National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

BND

Bundesamt für Verfassungsschutz

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

အကြံပြုချက်

BADBAZAAR နှင့် MOONSHINE: နည်းပညာဆိုင်ရာ စိစစ်ချက်နှင့် အန္တရာယ် လျော့ချခြင်း

ဇူလိုင် ၂၀၂၁

BADBAZAAR နှင့် MOONSHINE: နည်းပညာဆိုင်ရာ စိစစ်ချက်နှင့် အန္တရာယ် လျော့ချခြင်း

အကျဉ်းချုပ်

UK နိုင်ငံမှ ဆိုင်ဘာအဖွဲ့ချုပ် Cyber League ၏ ပံ့ပိုးမှုဖြင့် အမျိုးသားစင်တာ National Cyber Security Centre (NCSC UK) နှင့် အောက်ပါ နိုင်ငံတကာ ပါတနာများ ပူးပေါင်းကာ ဤအကြံပြုချက်အား ပူးပေါင်း ထုတ်ဝေခြင်း ဖြစ်ပါသည်။

- **ဆက်သွယ်ညွှန်ကြားရေးမှူးရုံး၏ အစိတ်အပိုင်းဖြစ်သည့် ဩစတြေးလျ ဆိုင်ဘာ လုံခြုံရေးစင်တာ The Australian Cyber Security Centre**
- **ဆက်သွယ်မှုဆိုင်ရာ လုံခြုံရေးဦးစီးဌာန၏ အစိတ်အပိုင်းဖြစ်သည့် ကနေဒါ ဆိုင်ဘာလုံခြုံရေးစင်တာ The Canadian Centre for Cyber Security**
- **ဂျာမန်နိုင်ငံ ဗဟို ထောက်လှမ်းရေး ဝန်ဆောင်မှုရုံး The German Federal Intelligence Service**
- **ဂျာမန်နိုင်ငံ ဖွဲ့စည်းအုပ်ချုပ်ပုံ အခြေခံ ဥပဒေ ကာကွယ်ရေး ဗဟိုရုံး The German Federal Office for the Protection of the Constitution**
- **အစိုးရ၏ ဆက်သွယ်မှုဆိုင်ရာ လုံခြုံရေးဗဟိုဌာန၏ အစိတ်အပိုင်းဖြစ်သည့် နယူးဇီလန်နိုင်ငံ ဆိုင်ဘာလုံခြုံရေးစင်တာ The New Zealand National Cyber Security Centre**
- **အမေရိကန် ဗဟိုထောက်လှမ်းရေး ဌာန The United States Federal Bureau of Investigation**
- **အမေရိကန်နိုင်ငံ အမျိုးသား လုံခြုံရေး အေဂျင်စီThe United States National Security Agency**

ဤအကြံပြုချက်သည် ထောက်လှမ်းရေး ဆော့ဖ်ဝဲ မျိုးကွဲနှစ်ခုဖြစ်သည့် BADBAZAAR နှင့် MOONSHINE တို့၏ ထောက်လှမ်းရေးဆိုင်ရာ ခြိမ်းခြောက်မှုအကြောင်းကို အချက်အလက်သစ်များနှင့် စုစည်းဖော်ပြထားခြင်းဖြစ်ကာ app store လုပ်ငန်းလုပ်ကိုင်သူများ၊ developer များနှင့် ဆိုရှယ်မီဒီယာ ကုမ္ပဏီများအနေဖြင့် ၎င်းတို့၏ ဝန်ဆောင်မှုကို ရယူသူများ၏ လုံခြုံဘေးကင်းရေးများ ဆောင်ရွက်ရာတွင် အထောက်အကူပြုရန် ထုတ်ဝေခြင်းဖြစ်သည်။

ဤအကြံပြုချက်နှင့်အတူ malware တိုက်ခိုက်မှုများ ခံရသည့်သူများအတွက် အကြံပြုချက်လည်း ထုတ်ဝေထားပါသည်။

ဤစာစောင်သည် NCSE ၏ spywareခက်ဆစ်အဓိပ္ပာယ် ဖွင့်ဆိုချက်များကို အသုံးပြုထားပါသည်- "malware သည် မသမာသည့် ဆော့ဖ်ဝဲ တစ်မျိုးဖြစ်ကာ အသုံးပြုသူ၏ ခွင့်ပြုချက်မပါပဲ စက်ထဲတွင် ထိုဆော့ဖ်ဝဲကို ထည့်သွင်းကာ အချက်အလက်များ စုဆောင်းပြီး အခြားသူကို ထိုအချက်အလက်များ ပို့ဆောင်သည့် အရာဖြစ်သည်။"

ဖြစ်ရပ်မှန် နမူနာ ၁ - MOONSHINE

MOONSHINEသည် Android spyware တစ်ခုဖြစ်ပြီး တိဘက်အုပ်စုများကို ပစ်မှတ်ထားသည့် ထောက်လှမ်းရေး ဆော့ဖ်ဝဲဖြစ်ကြောင်း ၂၀၁၉ ခုနှစ်တွင် Citizen Lab မှ ဖော်ထုတ်ခဲ့သည့် spyware ဖြစ်ပါသည်။ MOONSHINE သည် တရားဝင်သည့် app တစ်ခုလို ဟန်ဆောင်ကာ ၎င်းပစ်မှတ်ထားလိုသည့် သူများကို ထို app ကို ထည့်သွင်းအောင် လုပ်ဆောင်ခြင်း ဖြစ်ပါသည်။ ထို app ကို တယ်လီဂရမ် ချန်နယ်များနှင့် WhatsApp တို့မှတစ်ဆင့် လင့်ခ်များလို ဖြန့်ချိမှုဝေမှု ပြုလုပ်ခဲ့ပါသည်။

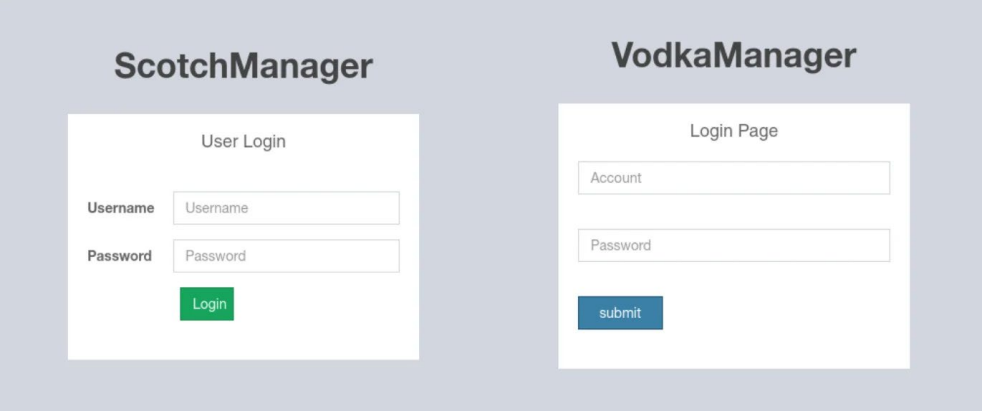
NCSC ၏ MOONSHINEသုတေသနအရ အောက်ပါအတိုင်း ဖော်ပြထားပါသည် -

- MOONSHINE သည် ပထမဆုံးအကြိမ် အစီရင်ခံသည့်အချိန်မှစ၍ အပြောင်းအလဲများ ပြုလုပ်ထားသော နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်ကို အသုံးပြုထားကြောင်း တွေ့ရှိရပါသည်။
- ထိုနည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်သည် ကျယ်ပြန့်သော ထောက်လှမ်းရေး အစွမ်းအစရှိကြောင်း တွေ့ရပြီး ထိုအထဲတွင် စက်ပစ္စည်းအတွင်းက ဖိုင်များကို ထုတ်ယူခြင်း၊ အသံများကို live ဖမ်းယူခြင်းနှင့် ဖန်သားမျက်နှာပြင်ကိုလည်း record လုပ်ထားနိုင်စွမ်း ရှိပါသည်။
- virtual နည်းဖြင့် host လုပ်ထားသည့် MOONSHINE ၏ နည်းပညာစီမံခန့်ခွဲရေး မျက်နှာပြင်အချို့ကို တွေ့ရှိထားပါသည်။ ထိုမျက်နှာပြင်များသည် UPSEC နှင့် ချိတ်ဆက်မှုရှိသည့် login panel များနှင့် အခြေခံအဆောက်အဦးဆိုင်ရာတွင် တစ်ခုနှင့်တစ်ခု ထပ်နေသည်ဟု Intelligence Online မှ'Sichuan Dianke Network Security Technology Co., Ltd.' အား ကိုးကားပြီး ဖော်ပြထားပါသည်။

နည်းပညာ စီမံခန့်ခွဲရေး မျက်နှာပြင်

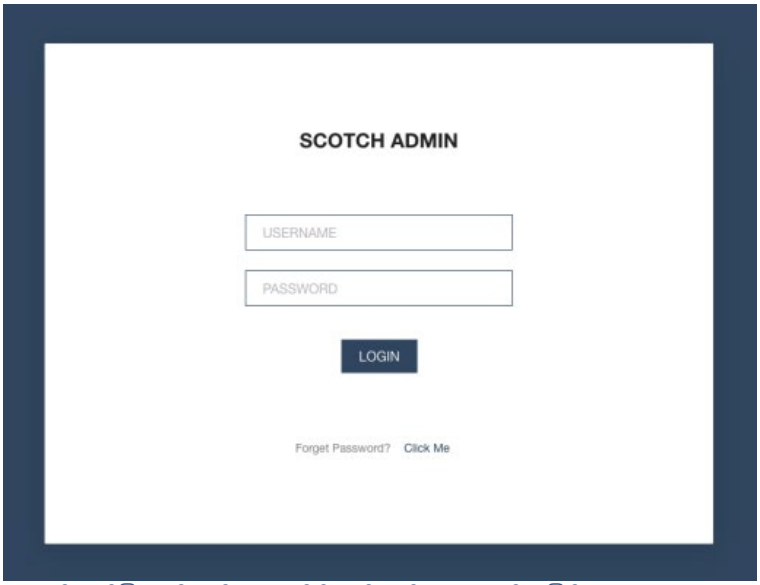
ယခင်က ဖော်ပြချက်အရMOONSHINE သည် နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်ကို ပြောင်းလဲထားပြီး တိုးတက်ရေးများ လုပ်ဆောင်နေကြောင်း ဖော်ပြထားပါသည်။

၎င်း၏ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်၏ ပထမဆုံး နမူနာကို ၂၀၁၉ ခုနှစ်တွင် ထုတ်ဝေသည့် Citizen Lab ၏ အစီရင်ခံစာတွင် ဖော်ပြထားပါသည်။



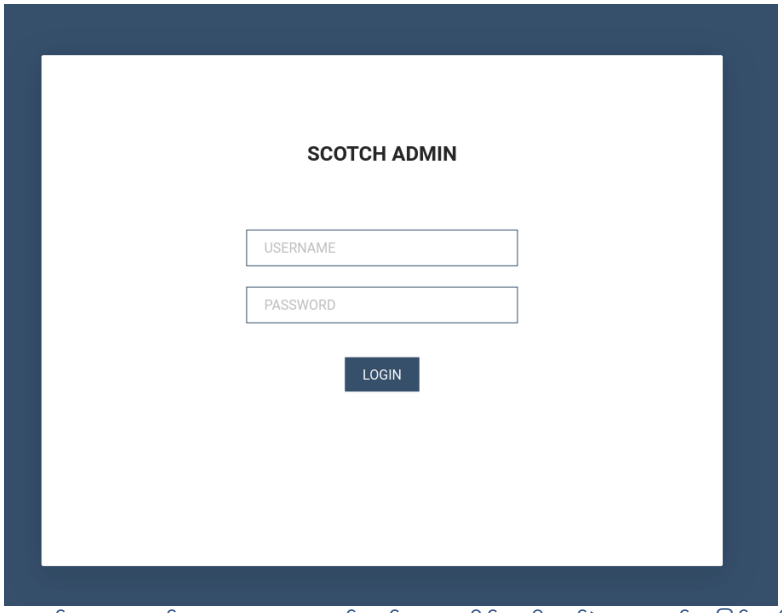
ပုံ ၁- ၂၀၁၉ ခုနှစ် အစောပိုင်းတွင် ထုတ်ဝေသည့် Citizen Lab ၏ အစီရင်ခံစာတွင် ဖော်ပြထားသည့် MOONSHINEနည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်မှာ 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits' ဖြစ်သည်။

၂၀၂၂ ခုနှစ် အစောပိုင်းတွင် Lookout မှ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်အား အောက်ပါကဲ့သို့ ၎င်း၏ မျက်နှာပြင်အား (ပုံ၁)-ပြန်လည်ပြင်ဆင်ထားကြောင်း ဖော်ပြထားပါသည်။



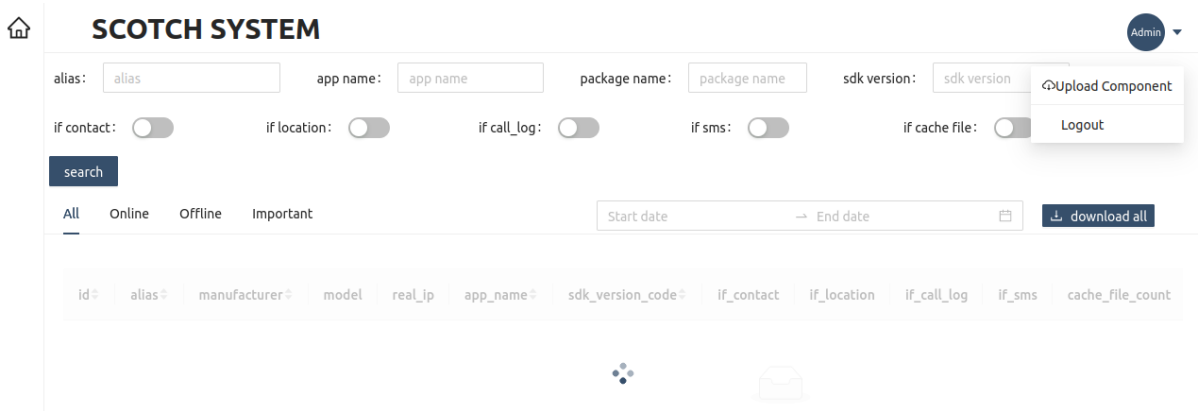
ပုံ ၂: Lookout ၏ အစီရင်ခံစာတွင် ဖော်ပြသည့် နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင် 2022 report 'MOONSHINE: တရုတ်နိုင်ငံမှ APT POISON CARP သည် တိဘက်နှင့် ဝိဂါများအား ပစ်မှတ်ထားသည့် ပြောင်းလဲတိုးတက်နေသည့် Android ထောက်လှမ်းရေး စက်ပစ္စည်းများကို တီထွင်ထားသည်။

၂၀၂၃ ခုနှစ် ဩဂုတ်လတွင် MOONSHINE ၏ အမိန့်ပေးခြင်းနှင့် ထိန်းချုပ်ခြင်း (C2)၏ scan တွင် ၂၀၂၂ ခုနှစ်မှ မျက်နှာပြင်နှင့် ဆင်တူကြောင်း ပြသထားသော်လည်း ပုံ ၂ တွင် ပါဝင်သည့် **'Forget Password'** လုပ်ဆောင်ချက်ပါဝင်ခြင်း မရှိတော့ကြောင်း ပြသထားပါတယ်။



ပုံ ၃: ၂၀၂၃ ခုနှစ် ဩဂုတ်လတွင် တွေ့ရသည့် MOONSHINE ၏ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်တွင် 'Forget Password' လုပ်ဆောင်ချက် မပါဝင်တော့ကြောင်း တွေ့ရပါသည်။

ထပ်မံစုံစမ်းမှုအရ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်တွင် panel အတွင်းမှ အကြောင်းအရာများကို ပြသထားကာ ထို panel တွင် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းအတွင်းမှ အသေးစိတ်အချက်အလက်များအား မည်ကဲ့သို့ သိုလှောင်ထားမည်ကို ဖော်ပြထားပါသည်။



ပုံ ၄: MOONSHINE ၏ နည်းပညာ စီမံခန့်ခွဲရေး မျက်နှာပြင်၏ login page နောက်ကွယ်တွင် ဖော်ပြထားသည့် ဝဘ်စာမျက်နှာ

Lookout ၏ လေ့လာမှုအရ **'score'** သည် တိုက်ခိုက်ခံရသူ၏ စက်ပစ္စည်းမှ MOONSHINE C2 server များသို့ ဖြတ်သန်းသွားသည်ကို တွေ့ရှိရပါသည်။ 'Score' ၏ တန်ဖိုးသည် တိုက်ခိုက်ခံရသူ၏ စက်ပစ္စည်းမှ မသမာသည့် လုပ်ရပ်များအား မည်မျှလောက် ခွင့်ပြုထားသည့်အပေါ် မူတည်ပါသည်။

စာတိုင်တွင် စာမျက်နှာထဲမှ 'if_contact'၊ 'if_location'၊ 'if_call_log' နှင့် 'if_sms' တို့၏ ဖော်ပြချက်အရ MOONSHINE samples များသည် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်း၏ အချက်အလက်များအားလုံးကို ရရှိနိုင်သည့် စွမ်းရည်မရှိကြောင်း တွေ့ရပါသည်။ ဤစာတိုင်များ၏ အသိတရားနှင့် 'score' များသည် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းများမှ C2 ကို ဖြတ်သန်းသွားခြင်းကို ကြည့်ခြင်းအားဖြင့် မသမာသူများသည် score ကို အသုံးပြုကာ မသမာသည့် malware မှ တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းမှ အချက်အလက် ခိုးယူနိုင်သည့် အတိုင်းအတာများအောင် ချိတ်ဆက်ပေးခြင်းဖြစ်ပြီး နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်ထဲ ဝင်ရောက်နေသူကို အချက်အလက်ပို့ဆောင်ခြင်း ဖြစ်ပါသည်။

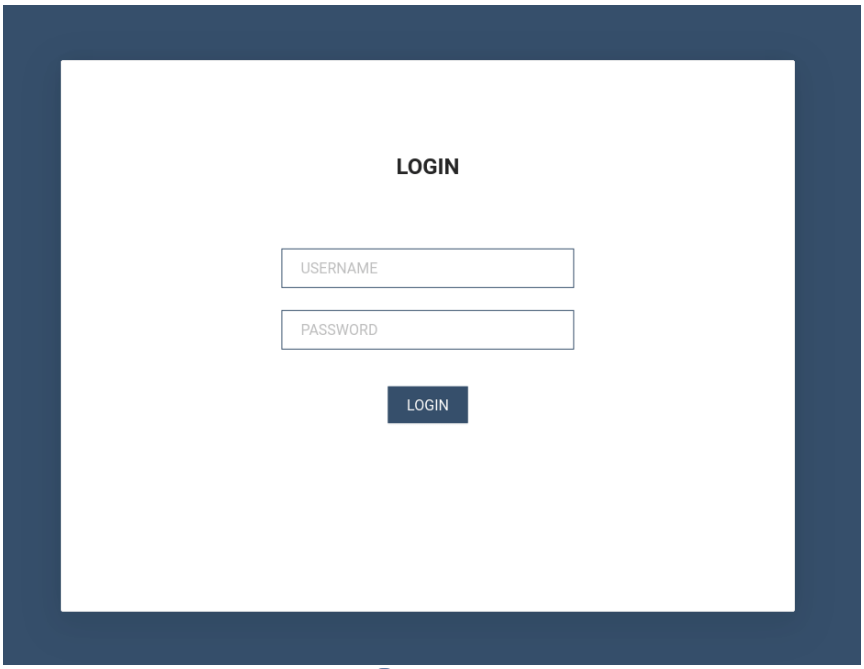
အထွေထွေအားဖြင့် app များသည် စက်ပစ္စည်းများ၏ အချက်အလက် စုဆောင်းမှုများ မလုပ်နိုင်ရန်အတွက် အကောင်းဆုံး ကာကွယ်နိုင်သည့် နည်းလမ်းမှာ app အား ဒေါင်းလုဒ် မလုပ်ခင်တွင် app တွင် မူမမှန်မှုများ ရှိမရှိနှင့် app ၏ ခွင့်ပြုချက်အား လေ့လာခြင်း ဖြစ်ပါသည်။ သို့သော် MOONSHINE sample တို့သည် app ၏ လုပ်ဆောင်မှုအတွက် လိုအပ်သည့် ခွင့်ပြုချက်များသာ တောင်းခံလေ့ရှိသည့်အတွက် သံသယ ဖြစ်ဖွယ်ရာ မရှိသလို ထင်ရတတ်ပါသည် သို့သော် ၎င်းသည် ထိုခွင့်ပြုချက်များအား အသုံးပြုကာ စက်ပစ္စည်းထဲမှာ အချက်အလက် စုဆောင်းခြင်းများ ပြုလုပ်နိုင်ပါသည်။

MOONSHINE တွင် Application Programming Interface (API) လည်းရှိသည်ကို ကြည့်ခြင်းအားဖြင့် ၎င်း၏ စွမ်းဆောင်နိုင်စွမ်းကို သိစေနိုင်ပါသည်။ အစောပိုင်းတွင် ရှိသည့် API စာရွက်စာတမ်းများတွင် Mandarin ဘာသာဖြင့် ရေးထားသော API နာမည်များ ပါဝင်ပါသည်။

Virtual hosts

MOONSHINE ၏ panel များကို ရှာကြည့်သည့်အခါတွင် host အတုများ အသုံးပြုထားသည်ကို တွေ့ရှိရပါသည်။ Hosting အတု Virtual hosting ဆိုသည်မှာ IP လိပ်စာတစ်ခုတည်းမှ တချိန်တည်းတွင် တစ်ခုထက် မနည်းသော ဝဘ်ဆိုက်များကို host လုပ်ထားခြင်း ဖြစ်ပါသည်။ ဤကဲ့သို့သော host အတု လုပ်ထားသည့် IP လိပ်စာနှင့် ဒိုမိန်း host များကို သိရှိထားသည့် malware samples များတွင် မတွေ့ရပါ။

ထို နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်သည် ကွာခြားမှုရှိပြီး စာမျက်နှာ၏ ခေါင်းစဉ်မှာ ယခင်က **SCOTCH ADMIN** အစား **LOGIN ဖြစ်ပါသည်။**



ပုံ ၅: MOONSHINE ၏ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်သည် SCOTCH ADMIN အစား LOGIN ဆိုသည့် နာမည် အသုံးပြုခြင်း

ထို့အပြင် panel တွင် ဖော်ပြထားသည့် အကြောင်းအရာသည် ပုံ ၄ နှင့် ကွာခြားပြီး ပုံ ၆ – ကဲ့သို့ ဖြစ်နေပါသည်။

ပုံ ၆: MOONSHINE ၏ နည်းပညာ စီမံခန့်ခွဲရေး မျက်နှာပြင်၏ login page နောက်ကွယ်တွင် ဖော်ပြထားသည့် ဝဘ်စာမျက်နှာ

ပုံ ၆ တွင် ဖော်ပြထားသည့် panel သည် ပုံ ၄ တွင် တွေ့ရသည့် ပုံစံနှင့် ကွာခြားသည်ကို တွေ့ရသည်။ Panel များ၏ အမူအကျင့်များထပ်တူမှု ဖြစ်နေခြင်းကို စာတိုင်၏ နာမည်များဖြစ်သော 'id'၊ 'manufacturer' နှင့် ဇယားတွင်ပါသည့် 'model' တို့တွင် တွေ့ရပါသည်။

MOONSHINE ၏ Host အတု များမှာ -

ဒိုမိန်း	IP လိပ်စာ
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

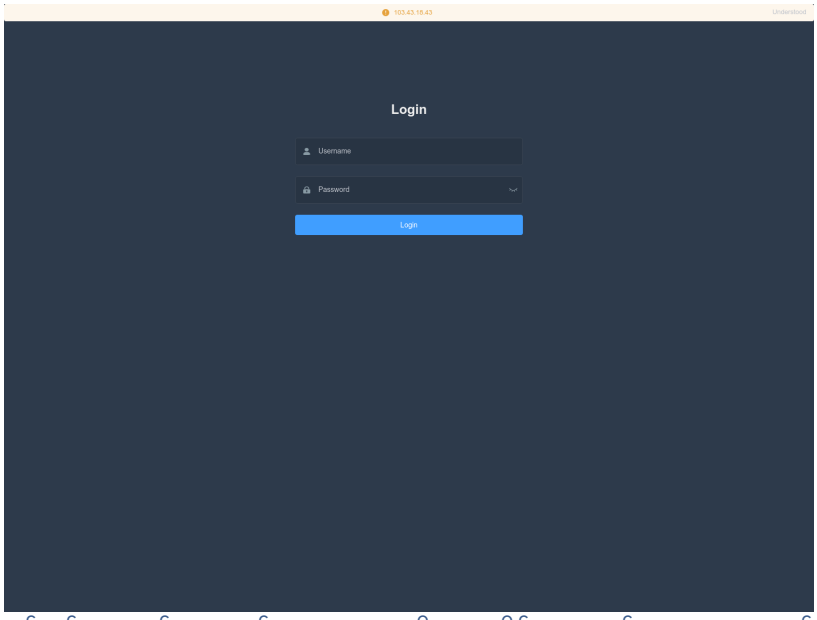
ထို ဒိုမိန်းများကို Trend Micro မှ စာရင်းပြုစုထားခြင်းဖြစ်ပြီး MOONSHINE ၏ အလွဲသုံးစား ကိရိယာများသည် browser ၏ ပျော့ကွက်ဟာကွက် အားနည်းချက်ကို အခွင့်ကောင်းယူကာ မိုဘိုင်းစက်ပစ္စည်းထဲတွင် မသမာသည့် malware များကို ထည့်သွင်းကာ အချက်အလက်များ စုဆောင်းခြင်း ဖြစ်ပါသည်။ ထိုကဲ့သို့ malware ကို Trend Micro က 'Dark Nimbus' ဟု နာမည်ပေးထားပါသည်။

ရှင်းလင်းချက်မှာ MOONSHINE ၏ နည်းပညာဆိုင်ရာ စီမံချက် မျက်နှာပြင်သည် MOONSHINE malware sample များ ဆက်သွယ်ထားသည့် အရာဖြစ်ပြီး ထိုမှတစ်ဆင့် တိုက်ခိုက်မှု ခံရသူ၏ အချက်အလက်များကို ရယူခြင်း ဖြစ်ပါသည်။ Trend Micro ၏ ဖော်ပြချက်အရ MOONSHINE ၏ အလွဲသုံးစား ကိရိယာသည် Dark Nimbus ဟုခေါ်သည့် malware ကို တိုက်ခိုက်ခံရသူများ၏ မိုဘိုင်းစက်ပစ္စည်းတွင် ထည့်သွင်းကာ broswer ၏ ပျော့ကွက် ဟာကွက် အားနည်းချက်များကို အခွင့်ကောင်းယူနိုင်စွမ်းရှိသည့် malware နှင့် ကွဲပြားသည်ဟု ဖော်ပြထားပါသည်။ ထို့အပြင် Dark Nimbus နှင့် MOONSHINE တို့သည် လုံးဝ မတူညီသော malware များ ဖြစ်ကြပါသည်။

သို့သော် MOONSHINE ၏ နည်းပညာဆိုင်ရာ စီမံခန့်ခွဲရေး မျက်နှာပြင်နှင့် MOONSHINE ၏ အလွဲသုံးစား ကိရိယာတို့ နှစ်မျိုးစလုံး၏ ကုဒ်မှာ တစ်ခုနှင့်တစ်ခု ထပ်နေသည့်အတွက် ပုံ ၃ နှင့် ၅ အပြင် ပုံ ၄ နှင့် ၆ တွင် ဖော်ပြထားသည့် အကြောင်းအရာ စာမျက်နှာတွင် ဖော်ပြသည့် login နည်းများတွင် ဆင်တူနေခြင်းကို တွေ့ရပါသည်။ နှစ်ခုစလုံး၏ ကုဒ်အရင်းအမြစ်တွင်လည်း 'webpackJsonpreact-scotchui' ပါဝင်နေပါသည်။

မသမာသူများသည် MOONSHINE ၏ အလွဲသုံးစား ကိရိယာကို URL လင့်ခ်များနှင့် ချိတ်ဆက်ကာ တိဘက်နှင့် ဝိဂါတို့နှင့် ဆက်စပ်သည့် ဗီဒီယိုများဆီ သွားရောက်မည့် လမ်းကြောင်းများဆီ ပို့ဆောင်ပြီး ထိုကဲ့သို့ လုပ်ရပ်သည် MOONSHINE ၏ ပစ်မှတ်နှင့် သွား၍ တစ်ထပ်တည်းကျနေသည်ကို တွေ့ရပါသည်။

MOONSHINE ၏ အလွဲသုံးစား ကိရိယာ၏ ဒိုမိန်းကို host လုပ်ထားသည့် IP လိပ်စာများတွင် 'VLiteUI' ဟု နာမည်ပေးထားသည့် login page ခေါင်းစဉ်ကို အသုံးပြုကြောင်း port 444 တွင် တွေ့နိုင်ပါသည်။ ထို စာမျက်နှာကို ကောင်းမွန်စွာ စောင့်ကြည့်မှု မလုပ်ခဲ့ပါ။ ၎င်းတည်ရှိသည့် IP လိပ်စာများတွင် မသမာသူများ၏ လုပ်ဆောင်ချက်နှင့် ချိတ်ဆက်နေသည့် အနေအထားများ ရှိနိုင်သည်ကို တွေ့ရပါသည်။



ပုံ ၇: 'VLiteUI' ဟု ခေါင်းစဉ်တပ်ထားသည့် HTML ၏ login panel ရှိရာ IP လိပ်စာများတွင် MOONSHINE ၏ အလွဲသုံးစား ကိရိယာများ ရှိကြောင်း တွေ့ရသည်။

Trend Micro မှ Dark Nimbus ကို အသေးစိတ် စိစစ်သည့်အခါတွင် ထို malware သည် စက်ပစ္စည်းမှ အချက်အလက်ပေါင်းများစွာကို စုဆောင်နိုင်သည့် စွမ်းရည်ရှိသည်ကို တွေ့ရပြီး ၎င်းသည် XMPP protocol ကို အသုံးပြုကာ C2 နှင့် ဆက်သွယ်မှု ရှိကြောင်း တွေ့ရှိရပါသည်။

Trend Micro မှ ထပ်မံ ဖော်ပြသည်မှာ Dark Nimbus ၏ ပုံစံ တချို့တွင် 'DKNS' ဆိုသည့် ပရိုဂမ်အချက်အလက်များ ပျံ့နှံ့နိုင်ခြင်းကို တွေ့ရှိခဲ့ပါသည်။

'**ansec[.]com**' (Trend Micro တွင်ဖော်ပြထားသည့် Dark Nimbus C2) သည် XMPP ဝန်ဆောင်မှုများ တွေ့ရပြီး DKNS ခေါင်းစဉ်ပါ ဝဘ်စာမျက်နှာများရှိသည့် အခြားသော IP လိပ်စာများတွင် တွေ့ရပါသည်။

- DKNS Android远程取证系统 (DKNS Android အဝေးထိန်း မှုခင်းဆေးပညာ စနစ်)
- DKNS云网侦控平台 (DKNS Cloud ကွန်ရက် စုံစမ်းစစ်ဆေးခြင်းနှင့် ထိန်းချုပ်ရေးပလက်ဖောင်း)
- DKNS 云网侦控平台 (DKNS Cloud ကွန်ရက် စုံစမ်းစစ်ဆေးခြင်းနှင့် ထိန်းချုပ်ရေး ပလက်ဖောင်း)
- DKNS远程控制侦查系统 (DKNS အဝေးထိန်း ထိန်းချုပ်စုံစမ်းစစ်ဆေးခြင်းစနစ်)

XMPP ဝန်ဆောင်မှုထဲတွင် '**ansec[.]com**' ပါဝင်သည့် တခြားသော IP address များ၏ ဝဘ်စာမျက်နှာများ၏ ခေါင်းစဉ်များမှာ အောက်ပါအတိုင်းဖြစ်သည် -

- UPSEC互联网控制指挥系统 (UPSEC အင်တာနက် ထိန်းချုပ်အမိန့်ပေးရေးစနစ်)
- UPSEC无线侦控系统 (UPSEC ကြိုးမဲ့ ထောက်လှမ်းရေးနှင့် ထိန်းချုပ်ရေးစနစ်)
- UPSEC重点人数据还原系统 (UPSEC အဓိကပုဂ္ဂိုလ် ဒေတာပြန်လည်ရယူခြင်းစနစ်)

Intelligence Online ၏ ဖော်ပြချက်အရ 'UPSEC' အနေဖြင့် HTML စာမျက်နှာများ၏ ခေါင်းစဉ်တွင် 'Sichuan Dianke Network Security Technology Co., Ltd'. အား ရည်ညွှန်းထားသည့်အကြောင်း ဖော်ပြထားသည်။

ဖြစ်ရပ်မှန် နမူနာ ၂ - BADBAZAAR

BADBAZAAR ဆိုသည်မှာ iOS နှင့် Andriod မျိုးကွဲ မိုဘိုင်းပစ္စည်းများကို တိုက်ခိုက်နိုင်သည့် malware ဖြစ်ပြီး ဝိဂါ၊ တိဘက်နှင့် ထိုင်ဝမ်အရေး လှုပ်ရှားသူ ပုဂ္ဂိုလ်အချို့ကို ပစ်မှတ်ထားသည့် ဆော့ဖ်ဝဲ ဖြစ်ပါသည်။ ထို ထောက်လှမ်ရေးဆော့ဖ်ဝဲသည် ဆိုရှယ်မီဒီယာနှင့် တရားဝင် app store များမှ တဆင့် ပျံ့နှံ့လျက် ရှိသည်။ မကြာခင်က ထုတ်ဝေသည့် Volexity ၏ ထုတ်ဖော်ချက်အရ BADBAZAAR ၏ မျိုးကွဲများကို ပြသထားပြီး ၎င်းသည် BadSolar၊BADBAZZAR နှင် BadSignal မတူညီကြောင်း ဖော်ပြထားပါသည်။ ထိုမျိုးကွဲ သုံးမျိုးစလုံး၏ လုပ်ဆောင်မှုသည် တစ်ခုနှင့်တစ်ခု ထပ်နေပြီး စက်ပစ္စည်းဆိုင်ရာ အချက်အလက်နှင့် operator ဆိုင်ရာ အချက်အလက်များ စုဆောင်းရေးအတွက် အသုံးပြုထားပါသည်။

NCSC ၏ MOONSHINEသုတေသနအရ အောက်ပါအတိုင်း ဖော်ပြထားပါသည် -

- C2 ဒိုမိန်းများကို ထပ်မံလေ့လာသောအခါ ၎င်းတို့သည် ယခင်က ထောက်လှမ်းရေးဆိုင်ရာ ခြိမ်းခြောက်မှုရှိသော ဒိုမိန်းများနှင့် ဆက်စပ်မှု ရှိကြောင်း တွေ့ရှိခဲ့ကြပါသည်။
- C2 server နှင့် malware များသည် မသမာမှု လုပ်ဆောင်သူများ၏ အခြေခံ အဆောက်အဦးနှင့် ဆက်စပ်နေသည့် host နာမည်များကို တွေ့ရှိခဲ့ရပါသည်။
- မသမာသူများသည် လူစိတ်ပညာကို အသုံးချပြီး ယုံကြည်မှု ရယူလှည့်ဖျားသည့်နည်းကို အသုံးပြုကာ တရားဝင် app store များတွင် ၎င်းတို့၏ malware ကို ပျံ့နှံ့အောင် ပြုလုပ်ကြပါသည်။

WHOIS clustering / ဒိုမိန်း ပွဲစား

'UJYJYUJ'

BADBAZAAR ဒိုမိန်းဖြစ်သည့် '**signalplus[.]org**' ၏ WHOIS အား အသေးစိတ် လေ့လာသည့်အခါတွင် **'State'** နေရာတွင် '**UJYJYUJ**' valueကို ပြသထားကြောင်း (ESET ၏ ဖော်ပြချက်အရ) တွေ့ရသည်။

အလားတူ value ရှိသည့် ဒိုမိန်းများအား ရှာဖွေကြည့်သည့်အခါ အောက်ပါ ဒိုမိန်းများအား တွေ့ခဲ့ရပါသည်
-

- thetubeplus[.]com
- tubevideoplus[.]org
- pmumail[.]com
- signalplus[.]org

(ပူးတွဲစာ က၊ ပုံ ၁ ကို ကြည့်ရန်)

signalplus[.]org, **tubevideoplus[.]org** နှင့် **thetubeplus[.]com** တို့သည် BADBAZAAR C2 ဒိုမိန်းများဖြစ်ကြောင်း တွေ့ရပြီး ESET ၏ ဖော်ပြချက်အရ ဒိုမိန်းခွဲ sub domain **mail.pmumail[.]com** မှာ FlyGram proxy server ဖြစ်ကြောင်း ဖော်ပြထားပါသည်။ FlyGram ဆိုသည်မှာ မသမာသည့် ဆိုင်ဘာသမားများက တီတွင်ထားသည့် BADBAZAAR app တစ်ခုဖြစ်ပါသည်။ (အခြားသော BADBAZAAR app များ၏ စာရင်းကို နောက်ဆက်တွဲ တွင် ဖော်ပြထားသည်)။

Keyboard walking values

မှတ်ပုံတင်ထားသည့် အခြားသော BADBAZAAR C2 ၏ ဒိုမိန်းများကို လေ့လာသည့်အခါတွင်လည်း အလားတူ keyboard walking လုပ်ဆောင်ပုံများ ရှိသည်ကို NCSC မှ တွေ့ရှိခဲ့ပါသည်။

ဥပမာ အောက်ပါ ဒိုမိန်းများအားလုံး၏ **'State'** နေရာတွင် **'REWR'** value များ တွေ့ခဲ့ရပါသည် -

- yumoftion[.]com
- fvbyavgyea[.]com
- jkiohreh[.]com
- pmstwocqn[.]com

(ပူးတွဲစာ က၊ ပုံ ၂ ကို ကြည့်ရန်)

‘FSDF’ state field vaule များပါဝင်သည့် ဒိုမိန်းများ

BADBAZAAR C2 ၏ တခြား ဒိုမိန်းတွင် ‘**FSDF**’ ‘**State**’ value ရှိသည်-

- tryhrwserf[.]com
- tibetone[.]org
- comeflxyr[.]com

(ပူးတွဲစာ က၊ ပုံ ၃ ကို ကြည့်ရန်)

Keyboard walking value များ၏ နောက်ခံအကြောင်း အစီရင်ခံမှု

BADBAZAAR ဒိုမိန်းများ၏ WHOIS မှတ်တမ်းတွင် အသုံးပြုသည့် keyboard walking value များကို လေ့လာသည့်အခါ တိဘက်လူမျိုးဆိုင်ရာ အဖွဲ့အစည်းများအား TA413 ဖြင့် ယခင်က ပစ်မှတ်ထားသည့် နောက်ခံများရှိသည်ကို တွေ့ရသည်။ Recorded Future ၏ လေ့လာချက်အရ မသမာသူများ ထိန်းချုပ်ထားသည့် ဒိုမိန်းများသည် တိဘက်အဖွဲ့အစည်းများကို ပျက်ရယ်ပြုခြင်းနှင့် မှတ်ပုံတင်ထားသည့် အဖွဲ့၏**“asfasf”** value ကို အသုံးပြုထားကြောင်း တွေ့ရပါသည်။

clublogs[.]com

Lookout မှ ရရှိထားသည့် BADBAZAAR samples ထဲတွင် C2 ဒိုမိန်းအဖြစ် **‘xle.clublogs[.]com’ ပါဝင်သည်ကို တွေ့ရသည်။** မူလ ဒိုမိန်း **‘clublogs[.]com’** ကို IP လိပ်စာ ‘**95.179.210[.]85**’ မှ host လုပ်ခဲ့သည်ကို တွေ့ရပြီး subject နှင့် issuer ရှိသည့်‘**CN=WIN-50QO3EIRQVP**’ တွင် SSL certificate ရှိကြောင်း တွေ့ရသည်။ ဤ value သည် BADBAZAAR samplesတွင် တွေ့ရသည့် SSL certificate များနှင့် ဆင်တူနေသည်ကို တွေ့ရပြီး ၎င်းတို့သည် ဆက်သွယ်ရေး အထောက်အထားများ ကြားဖြတ်သိခြင်းမျိုး မဖြစ်အောင် ရှောင်ရှားသည့်အနေဖြင့် SSL pinning ကို အသုံးပြုထားခြင်း ဖြစ်သည်။

IP လိပ်စာ **95.179.210[.]85** ၏ host သမိုင်းကြောင်းကို လေ့လာသည့်အခါတွင် အောက်ပါ ဒိုမိန်းများနှင့် ဆက်စပ်မှုရှိကြောင်း တွေ့ရသည် -

- actuallys[.]com
- bre.myloughborough[.]com
- rewrwer[.]com
- www.voiceoftibet[.]net
- clublogs[.]com

(ပူးတွဲစာ က၊ ပုံ ၄ ကို ကြည့်ရန်)

www.voiceoftibet[.]net

‘**www.voiceoftibet[.]net**’ ဒိုမိန်းသည် TA413 အသုံးပြုသည့် TTP နှင့် ဆင်တူသည့် ‘Voice of Tibet’ ရေဒီယို ဌာနကဲ့သို့ ဟန်ဆောင်ထားဟန် ရှိပါသည်။

‘**rewrwer[.]com**’ ဒိုမိန်းသည် BADBAZAAR ဒိုမိန်း၏ WHOIS မှတ်တမ်းတွင် တွေ့ရသည့် ‘**State**’ value ‘**REWR**’ နှင့် ဆင်တူနေသည်ကို တွေ့ရသည်။

‘**clublogs[.]com**’၊ ‘**rewrwer[.]com**’၊ ‘**voiceoftibet[.]net**’ နှင့် ‘**myloughborough[.]com**’ ဒိုမိန်း အားလုံးတို့သည် ‘**tplutalova@list[.]ru**’. ဆိုသည့် အီးမေးလ်လိပ်စာဖြင့် မှတ်ပုံတင်ထားပါသည်။

actuallys[.]com

‘**actuallys[.]com**’ အတွက် WHOIS မှတ်တမ်းတွင် ‘**tplutalova@list[.]ru**’ သည် နည်းပညာနှင့် အက်မင် အတွက် အီးမေးလ်ဖြစ်သော်လည်း မှတ်ပုံတင်သူ၏ အီးမေးလ်မှာ ‘**ivan_s81@mail[.]ru**’ ဖြစ်ပါသည်။

‘**actuallys[.]com**’ ဒိုမိန်း ၏ WHOIS အချက်အလက် သမိုင်းကြောင်းတွင် ‘**wangminghua6@gmail[.]com**’ အီးမေးလ်ဖြင့် ၂၀၁၆ ခုနှစ် ဖေဖော်ဝါရီလ ၂၄ ရက်အတွင် မှတ်ပုံတင်ထားကြောင်း တွေ့ရသည်။ ၂၀၁၆ ခုနှစ် မတ်လ ၁၁ ရက်နေ့တွင် ထိုအီးမေးလ်အား ‘**ivan_s81@mail.ru**’ သို့ ပြောင်းလဲခဲ့သော်လည်း မှတ်ပုံတင်သက်တမ်း ကုန်ဆုံးသည့် ရက်စွဲမှာ ယခင်ကဲ့သို့ အတူတူပင် ဖြစ်ပါသည်။

wangminghua6@gmail[.]com

‘wangminghua6@gmail[.]com’ ဆိုသည့် အီးမေးလ် လိပ်စာသည် ယခင်က ထောက်လှမ်းရေးဆိုင်ရာ ခြိမ်းခြောက်မှုရှိသည့် ဒိုမိန်းများအားမှတ်ပုံတင်ရာတွင် အသုံးပြုခဲ့ဖူးကြောင်း တွေ့ရှိရပါသည်။ ၂၀၁၅ ခုနှစ်တွင် Palo Alto ၏ တွေ့ရှိချက်အရ Cmstar malware အတွက် C2 ဒိုမိန်းများ မှတ်ပုံတင်သည့်အခါတွင် ထို အီးမေးလ်လိပ်စာကို အသုံးပြုခဲ့ကြောင်း တွေ့ရှိခဲ့ပါသည်။ ၂၀၁၄ ခုနှစ်တွင် APT3 မှ phishing ကမ်ပိန်း ပြုလုပ်ရန်အတွက် ဒိုမိန်းများ မှတ်ပုံတင်သည့်အခါတွင်လည်း ထို အီးမေးလ် လိပ်စာကို အသုံးပြုခဲ့ကြောင်း Mandiant မှ တွေ့ရှိခဲ့ပါသည်။ ၂၀၁၃ ခုနှစ်တွင် CrowdStrike မှ မှတ်ပုံတင်သည့် ဒိုမိန်းများတွင် Program Database (PDB) ပါဝင်သည့် malware dropper ၏ လမ်းကြောင်းထဲတွင် တရုတ်စာများ ပါဝင်နေသည်ကို တွေ့ခဲ့ရပါသည်။ ထိုအချက်များကို ကြည့်ခြင်းအားဖြင့် ၎င်းသည် တရုတ်စနစ်များနှင့် ဆက်စပ်မှု ရှိကြောင်း ယူဆနိုင်ပါသည်။

taoyujun@gmail[.]com

‘**hcjbtt[.]com**’ ဒိုမိန်းသည် ‘**taoyujun@gmail[.]com**’ အီးမေးလ်ဖြင့် မှတ်ပုံတင်ထားသော်လည်း ၎င်းအက်မင်၏ မှတ်ပုံတင် အီးမေးလ်လိပ်စာမှာ ‘**wangminghua6@gmail[.]com**’ ဖြစ်နေပါသည်။

‘**hcjbtt[.]com**’ ဒိုမိန်းနှင့် ပတ်သက်လျှင် မသမာသည့် လုပ်ဆောင်ချက်များ မတွေ့ရသော်လည်း ‘**taoyujun@gmail[.]com**’ အီးမေးလ် လိပ်စာသည် ယခင်က ထောက်လှမ်းရေးဆိုင်ရာ ခြိမ်းခြောက်မှု အစီရင်ခံစာတွင် ထိုလိပ်စာ ပါဝင်ပါသည်။ ၂၀၁၄ ခုနှစ်တွင် ဂျပန်အဖွဲ့အစည်းများကို ပစ်မှတ်ထားသည့် ‘**Cueisfry Trojan**’ sample များပါသည့် ဒိုမိန်းအတွက် မှတ်ပုံတင်ရာတွင် ထိုလိပ်စာအား အသုံးပြုခဲ့ကြောင်း Mandiant မှ တွေ့ရှိထားပါသည်။

၎င်း အီးမေးလ် လိပ်စာသည် ‘**iaea-international[.]org**’ ဒိုမိန်းအတွက် မှတ်ပုံတင်ရာတွင် အသုံးပြုမှု ရှိခဲ့ပြီး ထိုဒိုမိန်းသည် **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO) တွင် နိုင်ငံတကာ အာဏုမြူဗုံးအင်ဆိုင်ရာ အေဂျင်စီ** ကဲ့သို့ ဟန်ဆောင်ထားကာ ‘**idc-ctbto[.]org**’ ဒိုမိန်းသည် **နိုင်ငံတကာ ဒေတာစင်တာ** အဖြစ် ဟန်ဆောင်ထားကြောင်း တွေ့ရှိရပါသည်။

‘**iaea-international[.]org**’ ဒိုမိန်း၏ အစောပိုင်း Whois မှတ်တမ်းအတွက် မှတ်ပုံတင်သူ၏ အီးမေးလ်လိပ်စာမှာ ‘**wangminghua6@gmail[.]com**’ ဖြစ်ကြောင်း ဖော်ပြထားသည်။

udtglobals[.]com

‘**udtglobals[.]com**’ ဒိုမိန်းသည်လည်း ‘**wangminghua6@gmail[.]com**’ အား အက်မင်၏ အီးမေးလ်လိပ်စာအဖြစ် အသုံးပြုထားကာ ‘**ocean.nio@rediffmail[.]com**’ အတွက် အီးမေးလ်လိပ်စာအဖြစ်လည်း မှတ်ပုံတင်ထားပါသည်။ ဤဒိုမိန်းအတွက် အခြားသော WHOIS မှတ်တမ်းတွင် မှတ်ပုံတင်သူ၏ အီးမေးလ်လိပ်စာတူနေကြောင်း ပြသထားသော်လည်း အက်မင်ဖြစ်သူ၏ အီးမေးလ်လိပ်စာမှာ ‘**taoyujun@gmail[.]com**’ ဖြစ်ကြောင်း ဖော်ပြထားပါသည်။

‘**udtglobals[.]com**’ သည် ‘**UDT Global**’ ညီလာခံကဲ့သို ဟန်ဆောင်ပြီး ၎င်းသည် ရေအောက် ဆွေးနွေးရေးနှင့် လုံခြုံရေး ကုမ္ပဏီများအတွက် ကမ္ဘာလုံးဆိုင်ရာ ညီလာခံ ဖြစ်ပါသည်။ အသုံးပြုသူ နာမည် ‘**ocean.nio**’ ၏ လိပ်စာသည် နိုင်ငံတချို့တွင် ရှိသည့် **National Institute of Oceanography (NIO)** ကို တုပထားဟန်ရှိပါသည်။ ‘**Rediff**’ အီးမေးလ် ဝန်ဆောင်မှု (အိန္ဒိယတွင် အခြေစိုက်) ကို အသုံးပြုထားခြင်းသည် **Indian National Institute of Oceanography** ကို တုပထားခြင်း ဖြစ်နိုင်ပါသည်။

Djibdiplomatie[.]com

‘**djibdiplomatie[.]com**’ ဒိုမိန်းမှာ ဂျီဘူတီ Djibouti နိုင်ငံ သံတမန် ဝန်ဆောင်မှုကို တုပထားဟန်ရှိပြီး‘**utdglobals[.]com**’ **၏** WHOIS မှတ်တမ်းနှင့် တူညီမှု ရှိသည်ကို တွေ့ရပါသည်။ မှတ်တမ်း တစ်ခုတွင် မှတ်ပုံတင်သူမှာ ‘**ocean.nio@rediffmail[.]com**’ ဖြစ်ဟန်ရှိပြီး အက်မင်မှာ ‘**taoyujun@gmail[.]com**’ ဖြစ်ပြီး အခြားသော မှတ်တမ်းတွင် အက်မင်အဖြစ် ‘**wangminghua6@gmail[.]com**’ ဖြစ်ပြီး မှတ်ပုံတင်သူအဖြစ် ‘**ocean.nio@rediffmail[.]com**’ ဆိုသည့် အီးမေးလ်လိပ်စာကို အသုံးပြုထားကြောင်း တွေ့ရပါသည်။

ထိုဒိုမိန်း နှစ်ခုစလုံးသည် WHOIS မှတ်တမ်းတွေ ရှိသည့် keyboard walking type values များ ရှိနေသည်ကို တွေ့ရသည်။ ဥပမာ ‘**udtglobals[.]com**’ တွင် မှတ်ပုံတင်သည့် မြို့အဖြစ် ‘**ASDF**’ value ရှိပြီး ‘**djibdiplomatie[.]com**’ တွင် မှတ်ပုံတင်သူ၏ နာမည်အဖြစ် ‘**DAF DAGF**’ value ရှိကြောင်း ပြသထားပါသည်။ ထို value များသည် BADBAZAAR ဒိုမိန်းများတွင် တွေ့ရသည့် value များနှင့် ဆင်တူနေကြောင်း တွေ့ရပါသည်။

‘**wangminghua6@gmail[.]com**’ နှင့် ‘**taoyujun@gmail[.]com**’ အီးမေးလ်
လိပ်စာတို့သည် **global undersea defence event၊ Djibouti diplomacy services** နှင့်
International Atomic Energy Agency တို့ကို ဟန်ဆောင်ထားသည့် ဒိုမိန်းများအတွက်
အသုံးပြုသည့် WHOIS မှတ်တမ်းများတွင် တွေ့ရသကဲ့သို့ စစ်မှန်သော ဒိုမိန်းများအတွက် သုံးသည့်
WHOIS မှတ်တမ်းတွင်လည်း ရှိပါသည်။

အစစ်များကဲ့သို့ ဟန်ဆောင်သည့် ဒိုမိန်းနှင့် ဒိုမိန်းအစစ်များ ရောထွေးထားမှုကို ကြည့်ခြင်းအားဖြင့်
မသမာသည့် ဆိုင်ဘာသမားများ၏ လုပ်ငန်းများကို ကူညီပံ့ပိုးသည် အခြေခံအဆောက်အဦးများ ရှိပုံ
ရပါသည်။

‘**ocean.nio@rediffmail[.]com**’ အီမေးလ် လိပ်စာသည် အထက်ပါ ဖော်ပြသည့် ဟန်ဆောင်
ဒိုမိန်းများတွင်သာ တွေ့ရပါသည်။ ‘**ivan_s81@mail[.]ru**’ နှင့် ‘**tplutalova@list[.]ru**’ တို့မှာ
ဒိုမိန်းအနည်းငယ်ကိုသာ အသီးသီး မှတ်ပုံတင်ထားပြီး တခြို့သော ဒိုမိန်းများသည် BADBAZAAR ၏
အခြေခံ အဆောက်အဦးအတွက် host လုပ်ပေးထားပါသည်။ ဤအီးမေးလ် သုံးခုသည် မသမာသည့်
ဆိုင်ဘာဆိုင်ရာ လှုပ်ရှားသူများ၏ လုပ်ငန်းများနှင့် ပို၍ နီးစပ်မှု ရှိနိုင်ပါသည်။ အကြောင်းရင်းမှာ
၎င်းတို့သည် မသမာမှုများ
လုပ်သည့် လုပ်ငန်းများနှင့် ဆက်စပ်သည့် ဒိုမိန်းအရေအတွက်မှာ
‘**wangminghua6@gmail[.]com**’ နှင့် ‘**taoyujun@gmail[.]com**’. ကဲ့သို့သော
အီးမေးလ်များထက် စာလျှင် ပိုများနေသည့်အတွက် ဖြစ်ပါသည်။

(ပူးတွဲစာ က၊ ပုံ ၅ ကို ကြည့်ရန်)

အခြားသော မသမာသူများနှင့် ဆက်စပ်မှုများ

BADBAZAAR နှင့် ဆက်စပ်မှုရှိသည့် ‘**actuallys[.]com**’၊ ‘**clublogs[.]com**’၊
‘**myloughborough[.]com**’၊ ‘**rewrwer[.]com**’ နှင့် ‘**voiceoftibet[.]net**’ ကဲ့သို့သော
ဒိုမိန်းများ၏ သိသာထင်ရှားသော တူညီ လက္ခဏာများမှာ ၎င်းတို့ အားလုံးသည် ‘**255.255.255[.]254**’
တွင် 'parked' ထားသည့် eNom များနှင့် မှတ်ပုံတင်ထားခြင်း ဖြစ်ပါသည်။

မကြာခင်မှ ပြုလုပ်သည့် NCSC ၏ နောက်ဆက်တွဲ စုံစမ်းချက်အရ ထိုကဲ့သို့သော တူညီလက္ခဏာရှိသည့် အခြားသော ဒိုမိန်းများသည် ၂၀၁၉ ခုနှစ်တွင် **APT5** နှင့် ဆက်စပ်မှုရှိပြီး ၂၀၀၉ နှင့် ၂၀၁၁ တွင်**APT14** နှင့် ဆက်စပ်မှု ရှိကြောင်း တွေ့ရပါသည်။

APT5- နှင့် ဆက်စပ်သည့် ဒိုမိန်းများသည် '**taoyujun@gmail[.]com**' အီးမေးလ်ဖြင့် မှတ်ပုံတင်ထားသော ဒိုမိန်း၏ WHOIS များ နှင့် ဆက်စပ်နေကြောင်း တွေ့ရှိထားပါသည်။

APT14 နှင့် ဆက်စပ်သည့် ဒိုမိန်းများတွင် စာလုံးသုံးလုံးပါ ဒိုမိန်းခွဲများရှိပြီး ၎င်းတို့၏ မသမာသည့် တိုက်ခိုက်မှုအတွက် ပစ်မှတ်ထားသည့် သူများကို ထိုနေရာများတွင် စုစည်းထားဟန် ရှိပါသည်။ ၎င်း၏ ဥပမာ တစ်ခုမှာ BAE စနစ်အတွက် ပစ်မှတ်ထားရန် ရည်ရွယ်ထားသည့် '**bae.cisconline[.]net**' ကို '**Poison Ivy**' sample တွင် တွေ့ရှိရပါသည်။

ထိုကဲ့သို့သော အလားတူ လက္ခဏာများကို trojanised app နှင့် ဆက်စပ်မှု ရှိသည့် BADBAZAAR ၏ ဒိုမိန်းခွဲများတွင်လည်း တွေ့ရှိရပါသည်။

Application ခေါင်းစဉ်	C2 URL
Muslim Pro	**mpp**.pmstwocqn[.]com
Android အတွက် Video Player	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
ရေဒီယို အာဖဂန်နစ္စတန်	**afg**.collinformations[.]com
အခမဲ့ EN-UG အဘိဓာန်	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

ယခင်က APT5 အပြင် APT14 နှင့် ဆက်စပ်သည့် လှုပ်ရှားမှုများနှင့် eNom တွင် မှတ်ပုံတင်ထားသည့် အခြားသော ဒိုမိန်းများသည် '**255.255.255.254**' တွင် resolve လုပ်ထားသော်လည်း ၎င်းတို့သည် မသမာသည့် လုပ်ငန်းများနှင့် ဆက်စပ်မှု ရှိကြောင်း မသိရပါ။ ထို့ကြောင့် ဤကမ်ပိန်း၏ နောက်ကွယ်များတွင် ပါဝင်သည့် သူများ တူမတူ မသိရသကဲ့သို့ ဆက်စပ်မှု ရှိမရှိကိုလည်း သေချာ မသိနိုင်ပါ။

စက် နာမည်များ

BADBAZAAR C2s နှင့် sample များကို သေခြာ လေ့လာဆန်းစစ်သည့်အခါ SSL certificate များတွင် တွေ့ရသည့် 'Common Name' value ကို host နာမည်များအဖြစ် အသုံးပြုထားသည်ကို တွေ့ခဲ့ရပါသည်။ BADBAZAAR sample နှင့် အခြေခံအဆောက်အဦးတို့၏ host နာမည်များအား NCSC မှ စုံစမ်းလေ့လာသည့်အခါ ထို host နာမည်များကို IP လိပ်စာ တလွှားတွင် အသုံးပြုထားကြောင်း တွေ့ရှိရပါသည်။ ဤ IP လိပ်စာများကို BADBAZAAR sample များရှိရာ host ဒိုမိန်းများထဲတွင် တွေ့ရပါသည်။ Host နာမည်နှင့် ပတ်သက်သည့် အသေးစိတ် အကြောင်းအရာများ ဖော်ပြထားသည့် ကဏ္ဍသီးသန့်ရှိပြီး BADBAZAAR C2 ဒိုမိန်းများကို hostနာမည်များပါဝင်သည့် IP လိပ်စာများကိုလည်း ဖော်ပြထားပါသည်။

အားလုံးနည်းပါးတွင် host နာမည် value သည် ဖော်ပြထားသည့် မသမာသော ဒိုမိန်းနာမည်အတွက် IP resolution များပါသည့် certificate များနှင့် ထပ်တူဖြစ်နေကြောင်း တွေ့ရှိထားပြီး အနည်းငယ်သာ အထက်တွင် ဖော်ပြသည့်အတိုင်း မဟုတ်ကြောင်း တွေ့ရပါသည်။

WIN-EU0VLBL7TUJ

Host နာမည် '**WIN-EU0VLBL7TUJ**' ကို အောက်ပါ IP လိပ်စာများတွင် တွေ့နိုင်ပါသည် -

- '**116.203.53[.]21**' သည် BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့် '**uyapkfinder[.]com**' နှင့် '**thewestuniverse[.]com**' တို့ကို host လုပ်ခဲ့ပါသည်။

- **'95.216.169[.]27**' သည် BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့် '**adysfunction[.]com' နှင့် ဒိုမိန်းခွဲ** '**download.apkbazar[.]biz**' ကို host လုပ်ထားပြီး BADBAZAAR sample ကို ဒေါင်းလုဒ်လုပ်ရန် လင့်ခ်အဖြစ် ရပ်တည်ခဲ့ကြောင်း တွေ့ရပါသည်။

(ပူးတွဲစာ က၊ ပုံ ၆ ကို ကြည့်ရန်)

WIN-70E59JVOB9G

Host နာမည် '**WIN-70E59JVOB9G**' ကို အောက်ပါ IP လိပ်စာများတွင် တွေ့နိုင်ပါသည်။

- '**23.88.28[.]220**' သည် BADBAZAAR C2 ၏ ဒိုမိန်းခွဲများဖြစ်ကြသော **'aua.rondwsign[.]com'၊ 'nal.tokenmajorp[.]com'၊ 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**' နှင့် **'pls.rondwsign[.]com' တို့အား host ခဲ့ပါသည်။** Certificate ပါသည့် စက်၏ နာမည်ကို နောက်ဆုံးတွေ့ရချိန်နှင့် မသမာသည့် ဒိုမိန်း IP ဖြစ်ပေါ်လာချိန်ကို စတွေ့သည့်ကြားချိန်မှာ နှစ်ရက် ကြာခဲ့ပါသည်။

- '**23.88.28[.]221**' **သည်** BADBAZAAR နှင့် ဆက်စပ်သည့် '**bt.bhvghg[.]com**' ဒိုမိန်းခွဲကို host လုပ်ခဲ့သည်။

- **'23.88.28[.]222**' သည် BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့် '**tubevideoplus[.]org**' နှင့် '**cde.mpoxcases[.]com**' တို့ကို host လုပ်ခဲ့ပါသည်။

- '**65.21.92[.]67**' သည် BADBAZAAR C2 ဒိုမိန်းခွဲဖြစ်သည့် '**bat.androidupdated[.]net**' ကို host လုပ်ခဲ့သည်။ ၎င်းသည် DoubleAgent malware C2 ဖြစ်သည့် '**apps.androidupdated[.]net**' ဒိုမိန်းခွဲကိုလည်း host လုပ်ခဲ့ပါသည်။

- '**65.21.92[.]77**' သည် BADBAZAAR C2 ဒိုမိန်းခွဲများဖြစ်သော '**wyo.titeperformance[.]com**'၊ '**big.collinformations[.]com**' '**vpf.titeperformance[.]com**', '**eud.titeperformance[.]com**' နှင့် '**afg.collinformations[.]com**' တို့ကို host ခဲ့ပါသည်။

- '**65.108.192[.]134**' သည် BADBAZAAR C2 ဒိုမိန်းခွဲဖြစ်သည့် '**upd.whoscaller.net**'နှင့် '**ggl.whoscaller[.]net**' တို့ကို host ခဲ့ပါသည်။

- '**142.132.131[.]15**' သည် BADBAZAAR C2 ဒိုမိန်းခွဲဖြစ်သည့် '**bvn.lookincategory[.]com'** နှင့် '**edr.lookincategory[.]com' တို့ကို** host **ခဲ့ပါသည်။** Certificate ပါသည့် စက်၏ နာမည်ကို နောက်ဆုံးတွေ့ရချိန်နှင့် မသမာသည့် ဒိုမိန်း IP ဖြစ်ပေါ်လာချိန်ကို စတွေ့သည့်ကြားချိန်မှာ ဆယ့်တစ်ရက်ကြာခဲ့ပါသည်။

- **‘142.132.131[.]20’ သည် ဒိုမိန်းခွဲဖြစ်သည့် ‘son.onlinegamersgroup[.]com’** နှင့် **‘system.onlinegamersgroup[.]com’ တို့ကို** host **လုပ်ခဲ့ပါသည်၊ ၎င်းတို့ကို** BADBAZAAR C2 များအဖြစ် ယူဆရသည်မှာ BADBAZAAR နှင့် ဆက်စပ်မှုရှိသည့် SSL certificate များကို IP တစ်ခုတွင် ရှိနေချိန်အတွင်း ထို ဒိုမိန်းခွဲများကို host လုပ်ခဲ့သည့်အတွက် ဖြစ်ပါသည်။

- ‘**142.132.131[.]28’ သည်** BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့်‘**goldplusapp[.]net**’ နှင့် ဒိုမိန်းခွဲများဖြစ်သည့် ‘**who.goldplusapp[.]net**’ နှင့် ‘**cgf.goldplusapp[.]net**’ တို့ကို host လုပ်ခဲ့သည်။

- ‘**162.55.103[.]211**’ သည် BADBAZAAR C2 ဒိုမိန်းခွဲဖြစ်သည့် ‘**oha.alpinemap[.]net**’၊ ‘**aru.alpinemap[.]net’**၊ ‘**aso.alpinemap[.]net**’၊ ‘**afr.alpinemap[.]net**’ နှင့် ‘**aar.alpinemap[.]net**’ တို့ကို host ခဲ့ပါသည်။

- ‘**162.55.103[.]212**’ သည် BADBAZAAR C2 ဒိုမိန်းခွဲဖြစ်သော **‘pep.rondwsign[.]com’။ ‘ckp.jkiohreh[.]com’။ ‘aar.tokenmajorp[.]com’၊ ‘nal.tokenmajorp[.]com’၊ ‘pls.rondwsign[.]com’ နှင့် ‘aua.rondwsign[.]com’ တို့ကို** host **လုပ်ခဲ့ပါသည်။**

- ‘**195.154.47[.]99**’ သည် BADBAZAAR C2 ဒိုမိန်းခွဲ ဖြစ်သည့် ‘**ggl.whoscaller[.]net**’ နှင့် ‘**upd.whoscaller.net**’ တို့ကို host ခဲ့သည်။ Certificate ပါသည့် စက်၏ နာမည်ကို ပထမဆုံး တွေ့ရချိန်နှင့် မသမာသည့် ဒိုမိန်း IP ဖြစ်ပေါ်လာချိန်ကို နောက်ဆုံး တွေ့သည့် ကြာချိန်မှာ သုံးရက်ဖြစ်ပါသည်။

- ‘**195.154.60[.]3**’ သည် BADBAZAAR C2 ဒိုမိန်းခွဲ ‘**upd.whoscaller[.]net**’ ကို host ခဲ့သည်။ ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ သည် BADBAZAAR C2 ဒိုမိန်းခွဲ ‘**wyo.titeperformance[.]com**’၊ ‘**eud.titeperformance[.]com**’၊ ‘**vpf.titeperformance[.]com**’ နှင့် ‘**afg.collinformations[.]com**’ တို့ကို host ခဲ့သည်။

- ‘**212.129.21[.]168**’ သည် BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့် ‘**fre.lookincategory[.]com**’၊ ‘**tgr.lookincategory[.]com**’၊ ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ နှင့် ‘**bvn.lookincategory[.]com**’ တို့ကို host ခဲ့သည်။

(ပူးတွဲစာ က၊ ပုံ ၇ ကို ကြည့်ရန်)

WIN-50QO3EIRQVP

Hostနာမည် ‘**WIN-50QO3EIRQVP**’ ကို အောက်ပါ IP လိပ်စာများတွင် တွေ့ခဲ့ပါသည်။

- ‘**45.76.132[.]91**’ သည် ‘**yumoftion[.]com**’ နှင့် ‘**androidupdated[.]net**’ ဒိုမိန်းတို့ကို host ခဲ့သည်။ ထိုဒိုမိန်း နှစ်ခုစလုံးသည် BADBAZAAR နှင့် ဒိုမိန်းခွဲအဖြစ် ဆက်စပ်မှုရှိပြီး ‘**fow.yumoftion[.]com**’ နှင့် ‘**bat.androidupdated[.]net**’ တို့သည် BADBAZAAR C2 ဒိုမိန်းများ ဖြစ်ပါသည်။ ထို့အပြင် ဒိုမိန်းခွဲ ‘**apps.androidupdated[.]net**’ သည် DoubleAgent C2 ဒိုမိန်း ဖြစ်ပါသည်။ ထို့အပြင် ‘**pmstwocqn[.]com**’ ကိုလည်း host ခဲ့ပြီး ၎င်းသည် WHOIS မှတ်တမ်းမှတစ်ဆင့် BADBAZAAR နှင့် ဆက်စပ်မှု ရှိသည်။

- ‘**95.179.210[.]85**’ သည် ‘**clublogs[.]com**’ ကို host လုပ်ပြီး ‘**xle.clublogs[.]com**’ မှာ BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့်အပြင် BADBAZAAR နှင့် ဆက်စပ်သည့် ဒိုမိန်းများဖြစ်သော ‘**bre.myloughborough[.]com**’၊ ‘**img.rewrwer[.]com**’၊ '**www.voiceoftibet[.]net**' နှင့် ‘**actuallys[.]com**’ တို့ကို host ခဲ့ပါသည်။

- ‘**199.247.21[.]34**’ သည် ‘**titeperformance[.]com**’ နှင့် ‘**collinformations[.]com**’ တို့ကို host ခဲ့ပီး ၎င်း ဒိုမိန်းခွဲတို့သည် BADBAZAAR C2 ဒိုမိန်းများ ဖြစ်သည်။

- ‘**217.69.10[.]128**’ သည် BADBAZAAR C2 ဒိုမိန်းဖြစ်သည့် ‘**uyghurdict[.]com**’ ကို host ခဲ့သည်။

(ပူးတွဲစာ က၊ ပုံ ၈ ကို ကြည့်ရန်)

WMSvc-WIN-50QO3EIRQVP

Hostနာမည် ‘**WMSvc-WIN-50QO3EIRQVP**’ ကို အောက်ပါ IP လိပ်စာများတွင် တွေ့ခဲ့ပါသည် -

- **’78.46.185[.]251’ သည်** BADBAZAAR C2 ဒိုမိန်း **‘groupgram[.]org’ ကို** host **ခဲ့ပြီး မသမာသည့် ဆက်သွယ်မှုများ ရရန်အတွက်** port **၄၄၃၂ ကို အသုံးပြုခဲ့ကြောင်း** Volexity က ဖော်ပြခဲ့ပါသည်။

- **‘65.21.92[.]69’** နှင့် **‘163.172.205[.]207’ တို့သည် ဒိုမိန်း ‘widelygram[.]org’ ကို** host **ခဲ့ပြီး** BADBAZAAR C2 ဒိုမိန်းဟု ယူဆရဟန်ရှိပါသည်၊ အကြောင်းမှာ port ၄၄၃၂ ဖွင့်ထားသည့်အချိန် ထို ဒိုမိန်းနှစ်ခု၏ IP တွင် host လုပ်ထား သည့်အတွက် ဖြစ်ပါသည်။

- **‘163.172.198[.]206’** သည် ဒိုမိန်း **‘maxgram[.]org’ ကို host ပြီး** BADBAZAAR C2 ဒိုမိန်းဟု ယူဆရဟန်ရှိပါသည် အကြောင်းမှာ port ၄၄၃၂ ဖွင့်ထားသည့်အချိန် host လုပ်ထားသည့်အတွက် ဖြစ်ပါသည်။

(ပူးတွဲစာ က၊ ပုံ ၉ ကို ကြည့်ရန်)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Host နာမည် ‘**WMSvc-WIN-50QO3EIRQVP**’ နှင့် ‘**WIN-7LSBB9R0F1L**’ တို့အား အောက်ပါ IP လိပ်စာတွင် တွေ့ခဲ့ပါသည်။

- ‘**148.251.87[.]245**’ သည် BADBAZAAR C2 ဒိုမိန်းများဖြစ်သည့် ‘**flygram[.]org**’ နှင့် ‘**groupgram[.]org**’ တို့ကို host ခဲ့သည်။

(ပူးတွဲစာ က၊ ပုံ ၁၀ ကို ကြည့်ရန်)

WIN-N8H8S9BG2P0

Hostနာမည် '**WIN-N8H8S9BG2P0**' ကို အောက်ပါ IP လိပ်စာတွင် တွေ့ရသည် -

- '**148.251.87[.]247**' သည် BADBAZAAR C2 ဒိုမိန်းများဖြစ်သည့် '**omarwhatsapp[.]org**' နှင့် '**flygram[.]org**' တို့ကို host ခဲ့သည်။

(ပူးတွဲစာ က၊ ပုံ ၁၁ ကို ကြည့်ရန်)

WIN-I6VBN8MR92A

Hostနာမည် '**WIN-I6VBN8MR92A**' ကို အောက်ပါ IP လိပ်စာတွင် တွေ့ခဲ့သည် -

- '**148.251.87[.]197**' သည် BADBAZAAR C2 ဒိုမိန်း ဖြစ်သည့် '**tryhrwserf[.]com**' ကို host ခဲ့သည်။

(ပူးတွဲစာ က၊ ပုံ ၁၂ ကို ကြည့်ရန်)

ရရှိထားသည့် လုပ်ငန်းဆိုင်ရာ အချက်အလက်များအပေါ် အခြေခံကာ ဤစက်နာမည်များသည် အင်တာနက်ပေါ်တွင် ပုံနှိပ်လျက် ရှိသည်။ တချို့တို့ကို IP လိပ်စာ တချို့တို့တွင် တပြိုင်တည်း တွေ့ရပြီး ထိုအချက်ကို ကြည့်ခြင်းအားဖြင့် VM များသည် template ပုံစံ တစ်ခုကို အခြေခံကာ ပြုလုပ်ထားကြောင်း ပြသနေပါသည်။ တချို့သော host နာမည်များအတွက် ၎င်းတို့ ရှိနေသည့် IP လိပ်စာများသည် မသမာသည့် လုပ်ရပ်များနှင့် ဆက်စပ်မှု မရှိကြောင်းကိုလည်း သတိပြုရန် အရေးကြီးပါသည်။ Host နာမည်များကို အသုံးပြုခြင်းသည် မသမာသည့် လူများနှင့် မသက်ဆိုင်ကြောင်းလည်း ဖြစ်နိုင်ပါသည်။

သို့သော်၊ ဤစက်နာမည် တချို့တို့သည် BADBAZAAR C2 များကို host သည့် IP များတွင် ပုံနှိပ်သည့်အတွက် အခြေခံ အဆောက်အဦးရှိသည့် လုပ်ငန်းတစ်ခုမှ စက်များကို ပြုပြင်ကာ မသမာသူများ ဆိုင်ဘာဆိုင်ရာ လုပ်ငန်းများ လုပ်ကိုင်နိုင်ရန်အတွက် ကူညီခဲ့သည်ဟု ယူဆနိုင်ပါသည်။

ဆိုရှယ်မီဒီယာ တည်ရှိမှု

Volexity ၏ ဖော်ပြချက်အရ YouTube ဗီဒီယိုများ (မသမာသည့် အက်ပလီကေးရှင်းများကို အသုံးပြုရန် တိုက်တွန်းထားသည့် ကြော်ငြာဗီဒီယို) ကို မသမာသည့် ဆိုင်ဘာ သမားများက ဖန်တီးခဲ့တာ ဖြစ်ကြောင်း ဖော်ပြထားပါသည်။ ဤဗီဒီယိုများတွင် အက်ပလီကေးရှင်းများ တည်ဆောက်ရန်အတွက် သင်ကြားမှုများ ပြသထားပါသည်။

မသမာသူများနှင့် ဆက်စပ်သည့် YouTube ချန်နယ် နှစ်ခုကိုလည်း NCSC က သိရှိထားပါသည်။ '**@josephjoey3499**' ပါဝင်သည့် YouTube channel ၏ URL သည် '**Maxgram**' ကို promote လုပ်ထားဟန်ရှိပြီး '**@uyghurapks3096**' နှင့် မှတ်ပုံတင်ထားသော channel တွင် '**Uyghur APK Finder**' ကို အသုံးပြုမှု များအောင် လုပ်ဆောင်ထားပါသည်။

ထို့အပြင် '**Flygram**' နှင့် '**Signal Plus**' တို့ကို promote လုပ်ထားသည့် YouTube ဗီဒီယိုများအတွက် မသမာသူများမှ သိသာသည့် ဖုန်းနံပါတ်များကို အသုံးပြုထားကြောင်း တွေ့ရသည်။ '**Flygram**' video ၏ ၀:၃၆ စက္ကန့်တွင် ဖုန်းနံပါတ် '**+၁ (၅၇၀) ၃၇၈-၇၂၅၀**' ကို မြင်နိုင်ပြီး '**Signal Plus**' video တွင် ဖုန်းနံပါတ် '**+၁ (၂၆၇) ၂၉၈ ၄၂၅၉**' ကို ပြသထားပါသည်။

Volexity ၏ ဖော်ပြချက်အရ '**ignitetibet[.]net**' ဆိုက်သည် တိဘက်နှင့် ဆက်စပ်သည့် အကြောင်းအရာ Tibet-themed ကို အခြေခံသည့် သတင်းတု ဝဘ်ဆိုက်ဖြစ်ပြီး Telegram ချန်နယ်တွင် တွေ့ရှိချက်အရ ထိုဆိုက်ကို မသမာသူများက ဖန်တီးတင်ထားကြောင်း ဖော်ပြထားပါသည်။ '**choekyi.wangmo@ignitetibet[.]net**' ဆိုသည့် အီးမေးလ် လိပ်စာသည် '**tibetone.org**' တွင် မှတ်ချက်များ ရေးသားထားသည်ကို တွေ့ရပြီး ၎င်းသည် iOS မျိုးကွဲ BADBAZAAR အတွက် အသုံးပြုသည့် C2 ဝဘ်ဆိုက် စာမျက်နှာဖြစ်ကြောင်း Lookout က လူသိရှင်ကြား ဖော်ပြထားပါသည်။

ဤ အီးမေးလ် လိပ်စာသည် မသမာသူမှ ထိန်းချုပ်ထားသည့် အီးမေးလ်ဟု ယူဆရပြီး '**Choekyi Wangmo**' ၏ နာမည်ကို တုပ အသုံးပြုပုံ ရပါသည်။

လေ့လာဆန်းစစ်ချက်

BADBAZAAR နှင့် MOONSHINE တို့သည် လူစိတ်ဇေဒနှင့် ဆက်သွယ်မှုကို အသုံးချကာ မသမာသည့်နည်းဖြင့် အချက်အလက်ရယူခြင်း ဆိုရှယ်အင်ဂျင်နီယာနည်းလမ်းကို အသုံးပြုကာ ဝိဂါလူမျိုး၊ တိဘက်လူမျိုးနှင့် ထိုင်ဝမ်လူမျိုးတို့ကို ပစ်မှတ်ထားလေ့ရှိပြီး အဓိကအားဖြင့် -

- ဝိဂါလူမှုအသိုင်းအဝိုင်းများ စိတ်ဝင်စားနိုင်သည့် ဝိဂါဘာသာဖြင့် ပြုလုပ်ထားသည့် ကိုရမ် Quran app ကို တီထွင်ကာ တရားဝင် ဆော့ဖ်ဝဲများလို ဟန်ဆောင်ပြီး မသမာမှုများ လုပ်ဆောင်သည့် trojans app များဖြင့် ပစ်မှတ်ထားခြင်းများ
- ထိုမသာမှုများ လုပ်ဆောင်သည့် trojans app များကို တရားဝင် app store များပေါ်တွင် ထားရှိကာ စစ်မှန်သည့် app ဖြစ်ကြောင်း ထင်ယောင်ထင်မှားဖြစ်အောင် လုပ်ဆောင်ခြင်းနှင့် group chat များတွင် ၎င်းတို့ ပစ်မှတ်ထားသည့် လူမှုအသိုင်းအဝိုင်းတို့၏ ယုံကြည်မှုကို အလွဲသုံးစားလုပ်ခြင်း

BADBAZAAR နှင့် MOONSHINE တို့သည် တရုတ်အစိုးရအတွက် တန်ဖိုးရှိသည့် အချက်အလက်များကို စုဆောင်းပေးခြင်းမျိုးများ ပြုလုပ်ပါသည်။ BADBAZAAR နှင့် MOONSHINE တို့သည် ဝိဂါလူမျိုး၊ တိဘက်လူမျိုးနှင့် ထိုင်ဝမ်မှ တသီးပုဂ္ဂလများအား ပစ်မှတ်ထားသည်ကို သိရပြီး အခြားသော malware များသည် တရုတ်နိုင်ငံအတွင်းမှ အခြားသော လူနည်းစုများကို ပစ်မှတ်ထားကြောင်း သိရပါသည်။ တရုတ်နိုင်ငံ၏ တည်ငြိမ်မှုအား ခြိမ်းခြောက်နိုင်သည်ဟု ယူဆရသော တရုတ်နိုင်ငံပြည်တွင်းနှင့် ပြည်ပနိုင်ငံမှာ နေထိုင်သည့် အတူတကွ လက်မှတ်ရေးထိုးထားသည့် နိုင်ငံသားများသည် BADBAZAAR နှင့် MOONSHINE ကဲ့သို့သော မိုဘိုင်း malware တို့၏ တိုက်ခိုက်မှု အန္တရာယ်ကို ခံရဖို့ သေခြာသလောက် ရှိပါသည်။ ထိုလူများ၏ တည်နေရာ၊ အသံဖိုင်၊ ဓာတ်ပုံ စသည့် အချက်အလက်များကို ရရှိနိုင်သည့်အတွက် အနာဂတ်တွင် ထိုပစ်မှတ်ထား ခံရသူများ၏ လှုပ်ရှားမှု အချက်အလက်များအား အချိန်နှင့် တပြေးညီ ထောက်လှမ်းခြင်းများနှင့် နှောင့်ယှက်ခြင်းများ ပြုလုပ်နိုင်ရန် အခွင့်အလမ်း ရစေနိုင်ပါသည်။

MITRE ATT&CK®

ဤအစီရင်ခံစာသည် MITRE ATT&CK® ၏ မူဘောင်နှင့် တကမ္ဘာလုံးမှ ဗဟုသုတများဖြစ်သည့် ဖြစ်ရန်မှန်အတွေ့အကြုံကို အခြေခံပြီး ရရှိသည့် နည်းဗျူဟာနှင့် နည်းလမ်းများကို အခြေခံကာ စုစည်းတင်ပြထားခြင်း ဖြစ်ပါသည်။

နည်းဗျူဟာ	ID	နည်းလမ်း	လုပ်ပုံလုပ်နည်း
စူးစမ်းထောက်လှမ်းခြင်း	T1593.001	Open Websites/ Domains များ ရှာဖွေပါ - ဆိုရှယ် မီဒီယာ	မသမာသူများသည် ၎င်းတို့ ပစ်မှတ်ထားလိုသည့် အုပ်စုများရှိရာ အွန်လိုင်း group များနှင့် ဖိုရမ်များကို အသုံးချကာ ၎င်းတို့၏ malware များကို မျှဝေရန် လုပ်ဆောင်ပါသည်။
အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး	T1583.001	လိုအပ်သည့် အခြေခံ အဆောက်အဦး - ဒိုမိန်းများ	မသမာသူများသည် ၎င်းတို့၏ ကွပ်ကဲမှုနှင့် ထိန်းချုပ်ရေး server များအတွက် ဒိုမိန်းများကို မှတ်ပုံတင်ခြင်း
အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး	T1587.001	Develop Capabilities: Malware	တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan app များတွင် ထည့်သွင်းရန်အတွက် ပျက်လိုပျက်စီးပြုနိုင်သည့် ကုဒ်များကို တီထွင်ရေးသားခြင်း
အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး	T1608.001	အဆင့်အလိုက် စွမ်းရည်များ - Upload Malware	တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan apps များကို app store များအပါအဝင် အွန်လိုင် ပလက်ဖောင်းပေါ်တွင် တင်ထားခြင်း
အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး	T1585.001	အတည်တကျရှိသည့် အကောင့်များ - ဆိုရှယ် မီဒီယာ အကောင့်	မသမာသူများသည် malware များကို မျှဝေရန် သို့မဟုတ် ကြော်ငြာမှု လုပ်ရန်အတွက် ဝဘ်ဆိုက်နှင့် ဆိုရှယ်မီဒီယာများတွင် အကောင့်များဖွင့်ခြင်း
အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး	T1585.002	အတည်တကျရှိသည့် အကောင့်များ - အီးမေးလ် အကောင့်များ	မသမာသူများသည် ပုဂ္ဂလိက host နှင့် လုပ်ငန်းသုံး အီးမေးလ်အကောင့်များကို malware အား host လုပ်ရန်နှင့် မျှဝေရန်အတွက် အသုံးပြုခြင်း

ကနဦး ဝင်ရောက်ခြင်း	T1189	Drive-by Compromise	ကောင်းမွန်သည်ဟု ထင်ရသည့် app များထဲတွင် မသမာသည့် ဆော့ဖ်ဝဲများ၏ စာများကို ကွယ်ဝှက်ထားခြင်းနှင့် app store များပေါ်တွင် ထားရှိခြင်း
ကနဦး ဝင်ရောက်ခြင်း	T1566.003	အတုအယောင်လုပ်ကာ ခိုးယူခြင်း - ဝန်ဆောင်မှုမှတစ်ဆင့် အတုအယောင်လုပ်ကာ ခိုးယူခြင်း	မသမာသူများသည် တယ်လီဂရမ် အပါအဝင် ဆိုရှယ် မီဒီယာမှတစ်ဆင့် ၎င်းတို့ ပစ်မှတ်ထားသည့် အုပ်စုံထံ တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan apps များကို ပို့ဆောင်ခြင်း
အကောင်အထည်ဖော်ခြင်း	T1204.002	အသုံးပြုသူမှ အကောင်အထည်ဖော်ခြင်း- အန္တရာယ် ဖြစ်နိုင်သောဖိုင်	တိုက်ခိုက်ခံရသူများသည် payload ကို အကောင်အထည်ဖော်ရန်အတွက် တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan apps များကို ထည့်သွင်းရပါသည်။
လုံခြုံရေး စနစ်ကို ထိုးဖောက်ခြင်း	T1027.009	ရှုပ်ထွေးအောင် ပြုလုပ်ထားသည့် ဖိုင်များ သို့မဟုတ် အချက်အလက်များ - ကုဒ်များ မြှုပ်နှံထားသည့် Payloads	ကောင်းမွန်သည့် app များဟု ထင်ရသည့် app များအတွင်း မသမာသည့် payload များ ထည့်သွင်းခြင်း
လုံခြုံရေး စနစ်ကို ထိုးဖောက်ခြင်း	T1036.005	ဟန်ဆောင်လှည့်စားခြင်း - တရားဝင် နာမည် သို့မဟုတ် တည်နေရာနှင့် ဆင်တူခြင်း	တရားဝင်ဖိုင်များကဲ့သို့ ထင်ရသည့် Trojan ဖိုင်များသည် တရားဝင် app များကဲ့သို့ နာမည်၊ ပုံစံနှင့် လုပ်ပုံကိုင်ပုံ ဆင်တူမှု ရှိပါသည်။
လုံခြုံရေး စနစ်ကို ထိုးဖောက်ခြင်း	T1656	လူတစ်ယောက်ကဲ့သို့ တုပခြင်း	မသမာသူများသည် ယုံကြည်စိတ်ချရသည့် ပုဂ္ဂိုလ်များကဲ့သို့ ဟန်ဆောင်တုပကာ ဝဘ်ဆိုက်မျက်နှာဖုံး တီထွင်ခြင်း နှင့် ၎င်းတို့ ပစ်မှတ်ထားလိုသည့် အုပ်စုများနှင့် ဆက်စပ်သည့် နာမည်များကို အသုံးပြုခြင်း
စုဆောင်းခြင်း	T1123	အသံဖမ်းခြင်း	တရားဝင်ဖိုင်များကဲ့သို့ ထင်ရသည့် Trojan ဖိုင်များသည် မလိုအပ်ဘဲ မိုက်ခရိုဖုန်းထဲဝင်ခွင့်ကဲ့သို့သော ခွင့်ပြုချက်များ တောင်းခံခြင်း
စုဆောင်းခြင်း	T1125	ဗီဒီယို ရိုက်ယူခြင်း	တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan app များသည် မလိုအပ်ပဲ ကင်မရာထဲ ဝင်ရောက်ခွင့် ကဲ့သို့သော ခွင့်ပြုချက်များ တောင်းခံခြင်း

စုဆောင်းခြင်း	T1005	ဒေသန္တရ စနစ်မှ အချက်အလက်များ	တရားဝင် app များကဲ့သို့ ဟန်ဆောင်ထားသည့် Trojan app သည် မလိုအပ်ပဲ သင့်၏ ဖိုင်များထဲ ဝင်ရောက်ခွင့် တောင်းခံခြင်း
အမိန့်ပေးခြင်းနှင့် ထိန်းချုပ်ခြင်း	T1071.001	Application Layer Protocol: Web Protocols	Malware connects to C2 နှင့် ဆက်စပ်သည့် malware များသည် HTTPS နှင့် WebSocket's များကို သုံးသည်။
အမိန့်ပေးခြင်းနှင့် ထိန်းချုပ်ခြင်း	T1509	စံနှုန်းမညီသည့် port	စံမှုန်းမညီသည့် port များဖြစ်သည့် port ၄၄၃၂ နှင့် ၂၃၃၃ တို့ကို အသုံးပြုခြင်း
လျှို့ဝှက်စွာ ထုတ်ယူခြင်း	T1041	C2 ချန်နယ်သို့ လျှို့ဝှက်စွာ ထုတ်ယူခြင်း	Malware သည် HTTPS နှင့် WebSocket ကဲ့သို့သော ဆက်သွယ်မှုကို အသုံးချကာ ဒေတာများကို လျှို့ဝှက်စွာ ထုတ်ယူပို့ဆောင်ခြင်းများ ပြုလုပ်ပါသည်။
သက်ရောက်မှု	T1565.002	ဒေတာအချက်အလက် လှည့်စားမှု - ပို့ဆောင်သည့် ဒေတာများကို ပြင်ဆင်ပြောင်းလဲခြင်း	မသမာသူများသည် app ၏ ဆောင်ရွက်မှုအတွက် မလိုသည့် ဝဘ်စီးဆင်းမှု ဖြစ်စေသည့် app မှတစ်ဆင့် တိုက်ခိုက်ခံရသူ၏ အချက်အလက်များ ရရှိခြင်း

အညွှန်း

MOONSHINE –

– ၂၀၂၅ ခုနှစ် ဧပြီလ ၁ ရက်နေ့တွင် VliteUI panel တို့ကို ရှာကြည့်သည့်အခါ အောက်ပါ အချက်အလက်များ ရရှိခဲ့သည် –

IP လိပ်စာ	Port	ပထမဆုံးအကြိမ် တွေ့ရှိခြင်း	နောက်ဆုံးအကြိမ် တွေ့ရှိခြင်း
103.254.108[.]87	၈၈၈	၂၀၂၄-၁၀-၁၇	၂၀၂၅-၀၂-၁၄
43.159.192[.]7	၄၄၄	၂၀၂၄-၁၁-၂၁	၂၀၂၅-၀၂-၁၃
103.27.109[.]109	၄၄၄	၂၀၂၄-၀၇-၁၁	၂၀၂၅-၀၂-၀၇
45.119.99[.]83	၄၄၄	၂၀၂၄-၁၂-၂၆	၂၀၂၅-၀၁-၂၄
103.254.108[.]76	၄၄၄	၂၀၂၄-၀၉-၁၂	၂၀၂၄-၁၂-၀၅
194.71.107[.]160	၄၄၄	၂၀၂၃-၁၂-၁၀	၂၀၂၄-၁၁-၀၁
103.254.108[.]108	၄၄၄	၂၀၂၃-၁၁-၁၂	၂၀၂၄-၀၉-၂၅
103.56.17[.]194	၄၄၄	၂၀၂၄-၀၄-၀၃	၂၀၂၄-၀၈-၂၃
103.254.108[.]87	၄၄၄	၂၀၂၃-၁၁-၁၄	၂၀၂၄-၀၈-၁၅
62.72.58[.]168	၄၄၄	၂၀၂၄-၀၁-၂၉	၂၀၂၄-၀၈-၀၇
103.43.18[.]43	၄၄၄	၂၀၂၄-၀၂-၁၂	၂၀၂၄-၀၇-၁၉
77.91.123[.]208	၄၄၄	၂၀၂၄-၀၂-၀၄	၂၀၂၄-၀၄-၀၉
46.246.98[.]229	၄၄၄	၂၀၂၄-၀၃-၀၇	၂၀၂၄-၀၃-၂၆
2.58.15[.]101	၄၄၄	၂၀၂၄-၀၂-၂၃	၂၀၂၄-၀၂-၂၇
46.246.98[.]209	၄၄၄	၂၀၂၄-၀၁-၀၈	၂၀၂၄-၀၂-၁၄
103.254.108[.]87	၈၀၀၀	၂၀၂၃-၁၀-၁၇	၂၀၂၃-၁၀-၁၇
103.254.108[.]87	၈၀၈၀	၂၀၂၃-၀၄-၁၅	၂၀၂၃-၁၀-၁၆
103.254.108[.]108	၉၀၉၀	၂၀၂၃-၀၄-၁၃	၂၀၂၃-၁၀-၁၆
103.45.66[.]123	၉၀၉၀	၂၀၂၃-၀၃-၀၂	၂၀၂၃-၀၄-၀၈
103.45.66[.]32	၈၀၈၀	၂၀၂၂-၀၇-၂၉	၂၀၂၃-၀၄-၀၆
27.124.20[.]23	၉၀၉၀	၂၀၂၂-၀၅-၂၈	၂၀၂၃-၀၃-၂၄

27.124.20[.]22	๔๐๔๐	๗๗-๐๑-๗่	๗๗๲-๐๲-๗๲
27.124.20[.]24	๔๐๔๐	๗๗-๐๑-๗๒	๗๗๲-๐๲-๐๒
69.176.94[.]148	๔๐๔๐	๗๗๲-๐๲-๐๙	๗๗๲-๐๲-๐๐
69.176.94[.]228	๔๐๔๐	๗๗-๐๗-๗๙	๗๗๲-๐๗-๗๑
103.253.40[.]137	๓๐๐๐	๗๗-๐๖-๗๙	๗๗-๑๐-๐๗
27.124.4[.]80	๓๐๓๐	๗๗-๐๗-๗๑	๗๗-๐๖-๗๲
27.124.4[.]81	๓๐๓๐	๗๗-๐๗-๗๑	๗๗-๐๖-๗๲
47.242.46[.]79	๓๐๓๐	๗๗๐-๐๑-๐๲	๗๗-๐๖-๐๒
27.124.4[.]82	๓๐๓๐	๗๗-๐๗-๗๙	๗๗-๐๖-๐๑
27.124.4[.]165	๔๐๔๐	๗๗-๐๑-๐๙	๗๗-๐๑-๗่
27.124.4[.]184	๔๐๔๐	๗๗-๐๑-๐๙	๗๗-๐๑-๗๒
27.124.4[.]178	๔๐๔๐	๗๗-๐๑-๐๲	๗๗-๐๑-๗๖
103.15.28[.]165	๓๐๓๐	๗๗-๐๲-๐๑	๗๗-๐๑-๗๑
69.176.94[.]226	๓๐๓๐	๗๗-๐๲-๐๑	๗๗-๐๙-๗๗
27.124.4[.]3	๓๐๓๐	๗๗-๐๲-๐๐	๗๗-๐๙-๐๗
103.140.238[.]235	๓๐๓๐	๗๗-๐๲-๐๙	๗๗-๐๙-๐๐
27.124.4[.]2	๓๐๓๐	๗๗-๐๲-๐๗	๗๗-๐๙-๐๐
165.84.180[.]107	๓๐๐๐	๗๗-๐๗-๗๑	๗๗-๐๲-๐๔
69.176.94[.]156	๓๐๐๐	๗๗-๐๗-๗๑	๗๗-๐๲-๐๑
141.98.212[.]70	๔๐๔๐	๗๗๐-๐๐-๐๑	๗๗-๐๲-๐๙
5.188.33[.]50	๓๐๐๐	๗๗-๐๗-๐๑	๗๗-๐๲-๐๙
5.188.70[.]193	๓๐๐๐	๗๗-๐๗-๐๑	๗๗-๐๲-๐๙
69.176.94[.]140	๓๐๓๐	๗๗-๐๗-๗๙	๗๗-๐๗-๗๙
27.124.20[.]83	๓๐๐๐	๗๗-๐๗-๐๙	๗๗-๐๗-๐๓
208.87.200[.]106	๓๐๐๐	๗๗-๐๐-๐๗	๗๗-๐๐-๐๗
121.127.241[.]37	๓๐๐๐	๗๐๗-๐๗-๐๓	๗๐๗-๐๗-๐๓
156.255.2[.]211	๙๙๒	๗๐๗-๐๐-๐๑	๗๐๗-๐๐-๐๑
156.255.2[.]211	๓๐๐๐	๗๐๗-๐๐-๐๙	๗๐๗-๐๐-๐๙

156.255.2[.]203	၈၀၀၀	၂၀၂၁-၁၀-၀၃	၂၀၂၁-၁၀-၀၃
47.243.43[.]248	၈၀၀၀	၂၀၂၁-၀၇-၀၅	၂၀၂၁-၀၇-၀၅
45.115.236[.]6	၈၀၈၀	၂၀၂၁-၀၅-၀၃	၂၀၂၁-၀၅-၀၁
43.251.118[.]97	၈၀၀၀	၂၀၂၁-၀၁-၀၃	၂၀၂၁-၀၃-၀၁
185.243.43[.]138	၈၀၀၀	၂၀၂၁-၀၁-၀၄	၂၀၂၁-၀၂-၀၂
47.245.59[.]33	၈၀၀၀	၂၀၂၁-၀၁-၀၅	၂၀၂၁-၀၁-၀၅

– ၂၀၂၅ ခုနှစ် ဧပြီလ ၁ ရက်နေ့တွင် SCOTCH ADMIN panel များကို ရှာကြည့်ရာတွင် အောက်ပါ အချက်အလက်များ တွေ့ခဲ့ရပါသည်-

IP လိပ်စာ	Port	ပထမဆုံး တွေ့ရှိချိန်	နောက်ဆုံး တွေ့ရှိချိန်
104.194.152[.]24	၂၃၃၃	၂၀၂၅-၀၂-၀၆	၂၀၂၅-၀၂-၂၇
172.86.80[.]126	၂၃၃၃	၂၀၂၅-၀၂-၀၇	၂၀၂၅-၀၂-၂၇
154.90.59[.]62	၂၃၃၃	၂၀၂၄-၀၆-၂၀	၂၀၂၄-၀၉-၂၀
154.90.59[.]88	၂၃၃၃	၂၀၂၄-၀၆-၂၁	၂၀၂၄-၀၉-၂၀
154.90.58[.]210	၂၃၃၃	၂၀၂၄-၀၅-၁၆	၂၀၂၄-၀၆-၁၄
154.90.59[.]225	၂၃၃၃	၂၀၂၄-၀၅-၁၇	၂၀၂၄-၀၆-၁၃
38.60.199[.]208	၂၃၃၃	၂၀၂၃-၁၁-၂၆	၂၀၂၄-၀၁-၀၉
38.60.199[.]254	၂၃၃၃	၂၀၂၃-၁၁-၂၈	၂၀၂၄-၀၁-၀၉
38.60.199[.]99	၂၃၃၃	၂၀၂၃-၀၈-၂၆	၂၀၂၃-၁၁-၂၁
38.60.199[.]44	၂၃၃၃	၂၀၂၃-၀၇-၂၀	၂၀၂၃-၀၉-၁၁
194.163.34[.]23	၄၄၃	၂၀၂၂-၀၉-၃၀	၂၀၂၃-၀၄-၁၄
45.32.125[.]112	၁၀၄၄၃	၂၀၂၂-၁၀-၀၁	၂၀၂၃-၀၃-၁၇

- ၂၀၂၅ ခုနှစ် မတ်လ ၁၄ ရက်နေ့တွင် SCOTCH ADMIN panel များကို ရှာကြည့်ရာတွင် အောက်ပါ အချက်အလက်များ တွေ့ခဲ့ရပါသည်-

ဒိုမိန်း	IP လိပ်စာ
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

BADBAZAAR -

ရှင်းလင်းဖော်ပြချက်	BADBAZAAR C2 များတွင် တွေ့ရသည့် SSL certificate
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- ၂၀၂၅ ခုနှစ် ဧပြီလ ၁ ရက်နေ့တွင် BADBAZAARကို ရှာကြည့်ရာတွင် အောက်ပါ အချက်အလက်များ တွေ့ခဲ့ရပါသည်-

IP လိပ်စာ	Port	ပထမဆုံး တွေ့ရှိချိန်	နောက်ဆုံး တွေ့ရှိချိန်
157.90.129[.]73	၂၁၃၇	၂၀၂၅-၀၃-၁၄	၂၀၂၅-၀၃-၂၈
157.90.129[.]73	၃၁၂၆	၂၀၂၅-၀၃-၁၄	၂၀၂၅-၀၃-၂၈
157.90.129[.]73	၃၁၃၅	၂၀၂၅-၀၃-၁၄	၂၀၂၅-၀၃-၂၈

157.90.129[.]73	၃၁၂၃	၂၀၂၅-၀၃-၂၇	၂၀၂၅-၀၃-၂၇
142.132.131[.]15	၃၁၂၃	၂၀၂၄-၀၇-၂၄	၂၀၂၅-၀၃-၂၇
142.132.131[.]15	၃၁၂၃	၂၀၂၄-၀၇-၂၆	၂၀၂၅-၀၃-၂၇
142.132.131[.]20	၃၁၂၃	၂၀၂၃-၀၈-၁၁	၂၀၂၅-၀၃-၂၇
142.132.131[.]15	၃၁၂၃	၂၀၂၄-၀၇-၂၄	၂၀၂၅-၀၃-၂၇
142.132.131[.]20	၃၁၂၃	၂၀၂၃-၀၉-၂၇	၂၀၂၅-၀၃-၂၆
142.132.131[.]20	၃၁၂၃	၂၀၂၃-၁၀-၁၈	၂၀၂၅-၀၃-၂၆
65.108.192[.]155	၃၁၂၃	၂၀၂၄-၁၂-၀၅	၂၀၂၅-၀၂-၂၀
65.108.192[.]155	၃၁၂၃	၂၀၂၄-၁၂-၀၅	၂၀၂၅-၀၂-၂၀
65.108.192[.]155	၃၁၂၃	၂၀၂၄-၁၂-၀၅	၂၀၂၅-၀၂-၁၉
23.88.28[.]222	၃၁၂၃	၂၀၂၄-၀၄-၂၅	၂၀၂၄-၁၁-၂၉
23.88.28[.]222	၃၁၂၃	၂၀၂၄-၀၅-၀၂	၂၀၂၄-၁၁-၂၈
23.88.28[.]222	၃၁၂၃	၂၀၂၄-၀၅-၀၁	၂၀၂၄-၁၁-၂၈
212.129.21[.]168	၃၁၂၃	၂၀၂၃-၁၀-၁၆	၂၀၂၄-၀၃-၁၇
212.129.21[.]168	၃၁၂၃	၂၀၂၃-၀၈-၂၄	၂၀၂၄-၀၃-၁၇
212.129.21[.]168	၃၁၂၃	၂၀၂၃-၀၉-၂၆	၂၀၂၄-၀၃-၁၄

ရှင်းလင်းဖော်ပြချက်	**BADBAZAAR C2 များ အတွက် တွေ့ရသည့် SSL certificate**
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- ၂၀၂၁ ခုနှစ် ဧပြီလ ၁ ရက်နေ့တွင် BADBAZAAR ၏ certificate များ ရှာကြည့်ရာတွင် အောက်ပါ အချက်များ တွေ့ရှိရပါသည် -

IP လိပ်စာ	Port	ပထမဆုံး တွေ့ရှိချိန်	နောက်ဆုံး တွေ့ရှိချိန်
162.55.103[.]211	၂၀၁၁	၂၀၂၃-၀၁-၁၂	၂၀၂၅-၀၃-၂၈
162.55.103[.]212	၂၀၁၁	၂၀၂၂-၀၆-၃၀	၂၀၂၅-၀၃-၂၈
162.55.103[.]212	၂၀၁၂	၂၀၂၃-၀၇-၁၄	၂၀၂၅-၀၃-၂၈
162.55.103[.]211	၂၀၁၁	၂၀၂၂-၀၆-၀၃	၂၀၂၅-၀၃-၂၈
162.55.103[.]211	၂၀၁၃	၂၀၂၃-၀၇-၁၂	၂၀၂၅-၀၃-၂၇
162.55.103[.]212	၂၀၁၃	၂၀၂၃-၀၇-၁၂	၂၀၂၅-၀၃-၂၇
212.83.162[.]152	၉၀၉၀	၂၀၂၂-၁၀-၁၃	၂၀၂၅-၀၃-၂၇
23.88.28[.]221	၂၀၄၂	၂၀၂၃-၀၇-၂၈	၂၀၂၃-၀၉-၃၀
23.88.28[.]221	၂၀၄၁	၂၀၂၃-၀၅-၁၈	၂၀၂၃-၀၉-၂၈
23.88.28[.]221	၂၀၄၂၃	၂၀၂၃--၀၇-၂၈	၂၀၂၃-၀၉-၂၈
162.55.103[.]210	၂၀၁၁	၂၀၂၂-၀၉-၃၀	၂၀၂၃-၀၂-၂၃
65.21.92[.]67	၂၀၁၁	၂၀၂၁-၁၁-၀၂	၂၀၂၂-၁၀-၁၃
65.21.92[.]67	၂၀၁၂	၂၀၂၂-၀၈-၁၀	၂၀၂၂-၁၀-၁၃
23.88.28[.]220	၂၀၁၁	၂၀၂၁-၁၂-၀၈	၂၀၂၂-၀၅-၁၃
94.130.92[.]230	၂၀၁၁	၂၀၂၁-၀၁-၀၄	၂၀၂၁-၁၀-၀၅
88.99.150[.]246	၂၀၁၁	၂၀၂၁-၀၄-၀၆	၂၀၂၁-၀၉-၀၈
45.76.132[.]91	၂၀၁၁	၂၀၂၁-၀၂-၀၂	၂၀၂၁-၀၃-၀၁

WHOIS ဒိုမိန်းများ

အောက်ပါ ဇယားသည် BADBAZAAR C2 ဒိုမိန်းများ၏ value များနှင့်တူနေသည့် လက်ရှိနှင့် အတိတ်မှ WHOIS မှတ်တမ်းများကို ဖော်ပြထားပါသည်။

WHOIS Value	ဒိုမိန်းများ
မှတ်ပုံတင်သည့် ပြည်နယ် - UJYJYUJ **မှတ်ပုံတင်သည့် နိုင်ငံ - ဘိုလစ်ဗီးယား** **မှတ်ပုံတင်သူ၏ - eNom**	• ntc-mobile[.]com • microtik[.]net • ntc-ftth[.]net • axisupdating[.]com • axisupdate[.]com • telegramrouter[.]org • telegramtor[.]com • fufijxgkg[.]com • jindjjdtc[.]com • tubevideoplus[.]org • thetubeplus[.]com • tbgram[.]org • signalplus[.]org • pmumail[.]com
မှတ်ပုံတင်သည့် ပြည်နယ် - REWR **မှတ်ပုံတင်သည့် နိုင်ငံ - CF** **မှတ်ပုံတင်သူ၏ - eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
မှတ်ပုံတင်သည့် ပြည်နယ် - FSDF **မှတ်ပုံတင်သည့် နိုင်ငံ - AL** **မှတ်ပုံတင်သူ၏ - eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

အီးမေးလ်လိပ်စာများ
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

YouTube ချန်နယ်များ
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

အောက်ပါ လင့်ခ်များမှာ BADBAZAAR နှင့် MOONSHINE တို့နှင့် ဆက်စပ်သည့် အခြားသော လုံခြုံရေးအန္တရာယ် ကြုံရကြောင်း ပြသချက် indicators of compromise (IoCs) များ ဖြစ်ပါသည်။ ဤလင့်ခ်များတွင် ပါဝင်သည့် အချက်အလက်များ အားလုံး စစ်မှန်သည်ဟု NCSC အနေဖြင့် အတည်မပြုနိုင်ပါ၊ စာဖတ်သူများအနေဖြင့် ဤ အချက်အလက်များ မှန်ကန် ဆီလျော်ခြင်း ရှိမရှိ သီးသန့်လွတ်လပ်သည့် အချက်အလက်များ ရယူ၍ အတည်ပြုရန် အကြံပြုလိုပါသည်။

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity
- Citizen Lab

အန္တရာယ် လျော့ချခြင်း

NCSC အနေဖြင့် ဖြစ်ရပ်မှန် နမူနာများတွင် ဖော်ပြထားသည့် ခြိမ်းခြောက်မှု အန္တရာယ်ရန်မှ ကာကွယ်ရန်အတွက် အောက်ပါ အကြံပြုချက်များကို အသုံးပြုရန် တိုက်တွန်းလိုပါသည်။

- **တတိယပါတီ app store များအပါအဝင် App store operators များအနေဖြင့် ၎င်းတို့ ပလက်ဖောင်းပေါ်မှ app များသည် လုံခြုံဘေးကင်းမှုရှိပြီး အစိုးရ၏ ကျင့်ဝတ်နှင့် စည်းကမ်းများ လိုက်နာမှုရှိရန် လုပ်ဆောင်သင့်ပါသည်။** လမ်းညွှန်ချက်ကို လေ့လာရန် https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version

- **အခြားဘာသာ စကားများနှင့် ပံ့ပိုးမှု –** App developer များအနေဖြင့် ဒေသန္တရဆန်ပြီး လူကြိုက်များသည့် app များ တီထွင်ရေးတွင် ရင်းနှီးမြုပ်နှံမှု လုပ်သင့်ပြီး ဝဂါ၊ တိဘက်၊ ထိုင်ဝမ်၊ Hokkien နှင့် Cantonese စသည့် လူနည်းစုများအကြား အသုံးပြုမည့် app များတွင် ရင်းနှီးမြုပ်နှံ သင့်ပါသည်။ ဒေသန္တရဆန်သည့် app များတီထွင်ခြင်းနှင့် ပတ်သက်သည့် Apple ၏ လမ်းညွှန်ချက် - https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. ဒေသန္တရဆန်သည့် app များတီထွင်ခြင်းနှင့် ပတ်သက်သည့် Google ၏ လမ်းညွှန်ချက် - https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **သင်၏ ဆိုရှယ်မီဒီယာ ပလက်ဖောင်းကို လုံခြုံမှုရှိအောင် ပြုလုပ်ခြင်း** – ဆိုရှယ်မီဒီယာ ကုမ္ပဏီများအနေဖြင့် တရားဝင် အွန်လိုင်း လူမှုအသိုင်းအဝိုင်းများ စုဝေးရာ ပလက်ဖောင်းဟု ယူဆနိုင်သည့် ၎င်းတို့၏ ပလက်ဖောင်းပေါ်တွင် မသမာသည့် ဆိုင်ဘာသမားများ အကောင့်တုဖွင့်ခြင်းနှင့် အန္တရာယ်ရှိသည့် ဖိုင်များ သို့မဟုတ် လင့်ခ်များ မျှဝေခြင်းကို အလွယ်တကူ မလုပ်နိုင်ရန် လုပ်ဆောင်ထားနိုင်ပါသည်။ ဖြစ်နိုင်ပါက ကုမ္ပဏီများအနေဖြင့် မသမာမှုများ၏

မှတ်တမ်းများကို တခြား ကဏ္ဍများနှင့်လည်း မျှဝေမှုလုပ်ပါက ခြိမ်းခြောက်မှု အန္တရာယ်နှင့် ကာကွယ်ရေး နည်းလမ်းများကို အားလုံး နားလည်သဘောပေါက်ကြမည် ဖြစ်ပါသည်။

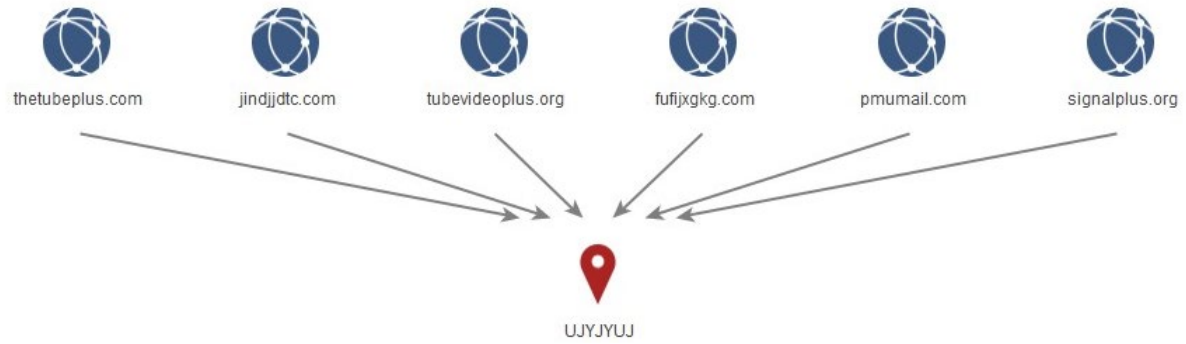
- **အသုံးပြုသူများအတွက် ပြန်လည် ပြုပြင်ထူထောင်ရန် အစီအစဉ် –** အဖွဲ့အစည်းများအနေဖြင့် ၎င်းတို့၏ ဝန်ဆောင်မှုကို အသုံးပြုရာမှ အန္တရယ်ရှိသည့် app များကို ထည့်သွင်းမိပါက ထိုအကြောင်းအရာအား အသုံးပြုသူများကို အသိပေးနိုင်သည့် နည်းလမ်းများ ထားရှိသင့်ပါသည်။ အာရုံစိုက်မှု ရှိစေသည့် တပ်လှန့်မှုနှင့် လိုအပ်သည့် အချက်အလက်များကို ပေးနိုင်သည့် သတိပေးချက်မျိုး ဖြစ်သင့်ပါသည်။ သင့်တော်မည် ဆိုပါက အဖွဲ့အစည်းများအနေဖြင့် ထိုဆော့ဖ်ဝဲများအား ဖယ်ရှားနိုင်သည့် လမ်းညွှန်ချက်များနှင့် တိုက်ခိုက်မှု ခံရသည့် သူများကိုလည်း ယူကေနိုင်ငံတွင် NCSC ကဲ့သို့သော အာဏာပိုင်များဆီ တိုင်တန်းမှု လုပ်ရန် တိုက်တွန်းမှု လုပ်သင့်ပါသည်။
  App Store ဆိုင်ရာ ကျင့်ဝတ်နှင့် စည်းမျဉ်းများကို ပိုမို လေ့လာရန် - https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **ပူးပေါင်းဆောင်ရွက်ရေး အဖွဲ့များ–** ဆိုရှယ်မီဒီယာ ကုမ္ပဏီများအနေဖြင့် အလုပ်အမှုဆောင်အဖွဲ့များကို ဖွဲ့စည်းကာ ထိုအဖွဲ့၏ လုံခြုံရေးအသင်းများအား TPP နှင့် observations များပါသည့် မသမာမှုများ၏ မှတ်တမ်းများကို မျှဝေခြင်းများ ပြုလုပ်စေပါက မသမာသူများအတွက် ၎င်းတို့၏ မသမာသော ကမ်ပိန်းများ ပြုလုပ်ရန် ခက်ခဲစေနိုင်ပါသည်။

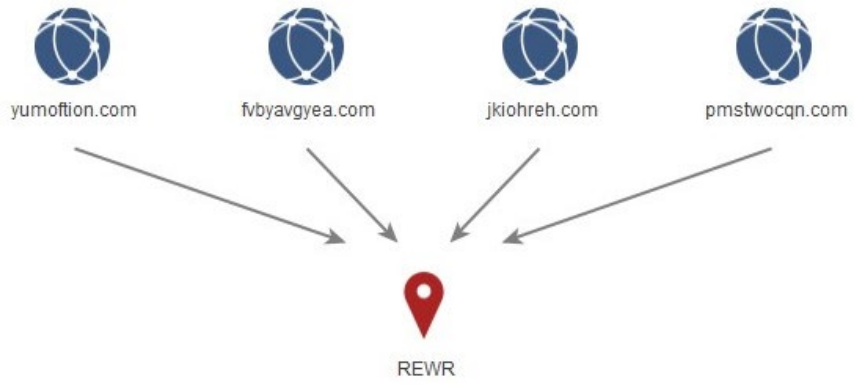
- **ပြုပြင်ပြောင်းလဲမှု လုပ်ထားသည့် apps များကို သိနိုင်အောင် ပြုလုပ်ခြင်း–** ဖြစ်နိုင်မည် ဆိုပါက app developer များ အနေဖြင့် 'တရားမဝင် တုပထားသည့်' app ကို အသုံးပြုသူများ ဒေါင်းလုဒ်လုပ်မိသောအခါ ထိုအကြောင်းကို အသုံးပြုသူအား အသိပေးနိုင်သည့် နည်းလမ်းကို ထည့်သွင်းနိုင်ပါက မရိုးမသား ကော်ပီ လုပ်သည့်ရန်မှ ကာကွယ်မှု ဖြစ်စေနိုင်ပါသည်။

ပူးတွဲစာ ခ – BADBAZAAR WHOIS clustering / domain broker အချက်အလက်များ၏ ဇယား

ပုံ ၁ – ‘UKYJYUJ’

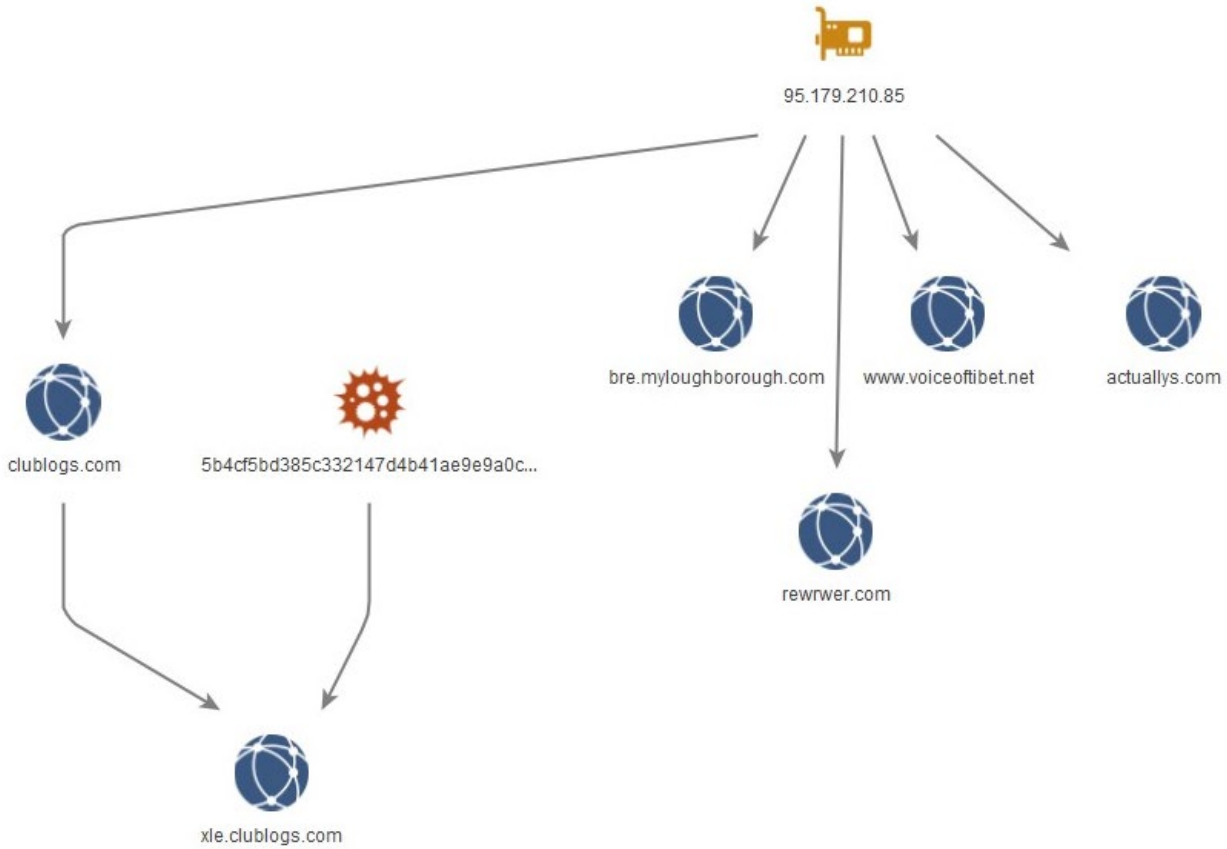


ပုံ ၂ – Keyboard walking values

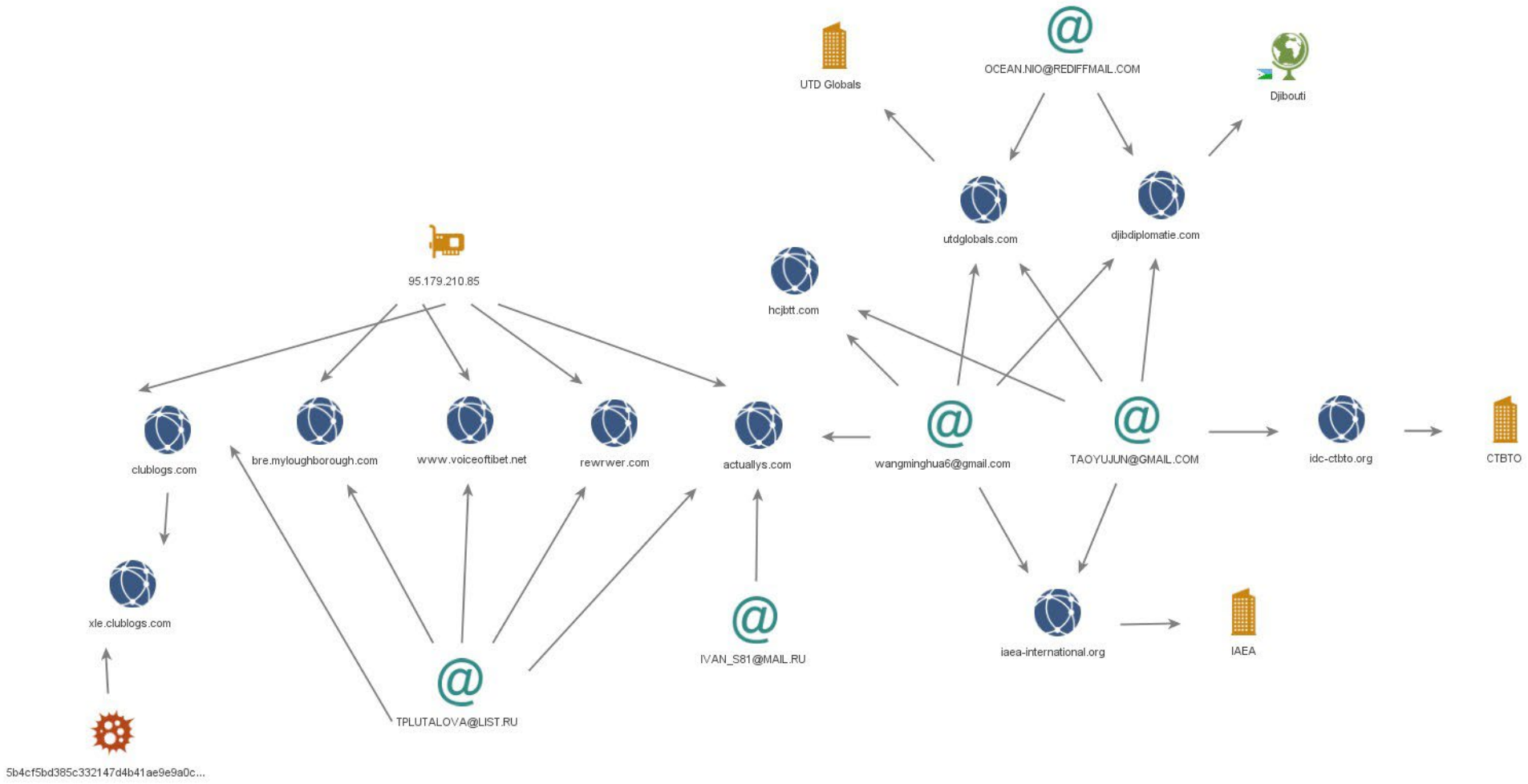


ပုံ ၃ – A‘FSDF’ state field values ပါသည့် ဒိုမိန်းများ

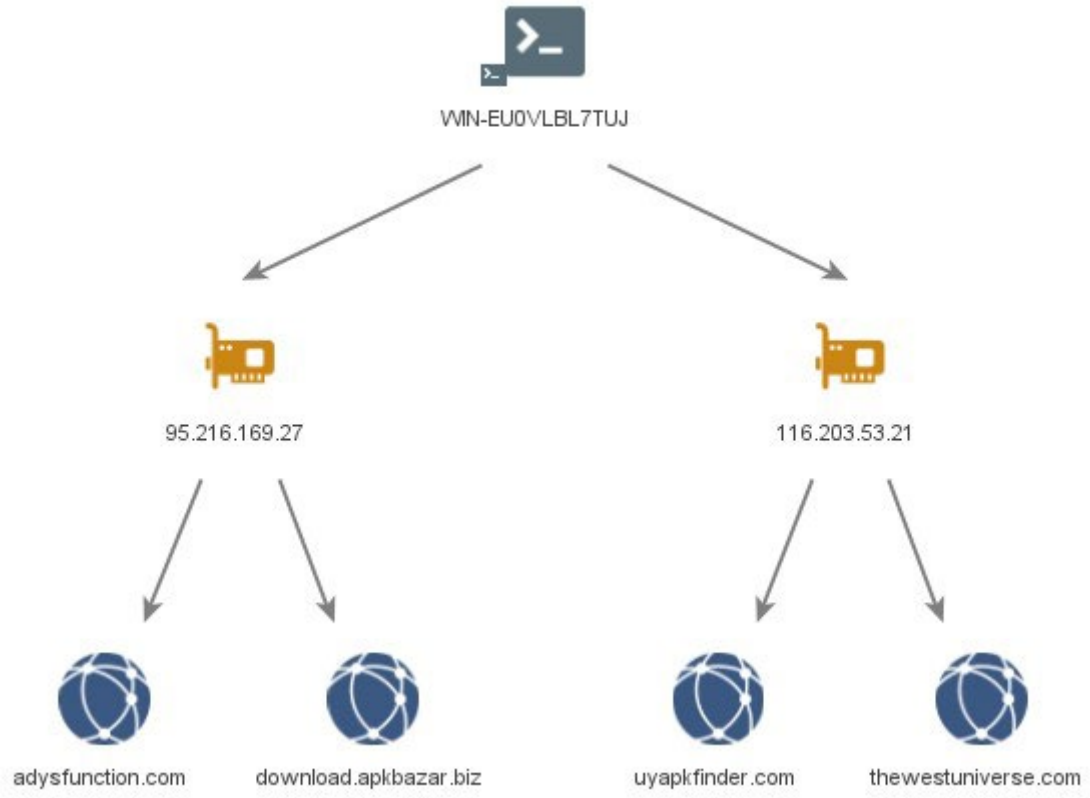
ပုံ ၄ – **95.179.210[.]85**



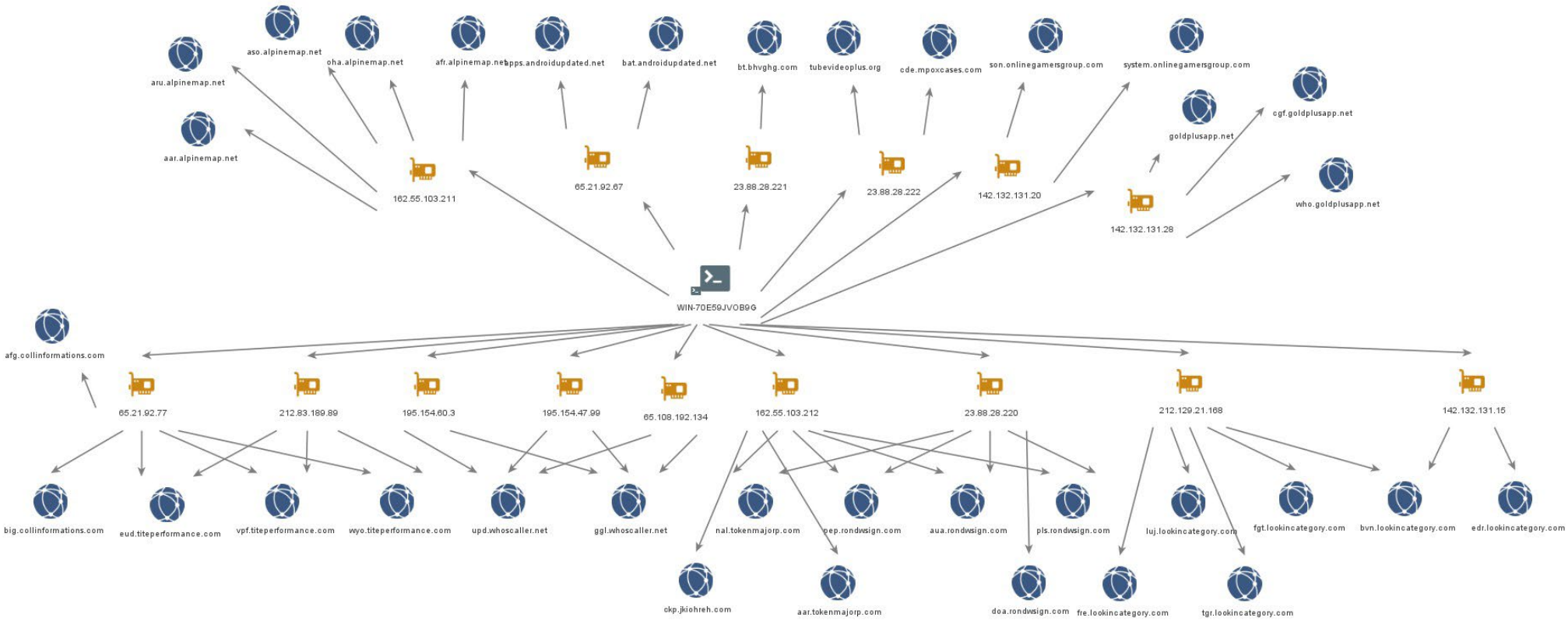
ပုံ ၅ – WHOIS လင့်ခ်များ



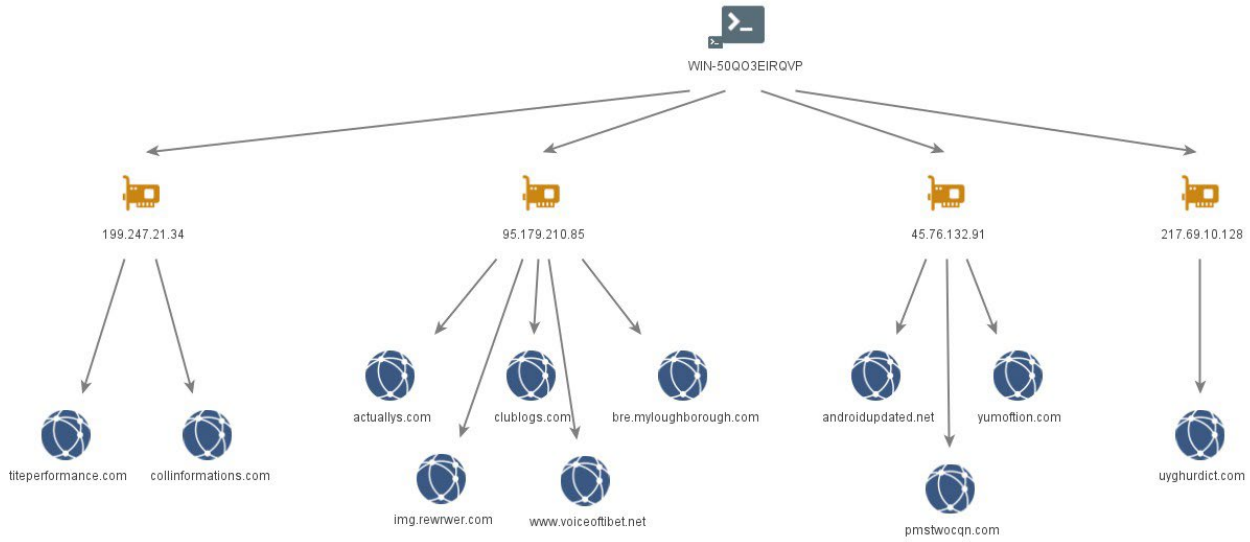
ပုံ ၆ – **WIN-EU0VLBL7TUJ**



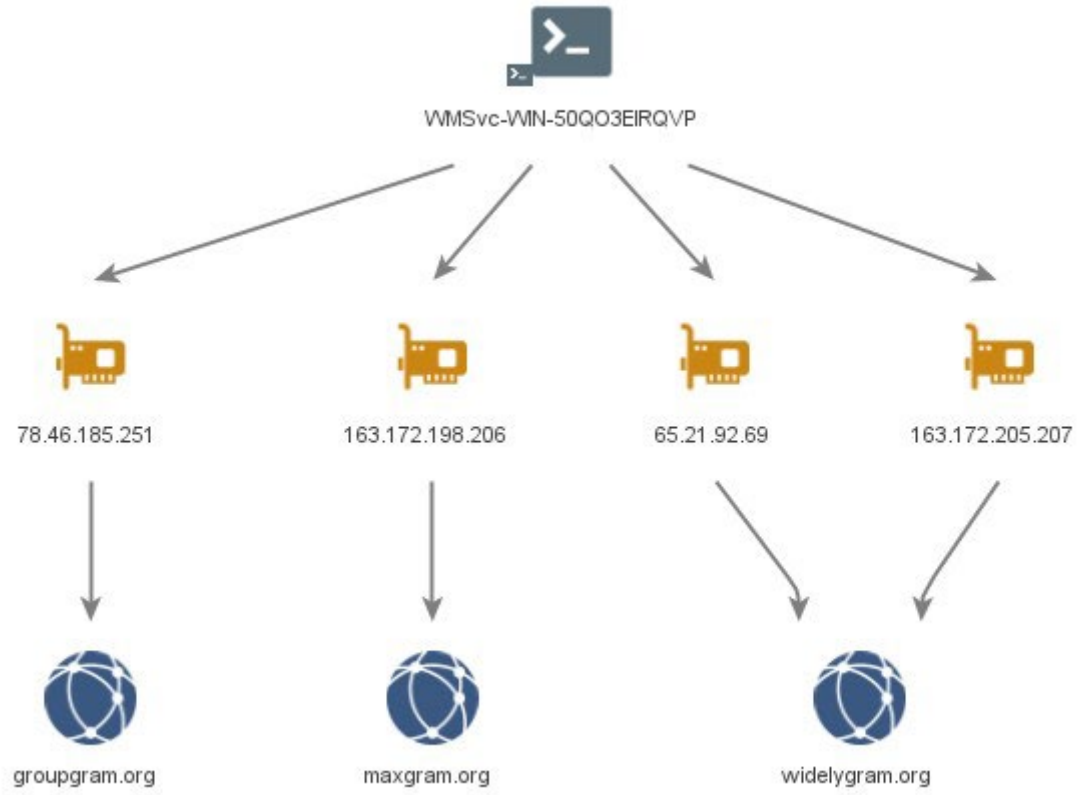
ပုံ ၇ – **WIN-70E59JVOB9G**



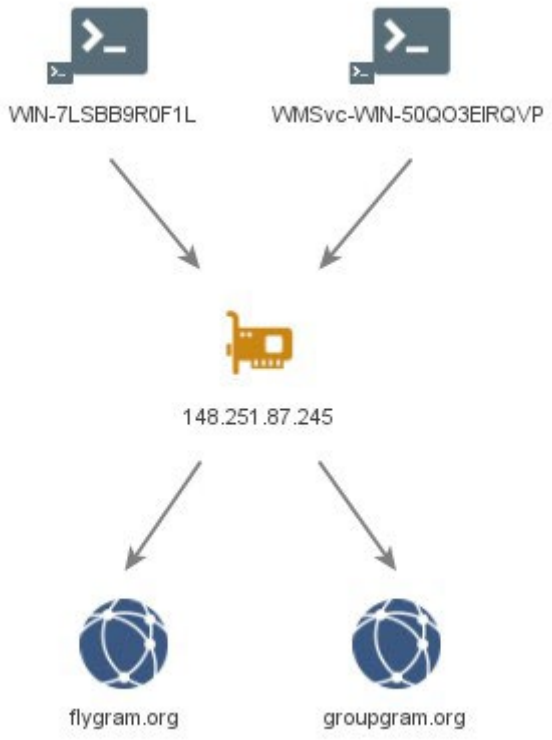
ပုံ ၈ - **WIN-50QO3EIRQVP**



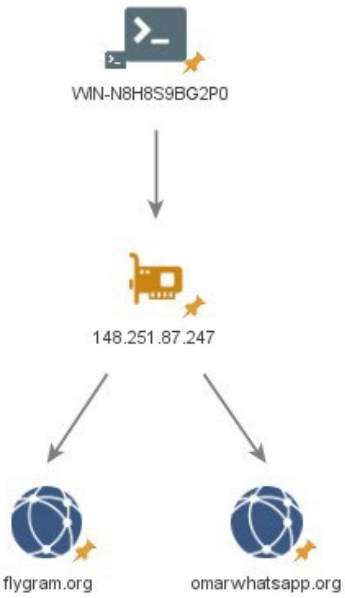
ပုံ ၉ - **VMSvc-WIN-50QO3EIRQVP**



ပုံ ၁၀ – **VMSvc-WIN-50QO3EIRQVP** and **WIN-7LSBB9R0F1L**



ပုံ ၁၁ - **WIN-N8H8S9BG2P0**



ပုံ ၁၂ – **WIN-I6VBN8MR92A**

ပူးတွဲစာ ခ - စောင့်ကြည့်ခဲ့သည့် MOONSHINE နှင့် BADBAZAAR ဥပမာများ

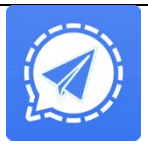
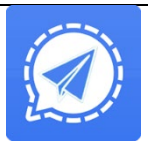
အောက်ပါ ဇယားသည် လွန်ခဲ့သည့် နှစ်နှစ်ကာလအတွင်း MOONSHINE နှင့် BADBAZAAR ကမ်ပိန်းအတွင်း အသုံးပြုခဲ့သည့် app များ၏ စာရင်းကို ထည့်သွင်းထားပါသည်။

ထို app အများစုတို့သည် အတည်တကျ ရှိနေပြီးသား app များနှင့် အများကြီး ဆင်တူကြောင်း ပြသထားပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် လူသိများကျော်ကြားသည့် အမှတ်တံဆိပ်များအား တမင်တကာ 'လှောင်ပြောင်' ခြင်း ဖြစ်နိုင်ပါသည်။

သတိပြုရမည့် အချက်မှာ app များ၏ နာမည်၊ package နာမည်နှင့် သင်္ကေတများ အားလုံးသည် တုပနိုင်သည့် အရာဖြစ်ပြီး application အစစ်များအတိုင်း လုပ်ဆောင်နိုင်သည့်အတွက် စက်ပစ္စည်း တစ်ခု တိုက်ခိုက်ခံရခြင်း ရှိမရှိ စစ်ဆေးရာတွင် app အစစ်အဖြစ် မှတ်ယူကာ အသုံးမပြုသင့်ပါ။

App ခေါင်းစဉ်	Package နာမည်	App သင်္ကေတ
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پینتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

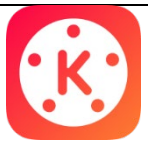
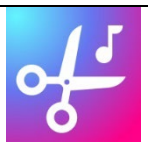
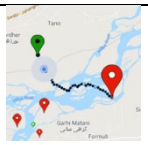
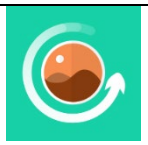
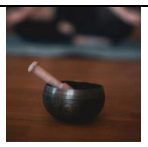
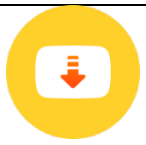
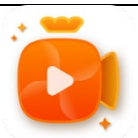
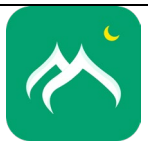
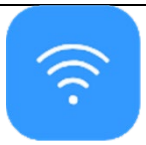
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	

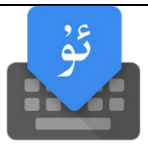
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	

SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO	net.rhombapp.mo	

Tibetan Prayer	com.chorig.tibetanprayer	
Translator AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter	com.inverseai.video_converter	
Video Cutter	com.naing.cutter	
Video Downloader	downloader.video.download.free	
Video Maker	com.bstech.slideshow.videomaker	

Video Player for Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Voice Recorder	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
YouTube Downloader	dentex.youtube.downloader	
Zom	im.zom.messenger	
iQuran Lite	com.guidedways.iQuran	
ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	

ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	
القرآن الكريم	com.maher4web.quran	
زىكرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
نۇر كىرگۈزگۈچ	com.nur.ime	
《心灵法门》念佛机	com.guanyincitta.chant	
汉藏英辞典	com.dacd.dictionary	

藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	

ထပ်မံဖတ်ရှု လေ့လာရန် အကြံပြုစာရင်း

သြစတြေးလျ ဆိုင်ဘာလုံခြုံရေးစင်တာ၏ လမ်းညွှန်ချက်များ

- ဆိုင်ဘာရာဇာဝတ်မှု၊ အခင်းဖြစ်ပွားမှုနှင့် အားနည်းချက်များအား တိုင်တန်းပါ
- သင်၏ စက်ပစ္စည်း လုံခြုံရန် မည်ကဲ့သို့ လုပ်နိုင်သနည်း
- သင်၏ မိုဘိုင်းဖုန်းအား လုံခြုံအောင် လုပ်ဆောင်ခြင်း
- Phishing
- လိမ်လည်ခြင်း
- သင်၏ ဆိုရှယ်မီဒီယာ အကောင့်ကို လုံခြုံအောင် လုပ်ဆောင်ခြင်း
- ဆိုရှယ်မီဒီယာနှင့် မက်ဆေ့ချ် app များ လုံခြုံဘေးကင်းရန်အတွက် အကြံပြုချက်များ Security tips for social media and messaging apps

UK ၏ NCSC နှင့် NPSA တို့၏ လမ်းညွှန်ချက်များ

- ဒီမိုကရေစီကို ကာကွယ်ခြင်း
- ဆိုရှယ်မီဒီယာ – လုံခြုံဘေးကင်းစွာ မည်ကဲ့သို့ အသုံးပြုနိုင်သနည်း
- မိုဘိုင်းအပါအဝင် အဖွဲ့အစည်းများ၏ စက်ပစ္စည်းများ လုံခြုံရေးအတွက် လမ်းညွှန်ချက်များ
- application store များပေါ်မှ ခြိမ်းခြောက်မှုဆိုင်ရာ အစီရင်ခံစာ
- ပစ်မှတ်ထားခံရနိုင်ခြေများသော သူများအတွက် ဘေးကင်းရေးနှင့် လုံခြုံရေးများ

အမေရိကန် ၏ NSA မှ လမ်းညွှန်ချက်များ

- မိုဘိုင်းပစ္စည်းများ လိုက်နာရန် အကောင်းဆုံး နည်းလမ်းများ

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤအကြံပြုချက်ပါ အချက်အလက်များသည် ထုတ်ဝေသည့်အချိန်အထိ အတည်ပြုပြီးကြောင်း အသိပေးလိုပါသည်။

ဤအစီရင်ခံစာသည် အာဏာပိုင် အေဂျင်စီနှင့် ဤကဏ္ဍတို့မှ ရရှိသည့် အချက်အလက် ရင်းမြစ်များအပေါ် အခြေခံကာ ထုတ်ဝေထားခြင်း ဖြစ်ပါသည်။ တွေ့ရှိချက်များနှင့် အကြံပြုချက်များ အားလုံးကြောင့် အန္တရာယ် လုံးဝ မရှိတော့ကြောင်း မဆိုလိုသကဲ့သို့ ဤအကြံပြုချက်များအားလုံး လိုက်နာလုပ်ဆောင်ပါက အန္တရာယ်အားလုံးကို ဖယ်ရှားနိုင်သည်ဟုလည်း မဆိုလိုပါ။ အချက်အလက်ဆိုင်ရာ အန္တရာယ်များ၏ ပိုင်ဆိုင်မှုသည် သင့်တော်သောစနစ်နှင့် သက်ဆိုင်ရာ တာဝန်ခံနှင့်သာ သက်ဆိုင်ပါသည်။

ယူကေနိုင်ငံတွင် ဤအချက်အလက်များသည် Freedom of Information Act 200 (FOIA) အရ ကင်းလွတ်ခွင့် ရရှိထားကာ တခြားသော ယူကေနိုင်ငံ၏ ဆက်သွယ်ရေးဆိုင်ရာ ဥပဒေ ကင်းလွတ်ခွင့်လည်း ရရှိနိုင်ပါသည်။

FOIA နှင့် ပတ်သက်သည့် စုံစမ်းမေးမြန်းမှု မှန်သမျှအတွက် ncscinfoleg@ncsc.gov.uk ကို ဆက်သွယ်ပါ။