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

# උපදේශන

# BADBAZAAR and MOONSHINE: තාක්ෂණික විශ්ලේෂණය සහ ලිහිල් කිරීම්

2025 අප්‍රේල් 9

# BADBAZAAR and MOONSHINE: තාක්ෂණික විශ්ලේෂණය සහ ලිහිල් කිරීම්

## සාරාංශය

එක්සත් රාජධානියේ සයිබර් ලීගයේ සහාය ඇතිව, මෙම උපදේශනය ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය (NCSC UK) සහ ජාත්‍යන්තර හවුල්කරුවන් විසින් ඒකාබද්ධව උත්පාදනය කර ඇත:

- **ඔස්ට්‍රේලියානු සංඥා අධ්‍යක්ෂ මණ්ඩලයේ කොටසක් වන ඔස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානය**
- **සන්නිවේදන ආරක්ෂක ආයතනයේ කොටසක් වන කැනේඩියානු සයිබර් ආරක්ෂාව සඳහා වූ මධ්‍යස්ථානය**
- **ජර්මානු ෆෙඩරල් බුද්ධි සේවය**
- **ආණ්ඩුක්‍රම ව්‍යවස්ථාව ආරක්ෂා කිරීම සඳහා වූ ජර්මානු ෆෙඩරල් කාර්යාලය**
- **රජයේ සන්නිවේදන ආරක්ෂක කාර්යාංශයේ කොටසක් වන නවසීලන්ත ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය**
- **එක්සත් ජනපද ෆෙඩරල් විමර්ශන කාර්යාංශය**
- **එක්සත් ජනපද ජාතික ආරක්ෂක ඒජන්සිය**

මෙම උපදේශනය BADBAZAAR සහ MOONSHINE ලෙස හඳුන්වන ඔත්තු මෘදුකාංග ප්‍රභේද දෙකක් පිළිබඳව නව සහ ඒකාබද්ධ තර්ජන බුද්ධිය සපයන අතර, එහි යෙදුම් ගබඩා ක්‍රියාකරුවන්, සංවර්ධකයින් සහ සමාජ මාධ්‍ය සමාගම් සඳහා ඔවුන්ගේ පරිශීලකයින් ආරක්ෂිතව තබා ගැනීමට උපකාර කිරීම සඳහා උපදෙස් ඇතුළත් වේ.

මෙම උපදේශනය මෙම අනිෂ්ට මෘදුකාංගවලට ගොදුරු වූවන් සඳහා වන උපදේශනයකට සමාන්තරව ප්‍රකාශයට පත් කෙරේ.

මෙම ලේඛනය ඔත්තු මෘදුකාංග පිළිබඳ NCSC පාරිභාෂික අර්ථ දැක්වීම භාවිතා කරයි: "පරිශීලකයාගේ අවසරයකින් තොරව උපාංගයක ස්ථාපනය කරන, දත්ත රැස් කර තෙවන පාර්ශවයකට යවන අනිෂ්ට මෘදුකාංග වර්ගයකි."

## පළමු ප්‍රත්‍යක්ෂ අධ්‍යයනය MOONSHINE

MOONSHINE යනු 2019 දී Citizen Lab විසින් ටිබෙට් කණ්ඩායම් ඉලක්ක කර ගනිමින් වාර්තා කරන ලද Android ඔත්තු මෘදුකාංගයකි. MOONSHINE යෙදුම ස්ථාපනය කිරීමට වින්දිනයින්ව පොළඹවා ගැනීම සඳහා එය නීත්‍යානුකූල යෙදුමක් බොරු වේශයෙන් පෙන්නුම් කරයි. මෙම යෙදුම Telegram නාලිකා හරහා සහ WhatsApp හරහා යවන ලද සබැඳි හරහා බෙදාගෙන ඇත.

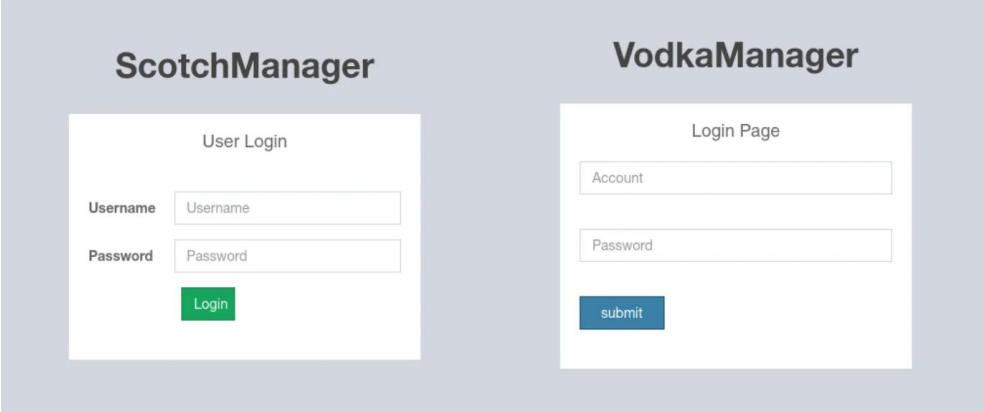
MOONSHINE පිළිබඳ NCSC පර්යේෂණයෙන් පහත සඳහන් දෑ පෙන්නුම් කෙරේ:

- MOONSHINE එය මුලින්ම වාර්තා කළ දා සිට වෙනස්කම් වලට භාජනය වී ඇති කළමනාකරණ අතුරුමුහුණතක් භාවිතා කරයි.
- කළමනාකරණ අතුරුමුහුණත මගින් හෙළි කරන්නේ උපාංගවලින් ගොනු ඉවත් කිරීමට මෙන්ම සජීවී ශ්‍රව්‍ය සහ තිර පටිගත කිරීම් ග්‍රහණය කර ගැනීමට ඇති හැකියාව ඇතුළුව පුළුල් නිරීක්ෂණ හැකියාවන් එයට ඇති බවය.
- අතථ්‍යව ධාරක MOONSHINE කළමනාකරණ අතුරුමුහුණත් කට්ටලයක් සොයාගෙන ඇත. මෙම අතුරුමුහුණත් වලට UPSEC හා සම්බන්ධ පිටිසුම් පැනල් සමඟ අතිච්ඡාදනය වී ඇති යටිතල පහසුකම් තිබෙන අතර, Intelligence Online ට අනුව 'Sichuan Dianke Network Security Technology Co., Ltd.' වෙත යොමු කරයි.

## කළමනාකරණ අතුරුමුහුණත

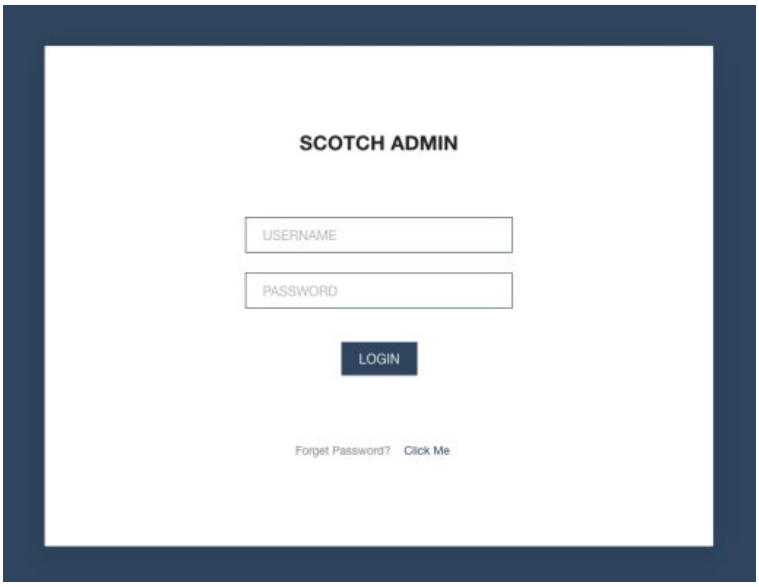
MOONSHINE කළමනාකරණ අතුරුමුහුණත් පිළිබඳ පෙර වාර්තා පෙන්නුම් කරන්නේ එය වෙනස්කම් වලට භාජනය වී ඇති අතර එය අඛණ්ඩව සංවර්ධනය වන බවය.

කළමනාකරණ අතුරුමුහුණත පිළිබඳ පළමු උදාහරණය Citizen Lab හි 2019 වාර්තාකරණයෙන් සොයාගත හැකිය.



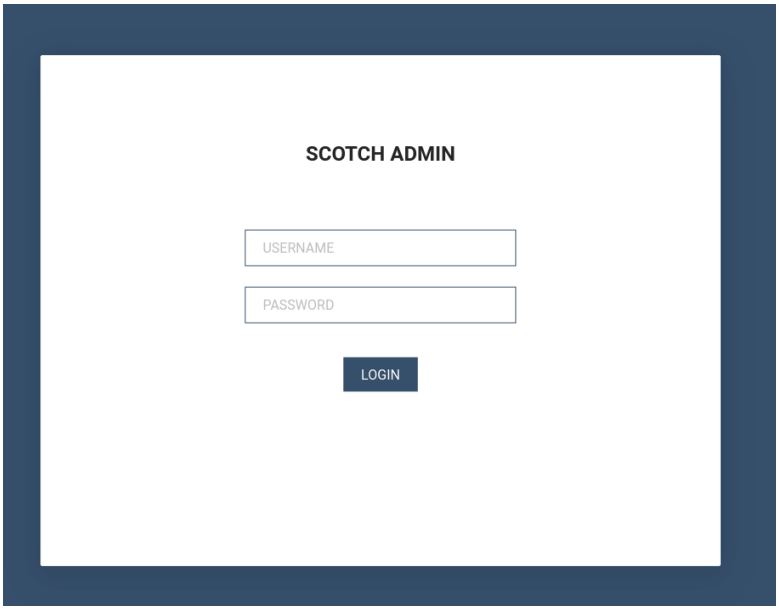

*රූපසටහන 1: 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.යන Citizen Lab's 2019 වාර්තාවේ දක්නට ලැබෙන MOONSHINE කළමනාකරණ අතුරුමුහුණත්.*

2022 මුල් භාගයේදී, Lookout විසින් පහත දැක්වෙන පරිදි නැවත සැලසුම් කරන ලද වෙනස් කළමනාකරණ අතුරුමුහුණතක් වාර්තා කරන ලදී (1 වැනි රූපසටහනේ ඇති පෙර අතුරුමුහුණත් ප්‍රතිස්ථාපනය කරමින්):



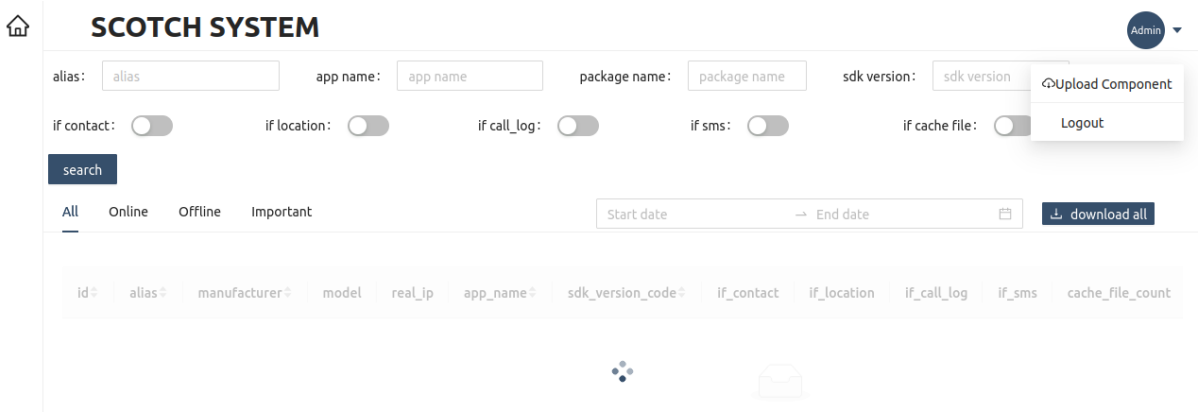

*රූපසටහන2: Lookout හි 2022 වාර්තාවේ දක්නට ලැබෙන MOONSHINE කළමනාකරණ අතුරුමුහුණත 'MOONSHINE: ටිබෙට් ජාතිකයන් සහ උයිගර්වරුන් ඉලක්ක කර ගැනීම සඳහා චීන APT POISON CARP විසින් Android Surveillanceware වර්ධනය කිරීම'.*

2023 අගෝස්තු මාසයේදී, MOONSHINE විධාන සහ පාලන (C2) ස්කෑන් මඟින් 2022 අතුරුමුහුණතට සමාන අතුරුමුහුණතක් අනාවරණය කළ අතර, රූපසටහන 2 අනුව **'මුරපදය අමතක කරන්න'** ක්‍රියාකාරකම තවදුරටත් ලබා ගත නොහැකි බව පැහැදිලිය.




*රූපසටහන 3:* 2023 අගෝස්තු මාසයේදී නිරීක්ෂණය කරන ලද MOONSHINE කළමනාකරණ අතුරුමුහුණතට තවදුරටත් 'මුරපදය අමතක කරන්න' යන විමසුමක් නොමැත.

කළමනාකරණ අතුරුමුහුණත පිළිබඳ වැඩිදුර විමර්ශනයේදී, අවදානමට ලක් වූ උපාංගවල විස්තර ගබඩා කරන ආකාරය හෙළි කරන ලද පැනලය තුළ අන්තර්ගතයක් පෙන්වන ලදී.




*රූපසටහන 4: MOONSHINE කළමනාකරණ අතුරුමුහුණතේ පිවිසුම් පිටුව පිටුපස ඇති වෙබ් පිටුව.*

වින්දින උපාංගයෙන් MOONSHINE C2 සේවාදායකයන් වෙත '**score**' එකක් මාරු කිරීම Lookout පර්යේෂණයෙන් පෙන්නුම් කරන ලදී. 'score' හි වටිනාකම වින්දින උපාංගයේ ඇති අනිෂ්ට සාම්පලයේ අවසරයන් මත පදනම් වේ.

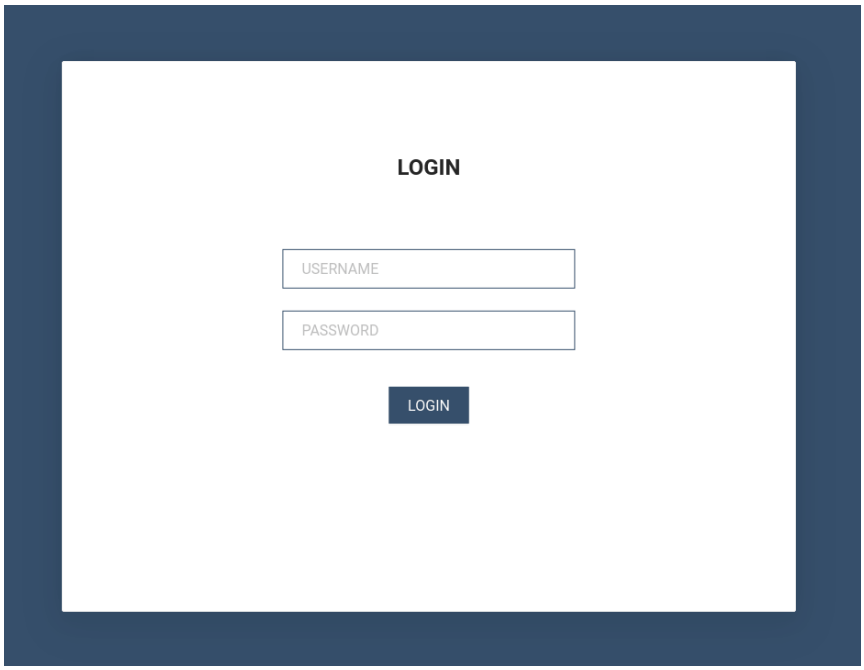
පිටුව තුළ ඇති 'if_contact', 'if_location', 'if_call_log' සහ 'if_sms' තීරු වලින් ඇඟවෙන්නේ සියලුම MOONSHINE සාම්පලවලට අවදානමට ලක් වූ උපාංග වෙත පූර්ණ ප්‍රවේශය නොමැති බවයි. මෙම තීරු සහ උපාංගයෙන් C2 වෙත ලබා දී ඇති 'score' පිළිබඳ දැනුමෙන් පෙනී යන්නේ තර්ජනාත්මක ක්‍රියාකාරීන් කළමනාකරණ අතුරුමුහුණතට ප්‍රවේශ වන පුද්ගලයින්ට අනිෂ්ට මෘදුකාංගයට ඇති ප්‍රවේශ මට්ටම සන්නිවේදනය කිරීමට score භාවිතා කරන බවයි.

සාමාන්‍යයෙන්, උපාංගවලින් තොරතුරු රැස් කරන යෙදුම් වැළැක්වීම සඳහා හොඳම ප්‍රායෝගික උපදෙස වන්නේ බාගත කිරීමට පෙර අසාමාන්‍ය ඕනෑම දෙයක් සඳහා යෙදුම් අවසරයන් පරීක්ෂා කිරීමයි. කෙසේ වෙතත්, MOONSHINE සාම්පල යෙදුමේ ක්‍රියාකාරීත්වයට අදාළ අවසර සොයන බැවින්, සැක සහිත බවක් පෙනෙන්නට තිබුණත්, ඒවා උපාංගවලින් තොරතුරු රැස් කිරීමට ද මෙම අවසර භාවිතා කරයි.

MOONSHINE සතුව ඇති Application Programming Interface (API) මගින් එහි අතුරුමුහුණත් හැකියාවේ පුළුල් බව හෙළිදරව් කරයි. API ලේඛනවල මුල් අනුවාදවල API නම් මැන්ඩරින් භාෂාවෙන් අඩංගු විය.

MOONSHINE පැනල් සඳහා වූ සෙවීම් වලදී, අනථ්‍යව සත්කාරක අවස්ථා සොයා ගන්නා ලදී. අනථ්‍ය සත්කාරකත්වය යනු එක් IP ලිපිනයකට එකවර වෙබ් අඩවි කිහිපයක් වෙත ධාරක සැපයීමට ඇති හැකියාවය. මෙම අනථ්‍ය ලෙස ධාරකත්වය දක්වන ලද අවස්ථා සහ වසම්වල IP ලිපිනයන් දැනහඳුනන කිසිදු අනිෂ්ට මෘදුකාංග සාම්පලයක නිරීක්ෂණය නොවීය.

කළමනාකරණ අතුරුමුහුණතේ මෙම අවස්ථා වෙනස් විය. ඒ මන්ද යත් පිටු වල නාමය කලින් දුටු **'SCOTCH ADMIN'** වෙනුවට '**LOGIN**' වූ බැවිනි.




*රූපසටහන 5: SCOTCH ADMIN වෙනුවට LOGIN නාමය භාවිතා කරන MOONSHINE කළමනාකරණ අතුරුමුහුණත.*

ඊට අමතරව, 6 වැනි රූපසටහනේ පෙන්නුම් කරන පරිදි, පැනලයේ අන්තර්ගතය 4 වැනි රූපසටහනට වඩා වෙනස් වේ.


*රූපසටහන 6: අනථ්‍යව ධාරකත්වය දරන MOONSHINE කළමනාකරණ අතුරුමුහුණතේ පිවිසුම් පිටුව පිටුපස ඇති වෙබ් පිටුව.*

6 වැනි රූපසටහනේ පෙන්නුම් කරන පැනලය 4 වැනි රූපසටහනේ පැනලයේ ඉවත් කරන ලද අනුවාදයක් ලෙස පෙනේ. පැනල්වල අතිච්ඡාදනය වන ලක්ෂණ වන්නේ වගුවේ 'id', 'නිෂ්පාදකයා' සහ 'ආකෘතිය' යන තීරු නම් වේ.

සොයාගත් ප්‍රායෝගිකව ධාරකත්වය දරන MOONSHINE අවස්ථා වූයේ:

| වසම | IP ලිපිනය |
|---|---|
| **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 |

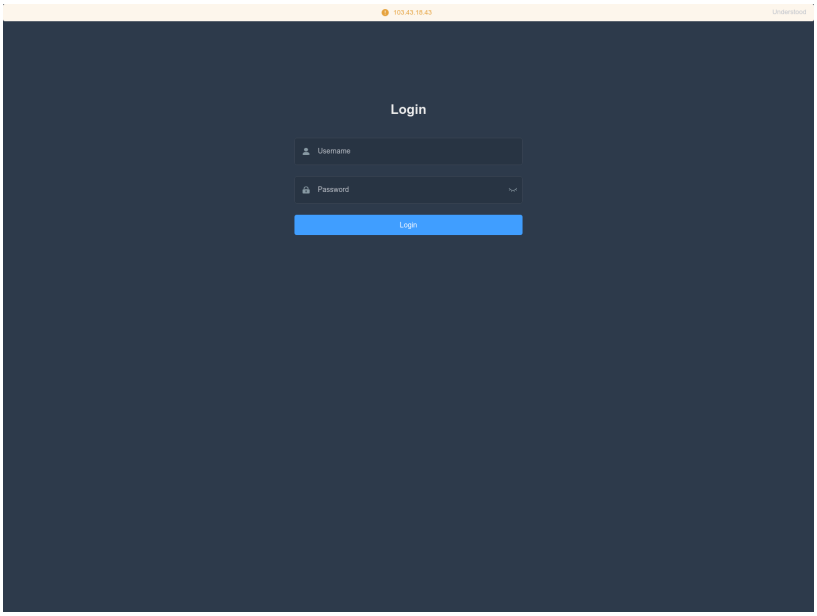
මෙම වසම් Trend Micro විසින් MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටල ලෙස ලැයිස්තුගත කර ඇති අතර, ජංගම උපාංගවලට අනිෂ්ට මෘදුකාංග ස්ථාපනය කිරීම සඳහා බුවුසර අවදානම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීම ගැන වගකිව යුතුය. Trend Micro මෙම අනිෂ්ට මෘදුකාංගය 'Dark Nimbus' ලෙස නම් කරයි.

පැහැදිලි කිරීම සඳහා, MOONSHINE කළමනාකරණ අතුරුමුහුණත් යනු MOONSHINE අනිෂ්ට මෘදුකාංග සාම්පල සමඟ සන්නිවේදනය සඳහා යොදා ගන්නා සහ වින්දින දත්ත බැහැර කරනු ලබන ඒවාය. Trend Micro විසින් වාර්තා කරන ලද MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටල යනු ජංගම උපාංගවල Dark Nimbus නම් අනිෂ්ට මෘදුකාංගයක් ස්ථාපනය කිරීම සඳහා බ්‍රවුසර් අවදානම් අයුතු ලෙස ප්‍රයෙජනයට ගන්නා වෙනම හැකියාවකි. තවද, Dark Nimbus සහ MOONSHINE සම්පූර්ණයෙන්ම වෙනස් අනිෂ්ට මෘදුකාංග වේ.

MOONSHINE කළමනාකරණ අතුරුමුහුණත සහ MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටලය යන දෙකේම කේත අනිච්ඡාදනය වන බැවින්, රූපසටහන් 3 සහ 5 හි මෙන්ම රූපසටහන් 4 සහ 6 හි අන්තර්ගත පිටුවේ සමාන පිවිසුම් විමසීම් ඇත. ඒ දෙකෙහිම මූලාශ්‍ර කේතයේ 'webpackJsonpreact-scotchui' යන රැහැන අඩංගු වේ.

තර්ජනාත්මක ක්‍රියාකාරීන් විසින් MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටලයට සම්බන්ධ වූ URL සබැඳි ජනනය කර, පසුව ටිබෙට් සහ උයිගර්වරුන්ට අදාළ වීඩියෝ වෙත හරවා යවන අතර, එය MOONSHINE ඉලක්ක කිරීම සමඟ අනිච්ඡාදනය වේ.

MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටල වසමට ධාරකත්වය සපයන බොහෝ IP ලිපින හරහා, 444 දොරටුවේ 'VLiteUI' නමින් පිවිසුම් පිටුවක් ඇත. මෙම පිටුව පුළුල් ලෙස නිරීක්ෂණය නොවන අතර මෙම IP ලිපිනවල පැවැත්ම ක්‍රියාකාරීන්ගේ මෙහෙයුම් සඳහා විය හැකි සබැඳියක් පෙන්නුම් කරයි.




*රූපසටහන 7: MOONSHINE අයුතු ප්‍රයෝජන ගන්නා කට්ටලයට ධාරකත්වය දරන IP ලිපින වල නිරීක්ෂණය කරන ලද 'VLiteUI' HTML නාමය සහිත පිවිසුම් පැනලය.*

Trend Micro හි Dark Nimbus පිළිබඳ විශ්ලේෂණයෙන් හෙළි වූයේ අනිෂ්ට මෘදුකාංගයට උපාංගයේ සම්පූර්ණ තොරතුරු ලැයිස්තුවක් රැස් කළ හැකි බවත්, එය XMPP ප්‍රොටෝකෝලය භාවිතයෙන් C2 සමඟ සන්නිවේදනය කරන බවත්ය.

Nimbus හි සමහර අනුවාදවල, 'DKNS' රැහැනේ පැවැත්ම හඳුනාගෙන ඇති බව Trend Micro ගෙනහැර දක්වයි.

DKNS නාමය සහිත වෙබ් පිටු වෙනුවෙන් සේවය කරන අනෙකුත් IP ලිපින සඳහා XMPP සේවාවන් තුළද **'ansec\[.]com'** (TrendMicro විසින් Dark Nimbus C2 ලෙස ලැයිස්තුගත කර ඇත) නිරීක්ෂණය විය:

- DKNS Android远程取证系统 (DKNS Android Remote Forensic System)
- DKNS云网侦控平台 (DKNS Cloud Network Investigation and Control Platform)
- DKNS 云网侦控平台 (DKNS Cloud Network Investigation and Control Platform)
- DKNS远程控制侦查系统 (DKNS Remote Control Investigation System)

XMPP සේවාවේ **'ansec\[.]com'** සහිත තවත් IP ලිපින කට්ටලයක නාමය සහිත වෙබ් පිටු නිබුණි:

- UPSEC互联网控制指挥系统 (UPSEC Internet Control Command System)
- UPSEC无线侦控系统 (UPSEC Wireless Surveillance and Control System)
- UPSEC重点人数据还原系统 (UPSEC Key Person Data Restoration System)

Intelligence Online ට අනුව, HTML පිටුවල නාමයන්ගෙන් නිරීක්ෂණය කරන ලද 'UPSEC', 'Sichuan Dianke Network Security Technology Co., Ltd' වෙත යොමු කර ඇත

# දෙවැනි ප්‍රත්‍යක අධ්‍යයනය: BADBAZAAR

BADBAZAAR යනු උයිගර්, ටිබෙට් සහ තායිවාන පුද්ගලයින් ඉලක්ක කරගත් iOS සහ Android ප්‍රභේද සහිත ජංගම අනිෂ්ට මෘදුකාංගයකි. මෙම ඔත්තු මෘදුකාංගය සමාජ මාධ්‍ය වේදිකා සහ නිල යෙදුම් ගබඩා ඔස්සේ පතුරවනු ලැබේ. Volexity වෙතින් මෑතකදී කළ වාර්තාකරණයේ BADBAZAAR හි විවිධ ප්‍රභේද පෙන්වන අතර, ඒවා BadSolar, BADBAZAAR සහ BadSignal ලෙස වෙන් කර ඇත. උපාංග සහ ක්‍රියාකරුගේ තොරතුරු රැස් කිරීමට භාවිතා කරන අනිච්ඡාදනය වන කාර්යයන් මගින් ප්‍රභේද තුනම එකට සම්බන්ධ කර ඇත.

BADBAZAAR පිළිබඳ NCSC පර්යේෂණයෙන් පහත සඳහන් කරුණු අනාවරණය විය:

- C2 වසම් පොකුරු කිරීම මගින් historical threat intelligence හි වාර්තා කර ඇති වසම්වල වැඩිදුර සම්බන්ධතා හෙළි කරයි.
- C2 සේවාදායකයන් සහ අනිෂ්ට මෘදුකාංග සාම්පල ක්‍රියාකාර යටිතල පහසුකම් සමඟ සම්බන්ධ ධාරක නාම හෙළි කරයි.
- නිල යෙදුම් ගබඩාවලින් ඔබ්බට ඔවුන්ගේ අනිෂ්ට මෘදුකාංග ව්‍යාප්ත කිරීම සඳහා තර්ජනාත්මක ක්‍රියාකරුවන් විසින් භාවිතා කරන තවත් පැතිකඩ.

## WHOIS පොකුරු කිරීම / වසම් තැරැව්කරු

'UJYJYUJ'

'**signalplus\[.]org**' නැමති BADBAZAAR වසම (ESET විසින් වාර්තා කරන ලද) සඳහා WHOIS සටහන් විශ්ලේෂණය කිරීමේදී **'State'** ක්ෂේත්‍රයේ **'UJYJYUJ'** අගය පෙන්නුම් කරයි.

එකම අගයක් ඇති වෙනත් වසම් සෙවීමක් මගින් පහත උනන්දුවක් දක්වන වසම් හෙළි කරයි:

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

(ඇමුණුම A හි, 1වැනි රූපය බලන්න)

**signalplus\[.]org, tubevideoplus\[.]org** සහ **thetubeplus\[.]com** යන වසම් BADBAZAAR C2 වසම් ලෙස වාර්තා කර ඇති අතර, **mail.pmumail\[.]com** උප වසම FlyGram ප්‍රොක්සි සේවාදායකයක් ලෙස ESET විසින් වාර්තා කරයි. FlyGram යනු ද්වේෂසහගත සයිබර් ක්‍රියාකරුවන් විසින් වර්ධනය කරන ලද BADBAZAAR යෙදුමකි (වෙනත් BADBAZAAR යෙදුම් ලැයිස්තුවක් සඳහා උපග්‍රන්ථය බලන්න).

### යතුරුපුවරු පරිසරණ අගයන්

NCSC විසින් අනෙකුත් ලියාපදිංචි BADBAZAAR C2 වසම් වලද සමාන යතුරුපුවරු පරිසරණ රටාවන් දැක ඇත.

උදාහරණයක් ලෙස, පහත සඳහන් සියලුම වසම්වලට **'State'** ක්ෂේත්‍රයේ නිරීක්ෂණය කරන ලද **'REWR'** අගය ඇත (පෙර භාවිතා කළ පරිදි):

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

(ඇමුණුම A, 2 වැනි රූපසටහන බලන්න)

'FSDF' ඉතා උසස් ක්ෂේත්‍ර අගයන් සහිත වසම්
වෙනත් BADBAZAAR C2 වසම් කට්ටලයක **'State'** අගය **'FSDF'** වන්නේය:

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

(ඇමුණුම A, 3 වැනි රූපසටහන බලන්න)

යතුරුපුවරු පරිසරණ අගයන් සමඟ ඓතිහාසික වාර්තාකරණය
BADBAZAAR වසම් පිළිබඳ WHOIS වාර්තාවල යතුරුපුවරු පරිසරණ අගයන් භාවිතය, TA413 විසින් ඓතිහාසිකව වාර්තා කරන ලද ටිබෙට් සංවිධාන ඉලක්ක කිරීමේදී ද දැකිය හැකිය. ක්‍රියාකරුවන් පාලනය කරන වසම් මගින් ටිබෙට් සංවිධාන වංචා කිරීම සහ "asfasf" හි ලියාපදිංචි සංවිධාන අගයක් භාවිතා කිරීම සිදු කරන බව Recorded Future නිරීක්ෂණය කර ඇත.

clublogs[.]com
Lookout මගින් ලබාගත් BADBAZAAR සාම්පලවල C2 වසම ලෙස **'xle.clublogs[.]com'** අඩංගු විය. **'clublogs[.]com'** මූල වසම **'95.179.210[.]85' IP** ලිපිනයේ ධාරකත්වය දරන ලද අතර එයට **'CN=WIN-50QO3EIRQVP'** විෂය සහ නිකුත් කරන්නාගේ අගය සහිත SSL සහතිකයක් තිබුණි. මෙම අගය BADBAZAAR සාම්පලවල ඇති SSL සහතික සමඟ ගැළපුණු අතර සන්නිවේදනයට බාධා කිරීම වැළැක්වීම සඳහා SSL හිර කිරීමට භාවිතා කළේය.

**95.179.210[.]85 IP** ලිපිනය සඳහා ධරකත්ව ඉතිහාසය පහත සඳහන් උනන්දුවක් දක්වන වසම් ආපසු ලබා දෙයි:

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

(ඇමුණුම A, 4 වැනි රූපසටහන බලන්න)

www.voiceoftibet[.]net

**‘ww.voiceoftibet\[.]net’** වසම, TA413 විසින් TTP භාවිතා කරන ආකාරයට සමානව, ‘Voice of Tibet’ ගුවන් විදුලි මධ්‍යස්ථානය ලෙස බොරු වේශයෙන් පෙනී සිටින බව පෙනේ.

**‘rewrwer[.]com’** වසම, BADBAZAAR වසම් පිළිබඳ WHOIS වාර්තාවල සොයාගන්න ලද කලින් හඳුනාගත් **‘State’** අගය **‘REWR’** ට සමාන වේ.

**‘clublogs[.]com’**, **‘rewrwer[.]com’**, **‘voiceoftibet[.]net’** සහ **‘myloughborough[.]com’** යන වසම් සියල්ලම **‘tplutalova@list[.]ru’** ඊමේල් ලිපිනයෙන් ලියාපදිංචි කර ඇත.

actuallys[.]com

**‘actuallys\[.]com’** සඳහා WHOIS වාර්තා තාක්ෂණික සහ පරිපාලක විද්‍යුත් තැපැල් ලිපින **‘tplutalova@list\[.]ru’** වූ නමුත් ලියාපදිංචිකරුගේ විද්‍යුත් තැපෑල **‘ivan_s81@mail\[.]ru’** වූ අවස්ථාවක් පෙන්නුම් කළේය.

**‘actuallys\[.]com’** වසම සඳහා ඓතිහාසික WHOIS තොරතුරු **‘wangminghua6@gmail\[.]com’** ලියාපදිංචි විද්‍යුත් තැපෑල 2016 පෙබරවාරි 24 වන දින ලැයිස්තුගත කර ඇති බව හෙළි කළේය. 2016 මාර්තු 11 වන දින, විද්‍යුත් තැපෑල පසුව **‘ivan_s81@mail.ru’** ලෙස වෙනස් කරන ලද නමුත් රෙජිස්ට්‍රාර් ලියාපදිංචි කිරීමේ කල් ඉකුත්වන දිනය එලෙසම පැවතුනි.

wangminghua6@gmail[.]com

ඓතිහාසික තර්ජනාත්මක බුද්ධි වාර්තාකරණයේදී සොයාගත් වසම් ලියාපදිංචි කිරීම සඳහා **‘wangminghua6@gmail\[.]com’** යන විද්‍යුත් තැපැල් ලිපිනය භාවිතා කරන ලදී. 2015 දී, Palo Alto (පැලෝ ඇල්ටෝ) විසින් Cmstar නම් අනිෂ්ට මෘදුකාංගය සඳහා C2 වසම් ලියාපදිංචි කිරීමට භාවිතා කරන විද්‍යුත් තැපෑල හඳුනා ගත්තේය. 2014 දී, APT3 විසින් සිදුකරන ලද වංචනිකව යවන සන්නිවේදනයන් මගින් Mandant විසින් හඳුනාගත් වසම් ලියාපදිංචි කිරීමට ද එය භාවිතා කරන ලදී. 2013 දී, චීන අක්ෂර අඩංගු Program Database (PDB) දත්ත සමුදායක් සහිත අනිෂ්ට මෘදුකාංග ඩ්‍රොපර් එකක CrowdStrike විසින් සොයාගත් වසම් ලියාපදිංචි කිරීමට එය භාවිතා කරන ලදී. මෙය චීන පද්ධතියකින් සම්පාදනය කල එකක් බව යෝජනා කෙරේ.

taoyujun@gmail[.]com

**‘hcjbtt\[.]com’** වසම **‘taoyujun@gmail\[.]com’** විද්‍යුත් තැපැල් ලිපිනයෙන් ලියාපදිංචි කර ඇති නමුත්, එහි පරිපාලක විද්‍යුත් තැපැල් ලිපිනය **‘wangminghua6@gmail\[.]com’** වෙතින් ලියාපදිංචි කර ඇත.

**‘hcjbtt\[.]com’** වසමට සම්බන්ධ කිසිදු ද්වේෂසහගත ක්‍රියාකාරකමක් නොමැත. කෙසේ වෙතත් **‘taoyujun@gmail\[.]com’** විද්‍යුත් තැපැල් ලිපිනය ඓතිහාසිකව තර්ජනාත්මක බුද්ධි වාර්තාවල දක්නට ලැබුණි. 2014 දී, ජපන් සංවිධාන ඉලක්ක කර ගැනීම සඳහා භාවිතා කරන ලද **‘Cueisfry Trojan’** සාම්පලවල, Mandiant විසින් සොයා ගන්නා ලද වසමක් ලියාපදිංචි කිරීමට එය භාවිතා කරන ලදී.

මෙම විද්‍යුත් තැපැල් ලිපිනය ‘iaea-international\[.]org’ වැනි වසම් ද ලියාපදිංචි කර ඇත. එය **International Atomic Energy Agency** සහ ‘**idc-ctbto[.]org**’ලෙස බොරු වෙබ්අඩවි පෙනී සිටිමින් **Comprehensive Nuclear-Test-Ban Treaty Organisation** හි **International Data Centre (CTBTO).** ලෙස බොරු වෙබ්අඩවි පෙනී සිට ඇත.

‘**iaea-international[.]org**’ වසම සඳහා පෙර සටහනකින් පෙන්නුම් කළේ ‘**wangminghua6@gmail[.]com**’. ලියාපදිංචි විද්‍යුත් තැපැල් ලිපිනය බවය.

## udtglobals[.]com

**‘wangminghua6@gmail\[.]com’** යන වසම පරිපාලක විද්‍යුත් තැපැල් ලිපිනය ලෙසත් **‘ocean.nio@rediffmail\[.]com’** ලියාපදිංචි විද්‍යුත් තැපැල් ලිපිනය ලෙසත් භාවිතා කරමින් **‘udtglobals\[.]com’** යන වසම නිරීක්ෂණය කරන ලදී. මෙම වසම සඳහා වන අනෙකුත් WHOIS සටහන්, එකම ලියාපදිංචි විද්‍යුත් තැපැල් ලිපිනය නමුත් **‘taoyujun@gmail\[.]com’** යන පරිපාලක විද්‍යුත් තැපැල් ලිපිනය පෙන්නුම් කළේය.

මුහුදු යට ආරක්ෂක සහ ආරක්ෂක සමාගම් සඳහා ගෝලීය ඉසව්වකදී **‘UDT Global’** ලෙස **‘udtglobals\[.]com’** බොරු වේශයක් ගත් බව පෙනෙන්නට තිබුණි. විද්‍යුත් තැපැල් ලිපිනය තුළ ඇති **‘ocean.nio’** යන පරිශීලක නාමය රටවල් ගණනාවක් සම්බන්ධිත **National Institute of Oceanography (NIO)** ආයතනය අනුකරණය කිරීමක් විය හැකිය. **‘Rediff’** විද්‍යුත් තැපැල් සේවාව (ඉන්දියාව පාදක කරගත්) භාවිතා කිරීම **Indian National Institute of Oceanography** (ඉන්දියානු ජාතික සාගර විද්‍යා ආයතනයේ) අනුකරණයක් යෝජනා කළ හැකිය.

## Djibdiplomatie[.]com

**‘djibdiplomatie\[.]com’** වසම ජිබුටි රාජ්‍ය තාන්ත්‍රික සේවා ලෙස බොරු වෙබ්අඩවි පෙනී සිටි අතර, එයට **‘utdglobals\[.]com’** හා සමාන WHOIS වාර්තාවක් තිබුණි. එක් වාර්තාවක ලියාපදිංචිකරු **‘ocean.nio@rediffmail\[.]com’** ලෙස සහ පරිපාලක **‘taoyujun@gmail\[.]com’** ලෙස පෙන්නුම් කරන ලද අතර, අනෙකුත් වාර්තාවල **‘wangminghua6@gmail\[.]com’** පරිපාලක විද්‍යුත් තැපැල් ලිපිනය ලෙස සහ **‘ocean.nio@rediffmail\[.]com’** ලියාපදිංචිකරුගේ විද්‍යුත් තැපැල් ලිපිනය ලෙස පෙන්වන ලදී.

මෙම වසම් දෙකෙහිම WHOIS වාර්තාවල යතුරුපුවරු පරිසරණ වර්ගයේ අගයන් ද තිබුණි. උදාහරණයක් ලෙස, **‘udtglobals[.]com’** හි එහි ලියාපදිංචි නගරය ලෙස **‘ASDF’** අගය ඇති අතර, **‘djibdiplomatie[.]com’** හි ලියාපදිංචි නාම අගය ලෙස **‘DAF DAGF’** ඇත. මෙය අනෙකුත් BADBAZAAR වසම්වල නිරීක්ෂණය කරන ලද අගයන් හා සැසඳිය හැකිය.

**‘wangminghua6@gmail\[.]com’** සහ ‘taoyujun@gmail\[.]com’ යන විද්‍යුත් තැපැල් ලිපින, **global undersea defence event**, **Djibouti diplomacy services** සහ **International Atomic Energy Agency** ලෙස බොරු වෙසින් පෙනී සිටින වසම් බව WHOIS වාර්තාවල දක්නට ලැබුණද, ඒවා බොහෝ ද්වේෂ සහගත නොවන වසම් බවට වන WHOIS වාර්තා ද ඇත.

බොරු වෙසින් පෙනී සිටින වසම් සහ ද්වේෂසහගත නොවන වසම් මිශ්‍රණය මගින් ද්වේෂ සහගත සයිබර් ක්‍රියාකාරීන්ගේ මෙහෙයුම් සඳහා සහාය වීමට භාවිතා කරන යටිතල පහසුකම්-ප්‍රසම්පාදන ආයතනයක පැවැත්ම පිළිබඳ යෝජනා කෙරේ.

**‘ocean.nio@rediffmail\[.]com’** යන විද්‍යුත් තැපැල් ලිපිනය ඉහත විස්තර කළ බොරු වෙසින් පෙනී සිටින වසම්වල පමණක් දක්නට ලැබේ. **‘ivan_s81@mail\[.]ru’** සහ **‘tplutalova@list\[.]ru’** පිළිවෙලින් ඉතා කුඩා වසම් සංඛ්‍යාවක් ලියාපදිංචි කර ඇති අතර, මෙම වසම්වලින් සමහරක් BADBAZAAR යටිතල පහසුකම් මත ධාරකත්වය ලබා දී ඇත. මෙම විද්‍යුත් තැපැල් ලිපින තුන ද්වේශසහගත සයිබර් ක්‍රියාකාරීන්ගේ මෙහෙයුම් සමඟ වඩාත් සමීපව සම්බන්ධ වී ඇති බව විශ්වාස කෙරේ. එයට හේතු වන්නේ ඔවුන් සම්බන්ධ වී ඇති වසම් වැඩි සංඛ්‍යාවක් **‘wangminghua6@gmail\[.]com’** සහ **‘taoyujun@gmail\[.]com’** යන විද්‍යුත් තැපැල් හා සසඳන විට ද්වේශසහගත ක්‍රියාකාරකම් සමඟ සම්බන්ධ වී ඇති බැවිනි.

(ඇමුණුම A, 5 වැනි රූපහටහන බලන්න)

### අනෙකුත් තර්ජනාත්මක ක්‍රියාකාරීන් සමඟ සම්බන්ධතා

BADBAZAAR-සම්බන්ධිත වසම් වන ‘**actuallys[.]com**’, ‘**clublogs[.]com**’, ‘**myloughborough[.]com**’, ‘**rewrwer[.]com**’, සහ ‘**voiceoftibet[.]net**’ හි තවත් පොදු ලක්ෂණයක් වන්නේ ඒවා සියල්ලම eNom හි ලියාපදිංචි කර ඇති අතර **‘255.255.255[.]254’** හි ‘ගාල් කර’ තිබීමය.

කලින් සිදුකළ NCSC විමර්ශනවලින් පසුව, මෙම ලක්ෂණ සහිත අනෙකුත් වසම්වල 2019 දී **APT5** සහ 2009 සහ 2011 අතර **APT14** හා සම්බන්ධ ක්‍රියාකාරකම් අනාවරණය විය.

APT5 සම්බන්ධිත වසම්ව සතුව ලියාපදිංචි විද්‍යුත් තැපැල් ලිපිනය ලෙස **‘taoyujun@gmail\[.]com’** ලැයිස්තුගත කර ඇති ඓතිහාසික WHOIS වාර්තා තිබුණි.

APT14-සම්බන්ධිත වසම්වල ඔවුන්ගේ ද්වේෂසහගත මෙහෙයුම්වල අපේක්ෂිත ඉලක්කය නියෝජනය කරන බව පැන්නුම් කරන අකුරු තුනක උපවසම් තිබුණි. ‘**bae.cisconline[.]net**’ මේ සඳහා උදාහරණයක් වන අතර එය BAE පද්ධතිය අපේක්ෂිතව ඉලක්ක කර ගැනීම යෝජනා කළ අතර එය ‘**Poison Ivy**’ සාම්පලයක් තුළින් හමු විය.

BADBAZAAR වසම්වල ද සමාන ලක්ෂණයක් නිරීක්ෂණය කෙරෙන අතර එහි උපවසම් ට්‍රෝජනීස් කරන ලද යෙදුමේ නමට සම්බන්ධ වේ:

| යෙදුමේ නාමය | 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 සහ APT14 සම්බන්ධ ක්‍රියාකාරකම් ඓතිහාසික වූ අතර eNom හි ලියාපදිංචි වී **‘255.255.255.254’** ලෙස විභේදනය වූ වෙනත් වසම් ද ඇති බව සැලකිල්ලට ගැනීම වැදගත්ය. ඒවා ද්වේෂසහගත ක්‍රියාකාරකම් සමඟ සම්බන්ධ කළ නොහැක. එබැවින් මෙම සංවිධානාත්මක මෙහෙයුම පිටුපස සිටින ක්‍රියාකාරීන් එකම හෝ සම්බන්ධ පුද්ගලයන් දැයි නිශ්චිත නැත.

## යන්ත්‍ර නාම

BADBAZAAR C2s සහ සාම්පල විශ්ලේෂණය කිරීමෙන් SSL සහතිකවල ‘පොදු නාම’ අගය ලෙස භාවිතා කරන ලද ධාරක නාමයන් අනාවරණය විය. BADBAZAAR සාම්පල සහ යටිතල පහසුකම් වෙතින් නිරීක්ෂණය කරන ලද ධාරක නාමයන් පිළිබඳ NCSC විමර්ශන මගින් පෙන්නුම් කළේ මෙම ධාරක නාමයන් බහු IP ලිපින හරහා භාවිතා වන බවය. මෙම IP ලිපින BADBAZAAR සාම්පලවල තිබෙන ධාරක වසම් වේ. පහත කොටසේ ධාරක නාම, සහ BADBAZAAR C2 වසම්වලට ධාරකත්වය සපයන ධාරක නාමය සහිත IP ලිපින පිළිබඳ වැඩි විස්තර ඇත.

සෑම අවස්ථාවකදීම පාහේ, ධාරක නාම අගය සහිත සහතිකයන් නිශ්චිත ද්වේෂසහගත වසම් නාම සඳහා IP විභේදන සමඟ අනිච්ඡාදනය වේ. මෙය එසේ නොවූ අවස්ථා කිහිපයක් ද දක්වා ඇත.

### WIN-EU0VLBL7TUJ

පහත සඳහන් උනන්දුවක් දක්වන IP ලිපිනයන් තුළ **‘WIN-EU0VLBL7TUJ’** ධාරක නාමය නිරීක්ෂණය කරන ලදී:

- ‘**116.203.53[.]21**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**uyapkfinder[.]com**’ සහ ‘**thewestuniverse[.]com**’.
- **‘95.216.169[.]27’** ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් **‘adysfunction[.]com’** සහ උප-වසම් **‘download.apkbazar[.]biz’** නිරීක්ෂණය කරන ලද්දේ BADBAZAAR සාම්පලයක් සඳහා බාගත කිරීමේ සබැඳියක් ලෙසය.

WIN-70E59JVOB9G

**‘WIN-70E59JVOB9G’** ධාරක නාමය පහත උනන්දුවක් දක්වන IP ලිපිනවල නිරීක්ෂණය කරන ලදී:

- ‘**23.88.28\[.]220**’ ධාරකත්වය දරන BADBAZAAR C2 උප-වසම්, **‘aua.rondwsign\[.]com’, ‘nal.tokenmajorp\[.]com’, ‘pep.rondwsign\[.]com’** ‘**doa.rondwsign\[.]com**’, සහ **‘pls.rondwsign\[.]com’.** යන්ත්‍රය සහිත සහනිකය අවසන් වරට දැකීම සහ අනිෂ්ට වසම් ප්‍රථම වරට IP ලිපිනයට විභේදනය වන ආකාරය දැකීම අතර කාලපරිච්ඡේදය දින දෙකක්විය

- ‘**23.88.28[.]221**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම ‘**tubevideoplus[.]org**’ and ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම ‘**bat.androidupdated[.]net**’. එය ‘**apps.androidupdated[.]net**’ උප-වසමට ද ධාරකත්වය සපයන අතර DoubleAgent C2 අනිෂ්ට මෘදුකාංගයක් වේ.

- ‘**65.21.92[.]77**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ සහ ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**upd.whoscaller.net**’. සහ ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131\[.]15**’ ධාරාකත්වය සපයන BADBAZAAR C2 උප-වසම් **‘bvn.lookincategory\[.]com’** and **‘edr.lookincategory\[.]com’.** යන්ත්‍ර නාමය සහිත සහනිකය අවසන් වරට දැකීම සහ අනිෂ්ට වසම් මුලින්ම IP වෙත විභේදනය වන ආකාරය දැකීම අතර කාලපරිච්ඡේදය දින එකොළහක්විය.

- **‘142.132.131\[.]20’** ධාරකත්වය සපයන උප-වසම්, **‘son.onlinegamersgroup\[.]com’** සහ **‘system.onlinegamersgroup\[.]com’**, BADBAZAAR C2s ලෙස විශ්වාස කෙරේ. BADBAZAAR ආශ්‍රිත SSL සහනික IP හි නිරීක්ෂණය කරන අතරතුර ඒවාට ධාරාකත්වය සපයන ලදී.

- ‘**142.132.131[.]28’** ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**goldplusapp[.]net**’ සහ උපවසම් ‘**who.goldplusapp[.]net**’ and ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, සහ

- ‘**162.55.103[.]212**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** සහ **‘aua.rondwsign[.]com’.**

- ‘**195.154.47[.]99**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**ggl.whoscaller[.]net**’ සහ ‘**upd.whoscaller.net**’. යන්ත්‍ර නාමය සහිත සහතිකය අවසන් වරට දැකීම සහ අනිෂ්ට වසම් මුලින්ම IP වෙත විභේදනය වන ආකාරය දැකීම අතර කාලපරිච්ඡේදය දින තුනක් විය.

- ‘**195.154.60[.]3**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**upd.whoscaller[.]net**’ ‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ සහ ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ සහ ‘**bvn.lookincategory[.]com**’.

(ඇමුණුම් A, 7 වැනි රූපය බලන්න)

WIN-50QO3EIRQVP

‘**WIN-50QO3EIRQVP**’ ධාරක නාමය උනන්දුවක් දක්වන පහත IP ලිපිනයේ නිරීක්ෂනය් කරන ලදී:

- ‘**45.76.132[.]91**’ ධාරාකත්වය සපයන වසම්, ‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. උපවසම් ලෙස BADBAZAAR හා සම්බන්ධිත වසම් දෙකම, එනම් ‘**fow.yumoftion[.]com**’ සහ ‘**bat.androidupdated[.]net**’, BADBAZAAR C2 වසම් වේ. ඊට අමතරව **‘apps.androidupdated[.]net’** උප-වසම DoubleAgent C2 වසමකි. එය WHOIS වාර්තා හරහා BADBAZAAR වෙත සම්බන්ධ කර ඇති **‘pmstwocqn[.]com’** වසමට ද ධාරකත්වය සපයයි.

- **‘95.179.210[.]85’** විසින් **‘clublogs[.]com’** වෙත ධාරකත්වය සපයනු ලබන අතර, BADBAZAAR C2 වසමක් වන **‘xle.clublogs[.]com’** විසින් ද **‘bre.myloughborough[.]com’, ‘img.rewrwer[.]com’, ‘www.voiceoftibet[.]net’** සහ **‘actuallys[.]com’** යන BADBAZAAR හා සම්බන්ධ වසම් වෙත ධාරාකත්වය ලබා දෙයි.

- ‘**199.247.21[.]34**’ විසින් ‘**titeperformance[.]com**’ සහ BADBAZAAR C2 වසම්වල උපවසමක් වන ‘**collinformations[.]com’** වෙත ධාරකත්වය සපයනු ලබයි.

- ‘**217.69.10[.]128**’ ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම, ‘**uyghurdict[.]com**’.

(ඇමුණුම් A, 8 වැනි රූපය බලන්න)

WMSvc-WIN-50QO3EIRQVP

‘**WMSvc-WIN-50QO3EIRQVP**’ ධාරක නාමය උනන්දුවක් දක්වන පහත IP ලිපිනයේ නිරීක්ෂණය කෙරේ:

- **’78.46.185[.]251’** ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම, **‘groupgram[.]org’**. එය Volexity විසින් වාර්තා කරන ලද පරිදි 4432 ද්වාරය භාවිතා කරමින් ද්වේශසහගත සම්බන්ධතාවල යෙදේ.

- **‘65.21.92[.]69’** and **‘163.172.205[.]207’** ධාරකත්වය සපයන වසම, **‘widelygram[.]org’** BADBAZAAR C2 වසමක් ලෙස විශ්වාස කෙරේ. Ips දෙකම මත ධාරාකත්වය සපයන අතර, 4432 ද්වාරය විවෘත විය.

- **‘163.172.198[.]206’** ධාරකත්වය සපයන වසම, **‘maxgram[.]org’** BADBAZAAR C2 වසමක් ලෙස විශ්වාස කෙරේ. Ip ලිපිනයන් දෙකම මත ධාරාකත්වය සපයන අතර, 4432 ද්වාරය විවෘත විය.

(ඇමුණුම් A, 9 වැනි රූපය බලන්න)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

WMSvc-WIN-50QO3EIRQVP’ සහ ‘WIN-7LSBB9R0F1L’ යන ධාරක නාම පහත IP ලිපිනයන්හි එකවර නිරීක්ෂණය විය:

- '**148.251.87[.]245**' ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් '**flygram[.]org**' සහ '**groupgram[.]org**'.

(ඇමුණුම A, 10 වැනි රූපහටහන බලන්න)

WIN-N8H8S9BG2P0
'**WIN-N8H8S9BG2P0**' ධාරක නාමය පහත IP ලිපිනයෙහි නිරීක්ෂණය විය:

- '**148.251.87[.]247**' ධාරකත්වය සපයන BADBAZAAR C2 උප-වසම් '**omarwhatsapp[.]org**' සහ '**flygram[.]org**'.

(ඇමුණුම් A, 11 වැනි රූපය බලන්න)

WIN-I6VBN8MR92A
Hostnames '**WIN-I6VBN8MR92A**' ධාරක නාමය පහත IP ලිපිනයෙහි නිරීක්ෂණය විය:

- '**148.251.87[.]197**' ධාරකත්වය සපයන BADBAZAAR C2 වසම, '**tryhrwserf[.]com**'.

(ඇමුණුම් A, 12 වැනි රූපය බලන්න)

ලබාගත හැකි වාණිජ දත්ත මත පදනම්ව, අන්තර්ජාලය පුරා මෙම යන්ත්‍ර නම්වල ව්‍යාප්තිය වෙනස් වේ. ඒවායින් සමහරක් එකවර බහු IP ලිපින හරහා නිරීක්ෂණය කෙරේ. එයින් පෙන්නුම් කරන්නේ එකම ආකෘතියෙන් VM නිර්මාණය කර ඇති බවයි. ධාරක නාමවලින් සමහරක් මත නිරීක්ෂණය කරන ලද සියලුම IP ලිපින අනිෂ්ට ක්‍රියාකාරකම් සමඟ සම්බන්ධ කළ නොහැකි බව සැලකිල්ලට ගැනීම වැදගත්ය. මෙයින් අදහස් කරන්නේ ධාරක නාම භාවිතය මෙම තර්ජන ක්‍රියාකාරීන්ට පමණක් සීමා නොවන බවයි.

කෙසේ වෙතත්, BADBAZAAR C2 වසම්වලට ධාරකත්වය සපයන IP ලිපින හරහා මෙම යන්ත්‍ර නාම කිහිපයක් පැහිරීම මගින් යෝජනා කළ හැක්කේ, ද්වේෂසහගත ක්‍රියාකාරීන්ගේ සයිබර් මෙහෙයුම් සඳහා සහාය වීම සඳහා යන්ත්‍ර වින්‍යාස කිරීමට යටිතල පහසුකම්-ප්‍රසම්පාදන ආයතනයක් භාවිතා කරන බවය.

## සමාජ මාධ්‍ය පැවැත්ම

Volexity විසින් කලින් වාර්තා කරන ලද YouTube වීඩියෝ (ද්වේෂසහගත යෙදුම් භාවිතය ප්‍රවර්ධනය කරමින්) ද්වේෂසහගත සයිබර් ක්‍රියාකාරීන් විසින් නිර්මාණය කරන ලද බව පෙන්නුම් කළේය. මෙම වීඩියෝ තුළ වර්ධනය කරන ලද යෙදුම් භාවිතා කරන ආකාරය පිළිබඳ නිබන්ධන ඇතුළත් විය.

NCSC විසින් තර්ජනාත්මක ක්‍රියාකාරීන්ගේ මෙහෙයුම් සමඟ සම්බන්ධ අතිරේක YouTube නාලිකා දෙකක් සොයාගෙන ඇත. '@josephjoey3499' URL හැඩලය සහිත YouTube නාලිකාව වන channel මගින් **'Maxgram'** භාවිතය සහ **'@uyghurapks3096'** සමඟ ලියාපදිංචි කර ඇති අතිරේක නාලිකාව **'Uyghur APK Finder'** ප්‍රවර්ධනය කරන බවක් පෙනෙන්නට තිබුණි.

ඊට අමතරව, **'Flygram'** සහ **'Signal Plus'** ප්‍රවර්ධනය කරන YouTube වීඩියෝවල, තර්ජනාත්මක ක්‍රියාකාරීන් විසින් දෘශ්‍යමාන දුරකථන අංක භාවිතා කරන ආකාරය පෙන්වන ලදී. '**Flygram'** වීඩියෝවේ, 0:36 හි **'+1 (570) 378-7250'** දුරකථන අංකය දිස් වූ අතර **'Signal Plus'** වීඩියෝව අතරතුර, **'+1 (267) 298 4259'** දුරකථන අංකය අනාවරණය විය.

Volexity විසින් ව්‍යාජ ටිබෙට් තේමා පුවත් වෙබ් අඩවියක් වන '**ignitetibet\[.]net**' පිළිබඳ වාර්තා කළේය. එය තර්ජනාත්මක ක්‍රියාකාරීන් විසින් ක්‍රියාත්මක කරනු ලබන බවට විශ්වාස කෙරෙන ටෙලිග්‍රෑම් නාලිකාවලින් බව ඔවුහු සොයා ගනීති. **'choekyi.wangmo@ignitetibet\[.]net'** යන විද්‍යුත් තැපැල් ලිපිනය මගින් **'tibetone.org'** පිටුවේ අදහස් දැක්වීම් පළ කරමින් සිටින බව නිරීක්ෂණය විය. එය the iOS variant of BADBAZAAR සඳහා භාවිතා කරන C2 පිටුවක් බව Lookout ප්‍රසිද්ධියේ වාර්තා කළේය.

මෙම විද්‍යුත් තැපැල් ලිපිනය '**Choekyi Wangmo**' ගේ පෞරුෂය භාවිතා කරමින් ක්‍රියාකාරීන් විසින් පාලනය කරනු ලබන බව විශ්වාස කෙරේ.

# ඇගයීම

BADBAZAAR සහ MOONSHINE විශේෂයෙන් උයිගර්, ටිබෙට් සහ තායිවාන ප්‍රජාවන් ඉලක්ක කර ගැනීම සඳහා සමාජ ඉංජිනේරු ක්‍රම කිහිපයක් භාවිතා කරයි. ඒවා නම්:

- උයිගර් භාෂාවෙන් සඳහන් කුරාන් යෙදුමක් වැනි මෙම ප්‍රජාවන් විසින් උනන්දුවක් දක්වන යෙදුම් ට්‍රෝජනීකරණය කිරීම, නිසැකවම ඉලක්කගත වින්දිත පදනමට ගැලපෙන පරිදි සකස් කර ඇත
- මෙම ට්‍රෝජන් කළ යෙදුම් නිල යෙදුම් ගබඩාවලට එකතු කිරීම මගින් ඒවායේ නීත්‍යානුකූලභාවය පිළිබඳ හැඟීමක් ලබා දෙන අතර, කණ්ඩායම් කතාබස් බෙදා ගැනීම තුලින් මෙම ප්‍රජාවන් තුළ විශ්වාසදායක සබඳතා ආයුතු ලෙස ප්‍රයෝජනයට ගැනීමට බොහෝ දුරට අදහස් කෙරේ.

BADBAZAAR සහ MOONSHINE චීන රජයට නිසැකවම වටිනාකමක් ඇති දත්ත රැස් කරයි. BADBAZAAR සහ MOONSHINE උයිගර්, ටිබෙට් සහ තායිවාන පුද්ගලයින්ව නිරීක්ෂණය කර ඉලක්ක කර ගනිමින් සිටින නමුත්, චීනයේ අනෙකුත් සුළුතර කණ්ඩායම් ඉලක්ක කරන වෙනත් අනිෂ්ට මෘදුකාංග තිබේ. පාලන තන්ත්‍රයේ ස්ථාවරත්වයට තර්ජනයක් වන ක්‍රියාවන්ට සහාය දක්වන බව සැලකෙන චීනයේ සහ විදේශ රටවල සිටින පුරවැසියන්, BADBAZAAR සහ MOONSHINE වැනි ජංගම අනිෂ්ට මෘදුකාංග මගින් නිසැකවම තර්ජනයට ලක්ව ඇත. ස්ථානය, ශ්‍රව්‍ය සහ ඡායාරූප දත්ත ග්‍රහණය කර ගැනීමේ හැකියාව, ඉලක්කයේ ක්‍රියාකාරකම් පිළිබඳ තත්‍ය කාලීන තොරතුරු ලබා දීමෙන් අනාගත නිරීක්ෂණය කිරීමේ සහ හිරිහැර කිරීමේ ඉරිමේමෙහෙයුම් දැනුම් දීමට නිසැකවම අවස්ථාව ලබා දෙයි.

# MITRE ATT&CK®

මෙම වාර්තාව MITRE ATT&CK® රාමුවට අදාළව සම්පාදනය කර ඇති අතර, එය සැබෑ ලෝක නිරීක්ෂණ මත පදනම් වූ විරුද්ධවාදී උපක්‍රම සහ ශිල්පීය ක්‍රම පිළිබඳව ගෝලීය වශයෙන් ප්‍රවේශ විය හැකි දැනුම් පදනමකි.

| උපක්‍රම | ID | ශිල්පීය ක්‍රමය | ක්‍රියා පටිපාටිය |
|---|---|---|---|
| **පිරික්සුම** | T1593.001 | Search Open Websites/Domains: සමාජ මාධ්‍ය | අනිෂ්ට මෘදුකාංග බෙදා ගැනීම සඳහා, ක්‍රියාකරුවෝ ඔවුන්ගේ අපේක්ෂිත වින්දිතයින්ට ගැලපෙන මාර්ගගත කණ්ඩායම් සහ සංසද සොයා ගනිති. |
| **සම්පත් සංවර්ධනය** | T1583.001 | යටිතල පහසුකම් ලබා ගැනීම: වසම් | ක්‍රියාකරුවෝ ඔවුන්ගේ විධාන සහ පාලන සේවාදායකයන් සඳහා වසම් ලියාපදිංචි කරති. |
| **සම්පත් සංවර්ධනය** | T1587.001 | හැකියාවන් වර්ධනය කිරීම: අනිෂ්ට මෘදුකාංග | ට්‍රෝජනීකරනය කළ යෙදුම් වලට ඇතුළු කිරීම |
| **සම්පත් සංවර්ධනය** | T1608.001 | හැකියාවන් වේදිකාගත කිරීම: අනිෂ්ට මෘදුකාංග උඩුගත කිරීම | යෙදුම් වෙළඳසැල් ඇතුළු මාර්ගගත වේදිකාවල ට්‍රෝජනීකරණය කරන ලද යෙදුම් උඩුගත කරනු ලැබේ. |
| **සම්පත් සංවර්ධනය** | T1585.001 | ස්ථාපිත ගිණුම්: සමාජ මාධ්‍ය ගිණුම් | අනිෂ්ට මෘදුකාංග බෙදාගැනීම හා ප්‍රචාරණය කිරීම සඳහා, ක්‍රියාකරුවෝ වෙබ් අඩවිවල සහ සමාජ මධ්‍යයේ ගිණුම් නිර්මාණය කරති |
| **සම්පත් සංවර්ධනය** | T1585.002 | ස්ථාපිත ගිණුම්: විද්‍යුත් තැපැල් ලිපින | ක්‍රියාකරුවෝ අනිෂ්ට මෘදුකාංග ධාරකත්වය සහ බෙදාගැනීම සඳහා පුද්ගලිකව ධාරකත්වය සපයන ලද සහ වාණිජ විද්‍යුත් තැපැල් ගිණුම් භාවිතා කරති. |
| **ආරම්භක ප්‍රවේශය** | T1189 | අවදානමට ලක් වූ දේ මගින් මෙහෙයවනු ලබන | අනිෂ්ට අක්ෂර මාලා වෙනත් ආකාරයකින් නීත්‍යානුකූල යෙදුම්වල සඟවා යෙදුම් ගබඩා වෙත උඩුගත කරනු ලැබේ. |
| **ආරම්භක ප්‍රවේශය** | T1566.003 | වංචනිකව යවන සන්නිවේදනයන්: එක් එක් පුද්ගලයන් ඉලක්ක කර සේවාවන් ඔස්සේ වංචනිකව යවන ඊමේල් හා පණිවිඩ | ක්‍රියාකරුවෝ ටෙලිග්‍රෑම් ඇතුළු සමාජ මාධ්‍ය ඔස්සේ ඉලක්කගත කණ්ඩායම් වෙත ට්‍රෝජනීකරණය කරන ලද යෙදුම් යවති |
| **ක්‍රියාත්මක කිරීම** | T1204.002 | පරිශීලිකයන් ක්‍රියාත්මක කිරීම: ද්වේශසහගත ලිපි ගොනුව | ගෙවුම් බර ක්‍රියාත්මක කිරීම සඳහා වින්දිතයින් හට ට්‍රෝජනීකරණය කරන ලද යෙදුම් ස්ථාපනය කිරීමට සිදුවේ |

| | | | |
|---|---|---|---|
| **ආරක්ෂක මගහැරීම** | T1027.009 | අපැහැදිලි ගොනු හෝ තොරතුරු: කාවද්දන ලද ගෙවුම් බර | අනිෂ්ට ගෙවුම් බර වෙනත් නීත්‍යානුකූල යෙදුම් තුළ සගවා ඇත |
| **ආරක්ෂක ආරක්ෂාව මගහැරීම** | T1036.005 | වෙනත් වේශයකින් පෙනී සිටීම: නීත්‍යානුකූල නම හෝ ස්ථානය ගලපන්න | ට්‍රෝජනීස් කරන ලද ගොනු නීත්‍යානුකූල යෙදුම්වල නම, පෙනුම සහ ක්‍රියාකාරිත්වයට ගැලපේ. |
| **ආරක්ෂක ආරක්ෂාව මගහැරීම** | T1656 | වෙන කෙනෙකු ලෙස පෙනී සිටීම | ක්‍රියාකරුවෝ ආවරණ වෙබ් අඩවි නිර්මාණය කරමින් සහ ඉලක්කගත කණ්ඩායම් හා සම්බන්ධ පරිශීලක නාම භාවිතා කරමින් විශ්වාසදායක පුද්ගලයින් ලෙස පෙනී සිටිති |
| **එකතු කිරීම** | T1123 | ශ්‍රව්‍ය ග්‍රහණය | ට්‍රෝජනීකරණය කරන ලද යෙදුම් මයික්‍රෆෝන ප්‍රවේශය ඇතුළු අනවශ්‍ය අවසර ඉල්ලා සිටිය හැකිය |
| **එකතු කිරීම** | T1125 | වීඩියෝ ග්‍රහණය | ට්‍රෝජනීකරණය කරන ලද යෙදුම් කැමරා ප්‍රවේශය ඇතුළු අනවශ්‍ය අවසර ඉල්ලා සිටිය හැකිය |
| **එකතු කිරීම** | T1005 | දේශීය පද්ධතියෙන් දත්ත | ට්‍රෝජනීකරණය කරන ලද යෙදුම් ප්‍රාදේශීය ගොනු ඇතුළු අනවශ්‍ය අවසර ඉල්ලා සිටිය හැකිය |
| **විධාන සහ පාලනය** | T1071.001 | යෙදුම් ස්ථර ප්‍රොටෝකෝලය: වෙබ් ප්‍රොටෝකෝල C2 නාලිකාව හරහා පිටකිරීම HTTPS සහ WebSocket සම්බන්ධතා භාවිතා කරමින් අනිෂ්ට මෘදුකාංග දත්ත පිට කරයි. | HTTPS සහ WebSocket භාවිතා කරමින් අනිෂ්ට මෘදුකාංග C2 වෙත සම්බන්ධ වේ. |
| **විධාන සහ පාලනය** | T1509 | අසම්මත ද්වාරය | ද්වාර 4432 සහ 2333 වැනි අසම්මත ද්වාරයන් භාවිතා කෙරේ |
| **තොරතුරු පද්ධතියකින් අනවසරයෙන් තොරතුරු මාරු කිරීම** | T1041 | C2 නාලිකාව හරහා පද්ධතියකින් අනවසරයෙන් තොරතුරු මාරු කිරීම | HTTPS සහ WebSocket සම්බන්ධතා භාවිතයෙන් අනිෂ්ට මෘදුකාංග මගින් පද්ධතියකින් දත්ත අනවසරයෙන් මරු කරයි. |
| **බලපෑම** | T1565.002 | වාසිය පිණිස දත්ත හැසිරවීම: සම්ප්‍රේෂණය කරන ලද දත්ත වාසිය පිණිස හැසිරවීම | යෙදුම් ක්‍රියාකාරිත්වය සඳහා අවශ්‍ය නොවන යෙදුම් වෙබ් ගමනාගමනය සක්‍රීය කිරීම හරහා ක්‍රියාකරුවෝ වින්දිතයින්ගෙන් දත්ත ලබා ගනිති |

# දර්ශක

MOONSHINE:

- 2025 අප්‍රේල් 1 වන දින, VLiteUI පැනල් සඳහා වූ සෙවුමකින් පහත සඳහන් දේ ලැබුණි:

| IP ලිපිනය | ද්වාරය | මුලින් දුටුවේ | අවසන් වරට දුටුවේ |
|---|---|---|---|
| **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 |

- 2025 අප්‍රේල් 1 වන දින, SCOTCH ADMIN පැනල් සඳහා වූ සෙවුමකින් පහත සඳහන් දේ ලැබුණි:

| IP ලිපිනය | Port | මුලින් දුටුවේ | අවසන් වරට දුටුවේ |
|---|---|---|---|
| **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 |

- 2024 මාර්තු 14 වන දින, අතථ්‍ය SCOTCH ADMIN පැනල් සඳහා කරන ලද සෙවුමකින් පහත සඳහන් දේ ලැබුණි:

| වසම | IP ලිපිනය |
|---|---|
| **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:

| විස්තරය | BADBAZAAR C2s මත නිරීක්ෂණය කරන ලද SSL සහතිකය. |
|---|---|
| **MD5** | ee6e0fc26e94e5b2e52d57ac035b36ff |
| **SHA-1** | 10f8806c72bf5d56efa41c430e8692d55dd49674 |
| **SHA-256** | 1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7 |

- 2025 අප්‍රේල් 1 වන දින, ඉහත BADBAZAAR සහතිකය සෙවීමේදී පහත සඳහන් දේ ලැබුණි:

| IP ලිපිනය | ද්වාරය | පළමුව දුටු | අවසන් වරට දුටු |
|---|---|---|---|
| **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 |

| විස්තරය | **BADBAZAAR C2s SSL** මත නිරීක්ෂණය කරන ලද **SSL** |
|---|---|
| **MD5** | 46923e10db90bde295960851245f199a |
| **SHA-1** | 87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc |
| **SHA-256** | 72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa |

- 2025 අප්‍රේල් 1 වන දින, ඉහත BADBAZAAR සහනිකය සඳහා කළ සෙවුමකදී පහත සඳහන් දේ ලැබුණි:

| **IP** ලිපිනය | **Port** | **මුලින් දුටුවේ** | **අවසන් වරට දුටු** |
|---|---|---|---|
| **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 වසම්

පහත දැක්වෙන්නේ BADBAZAAR C2 වසම්වල නිරීක්ෂණය කරන ලද අගයන්ට ගැලපෙන අගයන් සහිත WHOIS වාර්තා දැනට හෝ ඓතිහාසිකව අඩංගු වන වසම් පෙන්නුම් කරන වගුවකි.

| WHOIS අගය | වසම් |
|---|---|
| **ලියාපදිංචි පුද්ගලයාගේ ප්‍රාන්තය: UJYJYUJ**<br>**ලියාපදිංචි පුද්ගලයාගේ රට: බොලිවියාව**<br>**Registrar: eNom** | • ntc-mobile[.]com<br>• microtik[.]net<br>• ntc-ftth[.]net<br>• axisupdating[.]com<br>• axisupdate[.]com<br>• telegramrouter[.]org<br>• telegramtor[.]com<br>• fufijxgkg[.]com<br>• jindjjdtc[.]com<br>• tubevideoplus[.]org<br>• thetubeplus[.]com<br>• tbgram[.]org<br>• signalplus[.]org<br>• pmumail[.]com |
| **ලියාපදිංචි පුද්ගලයාගේ ප්‍රාන්තය: REWR**<br>**ලියාපදිංචි පුද්ගලයාගේ රට: CF**<br>**Registrar: eNom** | • yumoftion[.]com<br>• fvbyavgyea[.]com<br>• jkiohreh[.]com<br>• pmstwocqn[.]com<br>• ofsggcccreq[.]com<br>• verifyss[.]com<br>• tooenabled[.]com<br>• suguestions[.]com<br>• searching2[.]com |

| | |
|---|---|
| **ලියාපදිංචි පුද්ගලයාගේ ප්‍රාන්තය: FSDF**<br>**ලියාපදිංචි පුද්ගලයාගේ රට: AL**<br>**Registrar: eNom** | • tryhrwserf[.]com<br>• tibetone[.]org<br>• comeflxyr[.]com<br>• adoptewer[.]com<br>• bhvghg[.]com<br>• fgttgvh[.]com<br>• in7n[.]com<br>• o21q[.]com<br>• ophgfhfgt7[.]com |

| විද්‍යුත් තැපැල් ලිපින |
|---|
| **taoyujun@gmail.com** |
| **tplutalova@list.ru** |
| **wangminghua6@gmail.com** |
| **choekyi.wangmo@ignitetibet.net** |
| **ivan_s81@mail.ru** |
| **ocean.nio@rediffmail.com** |

| YouTube නාලිකා |
|---|
| **https://www.youtube.com/@flygram1665** |
| **https://www.youtube.com/@bradshannon334** |
| **https://www.youtube.com/@uyghurapks3096** |
| **https://www.youtube.com/@josephjoey3499** |

BADBAZAAR සහ MOONSHINE සමඟ සම්බන්ධ අනෙකුත් අවදානමට ලක් වූ දර්ශක (IoCs) සඳහා සබැඳි පහත දැක්වෙයි. මෙම සබැඳිවල ඇති සියලුම තොරතුරු වල වලංගුභාවය NCSC හට තහවුරු කළ නොහැකි අතර ඒවායේ නිරවද්‍යතාවය සහ අදාළත්වය ස්වාධීනව සත්‍යාපනය කිරීමට පාඨකයින්ට උපදෙස් දෙනු ලැබේ:

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

## ලිහිල් කිරීම

ප්‍රත්‍යක්ෂ අධ්‍යයනයන්හි විස්තර කර ඇති තර්ජන වලින් ආරක්ෂා වීම සඳහා පහත නිර්දේශ අනුගමනය කිරීමට NCSC දිරිමත් කරයි..

- **තෙවන පාර්ශවීය යෙදුම් ගබඩා ඇතුළු යෙදුම් ගබඩා ක්‍රියාකරුවන්, සහ සංවර්ධකයින් ඔවුන්ගේ වේදිකාවේ ඇති යෙදුම් ආරක්ෂිත බවත් ඒවා රජයේ විෂයභාර සංග්‍රහයට අනුකූල බවත් සහතික කළ යුතුය.** මාර්ගෝපදේශය බලන්න: 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

- **බහු-භාෂා සහාය**: උයිගර්, ටිබෙටන්, තායිවාන හොක්කියන් සහ කැන්ටනීස් ඇතුළු ඉලක්කගත කණ්ඩායම් අතර සුළුතර භාෂා කතා කරන පරිශීලකයින් සඳහා ජනප්‍රිය යෙදුම් ස්ථානගත කිරීමේ උත්සාහයන් සඳහා යෙදුම් සංවර්ධකයින් ආයෝජනය කළ යුතුය. App යෙදුම් ස්ථානාගත කිරීම සඳහා Apple මාර්ගෝපදේශය: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. යෙදුම් පරිවර්තනය කිරීම පිළිබඳ Google මාර්ගෝපදේශයhttps://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **ඔබගේ සමාජ මාධ්‍ය වේදිකාව ආරක්ෂිතව තබ ගැනීම:** සමාජ මාධ්‍ය සමාගම්වලට, අනිෂ්ට සයිබර් ක්‍රියාකාරීන්ට ව්‍යාජ ගිණුම් නිර්මාණය කිරීම සහ ඔවුන්ගේ වේදිකාවල අනිෂ්ට ලිපිගොනු හෝ සබැඳි වෙනත් ආකාරයකින් නීත්‍යානුකූල මාර්ගගත ප්‍රජාවන් සමඟ බෙදා ගැනීම වඩාත් අපහසු කළ හැකිය. හැකි සෑම විටම, තර්ජනය පිළිබඳ සාමූහික අවබෝධය වැඩිදියුණු කිරීමට සහ ආරක්ෂණ පියවරයන්ට සහාය වීමට සමාගම් විසින් පුළුල් කර්මාන්ත සමඟ අනිෂ්ට දර්ශක බෙදා ගත යුතුය.

- ***පාරිභෝගිකයින් සඳහා ප්‍රතිකර්ම සැලැස්ම:*** *තම සේවාවන් භාවිතා කරමින් අනිෂ්ට යෙදුම් ස්ථාපනය කර ඇති ගනුදෙනුකරුවන් හට දැනුම් දීම සඳහා ක්‍රියා පටිපාටි සංවිධාන සතුව තිබිය යුතුය. මෙම අනතුරු ඇඟවීම් අවධානය යොමුකර ගත හැකි සහ තොරතුරු සහිත විය යුතුය. සුදුසු අවස්ථාවලදී, සංවිධාන විසින් මෘදුකාංග ඉවත් කරන්නේ කෙසේද යන්න පිළිබඳ මගපෙන්විය යුතු අතර, එක්සත් රාජධානියේ NCSC වැනි ඔවුන්ගේ බලධාරීන්ට වාර්තා කිරීමට විනිදිනයින්ව දිරිමත් කළ යුතුය.*

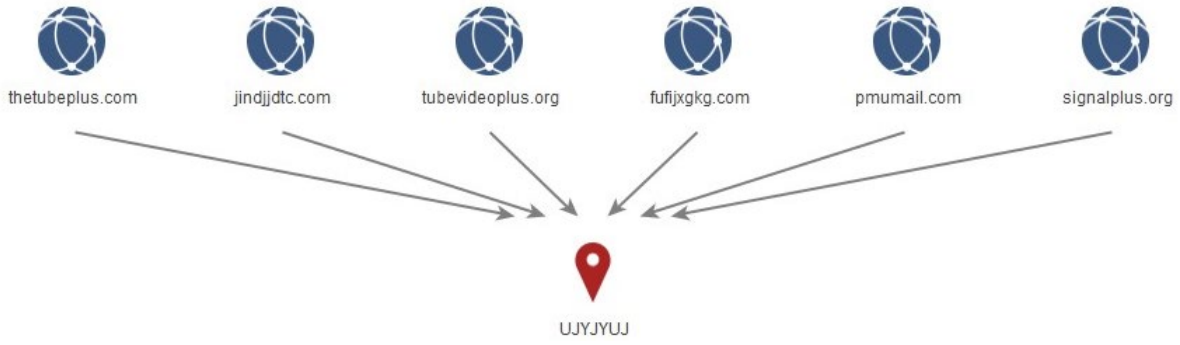
*වැඩිදුර තොරතුරු සඳහා App Store විව්‍යහාර සංග්‍රහය බලන්න:*
https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **සහයෝගීතාවය සඳහා වැඩ කරන කණ්ඩායම්:** *සමාජ මාධ්‍ය සමාගම්වලට ඔවුන්ගේ අදාළ ආරක්ෂක කණ්ඩායම්වලට ද්වේෂසහගත දර්ශක, TTP සහ නිරීක්ෂණ බෙදා ගැනීමට ඉඩ සලසමින්, වැඩ කිරීමේ කණ්ඩායම් පිහිටුවා ගත හැකිය. එමඟින් ක්‍රියාකාරීන්ට ද්වේෂසහගත ව්‍යාපාර සඳහා සහාය වීම සඳහා ඔවුන්ගේ වේදිකා භාවිතා කිරීම වඩාත් අපහසු වේ.*

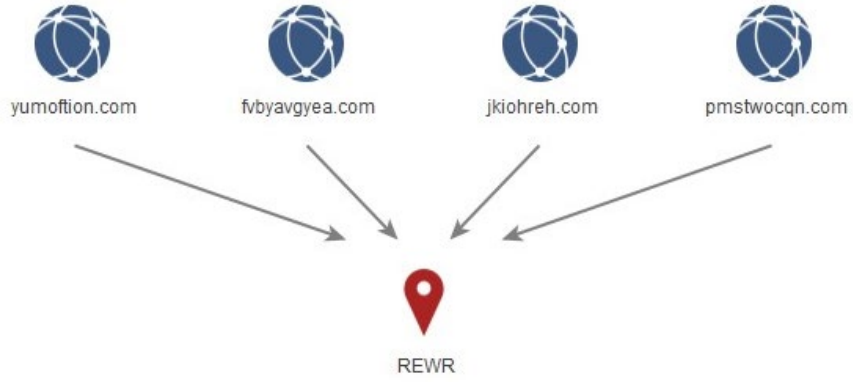
- **වෙනස් කළ යෙදුම් හඳුනා ගැනීම:** *හැකි සෑම විටම, යෙදුම් සංවර්ධනය කරන්නන් යෙදුමක 'නිල නොවන' අනුවාදයක් බාගත කර ඇත්නම්, එය ද්වේෂසහගත පිටපත් වලින් ආරක්ෂා වීමට උපකාරී වන පරිදි පරිශීලකයාට දැනුම් දෙන ක්‍රියාකාරීත්වය ඇතුළත් කළ යුතුය.*

# උපග්‍රන්ථ A: BADBAZAAR WHOIS පොකුරුකරණය / වසම් තැරැව්කරු තොරතුරු වල ප්‍රස්ථාර

1 වැනි රූපය - 'UKYJYUJ'

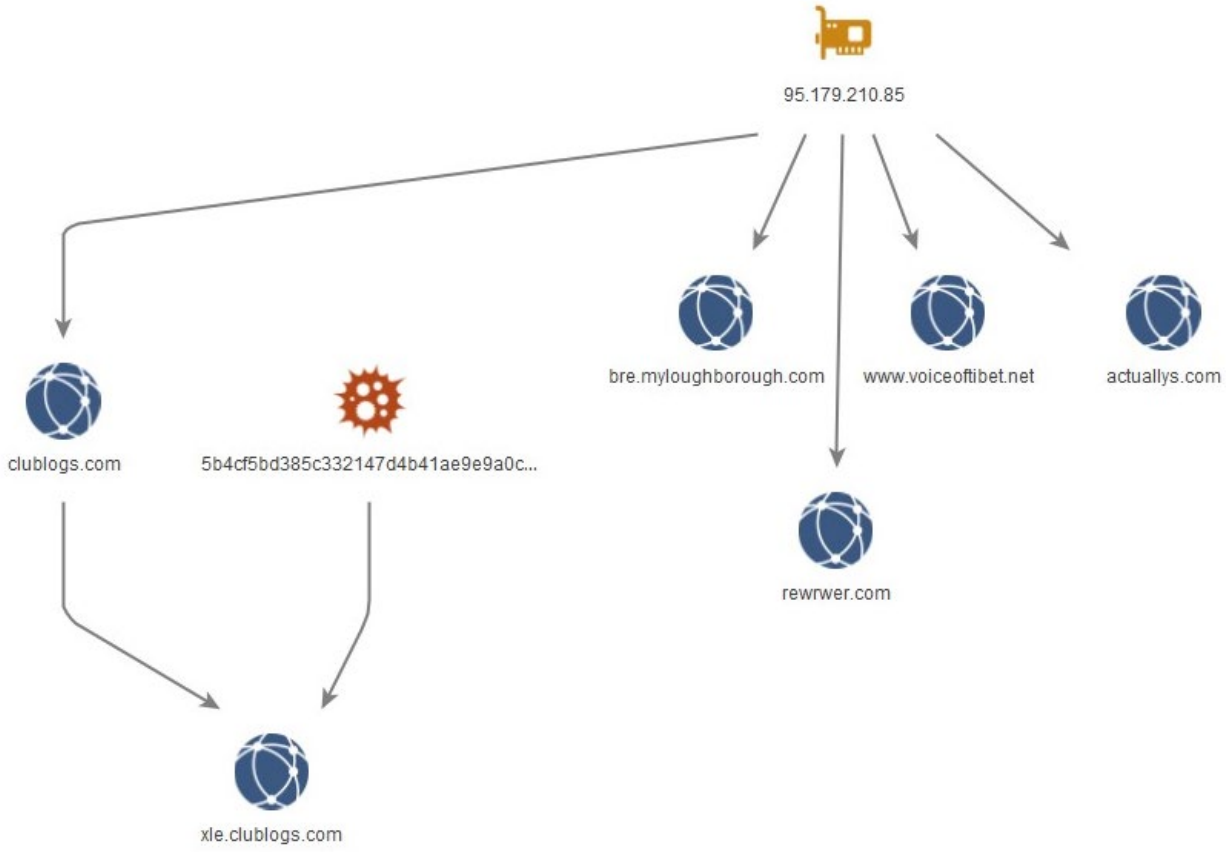



2 වැනි රූපය – යතුරුපුවරු පරිසරණ අගයන්

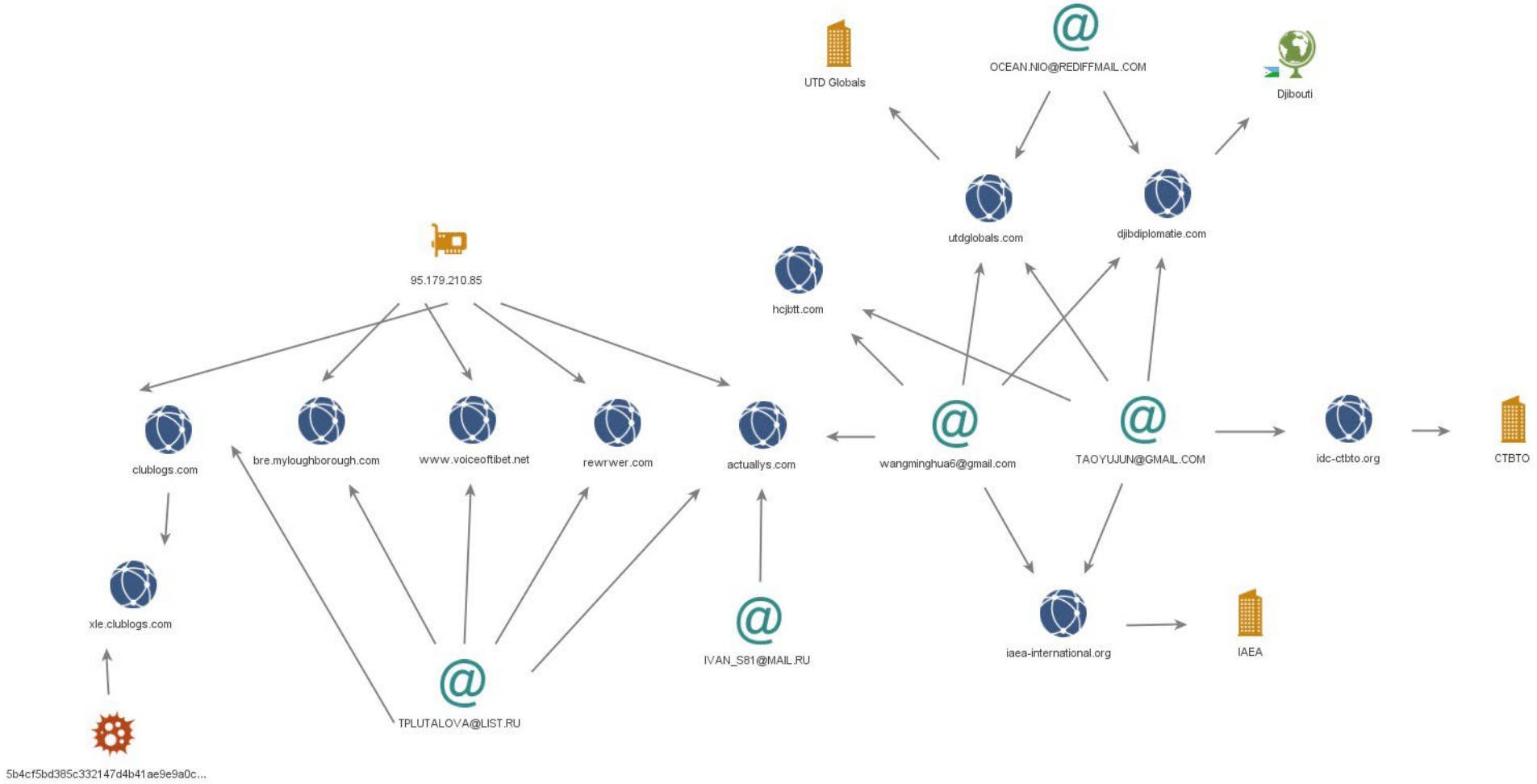



3 වැනි රූපය – 'FSDF' ඉතා උසස් ක්ෂේත්‍ර අගයන් සහිත වසම්

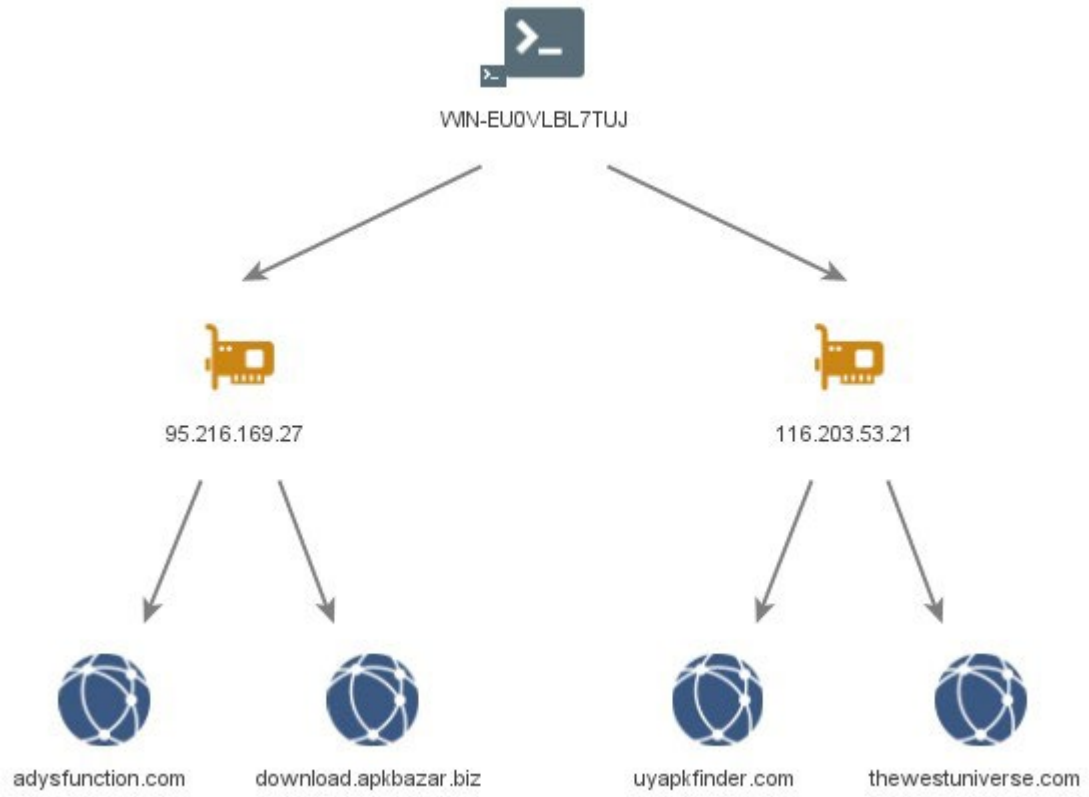
4 වැනි රූපය – **95.179.210[.]85**



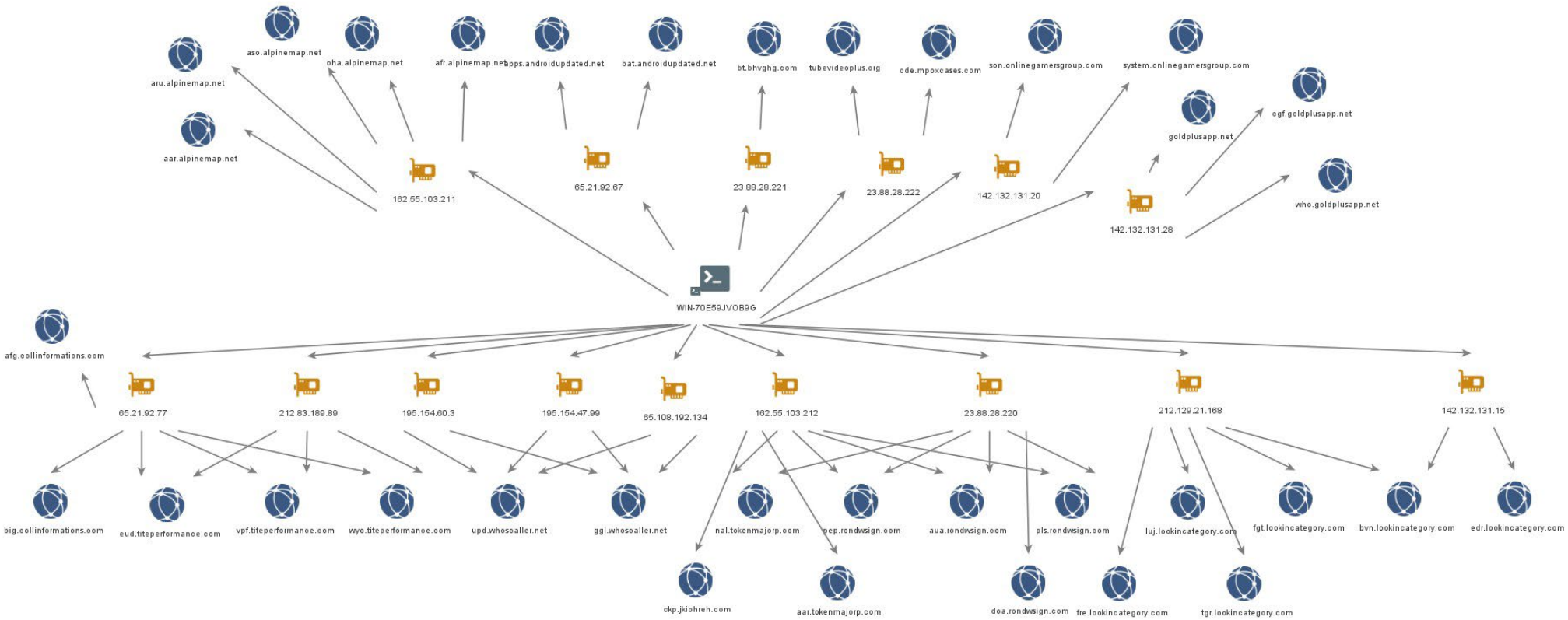
5 වැනි රූපය – WHOIS සබැඳි



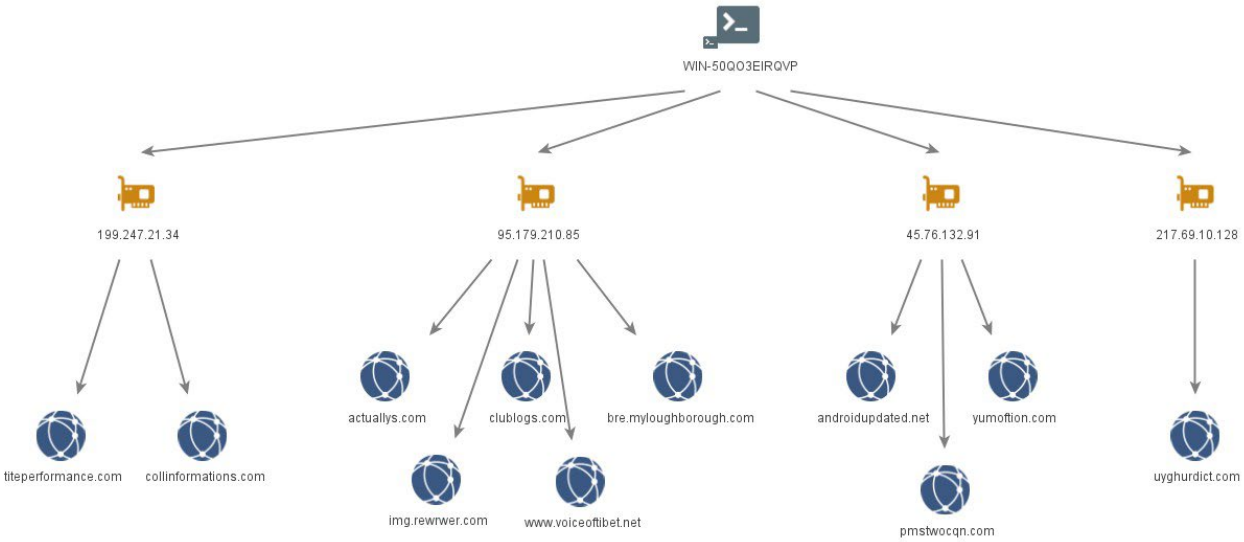
6 වැනි රූපය – **WIN-EU0VLBL7TUJ**



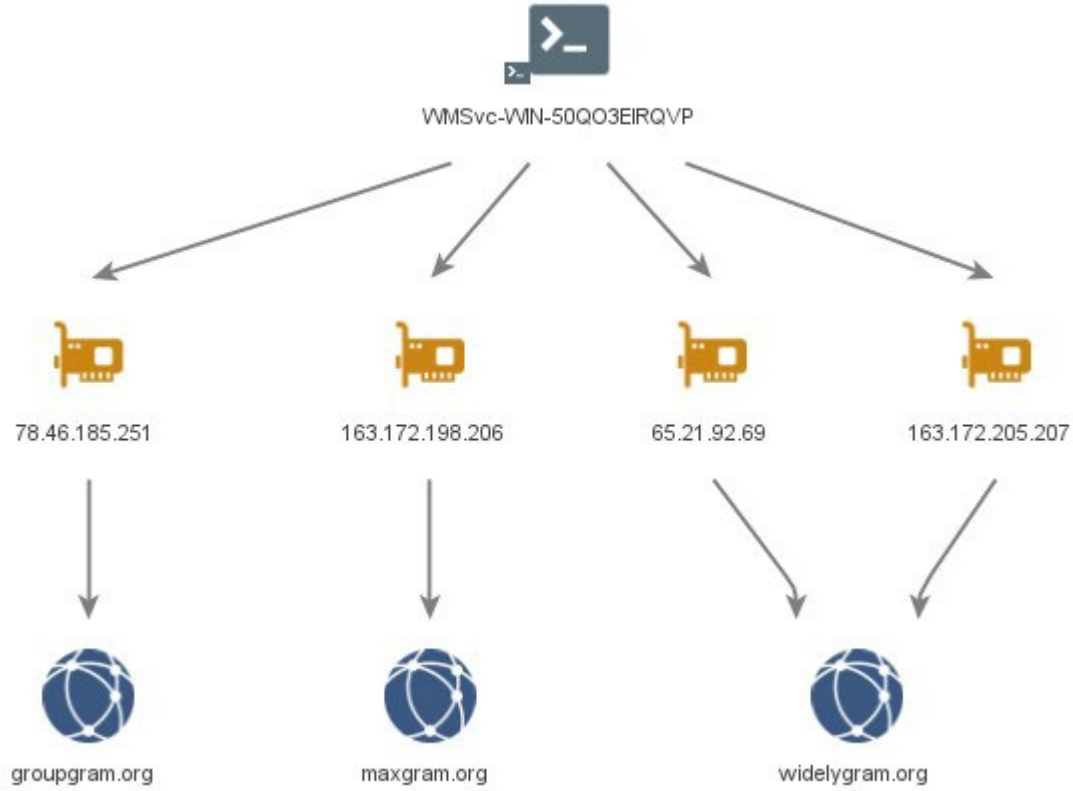
7 වැනි රූපය – **WIN-70E59JVOB9G**



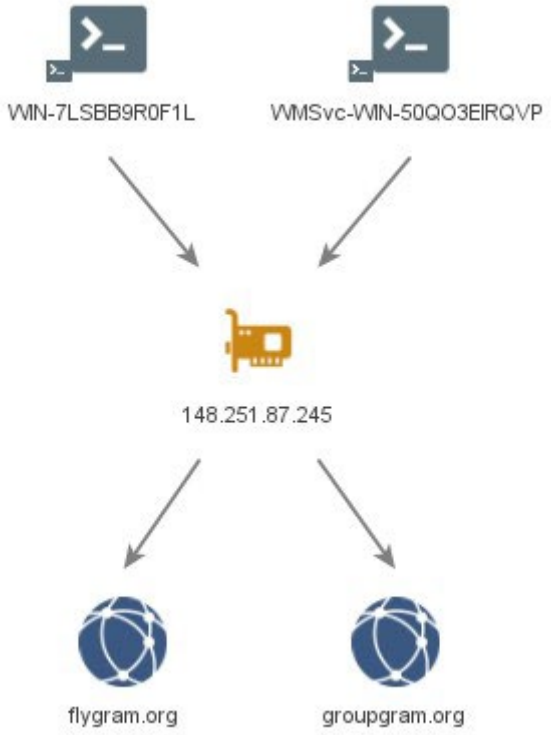
8 වැනි රූපය - **WIN-50QO3EIRQVP**



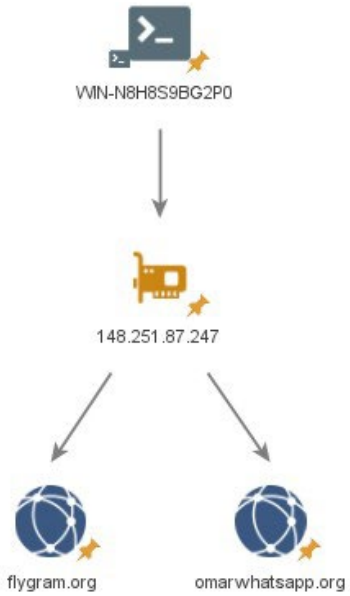

9 වැනි රූපය - **VMSvc-WIN-50QO3EIRQVP**



10 වැනි රූපය – **VMSvc-WIN-50QO3EIRQVP** සහ **WIN-7LSBB9R0F1L**



11 වැනි රූපය - **WIN-N8H8S9BG2P0**




12 වැනි රූපය – **WIN-I6VBN8MR92A**

# උපග්‍රන්ථ B: MOONSHINE & BADBAZAAR සාම්පල නිරීක්ෂණය කරන ලදී

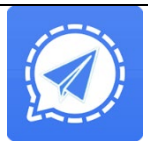
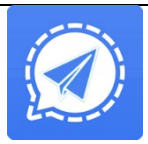
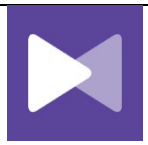
පසුගිය වසර දෙක තුළ MOONSHINE සහ BADBAZAAR ව්‍යාපාරවල භාවිතා කළ යෙදුම් පහත වගුවේ ලැයිස්තුගත කර ඇත.

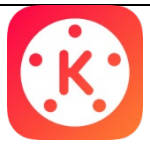
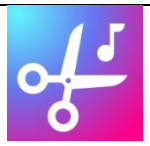
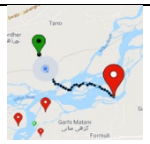
මෙම යෙදුම් බොහොමයක් ස්ථාපිත යෙදුම් වලට පැහැදිලි සමානකමක් පෙන්වයි. මෙය ප්‍රසිද්ධ වෙළඳ නාම 'රැවටීමට' හිතාමතාම භාවිතා කරන උපක්‍රමයක් වීමට ඉඩ ඇත.

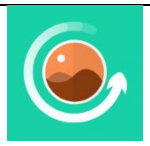
**යෙදුම් මාතෘකාව, පැකේජ නාමය සහ යෙදුම් නිරූපකය යන සියල්ලටම සැබෑ යෙදුම අනුකරණය කිරීමට හෝ ගැළපීමට හැකි බව සැලකිල්ලට ගැනීම වැදගත්ය, එබැවින් උපාංගයක් ආසාදනය වී ඇත්දැයි හඳුනා ගැනීමට පමණක් භාවිතා නොකළ යුතුය.**

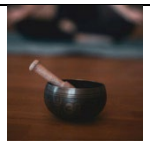
| යෙදුම් නාමය | පැකේජයේ නම | යෙදුම් අයිකොන |
|---|---|---|
| 99 Names of ALLAH | com.Apptriple.Namesofallah.Asmaulhusna |  |
| APKPure | com.apkpure.aegon |  |
| Adobe Acrobat | com.adobe.reader |  |
| Alpine(پښتو) | psyberia.pa.full |  |
| AlpineQuest Off-Road Explorer | psyberia.alpinequest.full |  |
| AlpineQuest Off-Road Explorer | psyberia.alpinequest.full |  |

| | | |
|---|---|---|
| AlpineQuest Off-Road Explorer (Lite) | psyberia.alpinequest.free |  |
| AppLock | com.alpha.applock |  |
| අරාබි යතුරුපුවරුව | com.arabic.keyboard.arabic.language.keyboard.app |  |
| ශ්‍රව්‍ය වීඩියෝ කටරය | bsoft.com.mp3.cutter.ringtone.video.maker.trimmer |  |
| Badam维语输入法 | com.ziipin.softkeyboard |  |
| Buddhist Songs (1) | com.bigkidsapps.buddhistsongs1 |  |
| කැල්කියුලේටරය | 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 |  |

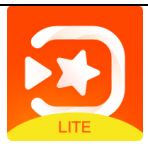
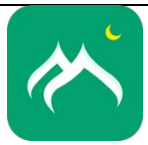
| | | |
|---|---|---|
| FMWhatsApp | com.fmwhatsapp |  |
| File Manager + | com.alphainventor.filemanager |  |
| FlyGram | org.telegram.FlyGram |  |
| Flygram | org.telegram.FlyGram |  |
| Free WiFi Pass | com.cl.wifipassword.share |  |
| GBWhatsApp | com.gbwhatsapp |  |
| Hefz Quran | com.golap.hefzquran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

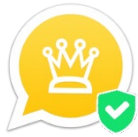
| | | |
|---|---|---|
| KineMaster | com.nexstreaming.app.kinemasterfree |  |
| MP3 Cutter & Ringtone Maker | ringtone.maker.mp3.cutter.audio |  |
| Malloc | com.mallocprivacy.antistalkerfree |  |
| Maps Distance Calculator | com.routemap.mapdownload.gpsroute planner |  |
| Media Recovery | com.aaa.media.recovery.androidapp |  |
| 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 |  |

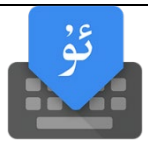
| | | |
|---|---|---|
| Photo Editor | com.iudesk.android.photo.editor |  |
| Photo Recovery | recover.restore.undelete.photo.video.file |  |
| Photo Studio | com.kvadgroup.photostudio |  |
| Plus | org.telegram.pluspro |  |
| Prayer Book | com.arashpayan.prayerbook |  |
| QuarkVPN | com.speedy.vpn |  |
| 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 |  |

| | | |
|---|---|---|
| ئەسەرلەر ئاۋازلىق | com.ewlat.eserler |  |
| قۇرئان ئاۋازلىق | com.c9.utilim |  |
| ئىزچى | com.yelken.izchi |  |
| ئىزدىگۈچى ئۇيغۇرچە APK | com.uygur.apkstore |  |
| قۇرئان ئۇيغۇرچە | com.c9.uyghurquran |  |
| الكريم القرآن | com.maher4web.quran |  |
| زىكىرلەر | com.my.newproject5 |  |
| كەرىم قۇرئان | ru.omdevelopment.ref.quranuyghur.free |  |
| لۇغىتى كۇھىقاپ | com.kuhiqap.lughitim |  |
| كىرگۈزگۈچ نۇر | 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 |  |

# වැඩිදුර කියවීම

## ඕස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානයේ මග පෙන්වීම

- සයිබර් අපරාධයක්, සිද්ධියක් හෝ අවදානමක් වාර්තා කිරීම
- ඔබගේ උපාංග සුරක්ෂිත කර ගන්නේ කෙසේද
- ඔබේ ජංගම දුරකතනයආරක්ෂාකර ගැනීම
- වංචනිකව යවන සන්නිවේදනයන්
- වංචනික ක්‍රියා
- ඔබගේ සමාජ මාධ්‍ය සුරක්ෂිත කර ගන්න
- සමාජ මාධ්‍ය සහ පණිවිඩ යෙදුම් සඳහා ආරක්ෂක උපදෙස්

## UK NCSC සහ NPSA වෙතින් මර්ගඋපදේශන

- ප්‍රජාතන්ත්‍රවාදය ආරක්ෂා කිරීම
- සමාජ මාධ්‍ය: එය ආරක්ෂිතව භාවිතා කරන්නේ කෙසේද
- සංවිධාන සඳහා උපාංග, ජංගම උපාංග ඇතුළු, ආරක්ෂක මාර්ගෝපදේශ
- යෙදුම් ගබඩා පිළිබඳ තර්ජන වාර්තාව
- අධි අවදානම් සහිත පුද්ගලයින් සඳහා පුද්ගලික ආරක්ෂාව සහ සුරක්ෂිත භාවය

## US NSA වෙතින් මර්ගඋපදේශන

- ජංගම උපාංග සම්බන්ධ හොඳම පිළිවෙත්

# හිමිකම් අත්හැරීම

මෙම උපදේශනය මගින් එය ප්‍රකාශනය කරන අවස්ථාවේ වලංගු කරන ලද තොරතුරු සපයන බව කරුණාවෙන් සලකන්න.

මෙම වාර්තාව කර්තෘ ආයතන සහ කර්මාන්ත මූලාශ්‍රවලින් ලබාගත් තොරතුරු මත පදනම් වේ. සියලු අවදානම් වළක්වා ගැනීමේ අරමුණින් කරන ලද කිසිදු සොයාගැනීමක් හෝ නිර්දේශයක් මෙහි සපයා නොමැති අතර නිර්දේශ අනුගමනය කිරීමෙන් එවැනි සියලු අවදානම් ඉවත් නොවේ. තොරතුරු අවදානම් වල හිමිකාරිත්වය සෑම විටම අදාළ පද්ධති හිමිකරු සතුව පවතී.

එක්සත් රාජධානියේ, මෙම තොරතුරු 2000 තොරතුරු පිළිබඳ නිදහස පනත (Freedom of Information Act 2000 (FOIA)) යටතේ නිදහස් කර ඇති අතර අනෙකුත් එක්සත් රාජධානියේ තොරතුරු නීති යටතේ වගමීමෙන් මුදාහැරිය හැකිය.

ඕනෑම FOIA විමසුමක් ncscinfoleg@ncsc.gov.uk වෙත යොමු කරන්න.