Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

AFP

cyber.gov.au

“ကျည်ကာ Bulletproof ” hosting provider များ - ဆိုင်ဘာရာဇဝတ်မှု ဆိုင်ရာ အခြေခံအဆောက်အဦး၏ သံချပ်ကာအတွင်း အက်ကြောင်းများ

အောင်မြင်သော ဆိုင်ဘာရာဇဝတ်သားများသည် လုံခြုံမှုရှိပြီး ခြေရာခံ၍ မရသည့်အပြင် ကြံ့ကြံ့ခံနိုင်သည့် အခြေခံအဆောက်အဦးများအပေါ် မှီခိုလေ့ရှိပါသည်။ ကွန်ရက် တိုက်ခိုက်ခံရမှု၊ အချက်အလက်အထောက်အထားများ အခိုးခံရမှု၊ ဝဘ်ဆိုက်အား တိုက်ခိုက်ပြီး အပေးအယူလုပ်မှု (ransomware)၊ အချက်အလက်ခိုးယူမှုများနှင့် တရားမဝင် ဖိုရမ်များအတွင်း ရောင်းချမှုဖြစ်ရပ်တိုင်း၏ နောက်ကွယ်တွင် လုံခြုံတောင့်တင်းခိုင်မာသည့် အခြေခံ အဆောက်အဦးများရှိနေပြီး ၎င်းသည် ဆိုင်ဘာရာဇဝတ်သားများကို ကောင်းမွန်စွာ လည်ပတ်စေနိုင်ပြီး လူသူမသိအောင် ဖုံးကွယ်ထားပါသည်။

သို့သော် ဆိုင်ဘာရာဇဝတ်သားများအတွက် မိမိတို့အား မရိပ်မိအောင်နေရန်နှင့် နောက်ယောင်မခံမိစေရန် လုပ်ဆောင်ရန်အတွက် စိန်ခေါ်မှုများ ပိုရှိလာပါသည်။ ကမ္ဘာ့ပေါ်ရှိ အစိုးရအခြင်းခြင်းတို့၏ ပူးပေါင်းမှု၊ ဥပဒေစိုးမိုးရေး ဆောင်ရွက်သူတွေအကြား ပူးပေါင်းမှုနှင့် ပုဂ္ဂလိက ကဏ္ဍများ၏ ပူးပေါင်းမှုကြောင့် ရာဇဝတ်သားများသည် အွန်လိုင်းပေါ်တွင် အမည်မသိအောင် လုပ်ဆောင်ရန် ပိုမို ခက်ခဲလာပါသည်။ ထို့အပြင် ဆိုင်ဘာရာဇဝတ်သား အနည်းငယ်ကသာ မိမိကိုယ်ကို ကာကွယ်ပေးမည့် လုံခြုံဘေးကင်းသော အခြေခံအဆောက်အဦးကို ဆက်လက် ထိန်းသိမ်းရန်နှင့် စီမံရန် လုံလောက်သည့် အရည်အချင်းနှင့် ကျွမ်းကျင်မှု ရှိကြပါသည်။ ထို့အတွက်ကြောင့် ၎င်းရာဇဝတ်သားများသည် သူတို့အား ကာကွယ်ပေးမည့် အခြေခံအဆောက်အဦးများ ရရှိရန် မသာမာသည့်နည်းဖြင့် အခြေခံ အဆောက်အဦးဝန်ဆောင်မှုပေးသည့် သူများကို ချည်းကပ်ကာ ဆိုင်ဘာရာဇဝတ်မှုများ ကျူးလွန်လျက်ရှိပြီး သားကောင်များနှင့် အမြတ်အစွန်းကို ပစ်မှတ်ထားကာ လုပ်ကိုင်ဆောင်ရွက်လျက် ရှိပါသည်။

“ဆိုင်ဘာ ရာဇဝတ်မှုအား ဝန်ဆောင်မှုတစ်ရပ်ကဲ့သို့ဆောင်ရွက်ခြင်း" ဟု ဆိုရာတွင် ဆိုင်ဘာတိုက်ခိုက်မှုလုပ်သည့် မသမာသည့် သူများအား ပံ့ပိုးရန်အတွက် တရားမဝင်ဈေးကွက်ထားရှိခြင်းကို ဆိုလိုခြင်း ဖြစ်ပါသည်။ တရားမဝင်ဈေးကွက်ဟု ဆိုရာတွင် ဆိုင်ဘာ ရာဇဝတ်သားများအား အွန်လိုင်းပေါ်တွင် သားကောင်များအား ပစ်မှတ်ထားနိုင်ရန်အတွက် အမြဲတစေ တိုးတက် ကောင်းမွန်လာနေသည့် ပစ္စည်းများရရှိရန်၊ ဝန်ဆောင်မှုများရရှိရန်နှင့် အချက်အလက်များ ရရှိရန် ဆောင်ရွက်ပေးခြင်းတို့ ပါဝင်ပါသည်။ ဆိုင်ဘာ ရာဇဝတ်မှု ကျူးလွန်လိုသူများသည် ကွန်ရက်များထဲ ဝင်ရောက်နိုင်ရန်အတွက် ဝင်ခွင့် ဝယ်ယူနိုင်သည့်အပြင် လုံခြုံရေး အတားအဆီးများအား ကျော်လွှားနိုင်စေသည့် ပစ္စည်းများလည်း ဝယ်ယူနိုင်ပါသည်။ ထို့အပြင် ဆိုင်ဘာအရင်းအမြစ်အား တိုက်ခိုက်ပြီး အချက်အလက်များ ခိုးယူနိုင်သည့်

malware များကိုလည်း ဝယ်ယူပြီး ပစ်မှတ်ထားသူများကို ထိခိုက်နစ်နာစေသည့် လုပ်ရပ်နှင့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို ခိုးယူမှု လုပ်နိုင်ပါသည်။ ကျည်ကာ bulletproof hosting provider BPH များသည် ဆိုင်ဘာ ရာဇဝတ်သားများအား လုံခြုံမှုပေးသည့် ဂေဟစနစ် ဖြစ်ပေါ်အောင် လုပ်ဆောင်ရာတွင် တစိတ်တပိုင်း ပါဝင်ပါသည်။ အရေးကြီးသည့်အချက်မှာ ထိုကဲ့သို့သော BPH တစ်ခုတည်းကပင် ဆိုင်ဘာရာဇဝတ်သား ရာနဲ့ချီအား တိုက်ရိုက် လှုပ်ရှားခွင့်ပေးကာ ကမ္ဘာတလွှားမှ ၎င်းတို့၏ သားကောင်များအား ပစ်မှတ်ထား တိုက်ခိုက်မှု လုပ်နိုင်ရန် ဆောင်ရွက် ပေးနိုင်ပါသည်။

“ကျည်ကာ bulletproof" hosting provider ဆိုသည်မှာ အဘယ်နည်း။

ရိုးရိုးရှင်းရှင်း ပြောရမည်ဆိုလျှင် BPH ဆိုသည်မှာ ဆိုင်ဘာ ရာဇဝတ်သားများအား အွန်လိုင်းကမ္ဘာတွင် နေရာရရှိ ရေး သို့မဟုတ် အပြင်လောကတွင် အလုပ်လုပ်နိုင်ရန် အခြေခံ အဆောက်အဦး ရရှိရေးအတွက် လုပ်ဆောင်ပေးသည့် သူများ ဖြစ်ပါသည်။ BHP များသည် အချို့သော အင်တာနက်၏ အခြေခံ အဆောက်အဦးဆိုင်ရာ ဝန်ဆောင်မှုပေး ကာ (ဆိုင်ဘာ ရာဇဝတ်သားများအပါအဝင်) မသမာသည့် သူများအား အွန်လိုင်းပေါ်တွင် မကောင်းသည့် အရာများကို ထုတ်ဝေနိုင်ရန်နှင့် အင်တာနက်အား ထိန်းချုပ်လည်ပတ်ခြင်းများကို လုပ်ကိုင်နိုင်ရန် ဝန်ဆောင်မှုပေးထားပါသည်။

“ကျည်ကာ bulletproof" ဆိုသည်မှာ ဈေးကွက်မြှင့်တင်ရေး အသုံးအနှုန်းတစ်ခုမျှသာ ဖြစ်ပါသည်။ အမှန်မှာ ထို ဝန်ဆောင်မှုများသည် အခြေခံအဆောက်အဦး ဝန်ဆောင်မှုပေးသည့် အခြားဝန်ဆောင်မှုများကဲ့သို့ပင် ပျက်တတ်သည့် ဝန်ဆောင်မှုများ ဖြစ်ပါသည်။ သို့သော် BPH provider များသည် ဥပဒေအားလိုက်နာရန် ငြင်းဆိုသကဲ့သို့ တင်ထားသ ည့် တချို့သော အကြောင်းအရာအား ဖယ်ရှားရန် တောင်းဆိုသည့်အခါ ငြင်းဆိုခြင်းနှင့် စော်ကားခံရသူဖက်မှ တိုင်တန်း မှုများအား လျစ်လျူရှုခြင်းအပြင် subscriber request notice များကိုလည်း လစ်လျူရှုမှုများ လုပ်လေ့ရှိပါသည်။ ဆိုလိုသည်မှာ ဆိုင်ဘာရာဇဝတ်သားများသည် ဆက်သွယ်မှုလုပ်နိုင်သည်၊ တရားမဝင် ဖိုရမ်များနှင့် တရားမဝင် ဝဘ် ဆိုက်များလည်ပတ်စေပြီး ဆိုင်ဘာအရင်းအမြစ်အား တိုက်ခိုက်ပြီး အချက်အလက်များ ခိုးယူနိုင်သည့် malware များ နှင့် ဖျားယောင်းသွေးဆောင်မှုလုပ်သည့် အရာများအား လည်ပတ်စေနိုင်သည့်အပြင် ဥပဒေ စိုးမိုးရေးသမားများနှင့် အခြားသူများ၏ ဖိအားပေးမှုကြောင့် ၎င်းတို့၏ လည်ပတ်မှုကို ရပ်တန့်သွားစေနိုင်သော်လည်း ကြောက်ရွံ့ခြင်း ကင်းမဲ့ စွာ ငွေမည်းကို ငွေဖြူဖြစ်အောင် ဆောင်ရွက်ခြင်းတို့ ပြုလုပ်လျက်ရှိပါသည်။

BPH provider များသည် သိသိကြီးနှင့် ဆိုင်ဘာ ရာဇဝတ်မှု ဂေဟစနစ်တွင် ပူးပေါင်းပါဝင်မှုလုပ်ကာ ငွေရေးကြေးရေး ကို ရှေးရှုထားသည့် ဆိုင်ဘာရာဇဝတ်များကို ကျူးလွန်နိုင်ရန် လုပ်ဆောင်ပေးပါသည်။ ကြီးမားသည့် ဆိုင်ဘာ လုံခြုံရေးချိုးဖောက်ခံရမှုများကြောင့် ဩစတြေးလျနိုင်ငံ၏ အဖွဲ့အစည်းများနှင့် ဝယ်ယူသုံးစွဲသူများ ထိခိုက်နစ်နာရပြီး ထိုနစ်နာမှုများသည် ရာဇဝတ်သားများကို ကာကွယ်ပေးသည့် BPH provider များကြောင့် ဖြစ်ပေါ်ရခြင်း ဖြစ်ပါသည်။ ထိုကဲ့သို့ ဖြစ်ရပ်များ၏ နောက်ဆက်တွဲ ဆိုးကျိုးထဲတွင် ခြိမ်းခြောက်မှုလုပ်သည့် ransomware တိုက်ခိုက်မှုကြောင့်

တရားမဝင်ဈေးကွက်တွင် ကျည်ကာ bulletproof hosting provider ကို ကိုယ်စားပြုခြင်း

ထိခိုက်နစ်နာရခြင်း၊ အချက်အလက်များ ခိုးယူခံရခြင်းနှင့် ထိလွယ်ရှလွယ်သော သတင်းအချက်အလက်များ ခိုးယူခံရခြင်းတို့ ပါဝင်ပါသည်။

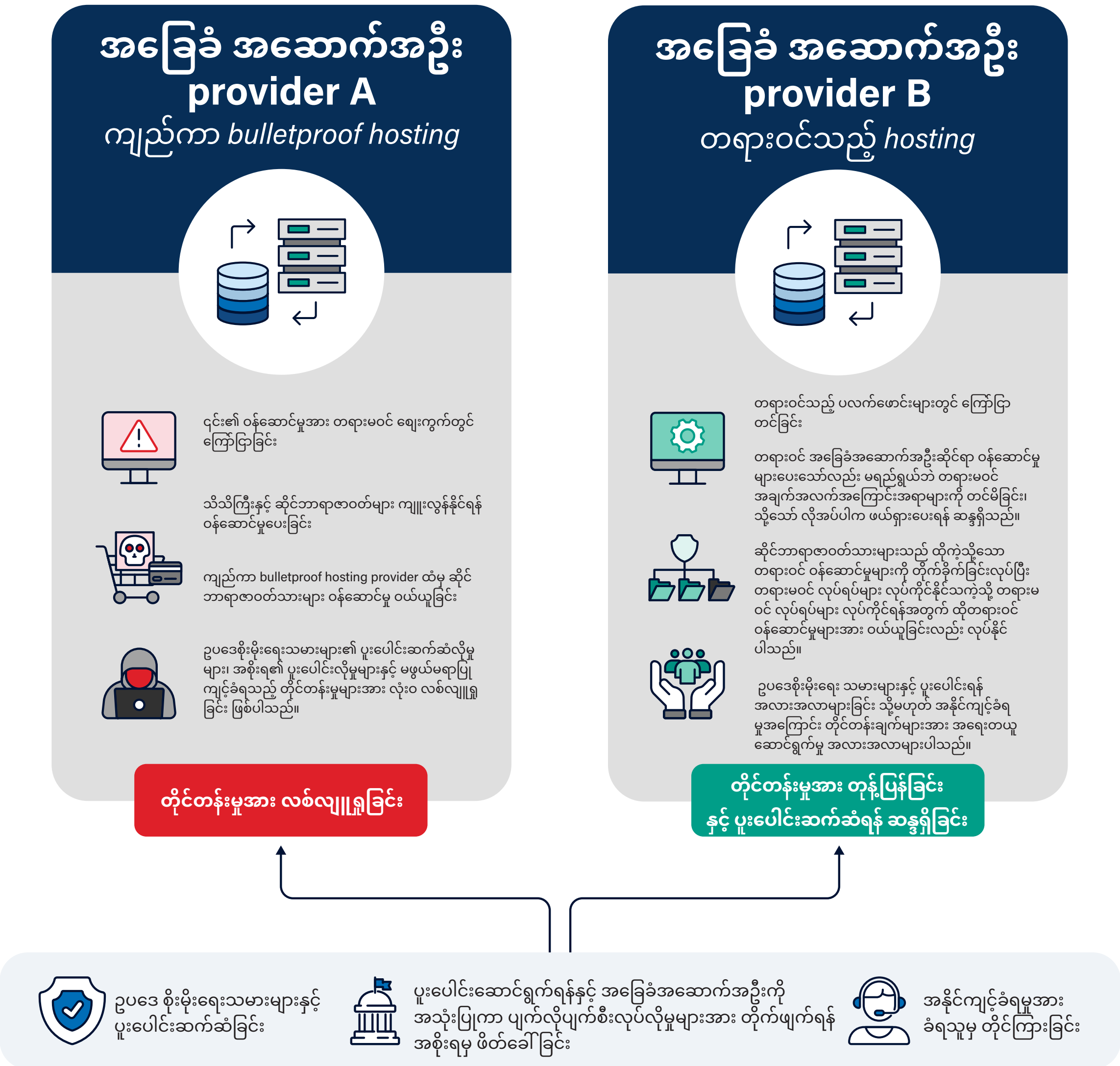
BPH provider က မည်ကဲ့သို့ အလုပ် လုပ်ဆောင်သနည်း။

BPH provider တစ်ခုနှင့်တစ်ခုအကြား စီးပွားရေးလုပ်ပုံလုပ်နည်းများ ကွာခြားကြပါသည်။ အများစု၏ လုပ်ကိုင်မှုနည်းလမ်းမှာ ဆိုင်ဘာရာဇဝတ်သားများအား IP လိပ်စာများကို ငှားရမ်းခြင်းဖြစ်ပြီး ရာဇဝတ်သားများ၏ တည်နေရာများ၊ မှတ်ပုံတင်များနှင့် လှုပ်ရှားမှုများကို လွယ်ကူစွာ နောက်ယောင်ခံ၍ မရအောင် ရှုတ်ထွေးသည့် ကွန်ရက်နည်းလမ်းများဖြင့် ကာကွယ်ပေးထားခြင်း ဖြစ်ပါသည်။ ကိစ္စအတော်များများအရ BPH provider များသည် ၎င်းတို့၏ IP လိပ်စာများနှင့်
servers များအား တရားဝင် hosting provider အပြင် ဒေတာစင်တာနှင့် အင်တာနက်ဝန်ဆောင်မှု ပေးသူများ (ISP) အဖြစ်လုပ်ကိုင်သူများထံ ပြန်လည်ရောင်းစားခြင်း သို့မဟုတ် ငှားရမ်းခြင်းများလုပ်ပါသည်။ ထိုကဲ့သို့သော

"တရားဝင်"provider များသည် သူတို့အနေဖြင့် သူတို့၏ အခြေခံအဆောက်အဦးများကို အသုံးပြု၍ တချို့ BPH provider များသည် 'တရားမဝင်' ဝန်ဆောင်မှုပေးသည့် ဆိုင်ဘာရာဇဝတ်သားများအား တဆင့် ငှားရမ်းထားသည်ကို သတိမမူမိတာမျိုး ဖြစ်နိုင်ပါသည်။

BPH provider များသည် ၎င်းတို့၏ ဝန်ဆောင်မှုကို ဝယ်ယူသုံးစွဲသည့် သူများမှာ မည်သူမည်ဝါဖြစ်ကြောင်း မသိနိုင်အောင် ၎င်းတို့၏ ကွန်ရက်နှင့် စနစ်များအား ကောင်းမွန်စွာ မွန်းမံလုပ်ဆောင်ထားပါသည်။ ဥပမာ - ၎င်းတို့၏ ဝန်ဆောင်မှုကို အသုံးပြုသူများ၏ internet facing identifiers associated များဖြစ်သည့် IP လိပ်စာများနှင့် ဒိုမိန်းနာမည်များအား မကြာခဏ အပြောင်းအလဲများ ပြုလုပ်ပေးခြင်း ဖြစ်ပါသည်။ ထိုကဲ့သို့သော လုပ်ဆောင်မှုများသည် ကာကွယ်သူများနှင့် စုံစမ်းသူများအတွက် ဖြစ်ရပ်တစ်ခုအား IP လိပ်စာတစ်ခုနှစ် ချိတ်မိအောင် ကြိုးစားလုပ်ဆောင်ရာတွင် ခက်ခဲစေပါသည်။ ဒါ့အပြင် BPH provider များသည် ဆိုင်ဘာရာဇဝတ်မှုကို မျက်ကွက်ပြုသည့် နိုင်ငံများတွင် ရှိသည့် အခြေခံအဆောက်အဦးများအား အသုံးပြုလေ့ရှိပြီး တရားဝင် စုံစမ်းစစ်ဆေးမှုများနှင့် မသမာသည့် ဆိုင်ဘာလှုပ်ရှားမှုများ မလုပ်နိုင်ရန် ကာကွယ်ပေးသော စနစ် မရှိသည့် နေရာ သို့မဟုတ် ထိုလုပ်ရပ်များအား သက်ညာသည့် နိုင်ငံများတွင် ထားရှိကာ လှုပ်ရှားလေ့ရှိပါသည်။

ကျည်ကာ bulletproof hosting provider သည် အခြားသော တရားဝင် အခြေခံအဆောက်အဦး ဝန်ဆောင်မှုပေးသည့် provider များနှင့် မည်ကဲ့သို့ ကွာခြားမှု ရှိသနည်း ။



BPH provider များအား ပစ်မှတ်ထားခြင်းအားဖြင့် ဆိုင်ဘာ ရာဇာဝတ်မှု ခြိမ်းခြောက်မှုအပေါ် ဘယ်လို သက်ရောက်နိုင်သနည်း ။

BPH provider များသည် ရာထောင်နှင့်ချီသော ဆိုင်ဘာ ရာဇာဝတ်မှုများ မလုပ်နိုင်ရန် လုပ်ဆောင်နိုင်စွမ်း ရှိပါသည်။ ဆိုင်ဘာရာဇာဝတ်သားများနှင့် အခြားသော မသမာသည့် ဆိုင်ဘာသမားများသည် ထိုဝန်ဆောင်မှုများကို အသုံးပြုကာ သူတို့၏ တရားမဝင် လုပ်ငန်းများကို လွယ်လွယ်ကူကူ လုပ်ကိုင်နေကြပါသည်၊ သူတို့၏ လုပ်ဆောင်ချက်များမှာ ခြေရာခံရန်ခက်ခဲပြီး၊ တင်ထားသည့် အရာများကို ဖျက်ပေးရန် တောင်းဆိုမှုများ သို့မဟုတ် မဖွယ်မရာ ပြုကျင့်ခံရ၍ ဖယ်ရှားပေးရန် တောင်းဆိုသည့် တိုင်တန်းမှုများအား တုန့်ပြန်ရန် မလိုဟု ယူဆကြပါသည်။

သို့သော် တရားရေးရာ ပုဂ္ဂိုလ်များ၊ အစိုးရအေဂျင်စီများနှင့် ပုဂ္ဂလိက ကဏ္ဍများ ပူးပေါင်းကာ ထိုကဲ့သို့ တရားမဝင်သည့် အခြေခံအဆောက်အဦးများကို လှူပ်ရှားခွင့်ပေးသော provider များအား ပစ်မှတ်ထားခြင်း အနှောင့်အယှက်ပေးခြင်းများ ပြုလုပ်လာကြပါသည်။ ထိုအထဲတွင် သိနှင့်ပြီးသား BPH provider များ၏ အင်တာနက် traffic ကို ပိတ်ချခြင်း စသည့် ကာကွယ်ရေးနည်းလမ်းများ သုံးကာ လုပ်ဆောင်လျက် ရှိပါသည်။ ထိုကဲသို့ လုပ်ရပ်များသည် ဩစတြေးလျကွန်ရက်နှင့် အခြား မိတ်ဖက်ကွန်ရက်များအတွက် ဆိုင်ဘာရာဇာဝတ်မှု ဖြစ်ပွားခြင်း အရေအတွက် နည်းပါးစေနိုင်ပါသည်။ ထိုအထဲတွင် "တရားဝင်" အခြေခံအဆောက်အဦး provider များနှင့် ISP တို့သည် သူတို့အနေဖြင့် သူတို့၏ အခြေခံအဆောက်အဦးများကို အသုံးပြု၍ တချို့ BPH provider များသည် ‘တရားမဝင်’ ဝန်ဆောင်မှုပေးသည့် ဆိုင်ဘာရာဇာဝတ်သားများအား တဆင့် ငှားရမ်းထားသည်ကို သတိမမူမိတာမျိုး ဖြစ်နိုင်ပါသည်။

ဆိုင်ဘာ ရာဇာဝတ်မှုအား ဝန်ဆောင်မှုတစ်ရပ်ကဲ့သို့ဆောင်ရွက်ခြင်း ဂေဟစနစ်တွင် BPH provider များသည် ဆိုင်ဘာ ရာဇာဝတ်မှုအား ဝန်ဆောင်မှုတစ်ရပ်ကဲ့သို့ လည်ပတ်သည့် တစ်ခုတည်းသော အခြေအခံ အဆောက်အဦး မဟုတ်ပေ။ ဤဝန်ဆောင်မှုများသည် ဆိုင်ဘာလုံခြုံရေး ကမ်ပိန်းများကို ပံ့ပိုးရာရောက်သကဲ့သို့ တရားဝင် စုံစမ်းစစ်ဆေးမှုနဲ့ တုန့်ပြန်မှုများအား တမင်တကာ ကြန့်ကြာစေကာ ဩစတြေးလျနိုင်ငံအား ဆိုင်ဘာရာဇာဝတ်မှု ခြိမ်းခြောက်ခံရမှုတည်တံ့စေသလို ဖြစ်စေပါသည်၊ BPH provider များအား အရေးယူခြင်းအားဖြင့် ၎င်းတို့၏ ပျော့ကွက်များနှင့် ၎င်းတို့၏ ဝန်ဆောင်မှုများကို အသုံးပြုသည့် မသမာသည့် ဆိုင်ဘာသမားများ၏ ပျော့ကွက်ဟာကွက်များကို သိသာစေနိုင်ပါသည်။