ဆောင်ပေးနိုင်သည့်အတွက် ဖြစ်ပါသည်။

MaaS ကဲ့သို့ ဝန်ဆောင်မှုပေးသည့် အချက်အလက်ခိုးယူသည့် ဆော့ဖ်ဝဲများကို ကြော်ငြာသည့်အခါတွင်း ၎င်းကို အသုံးပြုရန် အတွက် လစဉ်ကြေးမှာ မြင့်မားလေ့ရှိပြီး ၎င်းဝန်ဆောင်မှုကို ဝယ်ယူသည့် ဆိုင်ဘာရာဇဝတ်သားများကို အချက်အလက်ခိုးယူနိုင်သည့် dashboard ထဲ ဝင်ရောက်ခွင့်ပေးပါသည်။ ထို dashboard တွင် အချက်အလက်ခိုးယူသည့် malware ကို ဖန်တီးခြင်း၊ အခိုးခံရသည့် ဒေတာအချက်အလက်များကို စီမံစုစည်းကာ တိုက်ခိုက်ခံ ရသ ည့် စနစ်များ၏ အရည်အတွက်ကို ခြေရာခံခြင်းများလုပ်ဆောင်ပေးပါသည်။ MaaS ဝန်ဆောင်မှုပေးသူများသည် updates များ လုပ်ဆောင်ပေးပြီး ၎င်းတို့၏ ဝန်ဆောင်မှုကို ဝယ်ယူအသုံးပြုသူတို့၏ မသမာသည့် လုပ်ရပ်အား antivirus ဆော့ဖ်ဝဲများမှ ဖမ်းယူရမိခြင်းမျိုး မဖြစ်အောင် လုပ်ဆောင်ပေးသည့် ပစ္စည်းများနှင့် နည်းပညာများ အသုံးပြုကာ ၎င်းတို့၏ ဝန်ဆောင်မှုကို ရယူသူများပြားလာရန်နှင့် ရေရှည်အသုံးပြုရန်အတွက် လုပ်ဆောင်ပေးလျက် ရှိပါသည်။ အချက်အလက် ခိုးယူသည့် ဆော့ဖ်ဝဲ အများစုသည် ၎င်းတို့တိုက်ခိုက်သည့် စက်ပစ္စည်းအတွင်းမှ အချက်အလက်များကို ခိုးထုတ်ပြီးသည်နှင့် တပြိုင်နက် မိမိကိုယ်ကို မိမိ delete လုပ်နိုင်စွမ်းလည်း ရှိပါသည်။

အဆင့် ၂ - မျှဝေဖြန့်ဖြူးခြင်း

အချက်အလက်များခိုးယူသည့် ဆော့ဖ်ဝဲနှင့် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းများ၏ အချက်အလက်များကို စုဆောင်းသည့် ဆိုင်ဘာရာဇဝတ်သားများကို "Traffers" (အချက်အလက်စီးဆင်းမှုကို ဖြန့်ဝေသူ) ဟု ခေါ်ပါသည်။ Traffers များသည် အသုံးပြုသူများအား မသမာသည့် လင့်ခ်များကို နှိပ်မိအောင် လမ်းညွှန်ဖျားယောင်းမှု၊ အချက်အလက်ခိုးယူမှုကို ကျယ်ကျယ်ပြန့်ပြန့် ဖြစ်အောင် လုပ်ဆောင်ပေးပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ရာတွေ့ လူရွေးပြီး လုပ်ဆောင်ခြင်း မဟုတ်ပဲ အခွင့်အလမ်းအပေါ် မူတည်ပြီး မသမာသည့် ဆော့ဖ်ဝဲများကို ကူးစက်မှုများအောင် လုပ်ဆောင်လိုက်ခြင်း ဖြစ်ပါသည်။ သို့သော် ထိုကဲ့သို့ လုပ်ရပ်များသည် တချို့ ကဏ္ဍကို ပစ်မှတ်ထားလုပ်ဆောင်ခြင်းပါဝင်ပြီး ၎င်းတို့ ပစ်မှတ်ထားသည့် အုပ်စုကို ရည်ရွယ်ကာ ထိုအုပ်စုကို ဖျားယောင်းနိုင်မည့် spear-phishing များကို အသုံးပြုလေ့ရှိပါသည်။ Traffers သည် ၎င်းတို့၏ ဝယ်ယူသုံးစွဲသူများ လိုအပ်ချက်အပေါ် မူတည်ပြီး အလိုကျမှုဖြစ်စေရန် ထိုကဲ့သို့ ပစ်မှတ်ထားသော ကမ်ပိန်းများကို ပိုမိုလုပ်ဆောင်ပေးလျက် ရှိပါသည်၊ ဥပမာ ဝယ်ယူသူများက တန်ဖိုးမြင့်သော အဖွဲ့အစည်း၏ အချက်အလက်များ သို့မဟုတ် တန်ဖိုးမြင့် ကဏ္ဍများ၏ အချက်အလက်များ ရယူလိုမှု များလျင် ထို အချက်အလက်မျိုး ရအောင် လုပ်ဆောင်ပေးခြင်း ဖြစ်ပါသည်။

Traffers များသည် ၎င်းတို့ တိုက်ခိုက်သည့် စက်ပစ္စည်းများထံမှ အချက်အလက်များ ခိုးမှု လုပ်ရန်အတွက် နည်းလမ်းပေါင်းစုံကို အသုံးပြုလေ့ရှိပြီး ထိုအထဲတွင် -

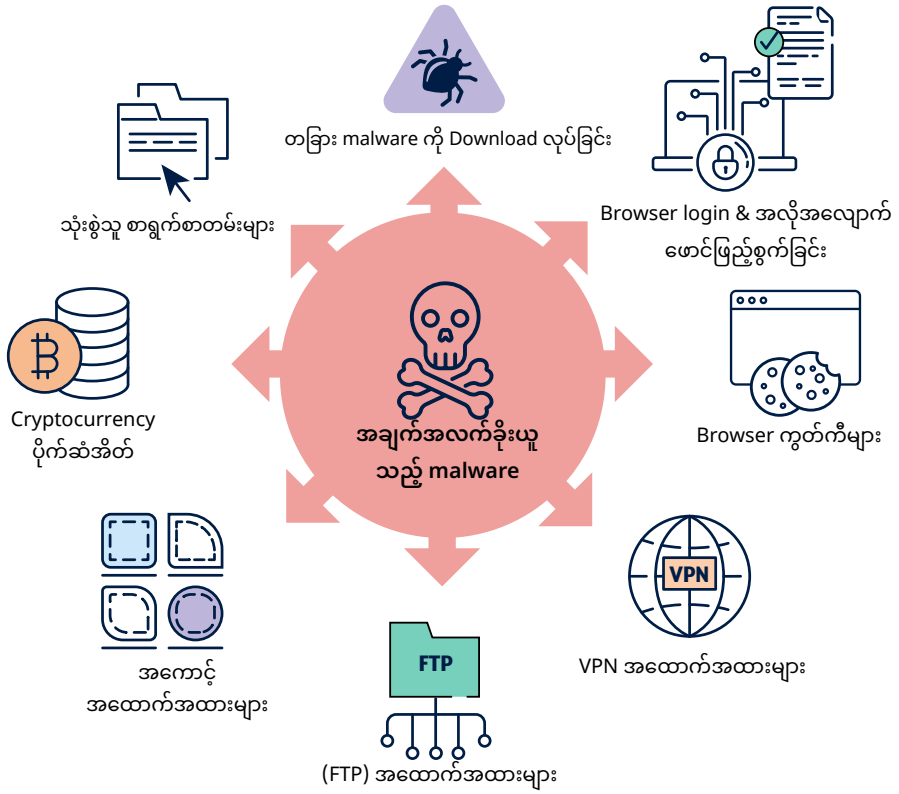
- **botnets** - ဆိုင်ဘာရာဇဝတ်သားများ ထိန်းချုပ်ထားသည့် တိုက်ခိုက်ခံထားရသော စနစ်များ၏ ကွန်ရက်များကို အသုံးချကာ မသမာသည့် လုပ်ရပ်များလုပ်ကိုင်သည့် နည်းလမ်း၊ ဥပမာ အစစ်အမှန်ကဲ့သို့ ဟန်ဆောင်ထားသည့် phishing မက်ဆေ့ချ်များ သို့မဟုတ် malware များကို ပို့ဆောင်သည့် နည်းလမ်းများ

- **phishing** - စစ်မှန်သည့် အီးမေးလ်ကဲ့သို့ သို့မဟုတ် ဆိုရှယ်မီဒီယာ၏ မက်ဆေ့ချ်များ၊ ဖိုရမ်များ၊ မက်ဆေ့ချ်ပို့နိုင်သည့် အက်ပလီကေးရှင်းများပေါ်တွင် စစ်မှန်သော မက်ဆေ့ချ်ကဲ့သို့ ဟန်ဆောင်ပြီး အချက်အလက်များကို ရယူကာ အဟန့်အတားများကို ကျော်လွှားရန် ကြိုးစားသည့်နည်းလမ်း
  - ၎င်းတို့ ပို့ဆောင်သည့် မက်ဆေ့ချ်များထဲတွင် မသမာသည့် လင့်ခ်နှင့် အီးမေးလ်တွင်လည်း မသမာသည့် ဖိုင်များ တွဲပါလာတတ်ပါသည်။
- **မသမာသည့် ရှာဖွေမှုရလဒ်များ** - malicious search results – အကြောင်းအရာကို ရှာဖွေသည့်အခါ search engine optimisation (SEO) နည်းလမ်းကို အသုံးပြုပြီး ထိုမှတဆင့် ဆော့ဖ်ဝဲ အစစ်အမှန်ကဲ့သို့ ဟန်ဆောင်ထားသော သို့မဟုတ် တခြားသော အကြောင်းအရာများရှိသော မသမာသည့် ဆော့ဖ်ဝဲများရှိရာ ဝဘ်ဆိုက်များဆီ ခေါ်ဆောင်သွားခြင်း
- **malvertising:** malware များကို ဖြန့်ဖြူးရန်အတွက် စစ်မှန်သော အွန်လိုင်းကြော်ငြာများထဲ ဖျက်လိုဖျက်ဆီးဖြစ်စေသည့် ကုဒ်များကို ထည့်သွင်းခြင်း
- **cracked သို့မဟုတ် pirated software** – ဒေါင်းလုဒ်များဖြစ်ပြီး ထိုအထဲတွင် ဗီဒီယိုဂိမ်းများ၊ You Tube ဗီဒီယိုမှတဆင့် ဗီဒီယိုအကြောင်း ရေးသားဖော်ပြသည့်နေရာ သို့မဟုတ် မှတ်ချက်ပြုသည့်နေရာတွင် မသမာသည့် လင့်ခ်များ ထည့်သွင်းခြင်း သို့မဟုတ် စိတ်မချရသည့် ဆိုက်မှ အရာများကို ဒေါင်းလုဒ် လုပ်ခြင်း
- **ဆိုရှယ်မီဒီယာအတွင်း ကြော်ငြာများနှင့် ပို့စ်များ** - malware ဖိုင်များကို လူတွေ့မသိရန်အတွက် ပစ်မှတ်လမ်းကြောင်းလွဲအောင် လုပ်ခြင်း
- **မသမာသည့် ဆော့ဖ်ဝဲ updates များ** - အများအားဖြင့် web browser updates များကဲ့သို့ ဟန်ဆောင်ခြင်း

အဆင့် ၃ - ဒေတာ အချက်အလက်များ သိမ်းယူခြင်း

တိုက်ခိုက်ခံရသူ၏ စက်ပစ္စည်းထဲသို့ အချက်အလက်ခိုးယူသည့် ဆော့ဖ်ဝဲများ ဝင်ရောက်နိုင်သည်နှင့် တပြိုင်နက် ထိုစက်ပစ္စည်းအတွင်းမှ ထိလွယ်ရှလွယ်သော အချက်အလက်များကို စုဆောင်းမှု လုပ်ပါသည်။ User credential များကို ခိုးယူမှုအပြင် အကယ်၍ အချက်အလက်ခိုးယူမှုသည် botnet ၏ အစိတ်အပိုင်းဖြစ်ပါက ထိုတိုက်ခိုက်ခံရသည့်စက်ကို အဝေးမှ ထိန်းချုပ်နိုင်စွမ်းရှိပြီး ထိုမှတဆင့် ၎င်းတို့၏ ကွပ်ကဲမှု စွမ်းရည်ကို တိုးမြင့်လုပ်ကိုင်နိုင်သကဲ့သို့ တခြားသော malware များကိုလည်း ထပ်မံပို့ဆောင်မှု လုပ်နိုင်ပါသည်။ အထွေထွေအားဖြင့် အချက်အလက်ခိုးယူမှုသည် အောက်ပါအရာများကို ခိုးယူနိုင်စွမ်းရှိပါသည် -

- User name နှင့် လျှို့ဝှက်ကုဒ် password များ၊ အထူးသဖြင့် web browser ၏ အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်း MFA user sessions/tokens များကို သိုလှောင်ထားခြင်း
- စစ်မှန်ကြောင်း အထောက်အထားပြ ကွတ်ကီများ
- Web browser တွင် အချက်အလက်များကို အလိုအလျောက် ဖောင်ဖြည့်ခြင်း
- အီးမေးလ်ဝင်ခွင့်ရရန်သုံးသည့် credential အချက်အလက်များ၊ အကြောင်းအရာနှင့် အဆက်အသွယ်များ
- ဝဘ်ထဲ ဝင်ကြည့်ထားသည့် စာရင်း
- အသုံးပြုသူ စာရွက်စာတမ်းများ
- ခရက်ဒစ်ကဒ် အချက်အလက်များ
- desktop messaging apps မှ စကားပြော မှတ်တမ်းများ
- စနစ် အချက်အလက်များ
- cryptocurrency wallets
- VPN or File Transfer Protocol (FTP) အထောက်အထားများ



ပုံ1. အချက်အလက်ခိုးယူသည့် malware ၏ စွမ်းရည်

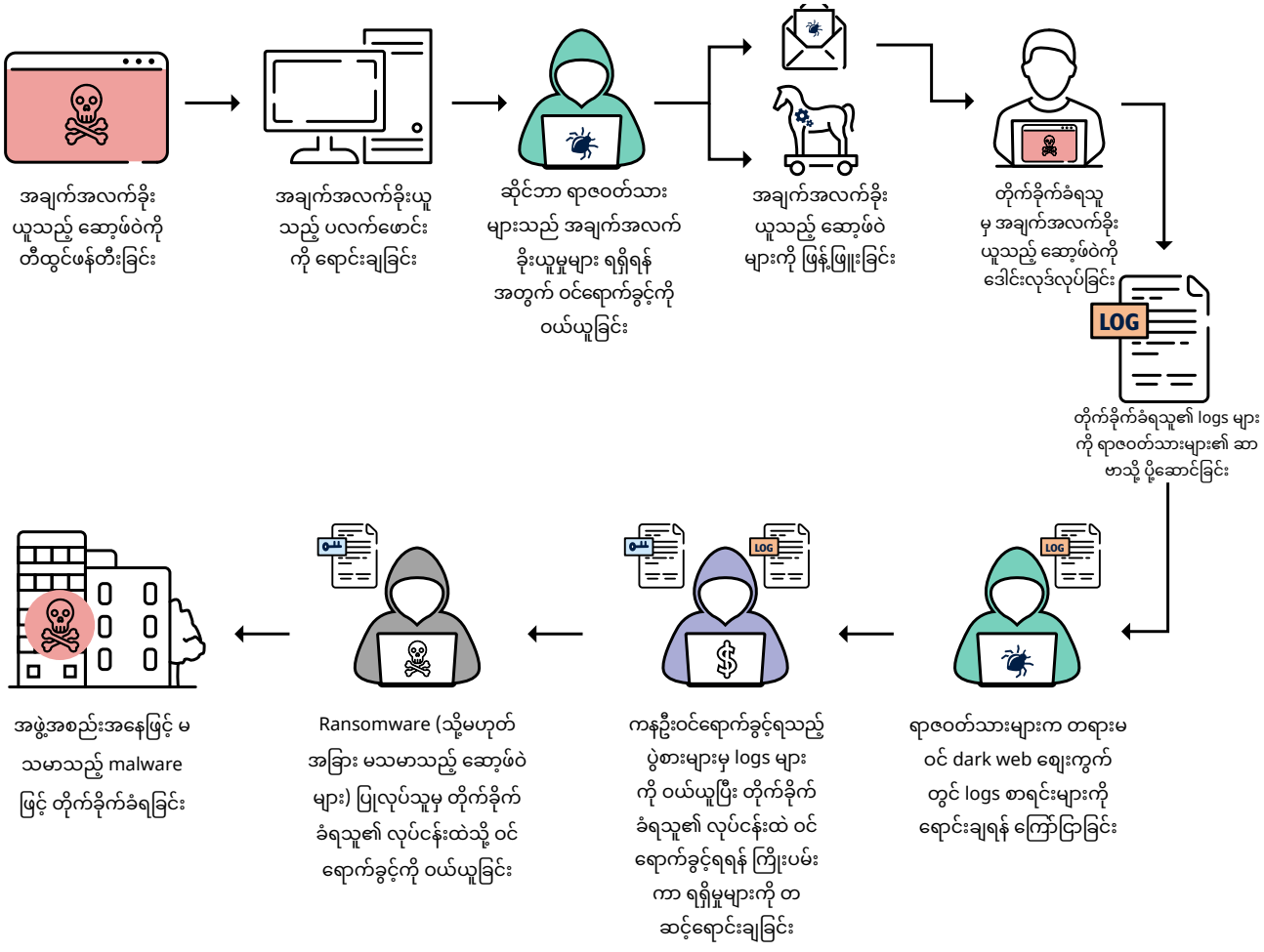
အချို့ web browser authentication cookies သည် အသုံးပြုသူ၏ မှတ်တမ်းကို အကောင့်ထဲ သို့မဟုတ် ဝန်ဆောင်မှု တစ်ခုထဲသို့ တခါ အသုံးပြုတိုင်း ရက်အနည်းငယ် သိမ်းထားပြီး ထိုကဲ့သို့ ပြုလုပ်ခြင်း သည် ထပ်ခါထပ်ခါ စစ်မှန်ကြောင်း authenticate လုပ်စရာ မလို အောင် ဆောင်ရွက်ပေးခြင်း ဖြစ်သည်။ သို့သော် အခိုးခံရမှု ဖြစ်ပေါ်ခဲ့ ပါက ထို authentication cookies သည် MFA ၏ လိုအပ်ချက်များကို အလိုအလောက်ကျော်လွှားနိုင်စေသည့်အတွက် ဆိုင်ဘာရာဇဝတ်သား များကို တိုက်ခိုက်ခံရသူ၏ အကောင့်ထဲ၊ လုပ်ငန်း၏ ကွန်ရက်၊ လုပ်ငန်း၏ စနစ်ထဲသို့ ဝင်ရောက်ခွင့် ပေးတာမျိုး ဖြစ်စေပါသည်။

အဆင့် ၄ - ဒေတာများ စုစည်းခြင်းနှင့် ငွေကြေးရရှိအောင် လုပ်ဆောင်ခြင်း

အချက်အလက် ခိုးယူသည့် ဆော့ဖ်ဝဲများကို တိုက်ခိုက်ခံရသူ၏ အချက်အလက်များအား ခိုးဝှက်ထုတ်ယူမှုလုပ်အောင် စီမံထားခြင်း ဖြစ်ပြီး ထိုအရာကို 'logs' ဟု ခေါ်ဆိုကာ ကွပ်ကဲခြင်းနှင့် ထိန်းချုပ် ရေး ဆာဗာများဆီကို ခိုးဝှက်ပို့ဆောင်ပေးခြင်း ဖြစ်ပါသည်။ အထွေထွေအားဖြင့် အချက်အလက်ခိုးယူမှုသည် Telegram၊ Discord စသည့် မက်ဆေ့ချ်များ ပို့နိုင်သည့် app များကို ပိုမို အသုံးပြုမှု ဖြစ်စေပြီး ထိုမှတဆင့် ဆိုင်ဘာရာဇဝတ်သားများ အတွက် logs များကို မျှဝေပေးခြင်းမျိုး လုပ်ပါသည်။

အထူးပြု ဈေးကွက်များ Telegram တွင်ရှိသည့်အပြင် dark web တလွှားတွင်လည်း trade of logs အဖြစ် ရောင်းချ မှု လုပ်ကြပါသည်။ ဆိုင်ဘာရာဇဝတ်သားများသည် logs များကို ငွေရေးကြေးရေး အမြတ်အစွန်းအတွက် နည်း မျိုးစုံဖြင့် အသုံးပြုလျက်ရှိပြီး ထိုအထဲတွင် -

- ရာဇဝတ်မှု ဈေးကွက်တွင် ကနဦးဝင်ရောက်ခြင်း ဆိုင်ရာ ပွဲစားအပါအဝင် logs များကို ရောင်းချခြင်း
- အချက်အလက်များ ခိုးယူခြင်းနှင့် ငွေညှစ်တောင်းဆိုခြင်းများ လုပ်ကာ တိုက်ခိုက်ခံရသူအပေါ် တိုက်ရိုက်အမြတ်ထုတ်ခြင်း
- ငွေညှစ်တောင်းခံခြင်းလုပ်ရန်အတွက် လုပ်ငန်း၏ ကွန်ရက်များထဲတွင် ကနဦးဝင်ရောက်မှုအတွက် အချက်အလက်များကို တိုးများစေခြင်း



ပုံ2. အချက်အလက်ခိုးယူသည့် ဂေဟစနစ်နှင့် ၎င်းတို့၏ အဖွဲ့အစည်းအပေါ် ဖြစ်နိုင်သည့် သက်ရောက်နိုင်မှုများ

ဆိုးကျိုး သက်ရောက်မှုများ

အချက်အလက်ခိုးယူမှုသည် တစ်ဦးတစ်ယောက်ချင်းအတွက်နှင့် အဖွဲ့အစည်းတစ်ခုလုံးအတွက် ဆိုးဝါးသည့် သက်ရောက်မှုများ ဖြစ်စေနိုင်ပါသည်။ အချက်အလက် ခိုးယူသူများအနေဖြင့် user credential များကို စုဆောင်းနိုင်သည့်အခါ ထိုစုဆောင်းသည့် အချက်အလက်များကို အသုံးချကာ ရာဇဝတ်သားများသည် လုပ်ငန်း၏ ကွန်ရက်များ၊ ကုမ္ပဏီ၏ စနစ်များထဲ user account အစစ်များဖြင့် ဝင်ရောက်နိုင်ပါသည်၊ ထိုလုပ်ရှားမှုများကို ပိုင်ရှင်များအနေဖြင့် အများအားဖြင့် နောက်ကျမှ သိရလေ့ရှိပါသည်။

အချက်အလက် အခိုးခံရသည့် **အဖွဲ့အစည်းများ** အနေဖြင့် ခံရနိုင်သည့် ဆိုးကျိုးများထဲတွင် -

- မသမာသည့် ဆော့ဖ်ဝဲ ransomware များ ကူးစက်ခံရခြင်း
- ဒေတာချိုးဖောက် ခံရခြင်း
- လုပ်ငန်းသုံး အီးမေးလ် ချိုးဖောက်ခံရခြင်း
- မူပိုင်ခွင့်ရ အရာများ အခိုးခံရခြင်း
- ထိလွယ်ရှလွယ်သော အချက်အလက်များ အခိုးခံရခြင်းတို့ ပါဝင်ပါသည်။

အချက်အလက် အခိုးခံရမှုကြောင့် **တစ်ဦးတစ်ယောက်ခြင်း အပေါ်** သက်ရောက်နိုင်သည့် ဆိုးကျိုးထဲတွင် -

- ခွင့်ပြုချက် မပါပဲ မိမိ၏ အီးမေးလ် သို့မဟုတ် ဆိုရှယ်မီဒီယာ အကောင်းများထဲ ဝင်ရောက်နိုင်ခြင်း
- ID များကို ခိုးယူနိုင်သည့် အန္တရာယ် ကျရောက်နိုင်ခြင်း
- အစစ်အမှန်ကဲ့သို့ ဟန်ဆောင်ကာ အချက်အလက်ရယူသည့် အန္တရာယ် ပိုများလာခြင်း
- ငွေရေးကြေးရေး ဆုံးရှုံးမှု သို့မဟုတ် ခွင့်ပြုချက်မပါပဲ ငွေရေးကြေးရေးအကောင့်ထဲ ဝင်ရောက်ခြင်း
- ကိုယ်ရေးကိုယ်တာ အချက်အလက် ဆုံးရှုံးခြင်းတို့ ပါဝင်ပါသည်။

ဖြစ်ရပ်မှန် နမူနာ

အများပြည်သူဆီ ကျယ်ကျယ်ပြန့်ပြန့် ဖြန့်ဖြူးရန် ရည်ရွယ်သည့်အတွက် ဤနမူနာကို ဖော်ပြရာတွင် နာမည်စစ်များ ဖော်ပြခြင်း မလုပ်ထားပါ။ ဤနမူနာသည် ASD ၏ ACSC ကို တိုင်ကြားလာသည့် ဩစတြေးလျရှိလုပ်ငန်းအချို့ ဆိုင်ဘာ လုံခြုံရေး ချိုးဖောက် တိုက်ခိုက်ခံရမှု၏ သက်ရောက်မှုများကို ဖော်ပြထားပါသည်။ တိုက်ခိုက်ခံရသည့် လုပ်ငန်းကို သည်နောက်ပိုင်းတွင် 'အဖွဲ့အစည်း' ဟုသာ ဖော်ပြသွားပါမည်။ ဤစာစောင်ပါ လူတစ်ဦးတစ်ယောက်ခြင်းစီ၏ နာမည်သည် နာမည်တုများသာဖြစ်ပြီး တိုက်ခိုက် ခံရသူများ မည်သူမည်ဝါဖြစ်သည်ကို ကာကွယ်လိုသည့်အတွက် အချက်အလက်အချို့ကို ချန်လှပ်ထားပါသည်။

ထိုအဖွဲ့အစည်းသည် ဩစတြေးလျအတွင်းမှ လုပ်ငန်းတစ်ခုဖြစ်ပြီး ၎င်း၏ အမှုထမ်းများကို မိမိ၏ ကိုယ်ပိုင်စက်ပစ္စည်းအား သုံးခွင့်ပြုကာ လုပ်ငန်း၏ စနစ်ထဲ ဝင်ရောက်ခွင့်ပေးသည့် လုပ်ငန်း ဖြစ်ပါသည်။ အဲလစ်စ် သည် ထိုအဖွဲ့အစည်း၏ အမှုထမ်းတစ်ဦးဖြစ်ပြီး အဝေးကနေ အလုပ်လုပ်သူ ဖြစ်ပါသည်။

အိမ်မှ အလုပ်လုပ်သည့်အခါ အဲလစ် သည် ၎င်း၏ ကိုယ်ပိုင် လက်ပ်တော့ကွန်ပြူတာကို အသုံးပြုကာ လုပ်ငန်း၏ ကွန်ရက်ထဲသို့ ဝင်လေ့ရှိပါသည်။ အဲလစ်သည် ယုံကြည်စိတ်ချရသည်ဟု ထင်ရသည့် ဝဘ်ဆိုက် တစ်ခုမှ Notepad++ (ကောက်နှုတ်ချက်ကို လိုက်မှတ်သားပေးသည့် ဆော့ဖ်ဝဲ တစ်မျိုး) ကို သူမ၏ **ကိုယ်ပိုင်လက်ပ်တော့ထဲ ဒေါင်းလုဒ်** လုပ်ခဲ့ပါသည်။ **အချက်အလက်ခိုးယူသည့်** malware က ထို Notepad++ ဆော့ဖ်ဝဲ၏ installer အဖြစ် အယောင်ဆောင်ကာ ရှိနေခဲ့ပါသည်။

ထိုဆော့ဖ်ဝဲကို အဲလစ် ထည့်သွင်းဖို့ ကြိုးစားသည့်အခါ အချက်အလက်ခိုးယူသည့် malware ကို အသက်ဝင်စေပြီး ထိုမှတဆင့် သူမ၏ လက်ပ်တော့ထဲမှ credential **အချက်အလက်များကို ခိုးယူခဲ့ပါသည်။** ခိုးယူခံရသည့် အချက်အလက်များတွင် သူမ web browser ၏ login feature တွင် သိုလှောင်ထားသည့် အလုပ်အတွက် အသုံးပြုသော username နှင့် password လျှို့ဝှက်ကုဒ်များလည်း ပါဝင်ပါသည်။ ထိုကဲ့သို့သော အချက်အလက်များကို ယူကာ အချက်အလက်ခိုးယူသည့် malware က ဆိုင်ဘာရာဇဝတ်သားများ အဝေးမှ ကွပ်ကဲ-ပြီး-ထိန်းချုပ်သည့် ဆာဗာဆီကို ပေးပို့ခဲ့ပါသည်။

ထိုကဲ့သို့ အခိုးခံရသည့် မှတ်တမ်းများကို အခြားသော အချက်အလက်များနှင့် အတူတူထုတ်ပိုးကာ dark web ဈေးကွက်မှတဆင့် **ဆိုင်ဘာရာဇဝတ်သားများဆီ ရောင်းချမှု** ပြုလုပ်ခဲ့ပါသည်။

ဘော့ဘ် ဟု ခေါ်သည့် ဆိုင်ဘာရာဇဝတ်သား တစ်ဦးက အဲလစ်၏ credential အချက်အလက်များကို ဝယ်ယူကာ သူမ အလုပ်၏ ကွန်ရက်ထဲသို့ စစ်မှန်သော အချက်အလက်များဖြင့် ဝင်ရောက်မှု လုပ်ကိုင်နိုင်သူ ဖြစ်သွားပါသည်။ အဲလစ် အလုပ်လုပ်သော အဖွဲ့အစည်းတွင် ဝန်ဆောင်မှုအတွက် **ပြုပြင်ထားသည့်** MFA မရှိသည့်အတွက် ဘော့ဘ် အနေဖြင့် အခိုးခံရသည့် အချက်အလက်များကို အသုံးပြုရုံမျှဖြင့် အလုပ်၏ ကွန်ရက်ထဲသို့ **စစ်မှန်သူအနေဖြင့် ဝင်ရောက်ခွင့်** ရရှိခဲ့ပါသည်။

ဘော့ဘ်သည် အခိုးခံရသည့် **စစ်မှန်သော** user credential များကို အသုံးပြုပြီး အဲလစ်စ် အလုပ်လုပ်သော အဖွဲ့အစည်း၏ ကွန်ရက်ထဲကို မည်သူမျှမသိအောင် ဝင်ရောက်မှု လုပ်နိုင်ခဲ့ပါသည်။ ဘော့ဘ်သည် လုပ်ငန်း၏ ကွန်ရက်ထဲသို့ အခိုင်အမာ ဝင်ရောက်ကာ အဖွဲ့အစည်းပိုင်သည့် ထိလွယ်ရှလွယ်သော ဒေတာအချက်အလက်များကို ရယူပြီး ကုမ္ပဏီကို ငွေညှစ်ရန်အတွက် အချက်အလက်များကို ခိုးထုတ်မှုများလုပ်ခဲ့ပါသည်။

အချက်အလက်များကို ခိုးယူပြီးသည်နှင့် ဘော့ဘ်သည် ထိုအချက်အလက်များကို တခြားလူများ ဝင်ကြည့်ခွင့်မရရန်အတွက် အဖွဲ့အစည်း၏ databases **နှင့် ဖိုင်စနစ်** များကို **လျှို့ဝှက်ကုဒ်များဖြင့် ကာကွယ်မှုပြုလုပ်** ခဲ့ပါသည်။

အန္တရာယ် လျော့ချနိုင်သည့် နည်းလမ်းများ

အဖွဲ့အစည်းများအနေဖြင့် ၎င်းတို့၏ ကွန်ရက်ဖြင့် ချိတ်ထားသည့် စက်ပစ္စည်းများအပေါ် ထိန်းချုပ်မှု လုပ်နိုင်မည်မဟုတ်ပါ၊ အထူးသဖြင့် အဝေးမှ အလုပ်လုပ်သည့် အမှုထမ်းများ ကိုယ်ပိုင်စက်ပစ္စည်းသုံးသည့် အနေအထားမျိုး ဖြစ်ပါသည်။ ASD ၏ ACSC အနေဖြင့် အဖွဲ့အစည်းများအား user credential များကို ပစ်မှတ်ထားသည့် အချက်အလက်ခိုးယူမှုများ၏ ရန်မှ ကာကွယ်ရန်အတွက် ထိန်းချုပ်ခြင်းနည်းလမ်းများ အသုံးပြုရန် တိုက်တွန်းလိုပါသည်။ အန္တရာယ် လျော့ချနိုင်သည့် နည်းလမ်းများထဲတွင် -

ဆိုင်ဘာလုံခြုံရေးကို သိနားလည်စေရန်အတွက် အမှုထမ်းများကို သင်တန်းပေးခြင်း

- ယုံကြည်စိတ်ချမှုကို အခွင့်ကောင်းယူကာ မသမာသည့်နည်းဖြင့် တိုက်ခိုက်ခြင်းနည်းလမ်းနှင့် မသမာသည့် ဖိုင်များကို ဒေါင်းလုဒ် လုပ်ခြင်းမှ ကာကွယ်ရန်အတွက် အမှုထမ်းများကို သင်တန်းပေးပါ။
- အချက်အလက်ခိုးယူနိုင်သည့် နည်းလမ်းအကြောင်းများကို ပညာပေးပြီး ၎င်းတို့ အသုံးပြုသည့် နည်းလမ်းများနှင့် သင့်အဖွဲ့အစည်းအပေါ် phishing ခြိမ်းခြောက်မှု အန္တရာယ်ရှိနိုင်သည့် အကြောင်းများကို ပညာပေးပါ။

လုပ်ငန်းသုံး အကောင့်များကို လုံခြုံအောင် ပြုလုပ်ခြင်း

- အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်း MFA နည်းလမ်းကို အသုံးပြုခြင်း -
- အတွင်းနှင့် ပြင်ပ ဝန်ဆောင်မှုများ၊ စနစ်များနှင့် ထိလွယ်ရှလွယ်သော ဒေတာများအတွက် အထူးသဖြင့် webmail၊ VPNs နှင့် အရေးကြီးသည့် စနစ်ထဲ ဝင်ရောက်ခွင့်ရှိသည့် အဆင့်မြင့် user account များအတွက် အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်း MFA နည်းလမ်းကို အသုံးပြုပါ။ အကောင်းဆုံးနည်းလမ်းမှာ phishing-resistant MFA နည်းကို အကောင့်များ အားလုံးအတွက် အသုံးပြုပါ။
- အသုံးမလိုတော့သည့်အခါ user account ကို အသုံးမပြုနိုင်အောင် လုပ်ပါ။
- အက်မင်အနေဖြင့် အထူး ဝင်ရောက်ခွင့်များကို ကန့်သတ်ချက်ထားပါ
- Locked-down အတွက် သီးသန့်သတ်မှတ်ထားသည့် ကွန်ပြူတာ (ဥပမာ လုံခြုံဘေးကင်းသည့် အက်မင် ကွန်ပြူတာ) ကို အသုံးပြုကာ ကွန်ရက် administration နှင့် အခြားသော အဆင့်မြင့် ခွင့်ပြုချက်ရထားသည့် အရာများကို စမ်းသပ်စစ်ဆေးမှုများ ပြုလုပ်ပါ။
- စနစ်ကို စီမံရန်အတွက် အဆင့်မြင့် ခွင့်ပြုချက်ရထားသည့် userအကောင့်ကို အသုံးပြုရန်အတွက် အနိမ့်ဆုံးလိုအပ်သည့် သတ်မှတ်ချက်နည်းလမ်းများအတိုင်း အသုံးပြုကာ သိပ်ပြီး အရေးကြီးသည့် လုပ်ငန်းများအတွက် သာမာန် user account ကို သုံးပါ။
- အဆင့်မြင့် ဝင်ခွင့်ရသည့် user account များကို (အွန်လိုင်း ဝန်ဆောင်မှုအတွက် ခွင့်ပြုချက်ရထားသည့် အကောင့်မှလွဲ၍) အင်တာနက်ထဲ ဝင်ရောက်ခြင်း၊ အီးမေးလ်နှင့် web service များထဲ ဝင်ရောက်ခွင့် ပိတ်ပင်ထားပါ။
- စနစ်များနှင့် အက်ပလီကေးရှင်းများအတွက် just-in-time administration ကို အသုံးပြုရန် ထည့်သွင်းစဉ်းစားပါ။
- အဆင့်မြင့် ဝင်ခွင့်ရသည့် user account များကို စီမံခြင်းနှင့် စစ်ဆေးမှုများ လုပ်နိုင်သည့် စည်းမျဉ်းများကို ချမှတ်ပါ။
- လျှို့ဝှက်ကုဒ် password များကို ပုံမှန် ပြောင်းပါ အထူးသဖြင့် ပြင်ပနှင့် ဆက်သွယ်ကာ အဝေးမှ ဝင်ရောက်ခွင့်ရှိသည့် အကောင့်များအတွက် အထူးလုပ်ဆောင်ပါ။
- Session tokens နှင့် cookies များအတွက် သက်တမ်းကြာချိန်နှင့် sunset မူဝါဒများ ချမှတ်ပါ။

လုပ်ငန်း၏ ရွှေ့လျားမှုများကို လုံခြုံရေး ခိုင်မာအောင် လုပ်ပါ

- လုပ်ငန်း၏ ရွှေ့လျားမှုဆိုင်ရာ အန္တရာယ် အနေအထားကို ဆန်းစစ်လေ့လာပြီး လုပ်ငန်း၏ ရွှေ့လျားမှုများကို လုံခြုံရေးခိုင်မာအောင် ပြုလုပ်ခြင်းလမ်းညွှန်ချက်များကို အသုံးပြုပါ။
- အကယ်၍ လုပ်ငန်းတွင် အမှုထမ်းများအား ၎င်းတို့၏ ကိုယ်ပိုင်စက်ပစ္စည်းများကို အသုံးပြုခွင့်ပြုပါက Bring Your Own Device (BYOD) မူဝါဒများ ချမှတ်ပါ၊ လုပ်ငန်းနှင့် ဆက်စပ်သည့် စက်ပစ္စည်းများသည် စီမံစောင့်ကြည့်မှု ပိုနည်းသည့် ကိုယ်ပိုင်စက်ပစ္စည်းများထက် လုံခြုံရေး ပိုကောင်းမွန်ပါသည်။

ကုန်ပစ္စည်းရောင်းချသူမှ သင်၏ ကွန်ရက်ထဲ ဝင်ရောက်ခြင်းရှိမရှိ ကုန်ပစ္စည်းထောက်ပံ့မှု ကွင်းဆက်ဆိုင်ရာ အန္တရာယ်ကို ဆန်းစစ် လေ့လာမှုလုပ်ပြီး ထိုအထဲတွင် Software-as-a-Service (Saas) vendors နှင့် Managed Service Providers တို့လည်း ပါဝင်ပါသည်။ Managed Service Provider ကို အသုံးပြုသည့် ကာလအတွင်း သင်၏ လုံခြုံရေးကို မည်ကဲ့သို့ စီမံခန့်ခွဲမည်နည်း။

သင့်လုပ်ငန်း၏ ကွန်ရက်ကို ကာကွယ်ပါ

- အက်ပလီကေးရှင်းနှင့် operating စနစ်များကို up to date ဖြစ်အောင် ထားပါ။
- အက်ပလီကေးရှင်းများကို တင်းကြပ်စွာကန့်သတ်သည့် ဒေသန္တရဆိုင်ရာ လုံခြုံရေး မူဝါဒများကို အသုံးပြုပါ။
- ကွန်ရက်တစ်ခုခြင်း လုပ်ဆောင်ရသည့် တာဝန်အလိုက် အကန့်များခွဲခြားနိုင်ရန်အတွက် ကွန်ရက်များကို အကန့်လိုက် ခွဲခြားသည့် နည်းလမ်းကို အသုံးပြုပါ။
- အသုံးပြုသူများ၏ လှုပ်ရှားမှု အထူးသဖြင့် အဝေးမှ အလုပ်လုပ်ကိုင်သည့် အမှုထမ်းများ၏ လှုပ်ရှားမှုကို ပုံမှန် စောင့်ကြည့် စစ်ဆေးမှုများ လုပ်ပါ။
- အဆင့်မြင့် အချက်အလက်များထဲ ဝင်ရောက်ခွင့်ရှိသည့် အခွင့်ထူးအကောင့်များကို စောင့်ကြည့်ခြင်းအားဖြင့် ခွင့်ပြုချက်မပါပဲ ထိလွယ်ရှလွယ်သော ဒေတာများထဲ ဝင်ရောက်ခြင်း သို့မဟုတ် သာမာန်မဟုတ်သည့် ဒေတာဖလှယ်မှုများ၊ ဥပမာ ဒေတာအများအပြားကို ကွန်ရက်ပြင်ပသို့ ပို့ဆောင်နေမှုများကို တွေ့ရှိနိုင်ပါသည်။
- ဒေတာများ ဆုံးရှုံးမှုကို ကာကွယ်ပေးမည့် မူဝါဒများနှင့် ခွင့်ပြုချက်မရှိပဲ ဒေတာလွှဲပြောင်းမှုများ မလုပ်နိုင်အောင် တားဆီးသည့် နည်းများကို အသုံးပြုပါ။

ASD ၏ ဆိုင်ဘာလုံခြုံရေးကွန်ရက် ဆိုင်ရာ ပါတနာအဖြစ် ပါဝင်ပြီး ASD ၏ ဆိုင်ဘာခြိမ်းခြောက်မှုထောက်လှမ်းရေး (CTIS) ဝန်ဆောင်မှုနှင့် ပူးပေါင်းပါ။

- CTIS သည် အပြန်အလှန်ဖလှယ်ရေး ပလက်ဖောင်းဖြစ်ပြီး အစိုးရနှင့် လုပ်ငန်းပါတနာများအနေဖြင့် မသမာသည့် ဆိုင်ဘာလှုပ်ရှားမှု အချက်အလက်များကို မျှဝေ ရယူရန်အတွက် ဖြစ်ပါသည်။
- ASD ၏ ACSC သည် အချက်အလက်ခိုးယူမှု၏ လှုပ်ရှားမှုကို နောက်ယောင်ခံပြီး CTIS ပလက်ဖောင်းမှတဆင့် ကွပ်ကဲခြင်းနှင့် ထိန်းချုပ်ခြင်းဆိုင်ရာ အချက်အလက်များကို ပြန်လည် မျှဝေပေးပါသည်။
- ပါတနာဖြစ်လာရန်အတွက် အဖွဲ့ဝင်အဖြစ် sign up လုပ်ကာ သင်၏ အဖွဲ့အစည်း ဒေတာနှင့် သင့်ဝန်ဆောင်မှုကို အသုံးပြုသူများ၏ ဒေတာကို ဆိုင်ဘာရာဇဝတ်သားများ၏ ရန်မှ ကာကွယ်ပါ။

တိုက်ခိုက်ခံရနိုင်ခြင်းအတွက် ပြင်ဆင်မှုလုပ်ခြင်း

- အချက်အလက် ခိုးယူသည့် ဆိုင်ဘာတိုက်ခိုက်ခံရသည့်အခါ တုန့်ပြန်နိုင်မည့် အစီအစဉ်များကို ချမှတ်ပါ။ သံသယဖြစ်ဖွယ်ရာ ဖိုင်များကို ဒေါင်းလုဒ် လုပ်မိသည်ဟု ထင်ရသည့်အခါ မိမိ၏ အမှုထမ်းများ မည်ကဲ့သို့ ဆောင်ရွက်ရမည်ကို အမှုထမ်းများ သိနားလည်အောင် လုပ်ဆောင်ပါ။

ASD နှင့် ဆက်စပ်သည့် ACSC ၏ Essential Eight နည်းလမ်းကို ကျင့်သုံးခြင်း

- အထက်ပါ လိုက်နာလုပ်ဆောင်သင့်သည့် နည်းလမ်းများအပြင် ASD ၏ ACSC အနေဖြင့် တိုက်တွန်းလိုသည့်အချက်မှာ ကျန်ရှိနေသည့် ASDနှင့် ဆက်စပ်သော ACSC ၏ Essential Eight နည်းလမ်းကို ကျင့်သုံးရန် လုံးလုံးလျားလျား တိုက်တွန်းလိုပါသည်။

အမှုထမ်းများအတွက် အဝေးမှ အလုပ်လုပ်သည့်အခါ အကြံပြုချက်

- သင်၏ အချက်အလက်များကို သင်၏ ကိုယ်ရေးကိုယ်တာသုံးစက်တွင် ထည့်ပြီး ကာကွယ်ရန်
  - ဆိုင်ဘာကို ပုံမှန်စိစစ်ထိန်းသိမ်းသည့်နည်းကို အသုံးပြုပြီး သံသယဖြစ်ဖွယ်ရာ လင့်ခ်များ သို့မဟုတ် pop-ups များ၊ သို့မဟုတ် မိမိမသိသော သို့မဟုတ် စိတ်မချရသော ဖိုင်နှင့် ဆော့ဖ်ဝဲများကို download လုပ်ခြင်းမျိုးကို ရှောင်ရှားပါ။
  - အလုပ်အတွက် အကောင့်နှင့် ကိုယ်ရေးကိုယ်တာ အကောင့်များအတွက် တမူထူးခြားသည့် လျှို့ဝှက်ကုဒ် password များကို အသုံးပြုပါ။ ဖြစ်နိုင်ပါက ကိုယ်ရေးကိုယ်တာသုံး အကောင့်များ အတွက် အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်း MFA နည်းလမ်းကို အသုံးပြုပါ။
  - သင့်အလုပ်၏ credential များကို သင်၏ အလုပ်ရှင် ခွင့်ပြုချက်မပါပဲ ကိုယ်ရေးကိုယ်တာသုံး password manager တွင် ထည့်သွင်းထားခြင်းများ မလုပ်သင့်ပါ။ ထိုအထဲတွင် web browser ၏ password manager လည်း ပါဝင်ပါသည်။ **ရှင်းလင်းမှုမရှိပါက သင်၏ လုပ်ငန်းရှင်အား လုပ်ငန်းသုံး** password manager ပေးရန် တောင်းခံနိုင်ပါသည်။
  - မျှဝေသုံးစွဲခြင်း သို့မဟုတ် အများသုံး ကွန်ပြူတာများမှတဆင့် သင်၏ အလုပ်အကောင့်ထဲသို့ ဝင်ရောက်ခြင်း မလုပ်သင့်ပါ။
  - သင့် web browser ၏ autofill နေရာတွင် မည်သည့် အရာများ သိုလှောင်ထားသည်ကိုလည်း သတိပြုပါ။ အချက်အလက် ခိုးယူသူများသည် browser မှ သိုလှောင်ထားသည့် autofill form များကို ပစ်မှတ်ထားလေ့ ရှိပါသည်။ Web ပေါ်တွင် ဖောင်ဖြည့်သည့်အခါ ခရက်ဒစ်ကဒ်နံပတ်များကဲ့သို့ ထိလွယ်ရှလွယ်သော အချက်အလက်များကို ဖောင်ဖြည့်တိုင်း ကိုယ်တိုင်ကိုယ်ကျ ဖြည့်စွက်ရသည့် နည်းလမ်းကို အသုံးပြုပြီး သင်၏ web browser ၏ ဖောင် အလိုအလျောက် ဖြည့်ပေးသည့် feature ကို မသုံးမိအောင် လုပ်ပါ။
  - အချက်အလက် ခိုးယူသူများအတွက် အသင့်မဖြစ်စေရန် အသုံးပြုမှု ပြီးသွားသည့်အခါတိုင်း သင်၏ အွန်လိုင်း ဝန်ဆောင်မှုမှ log out ထွက်ခွာမှုလုပ်ပြီး web browser များကို ရှင်းပစ်ပါ။
  - သင်၏ operating စနစ်တွင် အလိုအလျောက်ပါလာသည့် antivirus solution အား ဖွင့်ထားပါ။ third-party antivirus solution ကို အသုံးပြုပါက up to date ဖြစ်နိုင်အောင် လုပ်ဆောင်သင့်ပြီး နာမည်ရှိသည့် ကုမ္ပဏီထံမှ ရယူသုံးစွဲသင့်ပါသည်။

ကူညီပံ့ပိုးခြင်း

သြစတြေးလျအဖွဲ့အစည်းများအနေဖြင့် အချက်အလက်များ ခိုးယူသည့် တိုက်ခိုက်မှုကို ခံရပါက သို့မဟုတ် ကူညီပံ့ပိုးမှု လိုအပ်ပါက ASD ၏ ACSC ကို **1300 CYBER1 (၁၃၀၀ ၂၉၂ ၃၇၁)** ကို ဖုန်းခေါ်ဆိုနိုင်သကဲ့သို့ cyber.gov.au/report ကို စာရေးပြီး တိုင်တန်းမှုများ လုပ်နိုင်ပါသည်။

ASD ၏ ACSC အနေဖြင့် အဖွဲ့အစည်းများအား တိုက်တွန်းလိုသည်မှာ အချက်အလက်ခိုးယူမှုနှင့် ဆက်စပ်ပြီး သံသယဖြစ်ဖွယ်ရာ သို့မဟုတ် တိုက်ခိုက်ခံရနိုင်ကြောင်း ပြသမှုများ သိရှိရလျင် တိုင်တန်းရန် သို့မဟုတ် တိုက်ခိုက်ခံရပြီး ထိန်းထိမ်းနိုင်သည့် အခြေအနေရောက်ရှိသည့်အောင် တိုင်တန်းမှုများ လုပ်ရန် တိုက်တွန်းလိုပါသည်။ သင်တို့၏ သတင်းပေးပို့ချက်များကို အသုံးပြုကာ ကျွန်ုပ်တို့အနေဖြင့် ဆိုင်ဘာခြိမ်းခြောက်မှုများလုပ်သည့် မသမာသူများ အသုံးပြုသည့် နည်းဗျူဟာ၊ နည်းပညာနှင့် လုပ်ထုံးလုပ်နည်းများကို ပိုမိုသိနားလည်စေမည်ဖြစ်ပြီး အလားတူ ပစ်မှတ်ထားခံရသည့် အခြားသော အဖွဲ့အစည်းများကိုလည်း သတိပေးခြင်းမျိုး လုပ်ဆောင်စေနိုင်ပါသည်။

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤလမ်းညွှန်ချက်ပါ အကြောင်းအရာများသည် အထွေထွေအကြံပြုချက်သာဖြစ်ပြီး တရားရေးရာ အကြံပြုချက် အဖြစ် မမှတ်ယူသင့်သကဲ့သို့ တချို့အခြေအနေအတွက် အကူအညီ သို့မဟုတ် အရေးပေါ် အခြေအနေအတွက် အားထားရာ အကြံပြုချက်မဖြစ် မယူဆသင့်ပါ။ အရေးကြီးသည့်အခါ သင်ကြုံတွေ့ရသည့် အတွေ့အကြုံအတွက် သင့်တော်ပြီး သီးသန့် လွတ်လပ်မှုရှိသည့် ကျွမ်းကျင်ပညာရှင်များ၏ အကြံဉာဏ်များကို ရယူပါ။

ဤအကြံပြုချက်ပါ အချက်အလက်များအပေါ် မှီခိုရာက ပျက်စီးမှုဖြစ်ခြင်း၊ ဆုံးရှုံးရခြင်း သို့မဟုတ် ငွေကုန်ကြေးကျ ခံရပါက အစိုးရအနေဖြင့် တာဝန်ယူမည် မဟုတ်ပါ။

မူပိုင်ခွင့်

နိုင်ငံတော် အမှတ်တံဆိပ်ကို အသုံးပြုခြင်း

နိုင်ငံတော် အမှတ်တံဆိပ်အား မည်သည့်နေရာတွင် အသုံးပြုခြင်းဆိုင်ရာ အသေးစိတ်အချက်အလက်အား ဝန်ကြီးချုပ်နှင့် ဝန်ကြီးအဖွဲ့၏ ဝန်ကြီးဌာန၏ ဝဘ်ဆိုက်တွင် ဖော်ပြထားပါသည်၊ နိုင်ငံတော်၏ အမှတ်တံဆိပ် ဆိုင်ရာ အချက်အလက်နှင့် လမ်းညွှန်ချက်များ | pmc.gov.au

အချက်အလက်ပိုများနှင့် ဆိုင်ဘာလုံခြုံရေး ချိုးဖောက်ခံရမှုအား မည်သို့ တိုင်တန်းနိုင်သနည်း အကြောင်း လေ့လာရန် နှင့် ဆက်သွယ်မှုလုပ်လိုပါက-

cyber.gov.au | 1300 CYBER1 (1300 292 371) ကို ဆက်သွယ်ပါ။

ဤနံပါတ်ကို ဩစတြေးလျနိုင်ငံအတွင်းသာ အသုံးပြုနိုင်ပါသည်။

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre