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

ཀོས་སྒོན།

BADBAZAAR དང་ MOONSHINE:

འཕྲུལ་རིག་དབྱེ་ཞིབ་དང་ ཉེན་ཁ་སེལ་ཐབས།

BADBAZAAR དང་ MOONSHINE: འཕྲུལ་རིག་དབྱེ་ཞིབ་དང་ ཉེན་ཁ་སེལ་ཐབས།

བསྡུད་དོན།

UK གི་རྒྱུད་སྒྲིག་འཛིན་ལྟ་ རྩ་རྒྱའི་མཐུན་རྫོགས, ཤོག་སྣོན་འདི་རྒྱལ་ཡོངས་དྲ་རྒྱའི་བདེ་འཇགས་ཉེ་བ་ (NCSC UK) དང་རྒྱལ་སྤྱིའི་མཉམ་འབྲེལ་པ་ ཚུ་གིས་ མཉམ་འབྲེལ་ཐོག་བཟོ་ཡོངས་ཨིན།

- **མོ་སི་ཉེ་ལི་ཡའི་དྲ་རྒྱའི་བདེ་འཇགས་ཉེ་བ། མོ་སི་ཉེ་ལི་ཡའི་བརྡ་རྟགས་བགོ་ཁྲབ་ཀྱི་ཆ་ཤས།**
- **ཀེ་ན་ཌའི་དྲ་རྒྱའི་བདེ་འཇགས་ཉེ་བ། འཕྲེལ་བ་བདེ་འཇགས་གཞི་འདྲུག་གི་ཆ་ཤས།**
- **འཇར་མན་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་གསང་བའི་ལས་ཁུངས།**
- **འཇར་མན་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་རྩ་ཁྲིམས་སྡུང་སྐྱོབ་ལས་ཁང་།**
- **མེའུ་རྡོ་ལེནྡ་རྒྱལ་ཁབ་ཀྱི་དྲ་རྒྱའི་བདེ་འཇགས་ཉེ་བ། གཞུང་འཕྲེལ་བ་བདེ་འཇགས་ལས་ཁུངས་ཀྱི་ཆ་ཤས།**
- **ཡུ་ཞེས་ཀྱི་སྤྱི་མཐུན་ཞིབ་དཔྱད་ལས་ཁུངས།**
- **ཡུ་ཞེས་ཀྱི་རྒྱལ་ཡོངས་བདེ་འཇགས་ལས་ཁུངས།**

འདི་ཡང་ ཤོག་སྟོན་འདི་གིས་ བྷ་ད་བྷ་ཌོར་ (BADBAZAAR) དང་ ཟླུན་ཤིན་ (MOONSHINE) ཟེར་མི་ གསང་སྐྱལ་མཉེན་ཆས་ (spyware) འགའིས་ཀྱི་སྐོར་ལས་ ཉེན་ཁ་གསར་པ་དང་ བསྡུས་སྤྲིག་འབད་ཡོང་བའི་ བརྡ་དོན་ཚུ་ཁྱེན་དོ་ཡོདཔ་མ་ཚད་ མཉེན་ཆས་ཚོང་ཁང་བཏོལ་སྟོང་འབད་མི་དང་ ཁོང་འཛེལ་གཏམ་ཁྱེད་ལས་ཀྱང་མི་ དེ་ལས་ མི་སྟེ་བརྡ་བརྒྱུད་ལས་སྟེ་ཚུ་ལུ་ ཤོག་སྟོན་ཚུ་ཡང་ ཁྱེན་དོ་ཡོདཔ་ཨིན་མས།

ཤོག་སྟོན་འདི་ མཉེན་ཆས་འདི་ཚུ་གི་ཁུངས་རྩྭངས་ཚུ་ཁྱེད་ལུ་ ཤོག་སྟོན་ཚིག་དང་གཅིག་ལས་ དུས་མཉམ་སྟེ་ དཔེར་བསྟན་འབད་དོ་ཡོདཔ་ཨིན།

ཡིག་ཆ་འདི་གིས་ NCSC ཚོའི་མཇོད་ཀྱི་དེས་ཚོའི་འདི་ལས་ལེན་འཐབ་ཨིན། གསང་སྐྱལ་མཉེན་ཆས: "ལས་ལེན་པའི་གནང་བ་མེད་པར་ ཐབས་འཕྲལ་ཀུ་གཞི་བཙུགས་འབད་དེ་ གནད་སྡུད་བསྡུ་ལེན་འབད་དེ་ མི་གཞན་ཚིག་ལུ་གཏང་མི་ གནོད་སྐྱོན་ལས་ཆ་ (malware) རེགས་ཚིག"

དབེ་དོན་དང་པ་ : MOONSHINE

སྐྱན་ཤྲའིན (MOONSHINE) འདི་ཨེན་ཅོ་རོའིད (Android) གི་སྟོང་མཁན་ལ་ཤུ་རྐྱག་འབད་མི་ལས་ཀ་ཚིག་ཨིན། འདི་ ༢༠༡༨ ལོར་ མེ་ཏེར་ཞིབ་ཁང་། གིས་ སྐན་ཁུ་འབད་བ་ཤར་ན། བོད་པ་ཚུ་གི་སྟེ་ཚན་ཚུ་ལུ་དམིགས་བསལ་ཤུ་རྐྱག་འབད་ནི་ལུ་བཟོ་བར་འབད་མི་ཚིག་ཨིན། MOONSHINE གིས་ ཁ་མས་རྒྱང་པ་ཚུ་ གཞི་བསྡུགས་ འབད་བསྡུག་དོན་ལུ་ ཁྱེམས་མཐུན་གྱི་ མཉེན་ཆས་ཚིག་སྟེ་ མགུ་སྐོར་རྒྱབ་ཨིན། དེ་ཡང་ ཉེ་པི་གླར་མ་གྱི་ རྒྱུན་ལམ་དང་ ཁཏ་སྐལ་བརྒྱུད་དེ་ འཛེལ་མཐུད་བཏང་མི་ཚུ་བརྒྱུད་དེ་ བརྟེ་སོར་འབད་ཡོདཔ་ཨིན་པས།

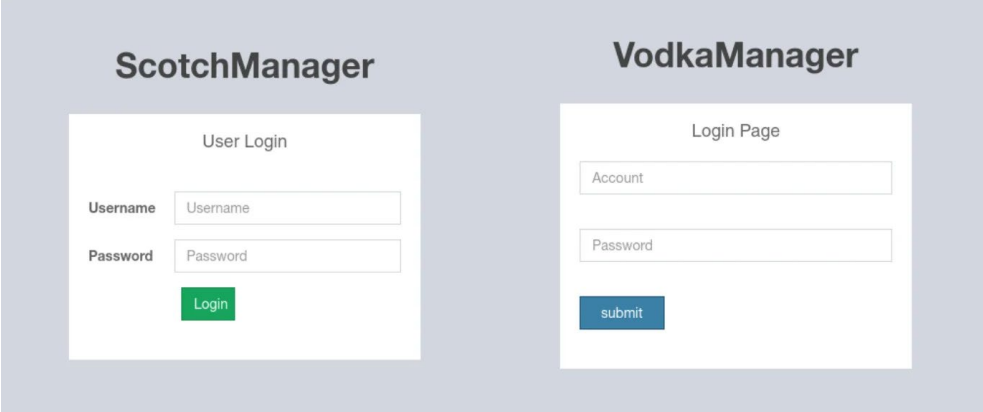
MOONSHINE གི་སྐོར་ལས་ NCSC ཞེབ་འཚོལ་གྱིས་ གཤན་གསལ་ཀྱི་བརྟ་མཚོན་སྟོན་མ་ཨིན།

- MOONSHINE གིས་ འགོ་དང་པ་སྐན་ཁུ་འབད་ཞིན་མ་ལས་རྒྱུ་ བཀྲུར་བཅོས་འབད་ཡོད་པའི་ འཇོན་སྐྱོང་ངོས་འཛུ་བ་ཅིག་ལག་ལེན་འཐབ་ཨིན།
- འཇོན་སྐྱོང་ངོས་འཛུ་བ་འདི་གིས་ ཐབས་འཕྲུལ་ཚུ་ནང་ལས་ ཡིག་སྟོང་ཚུ་ ཡིར་འཛེན་འབད་ཚུགས་པའི་ སྟོགས་ཐུབ་དང་ དེ་བཟུམ་སྟེ་ སྐུ་སྐད་དང་ གསལ་གཞི་སྐུ་བཟུང་ཚུ་ བཏོན་ཚུགས་པའི་ སྟོགས་ཐུབ་ཚུ་རྩིས་ཏེ་ བཀྲ་རྐྱག་འབད་ནི་ལུ་ སྟོགས་ཐུབ་རྒྱུ་ཆེཤ་སྟེ་ གསལ་སྟོན་འབད་ཨེ་ལུ།
- བརྟ་དོན་འཕྲུལ་རིག་ཐོག་ལས་ གསོ་བོར་བཏོན་ཡོད་པའི་ MOONSHINE འཇོན་སྐྱོང་ངོས་འབྲ་བ་ཚུ་གི་ཆ་ཚན་ཅིག་ འཚོལ་ཐོབ་ཡོདཔ་ཨིན། འབྲེལ་རིག་ཏུ་སྐུ་ གི་ཁྲོན་ཀྱི་ཡན་ཁུངས་བཏོན་ཐབས་འཕྲུལ་རིག་ལས་ཁུངས།ལུ་གོམ་ཨིན།

འཛིན་སྐྱོང་། འཕེལ་མཐུད་ངོས་འདེགས།

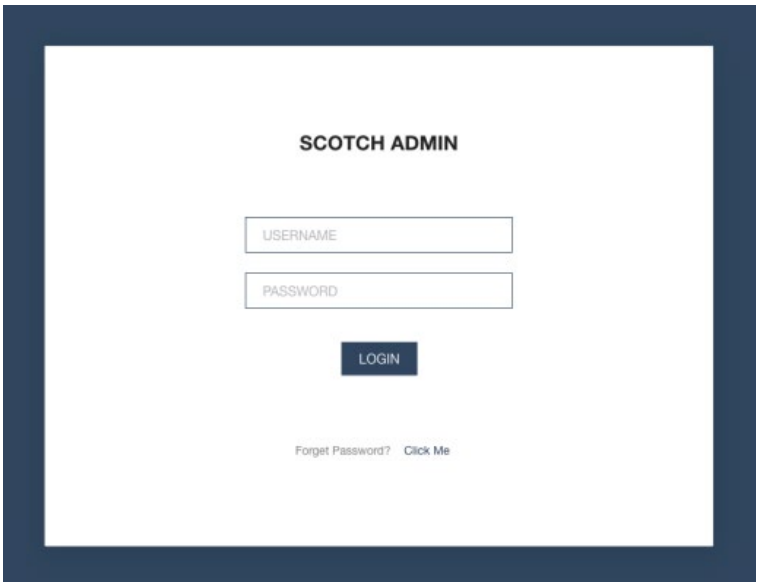
MOONSHINE འཛིན་སྐྱོང་འཕེལ་མཐུད་ངོས་འདེགས་ཚུ་གི་ཉེ་མའི་སྐན་ཞུ་གིས་ བསྒྲུར་བཅོས་འབད་ཡོང་བའི་རྐྱག་སྐྱོན་མེན་ལས་ འདི་གིས་ གོང་འཕེལ་འགྱོ་བའི་བསྒང་ཡོད་པ་སྟེ་ བསམ་འཆར་བགོད་པ་མེན།

འཛིན་སྐྱོང་འཕེལ་མཐུད་ངོས་འདེགས་ཀྱི་དུས་འགོ་དང་པ་འདི་ Citizen Lab's 2019 སྐན་ཞུ་ནང་ལུ་མཚོང་ཚུགས།



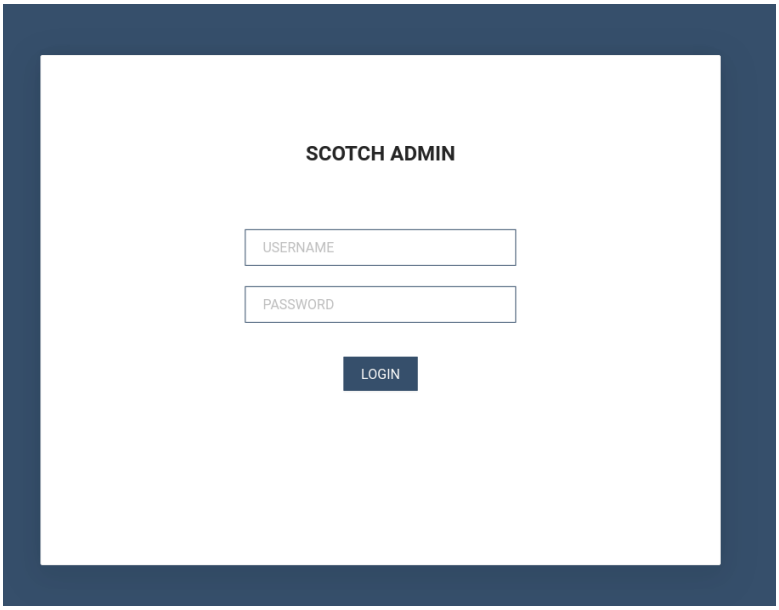
དུས་རིས་ 1: MOONSHINE འཛིན་སྐྱོང་འཕེལ་མཐུད་ངོས་འདེགས་ཚུ་ མི་སེར་ཞིབ་བང་གིས་ ལྷི་ལོ་༢༠༡༨ ལའི་སྐན་ཞུ་ 'Missing Link ཞེས་མི་རྟེ་ཚན་ཚུ་ དམིགས་གཏད་བསྐྱེད་དེ་ འགྱུར་འཛིན་ལས་ཁག་ལེན་འཐབ་མི་ཚུ་' ནང་མཚོང་ཡོདཔ་མེན།

སྤྱི་ལོ་༢༠༢༡ འགོ་བསྟུགས་ཁམས་ཅིག་ཁར་ Lookout གིས་ འཛིན་སྐྱོང་འཕེལ་མཐུད་ངོས་འདེགས་སོ་སོ་ཅིག་ སྐན་ཞུ་འབད་ཡོདཔ་ད་ དེ་ཡང་ གཤན་གསལ་སྐར་མཚོང་ཚུགསཔ་རྟེ་ འཕྲུ་རྟེ་བཟོ་བགོད་འབད་ཡོདཔ་མེན། ཥཤར་རིས་༡ བའི་ནང་ ཉེ་མའི་ངོས་འདུ་བ་ཚུ་ཚད་བསྟུགས་ཏེ།



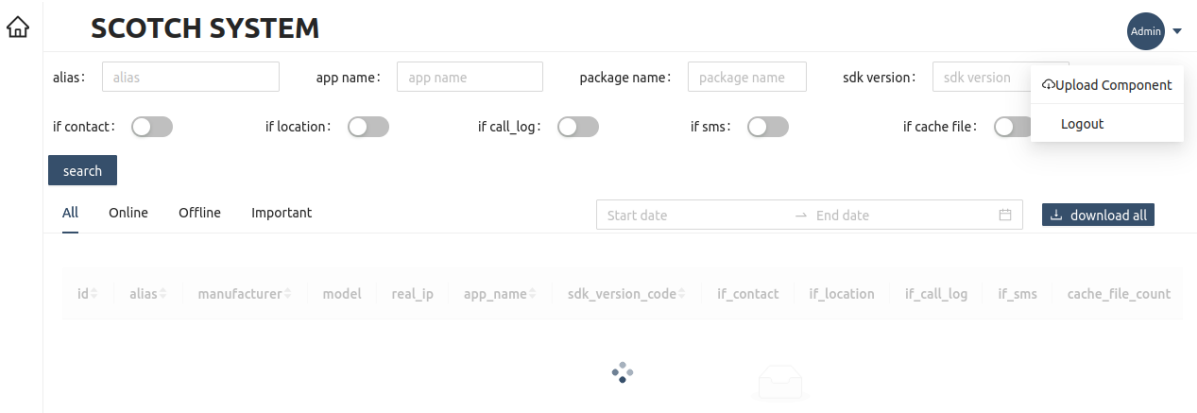
དུས་རིས་ 2: MOONSHINE འཛོངས་སྐྱོང་ངོས་འདུ་ཏེ་Lookout གི་ ༢༠༢༡ ~~སྤྱི་ཟླ~~ 'MOONSHINE ནང་མཚོང་ཡོད་ : ངོད་མི་དང་ཡུ་ཀུར་ཚུ་ཡུ་དམིགས་གཏད་བསྐྱེད་དེ་ ཐུ་ཅག་གི་ APT POISON CARP གིས་ Android Surveillanceware གོང་འཕེལ་གཏང་ཡོདཔ།

སྤྱི་ལོ་ ༢༠༢༡ ཟླ་བ་ ༤ བའི་ནང་ལུ MOONSHINE བགོད་སྐྱོད་དང་ཚད་འཛིན་ (C2) གི་ scan ཅིག་གིས། ༢༠༢༢ ལོའི་སྐྱོད་ཚུལ་དང་འབྲེལ་བའི་ སྐྱོད་ཚུལ་ ཅིག་མཚོང་སྟེ། **'གསང་ཚང་བརྟེད་ས'** ཟེར་བའི་ལས་འགན་འདི། རི་མོ་ ༢ བའི་ནང་ལུ་ཡོད་མི་བཟུམ་སྟེ་ད་སྔོ་ལགཔ་ལེན་འཐབ་མི་ཚུགས་པར་ཐོན་ཡོད།:



དཔེ་རིས་ 3: སྤྱི་ལོ་ ༢༠༢༤ ཟླ་བ་ ༤ ཐའི་ནང་ལྟ་མཆོང་བའི་ MOONSHINE འཛིན་སྐྱོང་འབྲེལ་མཐུད་ངོས་འདེགས་འདི་ལྟ་དུ་སྟེ་ 'གསང་ཡིག་བརྡེད་སེ་' ཟེར་བའི་དྲི་བ་མེད་པར་ཚོན་ཡོད།

འཛིན་སྐྱོང་འབྲེལ་མཐུད་ངོས་འདེགས་འདི་ དཔྱད་འཚང་བའི་སྐབས་ལྟ་ བེ་ནུལ་ནང་འགོད་ཀྱི་ ནང་དོན་ཚུ་སྐྱོན་ཡོད་པ་ལས་ དེ་གིས་ བདེ་སྐྱིག་བཟོ་ཡོད་པའི་ ཐབས་འཕྲུལ་ཚུ་ གི་ ཁ་གསལ་ཚུ་ ག་དེ་སྟེ་ གསོག་འཇོག་ འབད་ནི་ཕིན་ན་ གསལ་སྐྱོན་འབད་ཡོད་པ་ཨིན



དཔེ་རིས་ 4: MOONSHINE འཛིན་སྐྱོང་འབྲེལ་མཐུད་ངོས་འདེགས་བའི་ནང་བསྐོང་ཚོགས་ལེའུ་ཀྱི་ཆ་ཤས་ལྟ་ཡོད་པའི་སྐབས་ལེའུ།

Lookout ཞེན་འཇུག་གིས་ཚོར་བ་ཅན་གྱི་ཐབས་འཕྲུལ་ནས་ MOONSHINE C2 ལར་བར་ཚུ་ལུ་ **སྐུགས་** ཅེགཔ་བརྒྱུད་དེ་འགྱོ་བ་སྐྱོན་ཡོད། 'སྐུགས་' གི་གནས་གོང་འདི་ ཉམས་ཆུད་ཐབས་འཕྲུལ་ཀུ་ གནོད་པ་ཚུ་ལུ་གཞི་བཞག་སྟེ་ཨིན།

ཚོགས་ལེབ་ནང་འགོད་ཀྱི་ གེར་ཐིག་ 'if_contact', 'if_location', 'if_call_log' དང་ 'if_sms' ཚུ་གིས་ MOONSHINE དཔེ་ཚད་ཆ་མཉམ་ལུ་ བདེ་སྐྱིག་བཟོ་ཡོད་པའི་ཐབས་འཕྲུལ་ཚུ་ལུ་ འཕྲུལ་སྐྱོང་ཆ་ཚང་མེདཔ་སྟེ་ བསམ་འཆར་བགོདཔ་ཨིན། འདི་བརྒྱལ་ཀྱི་གེར་ཐིག་ཚུ་གི་ཤེས་ཡོན་དང་ ཐབས་འཕྲུལ་ལས་ C2 ལུ་སྐྱོང་མི་ 'སྐུགས་' འདི་གིས་ ཉེན་ཁ་ཅན་གྱི་འཐབ་རྩེད་ཚུ་གིས་ འཛིན་སྐྱོང་ངོས་འདུ་བ་ལུ་འཕྲུལ་སྐྱོང་འབད་མི་ མི་ངོ་ཚུ་ལུ་ མཉེན་ཆས་ངན་པའི་ འཕྲུལ་སྐྱོང་གི་གནས་ཚད་བཏང་སྟེ་ བསམ་འཆར་བགོདཔ་ཨིན།

སྒྲིར་བཏང་ལུ་ སྒོག་རིམ་ཚུ་གིས་ ཐབས་འཛུལ་ཚུ་ལས་ བརྟ་དོན་བསྡུ་ལེན་འབད་ནི་ལས་ བཀག་ཐབས་ལུ་ བསྒབ་བྱ་དུག་ཨོས་འདི་ ཁབ་ལེན་མ་འབད་བའི་ཉེ་མ་ སྒོག་རིམ་གྱི་གནང་བ་ཚུ་

སྒྲིར་བཏང་མེན་པའི་དོན་ལུ་ བརྟག་དཔྱད་འབད་ནི་འདི་ཨིན། ཨིན་རུང་ MOONSHINE དབེ་ཚད་ཚུ་གིས་ སྒོག་རིམ་གྱི་ལུ་འགན་དང་འཇེལ་བ་ཡོད་པའི་ གནང་བ་ཚུ་འཚོལ་ཤུ་ལས་ དོགས་པ་མེདཔ་སྒེ་མཐོང་ཨིན་རུང་ ཐབས་འཛུལ་ཚུ་ལས་ བརྟ་དོན་བསྡུ་ལེན་འབད་ནི་ལུ་ཡང་ གནང་བ་འདི་ཚུ་ལག་ལེན་འཐབ་ཨིན།

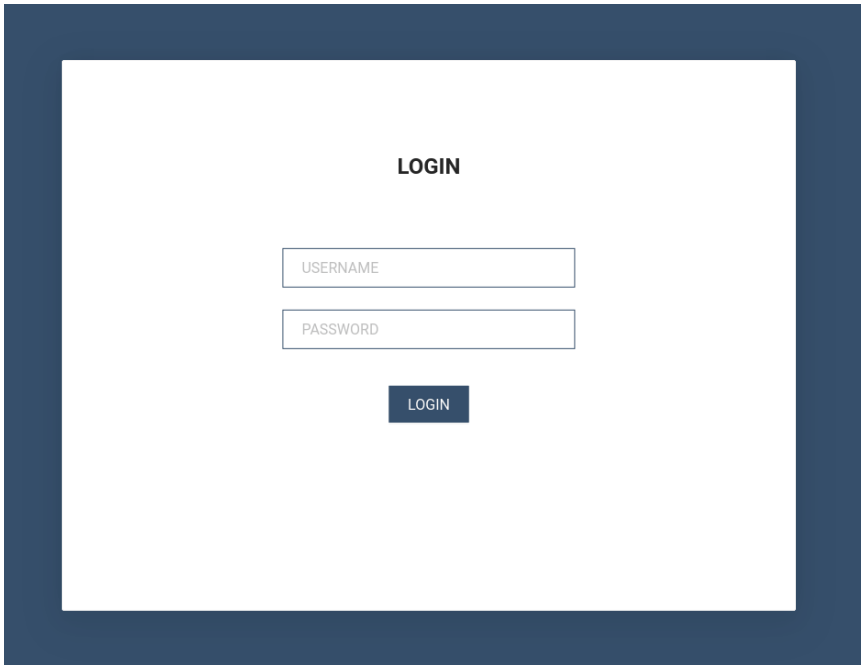
ཨིན་རུང་ MOONSHINE དབེ་ཚད་ཚུ་གིས་ སྒོག་རིམ་གྱི་ལུ་འགན་དང་འཇེལ་བ་ཡོད་པའི་ གནང་བ་ཚུ་འཚོལ་ཤུ་ལས་ དོགས་པ་མེདཔ་སྒེ་མཐོང་ཨིན་རུང་ ཐབས་འཛུལ་ཚུ་ལས་ བརྟ་དོན་བསྡུ་ལེན་འབད་ནི་ལུ་ཡང་ གནང་བ་འདི་ཚུ་ལག་ལེན་འཐབ་ཨིན། ཚེ་དེ་ཚའི་ཡིག་ཆའི་ཐོན་རིམ་སྤྱོད་མ་ཚུ་ནང་ མནཔ་རིན་ནང་ ཚེ་དེ་ཚའི་མིང་ཚུ་ཡོངས་ཨིན།

གཟུགས་བརྙན་ སྤྱོད་མཁན།

MOONSHINE ལེ་ནུལ་ཚུ་འཚོལ་ཞིབ་འབད་བའི་སྐབས་ ངོ་མ་སྟེ་ གཙོ་བོར་བཏོན་ཡོད་པའི་གནས་སྐྱངས་ཚུ་ མཐོང་ཡོངས་ཨིན། གཟུགས་བརྙན་སྤྱོད་མཁན་ཟེར་མི་འདི་ ཚའི་དེ་ཁ་བྱང་གཅིག་གིས་ ཡོངས་འཛེལ་འཛར་སྒོ་ལེ་ཤ་ཅིག་ ཚར་གཅིག་ལུ་ ཏོསིའེ་འབད་ཚུགས་པའི་སྐབས་ལུ་ཨིན། འ་ནི་ བརྟ་དོན་ཏོསིའེ་འབད་ཡོད་པའི་གནས་སྐྱངས་དང་ ཏོསིའེ་

འབད་ཡོད་པའི་མངའ་སྡེངས་ཚུ་གི་ IP ཁ་བྱང་ཚུ་ ཤེས་རྟོགས་ཡོད་པའི་ མཉེན་ཆས་ངན་པའི་དེ་ཚད་གང་རུང་ཅིག་ནང་ མཐོང་མ་ཚུགས།

འཛོན་སྐྱོང་འཛེལ་མཐུད་དོས་འདེགས་ཀྱི་དེ་ཚུ་འདི་ཁ་ཐང་ཡོད་དེ། ཤོག་ལེབ་ཚུ་གི་མཚོ་མིང་འདི་ སྒོན་མ་མཐོང་མི་ **'SCOTCH ADMIN'** གི་ཚབ་ལུ་ **'LOGIN'** སྟེ་ཡོད་མི་ལས་བརྟེན།



དེ་རིས་ 5: SCOTCH ADMIN གི་ཚབ་ལུ་ LOGIN མཚོ་མིང་ལག་ལེན་འཐབ་སྟེ་ MOONSHINE འཛོན་སྐྱོང་ངོས་འཛུ་བ།

དེ་མ་ཚད་ ལེ་ནུལ་གྱ་ཡོད་པའི་ནང་དོན་ཡང་ བར་རིས་ ཧ་ལས་ ཁྱད་བར་ཡོད་པ་ཞིན་ དེ་ཡང་ བར་རིས་ ༧ ནང་མཚོ་ཡོད་པ་ཞིན།

དེ་རིས་ 6: རྩོག་བཟོའི་གཏོང་ལེན་འབད་མི་ MOONSHINE འཛོན་སྐྱོང་འཛེལ་མཐུད་ངོས་འདེགས་ཀྱི་ནང་བསྐོད་ཨོག་ལེབ་ཚུ་ལག་ཡོད་པའི་ཐུ་ཨོག་ལེབ།

པར་རིས་ ७ པའི་ནང་ ཤེ་ན་ལ་འདི་ པར་རིས་ ९ ནང་ ཤེ་ན་ལ་གྱི་ བཏོན་བཏང་ཡོང་བའི་ཐོན་རིམ་ཅིག་ཤེས་མེད། ཐེག་ཁྲམ་ནང་ལ་ ཀེར་ཐེག་མེང་ ‘id’, ‘manufacturer’ དང་ ‘model’ ཟེར་མི་ ཤེ་ན་ལ་ཚུ་གི་ གཅིག་ཁར་བསྡོམས་པའི་ཁྱད་ཆོས་ཚུ་ཨིན།

དངོས་གནས་གཙོ་བོར་བཏོན་ཡོང་བའི་ MOONSHINE གནས་སྤྱངས་ཚུ་ འཚོལ་ཐོབ་ཡོངས་ཨིན།

ཉོ་མེན།	IP ཁ་བྱང་།
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

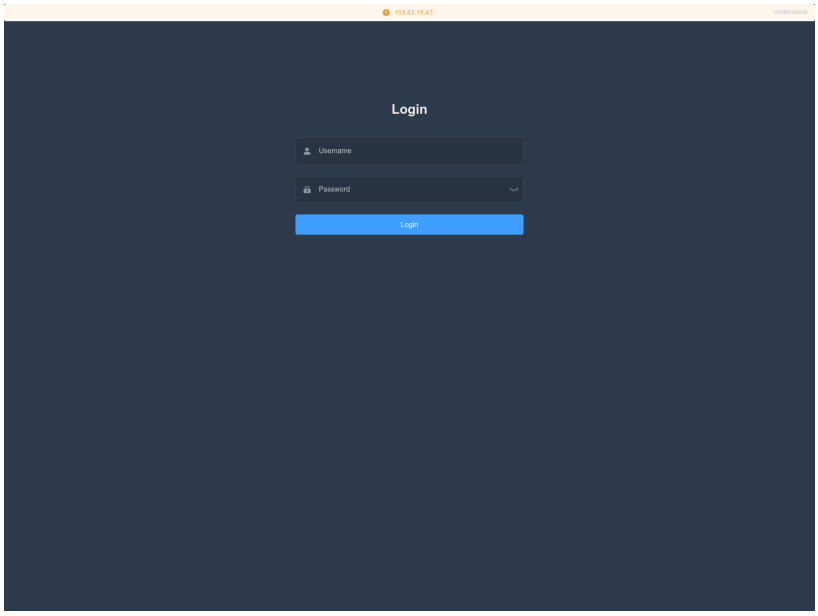
ཉོ་མེན་འདི་ཚུ་ འགྲོས་ལུ་ MOONSHINE སྒྲུབ་སྒྲིར་ཆས་ཚན།, མཉེན་ཆས་ངན་པ་གཞི་བཙུགས་འབད་ནི་འདི་ དོན་ལུ་ བརྟ་འཚོལ་གྱི་ཉེན་ཁ་ཚུ་ ལག་ལེན་འཐབ་ནི་འཐུན་ཤུར་འབདགས་ཨིན། འགྲུལ་འཕྲིན་ཐབས་འཕྲུལ་ཚུ་ཀྱ། མཉེན་ཆས་འདི་ལུ་ 'Dark Nimbus' ཟེར་ མིང་བཏགས་ཡོངས་ཨིན།

གསལ་བཤད་ཀྱི་དོན་ལུ་ MOONSHINE འཛིན་སྒྲིང་ངོས་འཛུ་བ་ཚུ་ MOONSHINE མཉེན་ཆས་ངན་པའི་དུས་ཚོད་ཚུ་གིས་ བརྒྱུད་འཕྲིལ་འཐབ་མི་དང་ ཉམས་ཆུད་པ་གི་གནས་སྟུད་ཚུ་ ཕྱིར་འཐེན་འབདཝ་ཨིན། Trend Micro གིས་སྐྱེན་ཞུ་ཐུལ་བའི་ MOONSHINE སྒྲུབ་སྒྲིར་ཆས་ཚན་ཚུ་འདི། འགྲུལ་ཆས་ཚུ་ལུ་ Dark Nimbus ཟེར་བའི་གནོད་སྐྱེན་མཉེན་ཆས་བརྒྱུ་ནི་འདི་ དོན་ལུ་ བར་ཞུ་ཟར་གྱི་ཉེན་ཁ་ཚུ་སྒྲུབ་སྒྲིར་འབད་མི་ཐ་དད་པའི་ཐེས་རྟོགས་ཅིག་ཨིན། གཞན་ཡང་། Dark Nimbus དང་ MOONSHINE འདི་ཤ་ཅང་ཐ་དད་པའི་གནོད་སྐྱེན་མཉེན་ཆས་ཨིན།

MOONSHINE འཛིན་སྒྲིང་ངོས་འཛུ་བ་དང་ MOONSHINE བཀོལ་སྒྲིང་ཅ་ཆས་གཉིས་ཆ་ར་ལུ་ གསང་ཡིག་གཅིག་ཁར་བསྡོམས་ཏེ་ཡོངས་ལས་ བར་རིས་༣ དང་༤ ནང་ ནང་བསྒྲིང་བརྟ་སྐྱེན་ཚུ་ ཅོག་འཐདཔ་སྣེ་ཡོངས་མ་ཚད་ བར་རིས་ཉ དང་༡ ནང་ ཐོག་ལེབ་ཀྱི་ནང་དོན་ཚུ་ཡང་ ཅོག་འཐདཔ་སྣེ་ཡོངས་ཨིན། དེ་མ་ཚད་ འབྲུང་ཁུངས་ཨང་རྟགས་ནང་ ‘webpackJsonpreact-scotchui’ ཡིག་རྒྱུན་ཡང་ཡོངས་ཨིན།

ཉེན་ཁ་སྒྲིང་མཐན་ཚུ་གིས་ MOONSHINE སྒྲུང་སྒྲིར་ཆས་ཚན་ལུ་སྣེའུ་ཁུངས་ཨཐུང་འབད་ཞིན་མ་ལས་ བོད་པ་དང་ཕྱི་ཡི་གུར་ཚུ་ལུ་འཛེལ་བ་ ཡོད་པའི་ གཏུབས་བརྐྱན་ཚུ་ལུ་ ལས་སྒྲིན་འབད་མི་ URL སྣེའུ་ལམ་ཚུ་བཟོ་ཡོད་དེ། འདི་གིས་ MOONSHINE གི་དམིགས་གཏད་དང་གཅིག་པར་འདུག

MOONSHINE སྒྲུང་སྒྲིར་ཆས་ཚན་གྱི་ཉོ་མེན་གང་ངེད་ལེན་འབད་མི་ IP ཁ་བྱང་མང་པོ་གི་ཁྲོད་ལུ port 444 ལུ་ 'VLiteUI' ཟེར་མིང་བཏགས་པའི་ ནང་བསྒྲིང་ཨོག་ལེབ་ཅིག་ཡོང། ཨོག་ལེབ་འདི་ ཁྱབ་ཚེཕ་སྣེ་ བཀྲ་མ་ཚུགསལ་ལས་ འ་མེ་ IP ་ཚུ་གུ་ཡོང་མི་འདི་གིས་ འཁྲབ་རྩེད་པ་ཚུ་གི་ལག་ལེན་ཚུ་ལུ་ འཛེལ་མཐུད་འབད་ཚུགས་པའི་ བང་མཚོན་སྒྲིན་མ་ཨིན།



དཔེར་ན། 7: MOONSHINE བཀོལ་སྤྱོད་ཅ་ཆས་ཀྱི་ཡང་ གཙོ་བོར་བཏོན་མི་ IPs ཚུ་ནང་ བཟླ་ཏོགས་འབད་མི་ HTML མིང་ 'VLiteUI' དང་ཅིག་ཁར་ ཅང་བསྒྱོད་པ་ཆུལ།

Trend Micro གི་ Dark Nimbus ལུ་ཞིབ་དཔྱད་འབད་མི་ དེ་གིས།གཞོན་སྐྱེན་ མཉེན་ཆས་འདི་གིས་ ཐབས་འཕྲལ་ལུ་ཡོང་བའི་ གནས་ཚུལ་ཚུ་ ཆ་ཚང་བའི་ ཐོ་ཡིག་བསྡུ་ལེན་འབད་ཚུགས་སྟེ། XMPP གནད་སྡེལ་བེད་སྤྱོད་འབད་དེ་ C2 དང་འབྲེལ་གཏུབ་འབད་ཚུགས་པའི་གནས་ཚུལ་མཐོང་སྟེ་ཡོད།

Trend Micro གིས་ཡང་ Dark Nimbus གི་ཐོན་རིམ་ལ་ལུ་ཅིག་ནང་ལུ་ 'DKNS' གི་ཡིག་རྒྱུན་འདི་ ཁྱབ་ཚེཔ་སྟེ་ཡོད་པ་སྟེ་ངོས་འཛིན་འབད་ནུག

'**ansec[.]com**' (TrendMicro གིས་ Dark Nimbus C2 སྟེ་ཐོ་བཀོད་འབད་མི་) འདི་ཡང་ མགོ་མེད་ནང་ལུ་ DKNS ཡོད་པའི་ད་ ཨོག་ལེབ་ཚུ་ཁག་ཏུ་ཡོད་མི་གཞན་གྱི་ IP ཁ་བྱང་ཚུ་གི་དོན་ལུ་ XMPP ཁབས་ཀྱི་ཚུ་ནང་ལུ་མཐོང་ཡོད།

- DKNS Android远程取证系统 (DKNS Android ཐག་རིང་ཞིབ་དཔྱད་མ་ལག)
- DKNS云网侦控平台 (DKNS Cloud སྤྲིན་དུ་རྒྱ་ཞིབ་དཔྱད་ཚད་འཛིན་སྐེགས་བུ)
- DKNS 云网侦控平台 (DKNS Cloud སྤྲིན་དུ་རྒྱ་ཞིབ་དཔྱད་ཚད་འཛིན་སྐེགས་ཏུ)
- DKNS远程控制侦查系统 (DKNS ཐག་རིང་ཚད་འཛིན་ཞིབ་འཚོལ་ལས་ལུགས)

XMPP ཁབས་ཀྱི་ནང་ལུ་ '**ansec[.]com**' ཡོད་པའི་གཞན་གྱི་ IP ཁ་བྱང་ཚུ་གི་ཚན་པ་ཅིག་ལུ་ འ་ནི་མགོ་མེད་ཡོད་པའི་དུ་ཨོག་ལེབ་ཚུ་ཡོད་པས།

- UPSEC互联网控制指挥系统 (UPSEC དྲ་རྒྱ་ཚད་འཛིན་བཀོད་སྤྱོད་མ་ལག)
- UPSEC无线侦控系统 (UPSEC Wireless བེད་མེད་ཉུ་རྐྱག་ཚད་འཛིན་མ་ལག)
- UPSEC重点人数据还原系统 (UPSEC གལ་ཆེན་མི་སྣ་གནས་ཚད་སོར་རྒྱང་ལས་ལུགས)

དང་འཁྲིལ་ན། ~~རྩ་རེག་དྲ་རྒྱ~~ , 'UPSEC' འདི་ HTML ཨོག་ལེབ་ཚུ་གི་མིང་ཚུ་ནང་ བཟླ་རྐྱག་འབད་དེ་ 'Sichuan Dianke Network Security Technology Co., Ltd' ལུ་ གོམ་ཚིན།

དབེ་ངོན་གཞིས་བ། : BADBAZAAR

BADBAZAAR རེར་མི་འདི་ ཡུ་གུར་དང་སོང་མི་ དེ་ལས་ ཐའི་ཤན་གྱི་མི་ངོ་ཚུ་ དཔེགས་གཏང་བསྒྲིད་དེ་ iOS དང་ Android གི་རིགས་ཚུ་ཡོད་པའི་ འགྲུལ་འཕེན་གྱི་ མཉེན་ཆས་ངན་པ་ཅིག་ཨིན། འདི་ཡང་ མི་སྡེ་བརྒྱུད་བརྒྱུད་གྱི་ ས་སྒོ་དང་ གཞུང་འཛིལ་གྱི་ མཉེན་ཆས་ཚོང་གང་ཚུ་ནང་ ཁྱབ་སྤེལ་འབད་ཤ་ཨིན་པས། Volexity ནས་ཉེ་ཆར་བྱང་བའི་སྐན་ཁུ་ལས། BADBAZAAR གི་རིགས་མི་འབྲ་བ་ཚུ་སྒོར་ཏེ་ BadSolar དང་ BADBAZAAR དེ་ལས་ BadSignal སྤེ་ཁ་གསེས་འབད་ཡོད། འགྲུར་ཐྲོག་གསུམ་ཆ་ར་ ཐབས་འཐུལ་དང་བགོ་སྐྱོང་བརྒྱ་དོན་བསྡུ་ལེན་འབད་ནི་ལུ་ལག་ལེན་འཐབ་མེ་ ལས་འགན་ཚུ་ གཅིག་ཁར་མཐུད་དེ་ཡོད་པ་ཨིན།

NCSC གིས་ BADBAZAAR གི་ཞིབ་འཚོལ་ནང་ གཤམ་གསལ་གྱི་གནད་དོན་ཚུ་ གསལ་སྟོན་འབད་ཡི།

- C2 domains ཚུ་སྤེ་ཚན་སྤེ་བཏུབ་མི་ལས་ལོ་རྒྱས་ཅན་གྱི་ཉེན་ཁ་གསལ་བའི་ནང་སྐན་ཁུ་འབད་མི་ domains ཚུ་དང་ འཛིལ་བ་ གཞན་ཡང་མངོན་གསལ་འགྱུར།
- C2 ས་བར་དང་ མཉེན་ཆས་ངན་པའི་དུས་ཚད་ཚུ་གིས་ འཁྲབ་རྩེད་པ་གཞི་རྟེན་དང་འཛིལ་བའི་ ཧོསིའི་མིང་ཚུ་ གསལ་སྟོན་འབད་ཤ་ཨིན།
- ཉེན་ཁ་སྤོུང་མཁན་ཚུ་གིས་ཁོང་རའི་གནོད་སྐྱོན་ས་ཁ་ཤེར་ཁུལ་ཡོངས་མེད་ས་ཀོར་ཚུ་ལས་ཐོན་ཏེ་ཁྱབ་བསྒྲགས་འབད་ནིའི་དོན་ལུ་ ལག་ལེན་འཐབ་མི་གཞན་གྱི་ངོ་སྤྲོད་ཚུ།

WHOIS སྤེ་ཚན་སྤེ་བཏུབ་ནི / Domain སྤྲོད་མཁན།

‘UJYJYUJ’

ESET གིས་སྐྱན་ཁུ་འབད་མི་ BADBAZAAR domain ‘**signalplus[.]org**’ གི་ WHOIS records ཚུ་དཔྱད་པ་འབད་བ་ལས་ **‘State’** field ནང་ **‘UJYJYUJ’** གི་གནས་གོང་འདུག

གནས་གོང་གཅིག་མཚུངས་ཡོད་པའི་ཅོ་མེན་གཞན་ཚུ་འཚོལ་ཞིབ་འབད་མི་འདི་གིས་ འོག་གི་སྤྲོ་བ་ཡོད་པའི་མངའ་ཁོངས་ཚུ་གསལ་སྟོན་འབད་ཤ་ཨིན།

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

(རྒྱུར་སྤྱགས་ཀ་ བར་རིས་ ༡ ལུ་གཟིགས།)

signalplus[.]org དང་ **tubevideoplus[.]org** དེ་ལས **thetubeplus[.]com** ཚུ་ BADBAZAAR C2 domains སྤེ་སྐྱན་ཁུ་འབད་ཡོད་མི་དང་ ESET གིས་ sub domain **mail.pmumail[.]com** འདི་ FlyGram proxy server སྤེ་སྐྱན་ཁུ་འབད་ཡོད། FlyGram འདི་ གནོད་བ་ཅན་གྱི་ཡོངས་འཛིལ་འཁྲབ་རྩེད་པ་ཚུ་གིས་ བཟོ་ཡོད་པའི་ BADBAZAR མཉེན་ཆས་ཅིག་ཨིན། (བེད་བ་ཧོར་ཚེས་གཞན་མིང་ཐོ་དོན་ལུ་རྒྱར་སྤྱར་ཤུ།)

ཉེ་སྤྲོམ་འགྱོ་བའི་གནས་གོང་ཚུ།

NCSC གིས་ ཐོ་བགོད་འབད་ཡོད་པའི་ BADBAZAAR C2 མངའ་ཁོངས་གཞན་ཚུ་ནང་ ཉེ་སྤྲོམ་གྱི་ འགྱོ་ཐངས་ཚུ་ ཅོག་འཐདཔ་སྤེ་ མཚོང་ཡོངས་ཨིན་པས།

དཔེར་ན་, འོག་གི་མངའ་སོངས་ཚུ་ཆ་མཉམ་ལུ་ གནས་གོང་ ' ཡོད་པ་ཨིན། **‘REWR’** ནང་བརྟག་དཔྱད་བྱས། **‘State’** ས་སྟོར་ (ཉེ་མ་ལག་ལེན་འཐབ་ཡོད་པ་བརྒྱམ):

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

(རྒྱུར་སྤྲུགས་ཀ་ པར་རིས་ 2 ལུ་གཟིགས།)

'FSDF' state field གནས་གོང་ཡོད་མི་ domains ཚུ།

BADBAZAAR C2 domains གི་སྡེ་ཚན་གཞན་ཅིག་ལུ་ **‘State’** གནས་གོང་ **‘FSDF’** ཡོད་:

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

(རྒྱུར་སྤྲུགས་ཀ་ པར་རིས་ 3 ལུ་གཟིགས།)

ཉེ་སྐོན་འགྱོ་བའི་བེ་ལུས་ཀྱི་དང་གཅིག་ཁར་ ལོ་རྒྱུས་སྒྲིན་ཞུ།

BADBAZAAR domains ཚུ་གི་ WHOIS records ནང་ keyboard walking གནས་གོང་ཚུ་ལག་ལེན་འཐབ་མི་འདི་ TA413 གིས་བོད་པའི་ཚོགས་ཐེ་ཚུ་ལུ་དམིགས་བསལ་གཏོ་གཞི་རིའི་ལོ་རྒྱུས་ཅན་གཅོད་ཚུགས། Recorded Future གིས་སྤྱོད་མཁན་ ཀྱིས་ ཚད་འཛིན་འབད་མི་ domains ཚུ་གིས་བོད་པའི་ཚོགས་ཐེ་ཚུ་ལུ་ལོག་སྟེ་འཛར་སྤྲོན་འབད་བ་དང་ ཐོ་འགོད་པའི་ཚོགས་ཐེ། གནས་གོང་ལུ་ **"asfasf"** ལག་ལེན་འཐབ་མི་ཚུ་གཟིགས་ཡོད།

clublogs[.]com

Lookout གིས་ཞོག་མི་ BADBAZAAR samples ཚུ་ནང་ C2 domain ཐེ་ **‘xle.clublogs[.]com’** འདུག་རྟ་བའི་ཅོ་མེན་ **‘clublogs[.]com’** འདི་ IP ཁ་བྱང་ **‘95.179.210[.]85’** ལུ་འཛོག་ཡོད་པ་དང་། SSL ལག་ཆྱེར་ ཅིག་ཡང་ ཡོད་དེ་ ཚོ་གི་བརྩོད་གཞི་དང་སྤྱོད་མི་གི་བེ་ལུ་ **‘CN=WIN-50QO3EIRQVP’** མིན། གནས་གོང་འདི་ SSL pinning ལག་ལེན་འཐབ་སྟེ་ འཛིལ་བ་ འདེན་སྤྱོད་བར་ཚད་མེད་དོན་ལུ་ BADBAZAAR samples ནང་རྒྱེད་མི་ SSL certificates ཚུ་དང་མཚུངས་པ་རེད།

IP address **95.179.210[.]85** གི་hosting ལོ་རྒྱུས་ལས་འདོད་ཚོ་ཡོད་མི་domains ཚུ་འབོག་ལུ་ཡོད:

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

(རྒྱུར་སྤྲུགས་ཀ་ པར་རིས་ 4 ལུ་གཟིགས།)

www.voiceoftibet[.]net

Domain ‘**www.voiceoftibet[.]net**’ འདི་ 'Voice of Tibet' ཆུང་འཕེན་ཁང་སྤེ་ལོག་སྤེ་འཚར་སྒོར་འབད་འབད་བའི་སྡང་ཡོད་མི་དང་ TA413 གིས་ལག་ལེན་འཐབ་མི་ TTP དང་འདྲ་ཏོ་ཡོད།

ཏོ་མེན་ ‘**rewrwer[.]com**’ འདི་ཀ་གོ་ལས་ BADBAZAAR ཏོ་མེན་ཚུ་གི་ WHOIS རེ་ཀོར་ནང་ལུ་ཐོབ་ཡོད་པའི་ ‘**State**’ གནས་གོང་ ‘**REWR**’ དང་འདྲ་མཉམ་ཅིག་མིན།

ཏོ་མེན་ ‘**clublogs[.]com**’,‘**rewrwer[.]com**’, ‘**voiceoftibet[.]net**’ དང་ ‘**myloughborough[.]com**’ འདི་ཚུ་ཆ་མཉམ་སྒོག་འཕེན་ཁ་བྱང་ ‘**tplutalova@list[.]ru**’ དང་གཅིག་ཁར་ ཐོ་འགོད་འབད་ཡོདཔ་མིན།

actuallys[.]com

‘**actuallys[.]com**’ གི་ WHOIS ཐོ་བཀོད་ཚུ་ལས་འཐུལ་རིག་དང་བདག་སྐྱོང་སྒོག་འཕེན་ཁ་བྱང་ཚུ་ ‘**tplutalova@list[.]ru**’ མིན་རུང་ ཐོ་འགོད་པའི་སྒོག་འཕེན་ཁ་བྱང་འདི་ ‘**ivan_s81@mail[.]ru**’ མིན་པའི་དཔེ་ཅིག་མཐོང་ཡོདཔ་མིན།

ཏོ་མེན་ ‘**actuallys[.]com**’ གི་ལོ་རྒྱུས་ཅན་གྱི་ WHOIS གནས་ཚུལ་ལས་ ༢༠༡༨ ཟླ་ ༢ ཚེས་ ༢༤ ལུ་ཐོ་འགོད་འབད་ཡོད་པའི་སྒོག་འཕེན་ཁ་བྱང་ ‘**wangminghua6@gmail[.]com**’ ཐོན་ཡོདཔ་མིན། ༢༠༡༨ ཟླ་ ༣ ཚེས་ ༡༡ ལུ་ སྒོག་འཕེན་འདི་ ‘**ivan_s81@mail.ru**’ ལུ་བསྒྱུར་ཡོདཔ་མིན་རུང་ ཐོ་འགོད་པའི་ཚུ་སེལ་ཚེས་གྲངས་འདི་གཅིག་པ་བཞག་ཡོདཔ་མིན།

wangminghua6@gmail[.]com

སྒོག་འཕེན་ཁ་བྱང་ ‘**wangminghua6@gmail[.]com**’ འདི་ ལོ་རྒྱུས་ཅན་གྱི་ཉེན་ཁ་ རིག་པའི་སྐན་ཁུ་ནང་ལུ་ ཐོབ་ཡོད་པའི་ ཏོ་མེན་ཚུ་ ཐོ་འགོད་འབད་ནི་དོན་ལུ་ལག་ལེན་འཐབ་ཡོདཔ་མིན། ༢༠༡༤ ལོར་ Palo Alto གིས་གཅོད་བྱེད་ལས་རིམ Cmstar གི་ C2 ཏོ་མེན་ཚུ་ ཐོ་འགོད་འབད་ནི་དོན་ལུ་ལག་ལེན་འཐབ་ཡོད་པའི་སྒོག་འཕེན་ཁ་བྱང་འདི་ངོས་འཛིན་འབད་ཡོདཔ་མིན། ༢༠༡༩ ལོར་ འདི་ APT3 གིས་འཐབ་ཡོད་པའི་ ཐེ་ཤིང་འཚར་གཞི་ཚུ་ནང་ལུ་ Mandiant གིས་ངོས་འཛིན་འབད་ཡོད་པའི་ ཏོ་མེན་ཚུ་ཐོ་འགོད་འབད་ནི་དོན་ལུ་ཡང་ཡག་ལག་ལེན་འཐབ་ཡོདཔ་མིན། ༢༠༢༣ ལོར་ འདི་ CrowdStrike གིས་རྒྱུ་ཡིག་ཡི་གེ་ཚུ་ཡོད་པའི་ Program Database (PDB) འགྲུལ་ལམ་དང་ བཅས་པའི་གནོད་བྱེད་ལས་རིམ་ བཟློས་མཁན་ནང་ལུ་ ཐོབ་ཡོད་པའི་ཏོ་མེན་ཚུ་ ཐོ་འགོད་ འབད་ནི་དོན་ལུ་ ལག་ལེན་འཐབ་ཡོདཔ་མིན། འདི་གིས་ རྒྱུ་མཁྱི་གི་ལམ་ཡུགས་ཀྱ་བསྡུ་སྒྲིག་འབད་ནི་གི་བསམ་འཆར་བཀོད་མིན།

taoyujun@gmail[.]com

ཏོ་མེན་ ‘**hcjbtt[.]com**’ འདི་སྒོག་འཕེན་ཁ་བྱང་ ‘**taoyujun@gmail[.]com**’ དང་གཅིག་ཁར་ཐོ་འགོད་འབད་ཡོད་རུང་ འདི་གི་ བདག་སྐྱོང་པའི་སྒོག་འཕེན་འདི་ ‘**wangminghua6@gmail[.]com**’ དང་གཅིག་ཁར་ཐོ་འགོད་འབད་ཡོདཔ་མིན།

ཏོ་མེན་ ‘**hcjbtt[.]com**’ འདི་དང་འབྲེལ་བའི་གནོད་བྱ་བ་གང་ཡང་མེད། འདི་རུང་སྒོག་འཕེན་ཁ་བྱང་ ‘**taoyujun@gmail[.]com**’ འདི་ཉེ་མའི་ཉེན་ཁ་ཤེས་རིག་སྐན་ཁུ་ཚུ་ནང་མཐོང་ནུག ༢༠༡༩ ལུ་ སྐན་ཀྱི་ཡན་ཏེ་གིས་ ཉེ་ཁོང་གི་གཙུག་ཏོ་ཚུ་ལུ་ དམིགས་གཏད་འབད་བའི་ ‘**Cueisfry Trojan**’ དབྱེ་ཚུ་ནང་ བཟུ་ཞིབ་འབད་ཐོབ་མི་ ཏོ་མེན་ཅིག་ ཐོ་བཀོད་འབད་ནི་དོན་ལུ་ ལག་ལེན་འཐབ་ཡོདཔ།

སློག་འཕེན་ཁ་བྱང་འདི་གིས་ ~~རྒྱལ་སྤྱིའི་རྡུལ་ཟློན་ནུས་ཤུགས་ལས་ཁུངས།~~ འདྲ་སྒེ་སྐབས་སུ་བགོལ་བའི་ **‘iaea-international[.]org’** དང་ རྒྱལ་ཡོངས་རྡུལ་ཟློན་ཉམས་ཚོད་བཀག་དམ་གྱི་ཚིངས་ཡིག་ལས་ཁུངས། **(CTBTO).** ནང་གི་ ~~རྒྱལ་སྤྱིའི་གནས་རྒྱལ་ཆེ་བ།~~ འདྲ་སྒེ་སྐབས་སུ་བགོལ་བའི་ **‘idc-ctbto[.]org’** ལྟ་བུའི་�future་ཨེན་ཚུ་ཡང་ཐོ་འགོད་འབད་ཡོདཔ་ཨིན།

future་ཨེན་ **‘iaea-international[.]org’** གི་ སྟོན་མའི་ Whois ཐོ་བགོད་ལས་ཐོ་འགོད་པའི་ སློག་འཕེན་ཁ་བྱང་འདི་ **‘wangminghua6@gmail[.]com’** ཨིན་པ་སྟོན་ཡོདཔ་ཨིན།

udtglobals[.]com

future་ཨེན་ **‘udtglobals[.]com’** འདི་བདག་སྐྱོང་པའི་ སློག་འཕེན་ཁ་བྱང་སྒེ་ **‘wangminghua6@gmail[.]com’** དང་ ཐོ་འགོད་པའི་ སློག་འཕེན་ཁ་བྱང་སྒེ་ **‘ocean.nio@rediffmail[.]com’** ལག་ལེན་འཐབ་སྟེ་ཡོད་པ་མཐོང་ཡོདཔ་ཨིན། future་འདི་གི་གཞན་པའི་ WHOIS ཐོ་བགོད་ཚུ་ལས་ཐོ་འགོད་པའི་ སློག་འཕེན་ཁ་བྱང་འདི་གཅིག་པ་ཡོད་རུང་ བདག་སྐྱོང་པའི་ སློག་འཕེན་ཁ་བྱང་འདི་ **‘taoyujun@gmail[.]com’** ཨིན་པ་སྟོན་ཡོདཔ་ཨིན།

‘udtglobals[.]com’ ཟེར་མི་འདི་ རྒྱ་མཚོའི་བོཐ་གི་སྲུང་སྐྱོབ་དང་ཉེན་སྲུང་གི་ཚོང་ལས་ཀྱི་དོན་ལུ་ རྒྱལ་སྤྱིའི་དོན་རྟགས་ཅིག་ཨིན་མི་ **‘UDT Global’** སྒེ་ བརྗེ་བར་སྤྲོད་ཡོདཔ། སློག་འཕེན་ཁ་བྱང་ནང་གི་ལག་ལེན་པའི་མིང་ **‘ocean.nio’** འདི་རྒྱལ་ཁབ་མང་པོ་ནང་ཡོད་པའི་ རྒྱ་མཚོ་རིག་པའི་རྒྱལ་ཡོངས་སྐོབ་སྒེ་ **(NIO)** འདྲ་སྒེ་མི་སྤྱ་བ་ཅིག་བཟོ་སྟེ་ཡོད་སྟིད། **‘Rediff’** སློག་འཕེན་ཞབས་ཏོག་(འདི་རྒྱ་གར་ལུ་གཞི་བཞག་ཡོད་པ་)ལག་ལེན་འཐབ་དོ་ཡོདཔ། འདི་གིས་ རྒྱ་གར་གྱི་ **རྒྱ་མཚོ་རིག་པའི་རྒྱལ་ཡོངས་སྐོབ་སྒེ་འདྲ་**སྒེ་མི་སྤྱ་བ་ཅིག་ཨིན་པའི་བར་སྟོན་ཡོད་སྟིད།

Djibdiplomatie[.]com

future་ཨེན་ **‘djibdiplomatie[.]com’** འདི་ཇི་བུ་ཏི་གི་ཕྱི་འཛེལ་ཞབས་ཏོག་འདྲ་སྒེ་སྐབས་སུ་བགོལ་བ་ཅིག་འདྲ་འདུག་སྟེ་ འདི་ལུ་ **‘utdglobals[.]com’** དང་འབྲེལ་བའི་ WHOIS ཐོ་བགོད་ཅིག་ཡོད། ཐོ་བགོད་ཅིག་ལས་ཐོ་འགོད་པ་ **‘ocean.nio@rediffmail[.]com’** དང་བདག་སྐྱོང་པ་ **‘taoyujun@gmail[.]com’** སྟོན་ཡོདཔ་དང་ གཞན་པའི་ ཐོ་བགོད་ཚུ་ལས་བདག་སྐྱོང་པའི་ སློག་འཕེན་ཁ་བྱང་སྒེ་ **‘wangminghua6@gmail[.]com’** དང་ཐོ་འགོད་པའི་ སློག་འཕེན་སྒེ་ **‘ocean.nio@rediffmail[.]com’** སྟོན་ཡོདཔ་ཨིན།

future་ཨེན་གཉིས་ཆ་ཨིན་མའི་ WHOIS ཐོ་བགོད་ནང་ལུ་ཇེ་སྨོམ་བགོད་པ་དང་འབྲེལ་བའི་གནས་གོང་ཚུ་ཡང་ཡོད། དཔེར་ན་ **‘udtglobals[.]com’** ལུ་ཐོ་འགོད་པའི་གོང་ཁྱེར་སྒེ་ **‘ASDF’** གི་གནས་གོང་ཡོད་པ་དང་ **‘djibdiplomatie[.]com’** ལུ་ཐོ་འགོད་པའི་མིང་གི་གནས་གོང་སྒེ་ **‘DAF DAGF’** ཡོད། འདི་གཞན་མི་གི་ BADBAZAAR future་ཨེན་ཚུ་ནང་མཐོང་བའི་གནས་གོང་ཚུ་དང་གཅིག་བཟུར་འབད་བཏུབ།

སློག་འཕེན་ཁ་བྱང་ **‘wangminghua6@gmail[.]com’** དང་ **‘taoyujun@gmail[.]** ཟེར་མི་འདི་ཚུ་ **རྒྱལ་སྤྱིའི་མཚོ་བོཐ་སྐྱོབ་ཀྱི་ཐ་བྱལ་རྒྱལ་སྤྱིའི་དོན་རྟགས་དང་། ཇི་བྱ་དེ་གི་ཕྱི་འཛེལ་ཞབས་ཀྱི་** གཅ་དེ་ལས་ **རྒྱལ་སྤྱིའི་རྡུལ་ཟློན་ཁྱུ་ཚན་ཚུ་སྒེ་ བརྗེ་བའི་**future་ཨེན་ **ཚུ་གི་** ཀཽཔ་ཡུ་ཨེ་ཨོ་ཚའི་ཨེས་ཐོ་དེབ་ཚུ་ནང་ བཤུ་ཞིབ་འབད་ཐོག་ཀྱི་future་ཨེན་ཚུ་ནང་ཡང་ བཤུ་ཞིབ་འབད་ཐོག་ཡོདཔ།

སྐབས་སུ་བགོལ་བའི་future་ཨེན་དང་གཅོད་སྐྱེན་ཨེད་པའི་future་ཨེན་ཀྱི་མཉམ་སྡེབ་འདི་གིས་གཅོད་སྐྱེན་ཀྱི་སྐད་ཅིས་ཁྲིད་ཐུབ་ཚུ་ཀཽཔ་ཡུ་ཨེ་ཨོ་ཚའི་ཨེས་ཐོ་དེབ་ཚུ་ནང་ཡང་ བཤུ་ཞིབ་འབད་ཐོག་ཡུ་རྒྱལ་སྤྱིར་འབད་བའི་ཅ་ཅོ་དོན་ལུ་ལག་ལེན་འཐབ་པའི་གཞི་ཁྲིད་ཇེས་ཐོག་ཨིན་པའི་ཐོ་བགོད་ཚུ་ཡང་ བཤུ་ཞིབ་འབད་ཡོདཔ།

སློག་འཕེན་ཁ་བྱང་ **‘ocean.nio@rediffmail[.]com’** ཟེར་མི་འདི་ གོང་ལུ་བཤད་ཡོད་མི་ བརྗེ་བའི་future་ཨེན་ཚུ་ནང་ལས་ རྒྱངས་གཅིག་ བཤུ་ཞིབ་འབད་ཡོདཔ། སློག་འཕེན་ཁ་བྱང་ **‘ivan_s81@mail[.]ru’** དང་ **‘tplutalova@list[.]ru’** གཉིས་ཀྱིས་ རེ་རེ་བཞིན་ future་ཨེན་གྱངས་ཁ་ཆུང་ཀུ་ཅིག་ཐོ་འགོད་འབད་ཡོདཔ་དང་། future་ཨེན་འདི་ཚུ་ལས་ལ་ལོ་ཅིག་ བྱ་ཏ་བྱ་ཇོར་གྱི་གཞི་རིམ་གྱབ་བཟོ་ནང་ འགེམས་སྤེལ་འབད་ཡོདཔ། སློག་འཕེན་ཁ་བྱང་གསུམ་འདི་ གཅོད་པ་ཅན་གྱི་ ཡོངས་འཛེལ་གྱི་ འཁྲབ་རྩེད་པ་ཚུ་ གླ་ཚུ་དང་ འཛེལ་བ་ཡོདཔ་སྟེ་ ཡིད་ཆེས་བསྒྲིདཔ་ཨིན་མས། འདི་ཡང་ སློག་འཕེན་

‘wangminghua6@gmail[.]com’ དང་ **‘taoyujun@gmail[.]com’** དང་ཁྱད་པ་ད་ དེ་ཚོ་དང་འབྲེལ་བ་ཡོད་པའི་མངའ་ཁོངས་གྱི་ངོས་ཁ་མཐོ་དྲགས་སྟེ། གནོད་པ་ཅན་གྱི་ལས་སྣ་ཚོ་དང་ འབྲེལ་མཐུད་འབད་དེ་ཡོདཔ་ལས་ཨིན་པས།

(ཟུར་སྦྲགས་ཀ་པའི་པར་རིས་ ༥ ལུ་གཟིགས།)

འཇིགས་སྐྱེལ་བྱེད་མི་གཞན་ཚུ་ལུ་འབྲེལ་མཐུད།

BADBAZAAR དང་འབྲེལ་བ་ཡོད་པའི་ཏོ་མེན་ **‘actuallys[.]com’**, **‘clublogs[.]com’**, **‘myloughborough[.]com’**, **‘rewrwer[.]com’**, དང་ **‘voiceoftibet[.]net’** ཚུ་གི་གཞན་པའི་མཚུངས་མཐུན་གྱི་ཁྱད་ཆོས་ཅིག་ཡང་ཡོད་དེ་ ཁོང་ཚུ་ཆ་མཉམ་ eNom དང་གཅིག་ཁར་ཐོ་འགོད་འབད་ཡོད་པ་དང་ **‘255.255.255[.]254’** ལུ་ 'parked' འབད་ཞག་ཡོདཔ་ཨིན།

སྔོན་མའི་ NCSC གི་བརྟག་དཔྱད་ཚུ་གི་རྗེས་སུ་འབྲངས་ཏེ་ འདི་འདྲའི་ཁྱད་ཆོས་ཡོད་པའི་གཞན་པའི་ཏོ་མེན་ཚུ་ལས་ ༢༠༡༩ ལོར་ **APT5** དང་ ༢༠༠༩ ལས་ ༢༠༡༡ བར་ན་ **APT14** དང་འབྲེལ་བའི་བྱ་གཞག་ཚུ་ཐོན་ཡོདཔ་ཨིན།

APT5 དང་འབྲེལ་བའི་ཏོ་མེན་ཚུ་ལུ་ཐོ་འགོད་པའི་སློག་འཕྲིན་ཁ་བྱང་སྟེ་ **‘taoyujun@gmail[.]com’** ཐོ་བཀོད་འབད་ཡོད་པའི་ལོ་རྒྱུས་ཅན་གྱི་ WHOIS ཐོ་བཀོད་ཚུ་ཡོད་པ་ཨིན།

APT14 དང་འབྲེལ་བའི་ཏོ་མེན་ཚུ་ལུ་ཡི་གེ་གསུམ་པའི་ཡན་ལག་ཏོ་མེན་ཚུ་ཡོད་པ་དང་ འདི་ཚུ་གིས་ཁོང་ཚུ་གི་གནོད་སྐྱོན་གྱི་བྱ་གཞག་གི་དམིགས་ཡུལ་དུ་བཏང་ཡོད་པ་ཅིག་ཚུད་སྟོན་པ་ཅིག་འདྲ་འདུག། འདི་གི་དཔེ་ཅིག་ལུ་ **‘bae.cisconline[.]net’** ཡོད་པ་དང་ འདི་གིས་ BAE Systems ལུ་དམིགས་བསལ་ འཛུལ་ཞུགས་འབད་ནིའི་ དམིགས་ཡུལ་བཏང་ཡོད་པ་བརྡ་སྟོན་འབད་ཡོད་པ་དང་ **‘[Poison Ivy](#)’** གི་དཔེ་མཚོན་ནང་ལུ་ཐོབ་ཡོདཔ་ཨིན།

ཁྱད་ཆོས་ཚོག་འཛདཔ་འདི་ BADBAZAAR ཏོ་མེན་ཚུ་ནང་ བརྟག་ཞིབ་འབད་ཡོདཔ་ད་ དེ་ནང་ ཡན་ལག་མངའ་ཁོངས་ཚུ་ ཏོ་རྟ་ནི་ཟེ་ཨེཔ་གི་མིང་དང་འབྲེལ་བ་ཡོདཔ་ཨིན།

ཞུ་ཡིག་བཀོ་མིང་།	C2 URL
Muslim Pro	**mpp**.pmstwocqn[.]com
Video Player for Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Radio Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

APT5 དང་ APT14 དང་འབྲེལ་བའི་བྱ་གཞག་ཚུ་ལོ་རྒྱུས་ཅན་ཨིན་པ་དང་ eNom དང་གཅིག་ཁར་ཐོ་འགོད་འབད་ཏེ་ **‘255.255.255.254’** ལུ་སེལ་འབད་ཡོད་པའི་གཞན་པའི་ཏོ་མེན་ཚུ་ཡང་ཡོད་རུང་ གནོད་སྐྱོན་གྱི་བྱ་བ་དང་འབྲེལ་བ་འཐབ་མ་ཚུགས་པ་ཚུ་ཡང་ཡོད་པ་གལ་ཆེ་བའི་ཁ་གསལ་འབད་དགོ། དེ་འབདལྟ་ལས་བརྟེན་འཆར་གཞི་འདི་ཚུ་གི་རྒྱབ་ལུ་ཡོད་པའི་བྱེད་མཁན་ཚུ་གཅིག་པ་ཨིན་ན་ཡང་ན་འབྲེལ་བ་ཡོད་མེད་ངེས་གཏན་མེད།

BADBAZAAR C2s ཚུ་དང་དེའི་མཚོན་ཚུ་གི་དཔྱད་ལས་ SSL ལག་ཆྱེར་ནང་ 'Common Name' གི་གནས་གོང་སྦེ་ལག་ལེན་ འཐབ་ཡོད་པའི་ འཁྲིད་སྟོན་མིང་ཚུ་ཐོན་ཡོདཔ་མིན། BADBAZAAR དེའི་མཚོན་དང་གཞི་རྟེན་ནང་མཐོང་བའི་འཁྲིད་སྟོན་མིང་ཚུ་གི་རྩིར་ཡུ་ NCSC གི་བརྟག་དཔྱད་ལས་ འཁྲིད་སྟོན་མིང་འདི་ཚུ་ IP ཁ་བྱང་མང་ཞོ་ལུ་ལག་ལེན་འཐབ་ཡོད་པ་སྟོན་ཡོདཔ་མིན། IP ཁ་བྱང་འདི་ཚུ་གིས་ BADBAZAAR དེའི་མཚོན་ནང་ཐོབ་ཡོད་ པའི་ ཅོ་མེན་ ཚུ་ སྤྲེགཔ་ལ་ འབད་ཡོདཔ་མིན། འཁྲིད་སྟོན་མིང་ཚུ་དང་ BADBAZAAR C2 ཅོ་མེན་ཚུ་སྤྲེགཔ་ལ་འབད་མི་འཁྲིད་སྟོན་མིང་ཡོད་པའི་ IP ཁ་བྱང་ཚུ་གི་ སྐོར་ལུ་ཏོག་གི་ ཚན་པ་ནང་རྒྱས་པར་ བཤད་ཡོད།

ཆ་ཤས་ཆ་མཉམ་ལུ་མིན་འཁྲིད་སྟོན་མིང་གི་གནས་གོང་ཡོད་པའི་ལག་ཆྱེར་ཚུ་ཡོད་པ་དེ་གསལ་བཀོད་འབད་ཡོད་པའི་གནོད་སྐྱོན་ཅོ་མེན་མིང་ཚུ་གི་ IP ནམ་པ་དང་མཐུན་ཡོདཔ་མིན། འདི་འདྲ་མིན་པའི་དཔེ་ཚད་སྣང་ཟད་བཀོད་དེ་ཡོད།

WIN-EU0VLBL7TUJ

འཁྲིད་སྟོན་མིང་ **‘WIN-EU0VLBL7TUJ’** འདི་ངོན་དགུ་ཡོད་པའི་ IP ཁ་བྱང་འདི་ཚུ་ལུ་མཚོང་ཡོདཔ་མིན

- **‘116.203.53[.]21’** གིས་ BADBAZAAR C2 ཅོ་མེན་ **‘uyapkfinder[.]com’** དང་ **‘thewestuniverse[.]com’** སྤྲེགཔ་འབད་ཡོད།
- **‘95.216.169[.]27’** གིས་ BADBAZAAR C2 ཅོ་མེན་ **‘adysfunction[.]com’** དང་ BADBAZAAR དེའི་མཚོན་ཀྱི་ཐབ་ལེན་འཛེལ་ལམ་སྦེ་མཚོང་བའི་ཡན་ལག་ཅོ་མེན་ **‘adysfunction[.]com’** སྤྲེགཔ་འབད་ཡོད།

(རྒྱུན་སྤྱིགས་ཀ་ པར་རིས་ ༥ ལུ་གཟིགས།)

WIN-70E59JVOB9G

འཁྲིད་སྟོན་མིང་ **‘WIN-70E59JVOB9G’** འདི་ངོན་དགུ་ཡོད་པའི་ IP ཁ་བྱང་འདི་ཚུ་ལུ་མཚོང་ཡོདཔ་མིན:

- **‘23.88.28[.]220’** གིས་ BADBAZAAR C2 ཡན་ལག་ཅོ་མེན་ **‘aua.rondwsign[.]com’**, **‘nal.tokenmajorp[.]com’**, **‘pep.rondwsign[.]com’**, **‘doa.rondwsign[.]com’** དང་ **‘pls.rondwsign[.]com’** སྤྲེགཔ་འབད་ཡོད། འཛུལ་འགོར་དང་བཅས་པའི་ལག་ཆྱེར་མཐར་མཚོང་བ་དང་ གནོད་སྐྱོན་ཀྱི་ཅོ་མེན་ཚུ་ IP ལུ་ སེལ་བ་ཐོག་མར་མཚོང་བའི་བར་ན་ ཉིན་གཉིས་ཀྱི་དུས་ཡུན་ཡོདཔ་མིན།
- **‘23.88.28[.]221’** གིས་ BADBAZAAR དང་འབྲེལ་བའི་ཡན་ལག་ཅོ་མེན་ **‘bt.bhvghg[.]com’**. སྤྲེགཔ་འབད་ཡོད།
- **‘23.88.28[.]222’** གིས་ BADBAZAAR C2 ཅོ་མེན་ **‘tubevideoplus[.]org’** དང་ **‘cde.mpoxcases[.]com’** སྤྲེགཔ་འབད་ཡོད།

- ‘**65.21.92[.]67**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**bat.androidupdated[.]net**’ སྒྲིག་ཡ་འབད་ཡོད། འདི་གིས་ DoubleAgent གཅོད་བྱེད་ལས་རིམ་ C2 ཡིན་པའི་ཡན་ལག་ཏུ་མེན་ ‘**apps.androidupdated[.]net**’ ཡང་སྒྲིགས་འབད་ཡོད།

- ‘**65.21.92[.]77**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ དང་ ‘**afg.collinformations[.]com**’ སྒྲིགས་འབད་ཡོད།

- ‘**65.108.192[.]134**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**upd.whoscaller.net**’ དང་ ‘**ggl.whoscaller[.]net**’ སྒྲིགས་འབད་ཡོད།

- ‘**142.132.131[.]15**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**bvn.lookincategory[.]com**’ དང་ ‘**edr.lookincategory[.]com**’ སྒྲིགས་འབད་ཡོད། འཕྲུལ་འཁོར་གྱི་མིང་དང་བཅས་བའི་ལག་ཆེར་མཐར་མཚོང་བ་དང་ གཅོད་སྐྱོན་གྱི་ཏུ་ཚུ་ IP ལུ་སེལ་བ་ཐོག་མར་མཚོང་བའི་བར་ན་ཉེན་བཀུ་གཅིག་གྱི་དུས་ཡུན་ཡོངས་ཤེན།།

- ‘**142.132.131[.]20**’ གིས་ཡན་ལག་ཏུ་མེན་ ‘**son.onlinegamersgroup[.]com**’ དང་ **system.onlinegamersgroup[.]com**’, སྒྲིག་ཡ་འབད་ཡོད་ཡ་དང་ འདི་ཚུ་ IP ལུ་ BADBAZAAR དང་ འབྲེལ་བའི་ SSL ལག་ཆེར་ཚུ་མཚོང་བའི་སྐབས་ལུ་སྒྲིག་ཡ་འབད་ཡོད་པས་ BADBAZAAR C2s ཚེན་པའི་ཡིད་ཆེས་བཏིང་ཡོད།

- ‘**142.132.131[.]28**’ གིས་ BADBAZAAR C2 ཏུ་མེན་ ‘**goldplusapp[.]net**’ དང་ཡན་ལག་ཏུ་མེན་ **who.goldplusapp[.]net**’ དང་ ‘**cgf.goldplusapp[.]net**’ སྒྲིགས་འབད་ཡོད།

- ‘**162.55.103[.]211**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net**’, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, དང་ ‘**aar.alpinemap[.]net**’ སྒྲིག་ཡ་འབད་ཡོད།

- ‘**162.55.103[.]212**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**pep.rondwsign[.]com**’, ‘**ckp.jkiohreh[.]com**’, ‘**aar.tokenmajorp[.]com**’, ‘**nal.tokenmajorp[.]com**’, ‘**pls.rondwsign[.]com**’ དང ‘**aua.rondwsign[.]com**’ སྒྲིགས་འབད་ཡོད

- ‘**195.154.47[.]99**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**ggl.whoscaller[.]net**’ དང་ ‘**upd.whoscaller.net**’ སྒྲིགས་འབད་ཡོད། འཕྲུལ་འཁོར་གྱི་མིང་དང་བཅས་པའི་ལག་ཆེར་ཐོག་མར་མཚོང་བ་དང་ གཅོད་སྐྱོན་གྱི་ཏུ་མེན་ཚུ་ IP ལུ་སེལ་བ་མཐར་མཚོང་བའི་བར་ན་ཉེན་གསུམ་གྱི་དུས་ཡུན་ཡོངས་ཤེན།

- ‘**195.154.60[.]3**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏུ་མེན་ ‘**upd.whoscaller[.]net**’ དང་ ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ གིས་ BADBAZAAR C2 ཡན་ལག་ཏོ་མེན་ ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ དང་ ‘**afg.collinformations[.]com**’ སྦྱིགས་འབད་ཡོད།

- ‘**212.129.21[.]168**’ གིས་ BADBAZAAR C2 ཏོ་མེན་ ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ དང་ ‘**bvn.lookincategory[.]com**’ སྦྱིགས་འབད་ཡོད།

(ཟུར་སྣགས་ཀ། པར་རིས་ ༢ ལུ་གཟིགས།)

WIN-50QO3EIRQVP

འཁྲིད་སྟོན་མིང་ ‘**WIN-50QO3EIRQVP**’ འདི་དོན་དག་ཡོད་བའི་ IP ཁ་ཆུང་འདི་ཚུ་ལུ་མཚོང་ཡོད་པ་མིན:

- ‘**45.76.132[.]91**’ གིས་ཏོ་མེན ‘**yumoftion[.]com**’ ‘**androidupdated[.]net**’ སྦྱིགས་འབད་ཡོད། ཏོ་མེན་གཉིས་ཆ་ཚིན་མ་ཡན་ལག་ཏོ་མེན་ ‘**fow.yumoftion[.]com**’ དང་ ‘**bat.androidupdated[.]net**’ ཚུ་ BADBAZAAR C2 ཏོ་མེན་ཚིན་པས་བརྟེན་ BADBAZAAR དང་འབྲེལ་བ་ཡོད། དེ་ལས་ཡན་ལག་ཏོ་མེན་ ‘**apps.androidupdated[.]net**’ འདི་ DoubleAgent C2 ཏོ་མེན་ཅིག་མིན། འདི་གིས་ WHOIS ཐོ་བཀོད་བརྒྱུད་དེ་ BADBAZAAR དང་འབྲེལ་བ་ཡོད་པའི་ཏོ་མེན་ ‘**pmstwocqn[.]com**’ ང་སྦྱིགས་འབད་ཡོད།

- ‘**95.179.210[.]85**’ གིས་ ‘**clublogs[.]com**’ སྦྱིག་པ་འབད་ཡོད་པ་དང་ འདི་ལས་ ‘**xle.clublogs[.]com**’ འདི་ BADBAZAAR C2 ཏོ་མེན་ཅིག་མིན། འདི་གིས་ BADBAZAAR དང་འབྲེལ་བའི་ཏོ་མེན་ ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, ‘**www.voiceoftibet[.]net**’ དང་ ‘**actuallys[.]com**’ ཡང་སྦྱིགས་འབད་ཡོད།

- ‘**199.247.21[.]34**’ གིས་ ‘**titeperformance[.]com**’ དང་ ‘**collinformations[.]com**’ འདི་གཉིས་ལུ་སྐུ་ཞབས་བྱིན་ཡོད་མི་འདི། འདི་གི་ཡན་ལག་ཚུ་ BADBAZAAR C2 ཝ་ཁུལ་ཚུ་མིན།

- ‘**217.69.10[.]128**’ གིས་ BADBAZAAR C2 ཝ་ཁུལ་ ‘**uyghurdict[.]com**’ ཡང་སྦྱིགས་འབད་ཡོད།

(ཟུར་སྣགས་ཀ། པར་རིས་ ༤ ལུ་གཟིགས།)

WMSvc-WIN-50QO3EIRQVP

ཅོས་དེ་མིང་ **‘WMSvc-WIN-50QO3EIRQVP’** འདི་འབག་གི་ IP ཁ་བྱང་གཡ་ཅན་ཚུ་གུ་མཐོང་ཡོད།:

- **’78.46.185[.]251’** གིས་ BADBAZAAR C2 ས་ལུལ་ **‘groupgram[.]org’** ལུ་སྐུ་ཞབས་བྱེད་ཡོད་མི་འདི། Volexity གིས་སྐན་ཁུ་བྱེད་མི་ནང་ལུ་འདི་གིས་མི་སྐྱོ་བའི་མཐུད་ལམ་ཚུ་གི་དོན་ལུ་ཐོང་སྟོ། ༡༩༢༡ ལགཔ་ལེན་འཐབ་དོ་ཟེར་བཤད།

- **‘65.21.92[.]69’** དང་ **‘163.172.205[.]207’** གཉིས་ཀ་གིས་ས་ལུལ་ **‘widelygram[.]org’** ལུ་སྐུ་ ཞབས་ བྱེད་ཡོད་མི་འདི་ BADBAZAAR C2 ས་ལུལ་ཅིག་ཤེན་པར་ཁུ་བ་ཅིན་ IP གཉིས་ཀ་ཀུ་སྐུ་ཞབས་བྱེད་པའི་སྐབས་ལུ་ཐོང་སྟོ། ༡༩༢༡ ཁ་ཤེ་སྐྱེ་ཡོད།

- **‘163.172.198[.]206’** གིས་ས་ལུལ་ **‘maxgram[.]org’** ལུ་སྐུ་ཞབས་བྱེད་ཡོད་མི་འདི་ BADBAZAAR C2 ས་ལུལ་ཅིག་ཤེན་པར་ཁུ་བ་ཅིན་སྐུ་ཞབས་བྱེད་པའི་སྐབས་ལུ་ཐོང་སྟོ། ༡༩༢༡ ཁ་ཤེ་སྐྱེ་ཡོད།

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

ཅོས་དེ་མིང་ **‘WMSvc-WIN-50QO3EIRQVP’** དང་ **‘WIN-7LSBB9R0F1L’** གཉིས་ཀ་འབག་གི་ IP ཁ་བྱང་གུ་དུས་མཚུངས་སུ་མཐོང་ཡོད།:

- **‘148.251.87[.]245’** གིས་ BADBAZAAR C2 ས་ལུལ་ **‘flygram[.]org’** དང་ **‘groupgram[.]org’** འདི་གཉིས་ལུ་སྐུ་ཞབས་བྱེད་ཡོད།

WIN-N8H8S9BG2P0

ཅོས་དེ་མིང་ **‘WIN-N8H8S9BG2P0’** འདི་འབག་གི་ IP ཁ་བྱང་གུ་མཐོང་ཡོད།:

- **‘148.251.87[.]247’** གིས་ BADBAZAAR C2 ས་ལུལ་ **‘omarwhatsapp[.]org’** དང་ **‘flygram[.]org’** འདི་གཉིས་ལུ་སྐུ་ཞབས་བྱེད་ཡོད།

WIN-I6VBN8MR92A

ཅོས་དེ་མིང་ **‘WIN-I6VBN8MR92A’** འདི་འབག་གི་ IP ཁ་བྱང་གུ་མཐོང་ཡོད།:

- **‘148.251.87[.]197’** གིས་ BADBAZAAR C2 ས་ལུལ་ **‘tryhrwserf[.]com’** སྐུ་ཞབས་བྱེད་ཡོད།

ཚོང་འབྲེལ་གྱི་གནས་སྟུང་ཡོད་མེ་ལྟ་གཞི་བཞག་སྟེ་ ཡོངས་འབྲེལ་ནང་ལྟ་ འཛུལ་ཚས་འདི་གི་མིང་ཚུ་ ཁྱབ་སྟེལ་འགྱོ་མི་འདི་ སོ་སོ་སྟེ་ཡོངས་ཤེན། དེ་ཚུ་ལས་ལ་ལྟ་ཅིག་ དུས་མཉམ་ལྟ་ ཨའི་པི་ཁ་བྱང་ལེ་ཤ་ཅིག་ནང་ བཀྲ་བརྩེགས་ཁྱེ་ཤིན་ནམ་ འདི་གིས་ ཉེམ་ཡེལེའི་ གཅིག་ལས་ ཕྱི་ཤེམ་ཚུ་གསར་བསྒྲུན་འབད་ཡོང་བའི་ བང་སྟེགས་ཤིན། ཅོསིའི་མིང་ལ་ལྟ་ཅིག་གི་དོན་ལྟ་ བཀྲ་བརྩེགས་འབད་མི་ IPs ཚུ་གཱ་ར་ གཙོདཔ་ཁ་ཅིག་ལས་ སྐྱ་ཚུ་ངང་ འཛེལ་མཐུད་འབད་མི་ཚུགས་ཟེར་ དྲན་འཛིན་འབད་དགོཔ་ཨཱ་ཚེ། འདི་གིས་ ཅོསིའི་མིང་ཚུ་ལག་ལེན་འཐབ་ནི་འདི་ ཉེན་ཁ་ཅན་གྱི་འཐབ་རྩེད་པ་འདི་ཚུ་ལྟ་རྒྱུངམ་ཅིག་མེན་ཟེར་བའི་དོན་དག་ཨིན།

ཨིན་རུང་ BADBAZAAR C2 ཝ་ཁྱལ་ཚུ་ལྟ་སྐྱ་ཞབས་བྱིན་ཡོད་མི་ IP ཚུ་ནང་ལྟ་འཛུལ་འགོར་མིང་འདི་ཚུ་མང་དུགས་སྟ་འཚུང་བ་འདི་གིས་ གཞི་རྟེན་ བཟོ་སྐྲུན་ཚན་པ་ ཅིག་གིས་མི་སྐྱོ་བའི་རེག་རྩུས་བྱ་བ་ཚུ་ལྟ་རམ་འདེགས་འབད་ནོའི་ དོན་ལྟ་འཛུལ་འགོར་ཚུ་བགོད་སྤེལ་འབད་ངོ་ཟེར་བསམ་དཔྱད་འབད་ཚུགས།

མི་སྟེ་བརྡ་བརྒྱུད་ཀྱི་གནས་སྟངས།

སྟོན་མའི་སྐྱན་ཞུ་ Volexity གིས་བཞད་མི་ནང་ལྟ་ YouTube བརྟན་འཛིན་ཚུ་ (མི་སྐྱོ་བའི་ཉེར་སྟོང་ལག་ལེན་འཐབ་ནི་གི་སྤེལ་སྐྱགས་) མི་སྐྱོ་བའི་རེག་རྩུས་ ལས་བྱེད་པ་ཚུ་གིས་བཟོ་ཡོད་ཟེར་སྟོན་ཡོད། བརྟན་འཛིན་འདི་དག་ནང་ བཟོ་ཡོད་པའི་ སྟོག་རིམ་ཚུ་ ལག་ལེན་འཐབ་ཨངས་ཀྱི་ སྟོབ་སྟོན་ཚུ་ ཚུད་དེ་ཡོངས་ཤེན་པས།

NCSC གིས་ཉེན་ཁ་བྱེད་མི་ཚུ་གི་བྱ་ག་ཚུ་ངང་འབྲེལ་བ་ཡོད་པའི་ YouTube རྒྱུ་ལས་ཁ་སྐོང་གཉིས་ཆ་ཚང་ཡོད། YouTube བརྒྱུད་ལས URL handle **‘@josephjoey3499’** ཡོད་མི་འདི་གིས་ **‘Maxgram’** ལག་ལེན་འཐབ་རིའི་སྤེལ་སྐྱགས་འབད་ངོ་བཟུམ་སྟོན་ཞིན་ནང་ ཁ་སྐོང་ རྒྱུ་ལས་ **‘@uyghurapks3096’** ཐུ་འགོད་བྱིན་ཡོད་མི་འདི་གིས་ **‘Uyghur APK Finder’** གི་སྤེལ་སྐྱགས་འབད་ཁ་ཤེན།

ཁ་སྐོང་གི་ཐོག་ལས་ **‘Flygram’** དང་ **‘Signal Plus’** གི་སྤེལ་སྐྱགས་འབད་བའི་ YouTube རིས་འགུལ་ཚུ་ནང་ལྟ་ཉེན་ཁ་ བྱེད་མི་ཚུ་གིས་ཀ་བར་ཨང་གངས་ཚུ་མཐོང་ཚུགས་པ་སྤེལ་ལག་ལེན་འཐབ་ངོ་སྟོན་ཡོད། **‘Flygram’** བརྟན་འཛིན་ ནང་ལྟ་ ০:৭৫ ཀྱ་ཀ་པར་ཨང་གངས་ **‘+1 (570) 378-7250’** མཐོང་ཚུགས་ཞིན་དང་ **‘Signal Plus’** བརྟན་འཛིན་ གི་སྐབས་ལྟ་ཀ་པར་ཨང་གངས་ **‘+1 (267) 298 4259’** འདི་གསལ་སྟོན་འབད་ཡོད།

Volexity གིས་བོད་ཀྱི་བརྩོང་གཞི་རྩུན་མ་ཅིག་གི་གནས་ཚུལ་དུ་ཀྱུ་ **‘ignitetibet[.]net’** གི་སྐན་ལྟ་བྱིན་ཡོད་མི་འདི། འདི་ཉེན་ཁ་བྱེད་མི་ཚུ་གིས་ འཐབ་སྟེར་འབད་ངོ་བསམ་པའི་ Telegram རྒྱུ་ལམ་ཚུ་ནང་ལྟ་ཐོབ་ཡོད། སྟོག་འཛིན་ཁ་བྱང་ **‘choekyi.wangmo@ignitetibet[.]net’** འདི་ཨོག་ངོས་ **‘tibetone.org’** ཀྱ་ཡོད་པའི་འགེམས་སྟེལ་ཚུ་ཀྱ་བསམ་ཚུལ་བཞག་པ་མཐོང་ཡོད། འདི་ Lookout གིས་མི་མང་ལྟ་སྐན་ལྟ་བྱིན་མི་ནང་ལྟ་ iOS variant of BADBAZAAR གི་ངོན་ལྟ་ལག་ལེན་འཐབ་མི་ C2 ཨོག་ངོས་ཅིག་ཨིན་ཟེར་བཤད་ཀྱག།

སྟོག་འཛིན་ཁ་བྱང་འདི་ འབྲལ་མཁན་གྱིས་ཚད་འཛིན་འབད་དེ་ཡོད་པར་ཡིད་ཆེས་འབད་ཤེས་ཨིན་པའི་ཁར་ དེ་ཡང་ **‘Choekyi Wangmo’** ཟེར་བའི་ མི་སྐེར་གྱི་ ངོ་བོ་ལག་ལེན་འཐབ་ཡོངས།

བརྟག་ཞིབ།

BADBAZAAR དང་ MOONSHINE གིས་ཡུ་གུར་ ཡོད་པ་ དེ་ལས་ཏའེ་ཁན་གྱི་མི་ཐེ་ཚུ་དམིགས་བསལ་དུ་དམིགས་འདེབས་འབད་ནི་དོན་ལུ་ མི་ཐེ་ག་གསོའི་ཤེས་ཡོན་ཐབས་ལམ་ལེ་ཤ་སྟོང་དོ་ དེ་ཡང་ :

- འདི་མི་ཐེ་ཚུ་ལུ་དོ་སྣང་ཡོད་པའི་མེས་ཚུ་ལུ་ trojanisation འབད་བ་ དཔེར་ན་ཡུ་གུར་སྐད་ཡིག་གི་ཀུར་ཨན་མེས་ཁ་ཤུ་ཏུ་ཚུ་ དམིགས་འདེབས་ཀྱི་ཤེས་ཚད་ཚུ་ལུ་ཁྱེད་པར་དུ་སྤེག་བཏོད་འབད་ཡོད་པ་ངེས་ཏེའུ་ཁ་ཅིག་ཨིན།
- trojanised མེས་ཚུ་འདི་ ཡོངས་ཁྱབ་མེས་སྐྱབ་ཁང་ཚུ་ལུ་ག་སྐོང་རྒྱབ་མི་འདི་གིས་ ཁྱིམས་མཐུན་གྱི་ཚོར་སྣང་ནི་ལུ་ བཅ་ཐོགས་ཡོད་པ་ནང་གསེས་མཐོ་ཤོས་ཨིན་ དེ་ལས་མཐུན་ཚུ་གི་ཁ་པར་ནང་ལུ་བཏོ་འདེམས་འབད་བ་འདི་ཡང་ མི་ཐེ་ཚུ་ནང་ ཡིད་ཆེས་ཡོད་པའི་ འབྲེལ་བ་ཚུ་ ལག་ལེན་འཐབ་ནིའི་དམིགས་ཡུལ་ཡོད་པ་ནང་གསེས་མཐོ་ཤོས་ཨིན།

BADBAZAAR དང་ MOONSHINE གིས་བསྡུ་ལེན་འབད་མི་གནས་ཚད་ཚུ་ཀུང་ཁ་མི་དམངས་སྤྱི་མཐུན་རྐུལ་ཁབ་ལུ་གཡོ་ཅན་པར་དུ་ཨིན།

BADBAZAAR དང་ MOONSHINE གིས་ཡུ་གུར། ཡོད་པ། ཁའེ་སྐན་གི་མི་སྐེར་ཚུ་ལུ་དམིགས་འཛུགས་འབད་དོ་ བཤུ་ཞིབ་འབད་ཡོངས། ཡོད་རྟང་། ཀུང་གོ་ནང་གི་གཞན་མི་ཞུང་ཚོགས་པ་ཚུ་ལུ་དམིགས་འཛུགས་འབད་མི་ གཞན། ཞབས་སྤྱིར་གནོད་པ་ཚུ་ཡང་ཡོད། ཀུང་གོ་དང་ཕྱིར་ཡོད་པའི་ ཐེབས་རྟགས་མཉམ་འདེགས་རྐུལ་ཁབ་ཚུ་གི་མི་སེར་ཚུ། གཞུང་གི་བརྟན་པོ་ལུ་ཉེན་ཁ་འབད་མི་ རྒྱ་རྒྱན་ཚུ་ལུ་རན་ཨང་ BADBAZAAR དང་ MOONSHINE ལ་བཟུམ་གྱི་འཐུལ་འཛིན་ཞྭོར་གནོད་པ་ཚུ་གི་ཉེན་ཁ་ཡོད་པ་ངེས་པར་དུ་ཨིན། ས་གནས་དང་སྐུ་སྐད་ དེ་ལས་ པར་གྱི་གནས་སྟུད་ཚུ་ བཟུང་ཚུགས་པའི་ ལྷོགས་གྲུབ་འདི་གིས་ དམིགས་གཏད་ཅན་གྱི་ལས་སྣ་ཚུ་གི་སྐོར་ལས་ དུས་ཚོད་ངོ་མའི་བརྡ་དོན་ཚུ་ ཁྱིན་ཐོག་ལས་ མ་འོངས་པའི་ བཟུ་རྐོག་དང་ གནོད་པའཚེ་གི་ལུ་ཚུ་ བརྡ་དོན་སྟོང་ནི་གི་ གོ་སྐབས་ཁྱིན་མ་ཨིན།

MITRE ATT&CK®

སྐབས་ཞུ་འདི་ དངོས་ཡོད་འཛིམ་སྒིང་གི་བཟླ་ཞིབ་ལུ་གཞི་བཞག་མི་ དག་མེ་གི་འཐབ་རིག་དང་ཐབས་ལམ་ཚུ་གི་ འཛིམ་སྒིང་ཐུ་ཡོངས་ལུ་འ ཐོབ་ཚུགས་པའི་ ཤེས་རྟོའི་གཞི་རྟེན་ ཅིག་ཨིན་མི་ སུ་ཡེ་ཏར་ཚེ་ཏེ་ཏེ་ཚེ་ཚེམ་གི་ག་ (MITRE ATT&CK®) གི་གྲུབ་བཟོ་དང་འབྲེལ་ཏེ་བསྒྲིགས་ཡོངས།

ཐུ་ཐབས།	ངོ་རྟགས།	ཐབས་ཤེས།	ཐུ་རིམ།
ཞིབ་འཚུག	T1593.001	ཁ་ཕྱེ་ཡོང་པའི་དུ་ཚུ་/ རྩ་མེན་ཚུ་འཚོལ་ཞིབ་འབད། : མི་སྤེ་བང་བརྒྱུད།	མི་ངན་ཚུ་གིས་ མཉེན་ཆས་ངན་པ་ བཏེ་སོར་འབད་ནི་ཅེན་ཤུ་ ཁོང་རའི་ དམིགས་གཏད་ཅན་གྱི་ ཉམས་རྒྱུངས་ཚུ་དང་ མཐུན་སྒྲིག་འབད་མི་ ཡོངས་འཛིལ་སྤེ་ཚན་དང་ གྲོས་འཛོམས་ཚུ་ འཚོལཁྱབ་ཨིན།
ཚོན་ལྡངས་གོང་འཛེལ	T1583.001	གཞི་རྟེན་མཐུན་རྐྱེན་ཚུ་ཐོབ་ནི། : ཅོ་མེན་ཚུ།	མི་ངན་ཚུ་གིས་ ཁོང་རའི་བང་བགོད་དང་ཚད་འཛིན་ས་བར་ཐུ་གི་ངོ་ཤུ་ ཅོ་མེ་ཚུ་ཐོ་བགོད་འབད་ཁ་ཨིན།
ཚོན་ལྡངས་གོང་འཛེལ	T1587.001	སྤྱོགས་གྲུབ་གོང་འཛེལ་གཏང་ནི། : མཉེན་ཆས།	གནོད་པ་ཅན་གྱི་ཨང་རྟགས་འདི་ ཅོ་ཅ་ནའི་ཟིཔ་སྒོག་རིམ་ཚུ་ནང་ བསྒོགས་ནི་ངོ་ཤུ་ དེས་ཡུ་ཐིས་ཡོངས་ཨིན།
ཚོན་ལྡངས་གོང་འཛེལ	T1608.001	འཕྲལ་སྐྱེགས་རྒྱས་ཐུགས། : མཉེན་ཆས་ངན་པ་སྤེལ་བསྒྲིགས་འབད།	Trojanised apps ཚུ་ app stores ཚུ་རྩིས་ཀ་ ཡོངས་འཛེལ་གྱི་སྐྱེགས་བུ་ཚུ་ནང་ སྤེལ་བསྒྲིགས་འབད་ཡོང་པ་ཨིན།
ཚོན་ལྡངས་གོང་འཛེལ	T1585.001	རྩིས་ཁྲ་གཞི་བསྒྲིགས། : མི་སྤེ་བང་བརྒྱུད་ཀྱི་རྩིས་ཁྲ།	མི་ངན་ཚུ་གིས་ མཉེན་ཆས་ངན་པ་ བཏེ་སོར་དང་ ཁྲབ་བསྒྲིགས་འབད་ནི་ཅེན་ཤུ་ ཡོངས་འཛེལ་འཚར་སྒོ་དང་ མི་སྤེ་བང་བརྒྱུད་ཚུ་ནང་ རྩིས་ཁྲ་བཟོཝ་ཨིན།
ཚོན་ལྡངས་གོང་འཛེལ	T1585.002	རྩིས་ཁྲ་གཞི་བསྒྲིགས། : སྒོག་འཛིན་རྩིས་ཀོ།	མི་ངན་ཚུ་གིས་ མཉེན་ཆས་ངན་པ་ དོ་སེའི་དང་ བཏེ་སོར་འབད་ནི་ཅེན་ཤུ་ ཆེར་ཡིག་ དོ་སེའི་དང་ ཚོང་འཛེལ་ཀྱི་ སྒོག་འཛིན་རྩིས་ཀོ་ཚུ་ ལག་ལེན་འཐབ་ཨིན།
འགོ་ཐོག་འཛུལ་སྐྱོད།	T1189	འཛེན་འཛུམ་ཀྱི་བདེ་སྐྱིག	གནོད་པ་ཅན་གྱི་ཡིག་གཟུགས་ཚུ་ དེ་མེན་པ་ཅིན་ ཁྱིམས་མཐུན་ཀྱི་སྒོག་རིམ་ཚུ་ནང་ ཐུ་བཞག་ཏེ་ སྒོག་རིམ་ཚོང་ཁང་ཚུ་ནང་ སྐྱེལ་བསྒྲིགས་འབད་ཡོངས་ཨིན།
འགོ་ཐོག་འཛུལ་སྐྱོད།	T1566.003	ཐེ་ཨིང་: ཞབས་ཏོག་བརྒྱུད་དེ་ Spearphishing	མི་ངན་ཚུ་གིས་ ཏེ་ཡེ་གུར་རྩིས་ཀ་ མི་ཐེ་བང་བརྒྱུད་བརྒྱུད་དེ་ དམིགས་གཏད་ཅན་གྱི་ཐེ་ཚན་ཚུ་ ཅོ་ཅ་ནི་ཟིཔ་ཚེལ་ཚུ་གཏང་མི་ཨིན།
ལག་ལེན་བསྐྱར་སྐྱོད།	T1204.002	ལག་ལེན་པ་བསྐྱར་སྐྱོད། : གནོད་ཅན་ཡིག་སྒོད།	ཉམས་རྒྱུངས་ཚུ་གིས་ པེ་ཡོ་ལག་ལེན་འཐབ་ནི་ཅེན་ཤུ་ ཅོ་ཅ་ནི་ཟིཔ་ཚེལ་ཚུ་ གཞི་བསྒྲིགས་འབད་དགོས་ཨིན།
ཉེན་སྐྱང་ལས་གཡོལ་བ།	T1027.009	མཁྱ་ཐོམ་ནི་ནི་གི་ཡིག་སྒོད་ཡང་ན་བརྡ་དོན། : ནང་འཇུག་འཛོ་སྐྱེས་རྩལ།	གནོད་པ་ཅན་བའི་འཛོ་སྐྱེས་རྩལ་འདི་དེ་མེན་ཚ་འཛོག་ངོ་མ་ཚུ་གི་ནང་དུ་ སྐབས་ཀ་བཞག་ཡོང།
ཉེན་སྐྱང་ལས་གཡོལ་བ།	T1036.005	མིང་ཟུར་དུ་འགྱུར་བ། : ཁྱིམས་མཐུན་ཀྱི་མིང་ཡང་ན་ས་གནས་མཐུན་སྒྲིག་འབད།	ཀོ་ཧོ་ཐན་ཡིག་ཚ་ཚུ་ཚ་འཛོག་ངོ་མ་ཚུ་གི་མིང་། ཕྱིར་སྐང་། ལས་དོན་ཚུ་དང་མཐུན་པ་བཅོ་སྐྱེས་ཡོངས།
ཉེན་སྐྱང་ལས་གཡོལ་བ།	T1656	མིང་ཟུར་འཛིན་པ།	ལས་བྱེད་པ་ཚུ་གིས་ཁེལས་སྐས་དུ་ཐུ་བཅོ་ཞེན་རྗེན་ཚ་དང་ངེམིགས་ཡུལ་ཚོགས་ཐུ་ཚུ་དང་འབྲེལ་བ་ཡོང་པའི་ལས་ལག་ལེན་པ་མིང་ལས་ཁུངས་ཀྱི་ཡིད་ཆེས་ཐོབ་ཡོང་པའི་མི་ཚུ་གི་ཚད་བྱེད་དོ།
བསྡུ་ལེན།	T1123	ཐུ་བཅུང་།	ཅོ་ཧོ་རྟེ་ཅེ་སྒོག་རིམ་ཚུ་གིས་ སྐད་འཛིན་འཛོལ་སྒྲིང་རྩིས་ཀ་ དབོས་མཚོ་མེད་པའི་གནང་བ་ཚུ་ ཞུ་བ་འབད་འོང།
བསྡུ་ལེན།	T1125	བརྙན་འཛིན་བཅུང་།	ཅོ་ཧོ་རྟན་ཀྱི་སྒོག་རིམ་གིས་ པར་ཆས་འཛོལ་སྒྲིང་ཚུ་རྩིས་ཀ་ དབོས་མཚོ་མེད་པའི་གནང་བ་ཚུ་ ཞུ་བ་འབད་འོང།
བསྡུ་ལེན།	T1005	ཉེ་གནས་རིམ་ལུགས་ལས་ གནད་སྤྲད།	ཀོ་ཧོ་ཐན་ཉེར་སྒྲིང་ཚུ་གིས་ས་གནས་ཡིག་ཚ་ཚུ་ཚུད་དེ་མི་དགོས་པའི་ཚོ་གཅིག་ཚུ་ཞུ་ཡིད།
བགའ་རྒྱ་དང་ཚད་འཛིན	T1071.001	སྒོག་རིམ་བང་རིམ་མཐུན་སྒྲིག : ད་རུ་ཐོག་མཐུན།	མཉེན་ཆས་འདི་གིས་ HTTPS དང་ WebSocket’s ལག་ལེན་འཐབ་སྟེ་ C2 ལུ་མཐུདཔ་ཨིན།
བགའ་རྒྱ་དང་ཚད་འཛིན	T1509	ཚད་ཟན་མ་ཡིན་པའི་འདྲེན་ལམ།	ཚད་ཟན་མེན་པའི་འདྲེན་ལམ་ཚུ་ འདྲེན་ལམ་ 4432 དང་ 2333 བཟུམ་ལག་ལེན་འཐབ་ཡོངས་ཨིན།

ཐྱི་བཞག་གཏང་ནི།	T1041	C2 རྒྱུན་ལམ་ལས་ཐྱིར་འཛེན་འབད་ནི།	ཞབས་སྟོར་གནོད་པ་གིས་ HTTPS དང་ WebSocket མཐུད་ལམ་ལག་ལེན་འཐབ་སྐྱེ་གནས་ཚད་ཐྱིར་འདོན་འབད་ཤ་ཕིན།
ཁན་གནོད།	T1565.002	གནད་སྡུད་གཡོ་སྐྱུ: བརྒྱུད་སྤེལ་འབད་ཡོད་པའི་གནས་སྡུད་གཡོ་སྐྱུ།	དུ་རྒྱུ་མི་ངན་ཚུ་གིས་ཉེར་སྟོངས་ཀྱི་ལས་དོན་ལུ་མི་དགོས་པའི་ཉེར་སྟོངས་དུ་རྒྱུ་འགྱལ་བཞུང་ཆོག་མཚན་ཉིན་པའི་སྐོ་ལས་ཀ་རྒྱག་པ་ཚུ་ལས་གནས་ཚད་ཇོ་བོ་དོ།

བང་སྟོན།

MOONSHINE:

- ༢༠༢༤ ལོ་ ཟླ་ ༤ ཏ་ ཚེས་ ༡ ལུ་ VLiteUI ལེ་ནལ་ཚུ་འཚོལ་བ་ལས་འདག་གི་ཚུ་ལོག་ཡོདཔ།:

IP ཁ་སྐོང།	འདྲེན་ལམ།	དང་པ་མཐོང་བ།	མཐའ་མ་མཐོང་བ།
103.254.108[.]87	888	2024-10-17	2025-02-14
43.159.192[.]7	444	2024-11-21	2025-02-13
103.27.109[.]109	444	2024-07-11	2025-02-07
45.119.99[.]83	444	2024-12-26	2025-01-24
103.254.108[.]76	444	2024-09-12	2024-12-05
194.71.107[.]160	444	2023-12-10	2024-11-01
103.254.108[.]108	444	2023-11-12	2024-09-25
103.56.17[.]194	444	2024-04-03	2024-08-23
103.254.108[.]87	444	2023-11-14	2024-08-15
62.72.58[.]168	444	2024-01-29	2024-08-07
103.43.18[.]43	444	2024-02-12	2024-07-19
77.91.123[.]208	444	2024-02-04	2024-04-09
46.246.98[.]229	444	2024-03-07	2024-03-26
2.58.15[.]101	444	2024-02-23	2024-02-27
46.246.98[.]209	444	2024-01-08	2024-02-14
103.254.108[.]87	8000	2023-10-17	2023-10-17
103.254.108[.]87	8080	2023-04-15	2023-10-16
103.254.108[.]108	9090	2023-04-13	2023-10-16
103.45.66[.]123	9090	2023-03-02	2023-04-08
103.45.66[.]32	8080	2022-07-29	2023-04-06
27.124.20[.]23	9090	2022-05-28	2023-03-24
27.124.20[.]22	9090	2022-05-28	2023-03-23
27.124.20[.]24	9090	2022-05-27	2023-03-17
69.176.94[.]148	9090	2023-03-04	2023-03-10
69.176.94[.]228	9090	2022-12-24	2023-02-25
103.253.40[.]137	8000	2022-06-24	2022-09-02
27.124.4[.]80	8080	2022-02-25	2022-06-23
27.124.4[.]81	8080	2022-02-25	2022-06-23
47.242.46[.]79	8080	2021-05-03	2022-06-17
27.124.4[.]82	8080	2022-02-24	2022-06-15
27.124.4[.]165	9090	2022-05-14	2022-05-28

27.124.4[.]184	9090	2022-05-14	2022-05-27
27.124.4[.]178	9090	2022-05-13	2022-05-26
103.15.28[.]165	8080	2022-03-05	2022-05-25
69.176.94[.]226	8080	2022-03-05	2022-04-22
27.124.4[.]3	8080	2022-03-11	2022-04-02
103.140.238[.]235	8080	2022-03-04	2022-04-01
27.124.4[.]2	8080	2022-03-12	2022-04-01
165.84.180[.]107	8000	2022-02-25	2022-03-19
69.176.94[.]156	8000	2022-02-25	2022-03-05
141.98.212[.]70	9090	2021-10-05	2022-03-04
5.188.33[.]50	8000	2022-02-15	2022-03-04
5.188.70[.]193	8000	2022-02-15	2022-03-04
69.176.94[.]140	8080	2022-02-24	2022-02-24
27.124.20[.]83	8000	2022-02-14	2022-02-18
208.87.200[.]106	8000	2022-01-02	2022-01-02
121.127.241[.]37	8000	2021-12-08	2021-12-08
156.255.2[.]211	443	2021-10-05	2021-10-05
156.255.2[.]211	8000	2021-10-04	2021-10-04
156.255.2[.]203	8000	2021-10-03	2021-10-03
47.243.43[.]248	8000	2021-07-05	2021-07-05
45.115.236[.]6	8080	2021-05-03	2021-06-01
43.251.118[.]97	8000	2021-01-03	2021-03-01
185.243.43[.]138	8000	2021-01-04	2021-02-02
47.245.59[.]33	8000	2021-01-05	2021-01-05

- ༢༠༢༤ ལོ་ ཟླ་ ༤ ར་ ཚེས་ ༡ ལུ་ SCOTCH ADMIN ལེ་ནལ་ཚུ་འཚོལ་བ་ལས་འགེལ་གི་ཚུ་རྐྱེད་ཡོདཔ།:

IP ཁ་སྐོང་།	འདྲེན་ལམ།	དང་པ་མཐོང་བ།	མཐའ་མ་མཐོང་བ།
104.194.152[.]24	2333	2025-02-06	2025-02-27
172.86.80[.]126	2333	2025-02-07	2025-02-27
154.90.59[.]62	2333	2024-06-20	2024-09-20
154.90.59[.]88	2333	2024-06-21	2024-09-20
154.90.58[.]210	2333	2024-05-16	2024-06-14
154.90.59[.]225	2333	2024-05-17	2024-06-13
38.60.199[.]208	2333	2023-11-26	2024-01-09
38.60.199[.]254	2333	2023-11-28	2024-01-09
38.60.199[.]99	2333	2023-08-26	2023-11-21

38.60.199[.]44	2333	2023-07-20	2023-09-11
194.163.34[.]23	443	2022-09-30	2023-04-14
45.32.125[.]112	10443	2022-10-01	2023-03-17

- ༢༠༢༤ ལོ་ ཟླ་ ༣ ཚ་ ཚེས་ ༡༤ ལུ་ virtual SCOTCH ADMIN འེ་ནལ་ཚུ་འཛོལ་བ་ལས་འདེག་གི་ཆུ་འོག་ཡོངས།:

རྩ་མེན།	IP ཁ་བྱང་།
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:

འགྲེལ་བཤད།	BADBAZAAR C2s ཚུ་གུ་ SSL ལག་ཆེར་མཐོང་ཡོད།
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- ༢༠༢༥ ལོ་ ཟླ་ ༦ ཚ་ ཚེས་ ༧ ལུ་ སྟོང་ཀྱི་ BADBAZAAR ལག་ཆེར་འཛོལ་བ་ལས་འདེག་གི་ཆུ་འོག་ཡོངས།:

IP ཁ་བྱང་།	འདྲེན་ལམ།	དང་པ་མཐོང་བ།	མཐའ་མ་མཐོང་བ།
65.108.192[.]173	31237	2025-03-14	2025-03-28
65.108.192[.]173	31236	2025-03-14	2025-03-28
65.108.192[.]173	31235	2025-03-14	2025-03-28
157.90.129[.]73	31236	2025-03-27	2025-03-27
142.132.131[.]15	31236	2024-07-24	2025-03-27
142.132.131[.]15	31235	2024-07-26	2025-03-27

142.132.131[.]20	31237	2023-08-11	2025-03-27
142.132.131[.]15	31237	2024-07-24	2025-03-27
142.132.131[.]20	31236	2023-09-27	2025-03-26
142.132.131[.]20	31235	2023-10-18	2025-03-26
65.108.192[.]155	31236	2024-12-05	2025-02-20
65.108.192[.]155	31237	2024-12-05	2025-02-20
65.108.192[.]155	31235	2024-12-05	2025-02-19
23.88.28[.]222	31237	2024-04-25	2024-11-29
23.88.28[.]222	31235	2024-05-02	2024-11-28
23.88.28[.]222	31236	2024-05-01	2024-11-28
212.129.21[.]168	31235	2023-10-16	2024-03-17
212.129.21[.]168	31237	2023-08-24	2024-03-17
212.129.21[.]168	31236	2023-09-26	2024-03-14

འགྲེལ་བཤད།	**BADBAZAAR C2s ཚུ་གུ་ SSL** ལག་ཆྱེར་མཐོང་ཡོད།
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- ༢༠༢༥ ལོ་ ཟླ་ ༤ ཚ་ ཚེས་ ༡ ཉིན་གྱི་ BADBAZAAR ལག་ཆྱེར་འཚོལ་བ་ལས་འོག་གི་ཚུ་ཡོག་ཡོད།:

IP གནས།	འདྲེན་ལམ།	དང་པ་མཐོང་བ།	མཐའ་མ་མཐོང་བ།
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28
162.55.103[.]210	20121	2022-09-30	2023-02-23
65.21.92[.]67	20121	2021-11-02	2022-10-13

65.21.92[.]67	20122	2022-08-10	2022-10-13
23.88.28[.]220	20121	2021-12-08	2022-05-13
94.130.92[.]230	20121	2021-01-04	2021-10-05
88.99.150[.]246	20121	2021-04-06	2021-09-08
45.76.132[.]91	20121	2021-02-02	2021-03-01

- WHOIS མངའ་ཐོངས་ཚུ།

འོག་ལུ་དེ་སྤྲོ་ཡང་ན་ཚོ་རྒྱས་ནང་ལུ་ BADBAZAAR C2 ས་ཁུལ་ཚུ་ནང་མཐོང་ཡོད་པའི་གནས་གོང་ཚུ་དང་མཐུན་པའི་ WHOIS ཐོ་བཀོད་ཡོད་པའི་ས་ཁུལ་ཚུ་གི་རེའུ་མིག་ཅིག་ཡོད།

WHOIS གནས་གོང་།	ངོ་མཚན་ཚུ།
ཐོ་བཀོད་མངའ་སྡེ། **UJYJYUJ** ཐོ་བཀོད་འབད་སའི་རྒྱལ་ཁབ། ཝོ་ཕི་ཤྲི་ཡ། ཐོ་བཀོད་པ། **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
ཐོ་བཀོད་མངའ་སྡེ། **REWR** ཐོ་བཀོད་འབད་སའི་རྒྱལ་ཁབ། **CF** ཐོ་བཀོད་པ། **eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
ཐོ་བཀོད་མངའ་སྡེ། **FSDF** ཐོ་བཀོད་འབད་སའི་རྒྱལ་ཁབ། **AL**	• tryhrwserf[.]com • tibetone[.]org

ཐོ་བཀོད་པ: eNom	• comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

སློབ་འཛིན་ཀ་ཤོང་ཚུ།
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

ཡུ་ཏུབ་རྒྱུ་ལམ།
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

འོག་གི་ཚུ་ BADBAZAAR དང་ MOONSHINE དང་འབྲེལ་བ་ཡོད་པའི་གཞན་ཡི་འགྲོ་སྐྱངས་མཚོན་རྟགས་ (IoCs) ཚུ་གི་འབྲེལ་ལམ་ཚུ་ཨེན། NCSC གིས་འབྲེལ་ལམ་འདི་ཚུ་ནང་གི་གནས་ཚུལ་ཚང་མའི་ངོ་མ་ཡིན་མེན་ངེས་ཏིག་མ་བཏུབ་ཞེན་པ་དང་ ཤུག་མེ་ཚུ་ཡུ་འདི་ཚུ་གི་ ངེས་བདེན་དང་འབྲེལ་བ་ཡོད་མེད་རང་སོར་ར་ སྤྱོད་འབད་ནི་ གནས་འདེགས་བྱེད་མ་ཨིན།:

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity
- སི་ཏི་ཟེན་ལེབ་

སེལ་ཐབས།

རྒྱལ་ཁབ་སི་དི་ཤར་སེ་ཀུ་རི་ཏི་སེན་ཏར་ (NCSC) གིས་ཞེད་འཇུག་དུ། མཚོན་རང་ལུ་གསལ་བའི་ཉེན་ཁ་ཚུ་ལས་སྐྱང་སྐྱོབ་འབད་ནི་དོན་ལུ་འོག་གི་བསམ་འཆར་ཚུ་བསྟེན་པར་སྤོ་བཅོལ་འབད་ཨེ།

- **ཕྱོགས་གསུམ་པའི་མཉེན་ཆས་ཚོང་གཙུ་རྩིས་ཀྱི་ མཉེན་ཆས་ཚོང་གཅོལ་སྤྱོད་འབད་མི་དང་ གོང་འཕེལ་གཏང་མི་ཚུ་གིས་ ཁང་རའི་སྟེགས་བུ་གུ་ཡོང་པའི་ མཉེན་ཆས་ཚུ་ ཉེན་སྐྱང་དང་ཐུན་མཐུན་སྤེ་ གཞུང་གི་ལག་ལེན་སྤྱིག་གཞི་དང་འཁྱིལ་ཀྱི་ འབད་དགོས་དེས་གཏན་འཁེལ་བའི་དགོ།** ལམ་སྟོན་ལུ་བལྟ།:
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

- **སྐད་ཡིག་སྣ་ཚོགས་ཀྱི་རྒྱབ་སྐྱོར།:** མཉེན་ཆས་བཟོ་མི་ཚུ་གིས་ ཡུ་གུར་དང་ ཡོད་ ཐའི་ཡུན་གྱི་ ཀྱ་ཀི་ཡན་ དེ་ལས་ ཀེན་ཏོ་ནེའེ་ཚུ་རྩིས་ཀྱི་ དམིགས་གཏཀ་ཅན་གྱི་ རྩེ་ཚན་ཚུ་གི་གྲས་ལས་ སྐད་ཡིག་གྲངས་ལྟང་སྐལ་མི་ཚུ་གི་དོན་ལུ་ ཡོངས་གྲགས་ཅན་གྱི་ མཉེན་ཆས་ཚུ་ ས་གནས་ནང་ བཟོ་ནི་དོན་ལུ་ ཨ་རྩ་བཙུགས་དགོཔ་ཨིན་པས། ཨེ་པུལ་ཀྱིས་ཨེཔ་ཚུ་ནང་ལུ་ས་གནས་ཀྱི་སྐད་ཡིག་བཀོལ་སྤྱོད་འབད་ནིའི་ལམ་སྟོན་:
https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. གུ་གུལ་ཀྱིས་ཨེཡ་ཚུ་བསྒྲུབ་བ་འབད་ནིའི་ལམ་སྟོན་:
https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **ཁྱོད་རའི་མི་སྡེ་བང་བཙུང་ཀྱི་སྟེགས་བུ་འདི་ཉེན་སྐྱང་དང་ཕྲུན་སྡེ་བཞག་ནི།:** མི་སྡེ་བང་བཙུང་ལས་སྡེ་ཚུ་གིས་ གནོད་པ་བཀག་ལ་མི་ཚུ་ལུ་ རྩིས་ཁྲ་རྩྭས་མ་བཟོ་ནི་དང་ གནོད་པ་ཅན་གྱི་ཡིག་སྒོང་ཚུ་ ཡང་ན་ འབེལ་མཐུད་ཚུ་ དེ་མེན་པ་ཅིན་ ཁྲིམས་མཐུན་གྱི་ ཡོངས་འབེལ་གྱི་མི་སྡེ་ཚུ་ནང་ བརྩེ་སོར་འབད་ནི་ལུ་ ལྟ་ཁག་བཏང་བོང་། འབད་ཚུགས་ས་ལུ་ ལས་སྡེ་ཚུ་གིས་ ཉེན་ལ་གི་སྐོར་ལས་ མཉམ་འཇེལ་གྱི་གོ་ཆོགས་ཡར་དྲག་གཏང་ནི་དང་ ཉེན་སྤུང་གི་ཐབས་ལམ་ཚུ་ལུ་ ཐོག་ས་རམ་འབད་ནིའི་དོན་ལུ་ བཟོ་གྲ་ཆུ་ཚེལ་ཚུ་དང་གཅིག་ཁར་ གནོད་འཇེལ་གྱི་གོ་ཆོགས་ཡར་དྲག་གཏང་ནི་དང་ ཉེན་སྤུང་གི་ཐབས་ལམ་ཚུ་ལུ་ ཐོག་ས་རམ་འབད་ནིའི་དོན་ལུ་ བཟོ་གྲ་ཆུ་ཚེལ་ཚུ་དང་གཅིག་ཁར་ གནོད་འཇེལ་ཚུ་ དེ་ཚུ་ལས་ འཛོལ་ཚུ་ བཟོ་ནི་ལུ་ ཐུབ་པའི་ཐབས་ལམ་ཚུ་ བརྩེ་སོར་འབད་དགོ།

- **ཞབས་ཏོག་སྤྱོད་མཁན་ཚུའི་དོན་ལུ་སེལ་ཐབས་འཚར་གཞི།:** ལས་སྡེ་ཚུ་གིས་ ཁོང་རའི་ཞབས་ཏོག་ཚུ་ལས་ལེན་འཐབ་སྟེ་ གནོད་པ་ཅན་གྱི་མཉེན་ཆས་ཚུ་ གཞི་བཙུགས་འབད་མི་ ཚོང་མཁོན་པ་ཚུ་ལུ་ བརྩེ་དགོས་ཨིན་པས། ཉེན་བརའི་ཚུ་ སེམས་ཤར་འབད་ཚུགས་པ་དང་ བརྩེ་སྤྱོད་ཚུགས་སྟེ་དགོ། འོས་འབབ་ཡོད་ས་ལུ་ ལས་སྡེ་ཚུ་གིས་ མཉེན་ཆས་འདི་ བཏོག་གཏང་ཐངས་སྐོར་ལས་ ལམ་སྟོན་བྱིན་དགོཔ་དང་ ཉམས་རྒྱངས་ཚུ་གིས་ ཡུ་གེ་ལུ་ཡོད་པའི་ NCSC བཟུམ་གྱི་ དབང་འཛིན་ཚུ་ལུ་ སྐན་ཞུ་འབད་དགོཔ་སྟེ་ སེམས་ཤྲུགས་བྱིན་དགོ།

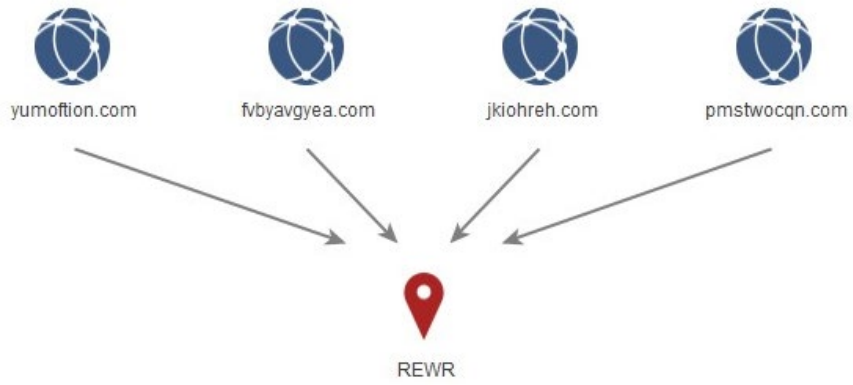
བརྩེ་དོན་ཁ་གསལ་ཡ་གྱི་དོན་ལུ་ App Store གི་ལག་ལེན་སྤྱིག་གཞི་ལམ་ལུགས་ལུ་སྐྱ།:
https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **མཉམ་འཇེལ་གྱི་དོན་ལུ་ ལྟ་འབད་མི་སྡེ་ཚན།:** མི་སྡེ་བརྩ་བརྩུད་ལས་སྡེ་ཚུ་གིས་ ལྟ་འབད་མི་སྡེ་ཚན་ཚུ་ བཟོ་སྟེ་ རང་སོའི་ཉེན་སྤུང་སྡེ་ཚན་ཚུ་གིས་ གནོད་པ་ཅན་གྱི་ བརྩ་མཚོན་དང་ TTPs དེ་ལས་ བཟྱ་བརྟོག་ཚུ་ བརྩེ་སོར་འབད་བཏུག་སྟེ་ འཁྲབ་ཟིངས་ཚུ་གིས་ གནོད་པ་ཅན་གྱི་སྐལ་བསྟགས་ཚུ་ལུ་ རྒྱབ་སྐྱོར་འབད་ནི་ལུ་ ཁོང་རའི་ ས་སྐོ་ཚུ་ ལག་ལེན་འཐབ་ནི་ལུ་ ལྟ་ཁག་བཏང་མ་ཨིན་པས།

- **བསྐྱར་བཅོས་འབད་ཡོད་པའི་སྒོག་རིམ་ཚུ་ ཤེས་རྟོགས་འབད་དོ།:** འབད་ཚུགས་ཚུགས་ཅིག་ སྒོག་རིག་བཟོ་མི་ཚུ་གིས་ སྒོག་རིག་ཅིག་གི་ ‘གཞུང་འཛིལ་མེན་པའི་’ ཐོན་རིམ་ཁག་ལེན་འབད་དེ་ཡོད་པ་ཅིན་ ལག་ལེན་པ་ལུ་ བརྩ་དོན་སྐྱོང་མི་ ལྟ་འགན་ཚུ་ བསྟུགས་དགོས་ཨིན།

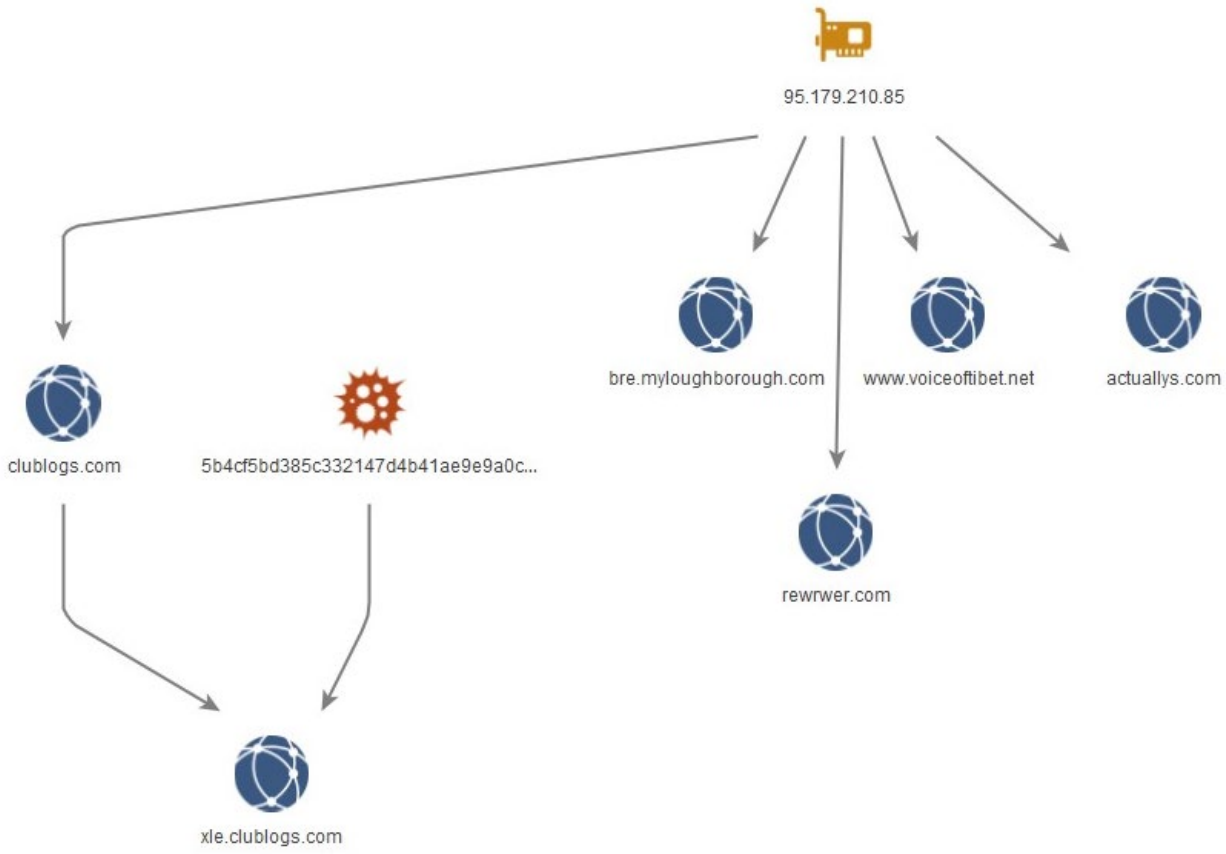
པར་རིས་ ༡ – ‘UKYJYUJ’

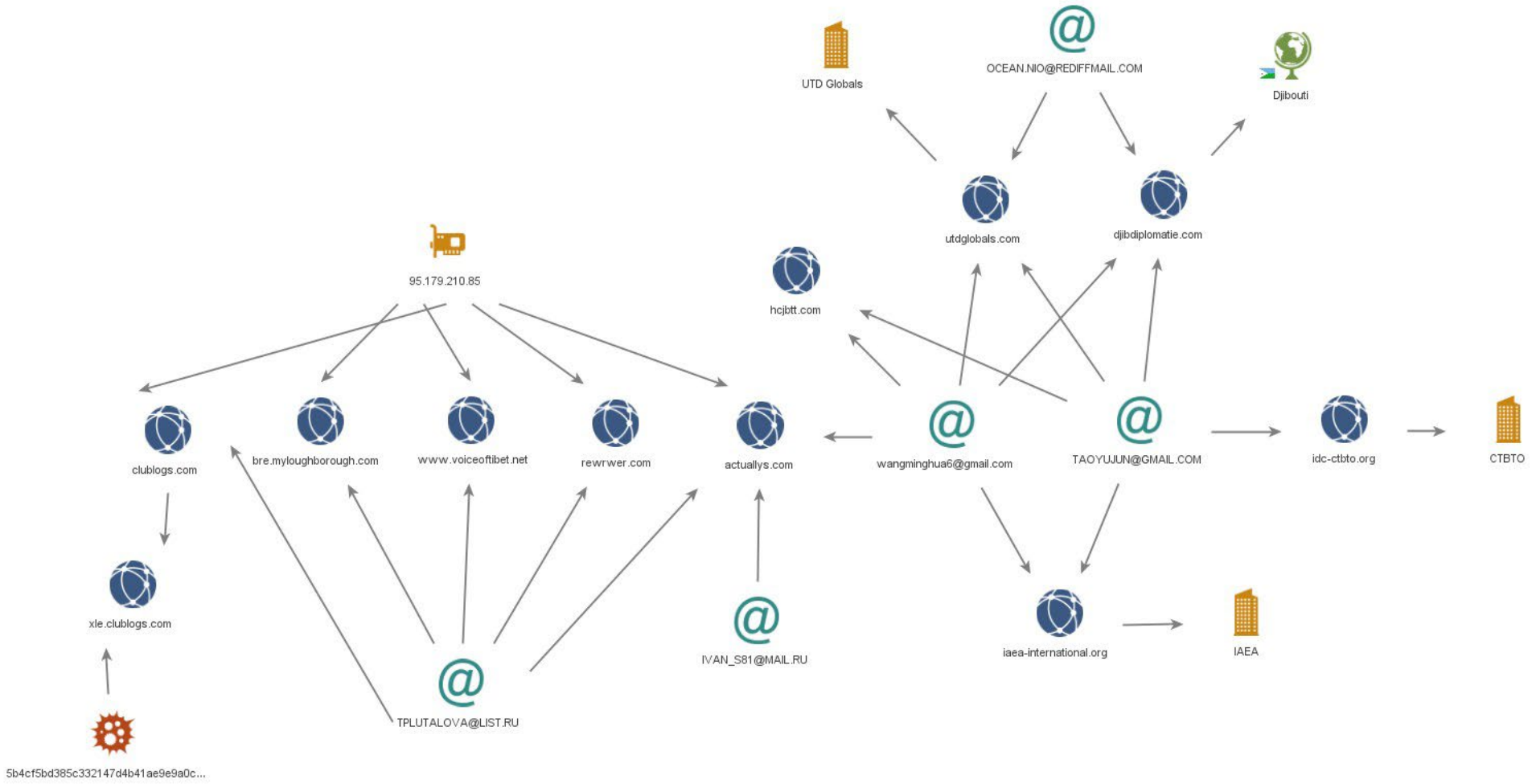
པར་རིས་ ༢ – ཉེ་སྒྲོམ་འགྱོ་བའི་གནས་གོང་ཚུ།



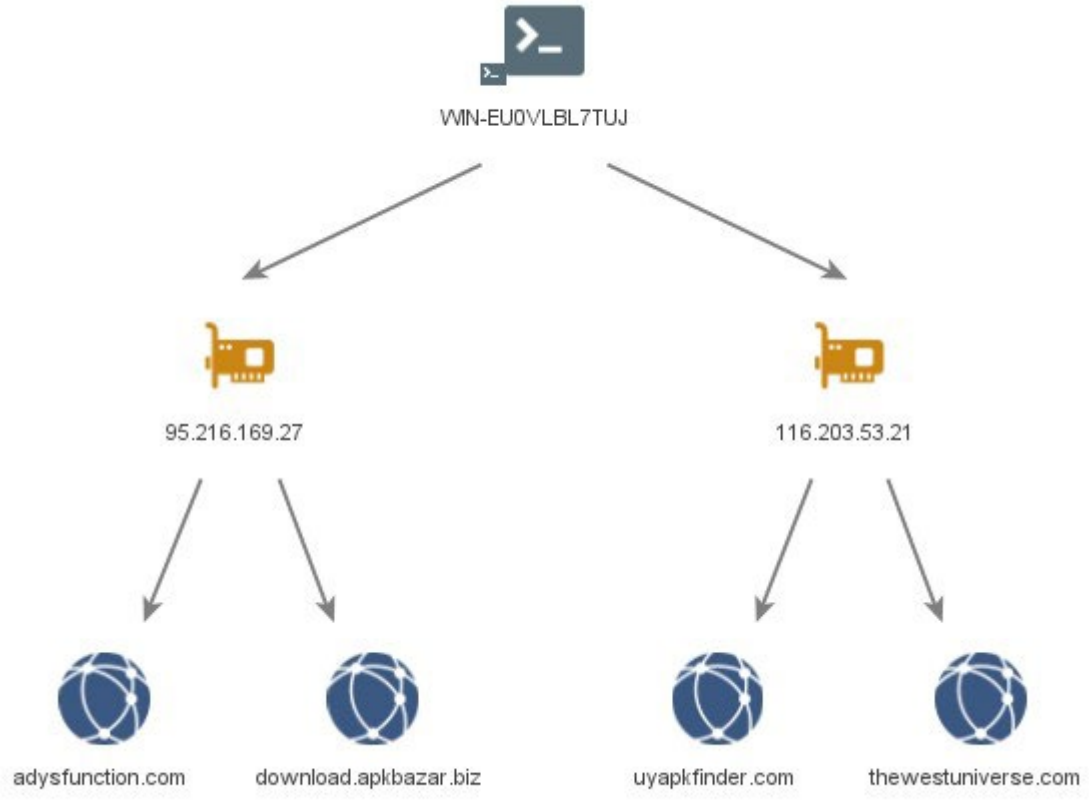
པར་རིས་ ༣ – ‘FSDF’ གནས་སྡུད་ས་སྒོའི་གནས་གོང་ཚུ་དང་གཅིག་ཁར་ ལ་སྐོང་མངའ་ཐོངས་ཚུ།

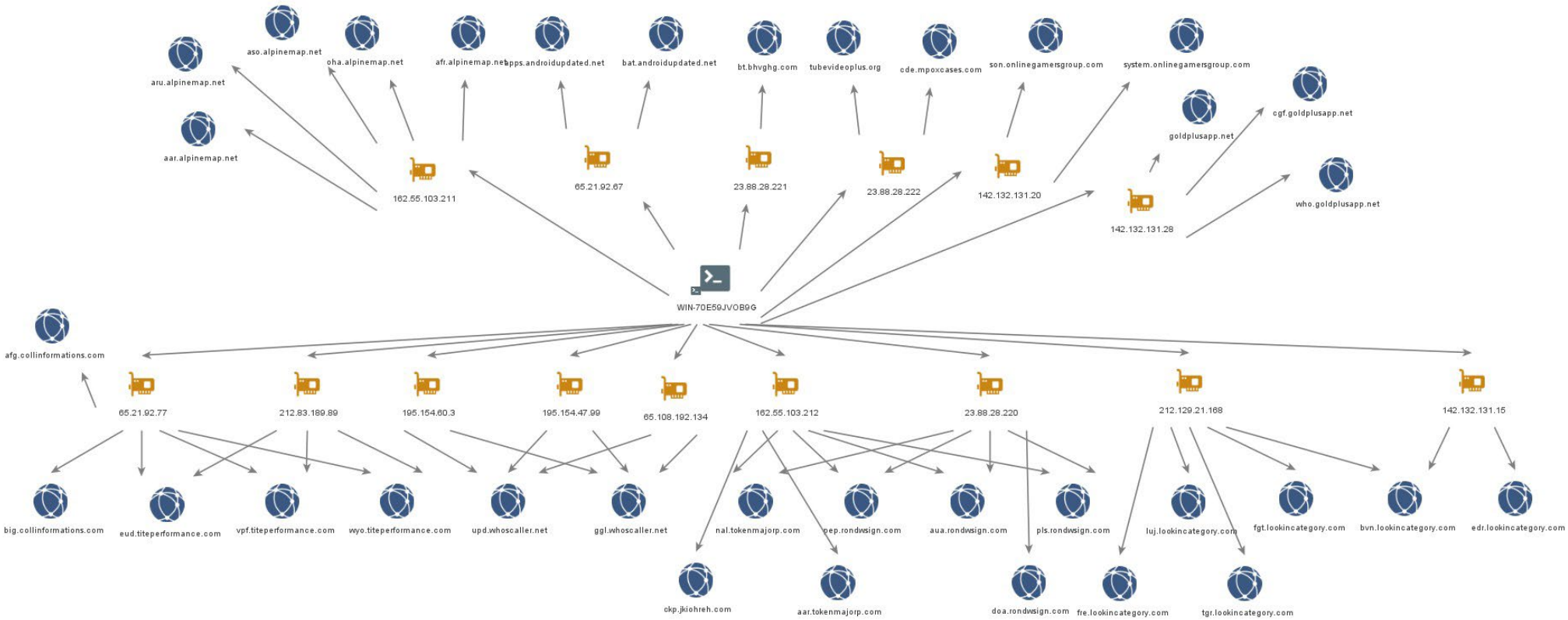
དཔར་རིས་ ༤ – **95.179.210[.]85**



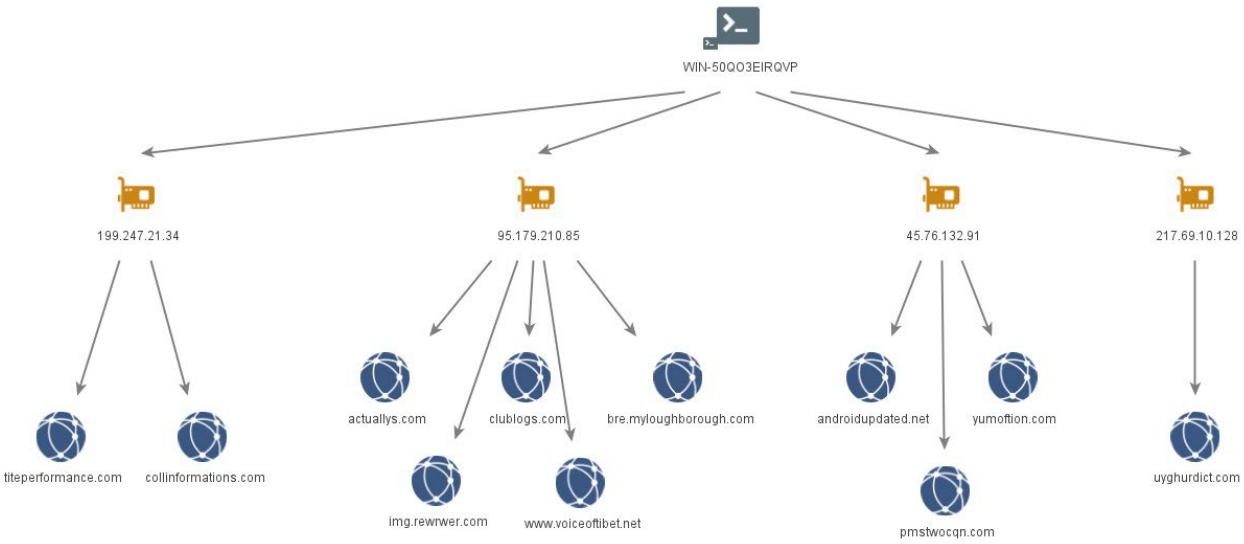

UTD Globals
OCEAN.NIO@REDIFFMAIL.COM
Djibouti
utdglobals.com
djibdiplomatie.com
95.179.210.85
hcjbtt.com
clublogs.com
bre.myloughborough.com
www.voiceoftibet.net
rewrwer.com
actuallys.com
wangminghua6@gmail.com
TAOYUJUN@GMAIL.COM
idc-ctbto.org
CTBTO
xle.clublogs.com
IVAN_S81@MAIL.RU
iaea-international.org
IAEA
TPLUTALOVA@LIST.RU
5b4cf5bd385c332147d4b41ae9e9a0c...

དཔར་རིས། ༤ – **WIN-EU0VLBL7TUJ**

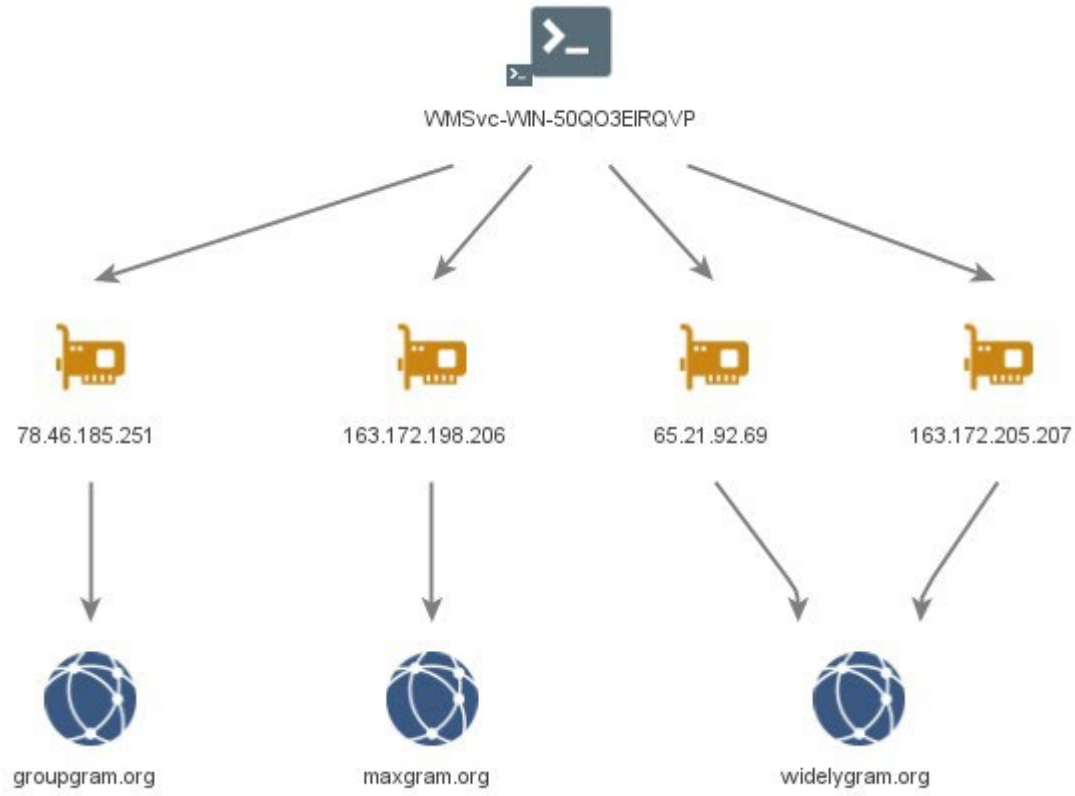



aru.alpinemap.net
aso.alpinemap.net
oha.alpinemap.net
afr.alpinemap.net
apps.androidupdated.net
bat.androidupdated.net
bt.bhvghg.com
tubevideoplus.org
cde.mpoxcases.com
son.onlinegamersgroup.com
system.onlinegamersgroup.com
cgf.goldplusapp.net
goldplusapp.net
who.goldplusapp.net
aar.alpinemap.net
162.55.103.211
65.21.92.67
23.88.28.221
23.88.28.222
142.132.131.20
142.132.131.28
WIN-70E59JVOB9G
afg.collinformations.com
65.21.92.77
212.83.189.89
195.154.60.3
195.154.47.99
65.108.192.134
162.55.103.212
23.88.28.220
212.129.21.168
142.132.131.15
big.collinformations.com
eud.titeperformance.com
vpf.titeperformance.com
wyo.titeperformance.com
upd.whoscaller.net
ggl.whoscaller.net
nal.tokenmajorp.com
pep.rondwsign.com
aua.rondwsign.com
pls.rondwsign.com
luj.lookincategory.com
fgt.lookincategory.com
bvn.lookincategory.com
edr.lookincategory.com
ckp.jkiohreh.com
aar.tokenmajorp.com
doa.rondwsign.com
fre.lookincategory.com
tgr.lookincategory.com

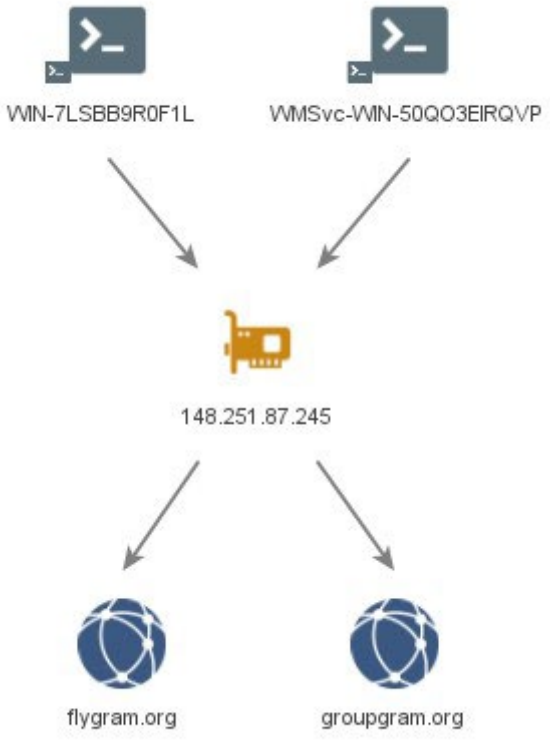
བར་རིས་ ༤ – WIN-50QO3EIRQVP



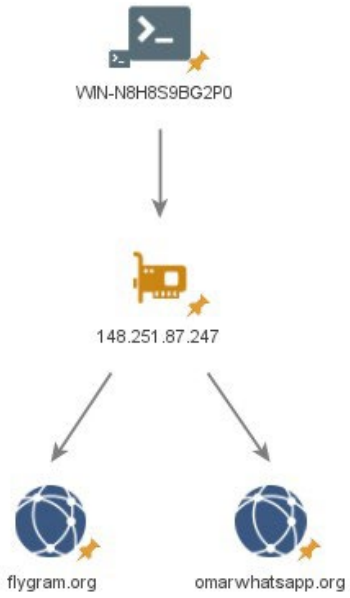
བར་རིས་ ༥ – VMSvc-WIN-50QO3EIRQVP



ཡར་རེས་ ༡༠ – **VMSvc-WIN-50QO3EIRQVP དང་ WIN-7LSBB9R0F1L**



པར་རིས་ ༧༧ - **WIN-N8H8S9BG2P0**



པར་རིས་ ༧༢– **WIN-I6VBN8MR92A**

ཟུར་འཛོར་ཁ་བྱ: MOONSHINE དང་ BADBAZAAR དེ་ལ་ཚད་བཟུང་རྩོགས་འབད་ཡོདཔ།

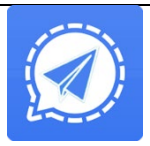
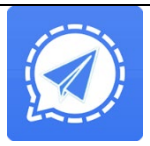
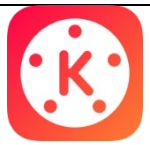
འོག་གི་ཐིག་ཁྲམ་ནང་ འདི་ལ་བའི་ཚོ་གཉིས་ཀྱི་ནང་འཛོད་ལུ་ MOONSHINE དང་ BADBAZAAR གི་རྒྱལ་བསྟུགས་ནང་ ལག་ལེན་འཐབ་མི་ མཉེན་ཆས་ཚུ་ ཐོ་བཀོད་འབད་དེ་ཡོདཔ་ཨིན།

འ་ནི་སྒོག་རིམ་མང་ཤོས་ཅིག་གིས་ གཞི་བཙུགས་འབད་ཡོད་པའི་སྒོག་རིམ་ཚུ་དང་ གསལ་ཏོག་ཏོ་སྟེ་ ཅོག་འཐདཔ་སྟེ་སྤོན་ཨིན། འདི་མཐོངས་གྲགས་ཅན་ཀྱི་ཚོང་ཁྲ་ཚུ་ 'spoof' འབད་ནི་དོན་ལུ་དགོས་དམ་གྱིས་ཟུངཔ་མི་གི་ཐབས་ལམ་ཅིག་ཨིན་པ་ངེས་གསལ་ཏོག་ཏོ་ཅིག་ཨིན།

གལ་ཆེ་བའི་གནད་དོན་ཅིག་བརྗོད་དགོ་པ་ཅིན། མེལ་གྱི་འགོ་མེང་། པེ་ཀེཇ་གྱི་མེང་། དང་ཞེལ་གྱི་རི་མོ་ཚུ་ཡང་དངོས་འབྲེལ་མེལ་ལི་ཀེ་ཤན་དང་འབྲ་བ་ཡང་ན་གཅིག་པ་བཙོ་བཏུབ་པས། དེ་འབདཝ་ལས་ཐབས་འཕྲུལ་ཅིག་གིས་ནད་ཡོད་མེད་ངོས་འཛིན་འབད་ནིའི་དོན་ལུ་འདི་ཚུ་ཀང་པ་གཅིག་རང་ལུ་བརྟེན་མི་ཆོག

App མིང་།	ཁྲམ་སྤྱིལ་མིང་།	App ངོས་དཔར།
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	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	

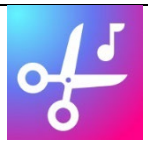
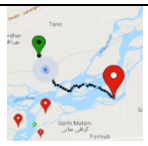
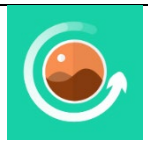
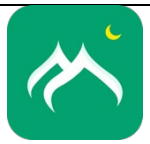
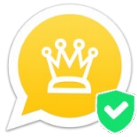
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	

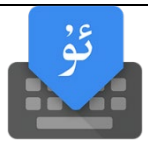
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
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 ئۇيغۇرچە APK	com.uygur.apkstore	
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	
القرآن الكريم	com.maher4web.quran	
زىكىرلەر	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	

ཉེར་བཀལ་སྤྲག་ནི།

ཚོ་སི་ཏོ་ལེ་ཡའི་དྲ་རྒྱའི་བདེ་འཇགས་ལྷེ་གནས་ཀྱི་ལམ་སྟོན།

- དྲ་རྒྱའི་ནགས་ཉེས་དང་དོན་རྒྱན་ཡང་ན་ཉེན་ཁ་ཡོད་པའི་གནས་ཚུལ་སྐྱན་སེང་ཞུ་བ།
- རང་གི་ཡོ་བྱད་བདེ་འཇགས་བཟོ་ཐབས།
- ཁྱོད་ཀྱི་འགྲུལ་འཕྲིན་ཉེན་མེད་བཟོ
- ཐེ་ཧིང་།
- མཁོ་སྒོར་
- ཁྱོད་ཀྱི་མི་སྡེ་བརྒྱུད་ལམ་ཉེན་མེད་བཟོ
- མི་སྡེ་བརྒྱུད་ལམ་དང་འཕྲིན་གཏད་མེད་ཀྱི་འདོན་ལ་བདེ་འཇགས་གི་གསལ་བཤད

ཡུ་ཀེ་ NCSC དང་ NPSA ལས་ལམ་སྟོན།

- མང་གཙོའི་རིང་ལུགས་སུང་སྐྱོབ།
- མི་སྡེ་བརྒྱུད་ལམ་: ཉེན་མེད་སྡེ་ཚོད་སྐྱོང་འབད་ཐབས།
- འགྲུལ་འཕྲིན་གྲངས་སུ་བཏབ་པའི་ཚོགས་སྡེ་ཀྱའི་དོན་ལུ་ཐབས་འཕྲུལ་བདེ་འཇགས་ལམ་སྟོན
- ཉེར་སྤྱོད་ཚོང་ཁང་གི་ཉེན་ཁའི་སྐྱན་ཞུ།
- ཉེན་ཁ་མཐོ་བའི་གང་ཟག་ཀྱའི་དོན་ལུ་རང་དོན་འདོན་ལུ་བདེ་འཇགས་དང་ཉེན་སུང

ཨ་མེ་རི་ཀའི་རྒྱལ་ཁབ་འདོན་ལུ་བདེ་འཇགས་ཡོངས་ཁྱབ་ (NSA) གི་ལམ་སྟོན

- འགྲུལ་འཕྲིན་ཐབས་འཕྲུལ་གྱི་ལག་ལེན་ལེགས་ཤོས

ཁས་ལེན་འཁོད་མེད།

གོས་སྟོན་འདི་གིས་ དཔར་བསྐྲུན་འབད་བའི་སྐབས་ བདེན་དཔྱད་འབད་ཡོད་པའི་བརྡ་དོན་ཚུ་ཅིན་མེན་ལས་ དྲན་འཛིན་འབད་གནང་།

སྐན་ཁུ་འདི་གིས་ རྩོམ་སྒྲིག་ལས་ཁྲེ་དང་ བཟོ་གྲའི་འཚུང་ཁུངས་ཚུ་ལས་ བརྡ་དོན་ཚུ་ བགོོ་ནས་ཡོད་པ་མིན། ཞིབ་འཇུག་དང་གོས་འཚར་གི་ཅ་ར་འབད་རྩད་ ཉེན་ཁ་གི་ར་ལས་ བཀག་ཐབས་ འབད་ནའི་དོན་ལུ་ མ་བྱིན་པར་ཡོད་པ་ལས་ གོས་འཚར་ཚུ་ལུ་གཞི་བཞག་སྟེ་ དེ་བཟུམ་གྱི་ཉེན་ཁ་ཚུ་གི་ར་ བགོོ་མི་ཚུགས། བརྡ་དོན་ཉེན་ཁ་གི་བདག་དབང་འདི་ དུས་རྒྱུན་དུ་ འཛེལ་ཡོད་ལམ་ལུགས་ཀྱི་ཇོ་བདག་ལུ་རང་ ལུགང་ཨིན།

ཡུ་ཀེ་ལུ་ བརྡ་དོན་འདི་ བརྡ་དོན་རང་དབང་བཅའ་ཁྲིམས་ ༢༠༠ (FOIA) གི་འོག་ལུ་ ཆ་མེད་བཏང་ཡོངས་མ་ཚད་ ཡུ་ཀེ་གི་བརྡ་དོན་ཁྲིམས་ལུགས་གཞན་ཚུ་གི་འོག་ལུ་ཡང་ ཆ་མེད་བཏང་རྒྱུགས་ནི་ཨིན་མས།

ཨེཕ་ཨོ་ཨའི་ཨེ་ (FOIA) གི་འདི་དཔྱད་གང་རུང་ ncscinfoleg@ncsc.gov.uk ལུ་གཏང་།

རྒྱུ་ཆ་ཆ་མཉམ་·· UK Crown ཀྱི་ཡར་དབང་ཨིན། ©