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

ஆலோசனை

BADBAZAAR மற்றும் MOONSHINE: தொழில்நுட்ப பகுப்பாய்வு மற்றும் தணிப்புகள்

9 ஏப்ரல் **2025**

BADBAZAAR மற்றும் MOONSHINE: தொழில்நுட்ப பகுப்பாய்வு மற்றும் தணிப்புகள்

தொகுப்பு

இந்த ஆலோசனை UKயின் Cyber League அமைப்பின் ஆதரவுடன், the National Cyber Security Centre (NCSC UK) என்ற தேசிய சைபர் பாதுகாப்பு மையம் மற்றும் பின்வரும் சர்வதேச கூட்டாளர்களால் கூட்டாகத் தயாரிக்கப்பட்டுள்ளது:

- **ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையம், ஆஸ்திரேலிய சமிக்ஞைகள் இயக்குநரகத்தின் ஒரு பகுதி**
- **சைபர் பாதுகாப்பிற்கான கனேடிய மையம், தகவல் தொடர்பு பாதுகாப்பு ஸ்தாபனத்தின் ஒரு பகுதி**
- **ஜெர்மன் ஃபெடரல் புலனாய்வு சேவை**
- **ஜெர்மன் ஃபெடரல் அரசியலமைப்பு பாதுகாப்பு அலுவலகம்**
- **நியூசிலாந்து தேசிய சைபர் பாதுகாப்பு மையம், அரச தகவல் தொடர்பு பாதுகாப்பு பணியகத்தின் ஒரு பகுதி**
- **அமெரிக்காவின் குற்றப் புலனாய்வுத்துறை - Federal Bureau of Investigation (FBI)**
- **அமெரிக்க தேசிய பாதுகாப்பு நிறுவனம்** (NSA)

BADBAZAAR மற்றும் MOONSHINE எனப்படும் உளவுமென்பொருட்கள் குறித்த, புதிய மற்றும் தொகுக்கப்பட்ட அச்சுறுத்தல் நுண்ணறிவை இந்த ஆலோசனை அறிக்கை வழங்குகிறது. செயலிகளை உருவாக்குபவர்கள் மற்றும், விநியோகம் செய்பவர்களுக்கும் சமூக ஊடக நிறுவனங்களுக்கான ஆலோசனைகளையும் இது உள்ளடக்கியது.

இந்த ஆலோசனை அறிக்கை, தீம்பொருளால் பாதிக்கப்பட்டவர்களுக்கான ஆலோசனையுடன் இணையாக வெளியிடப்படுகிறது.

இந்த ஆவணம் உளவு மென்பொருள் குறித்த NCSCஇன் சொற்களஞ்சிய வரையறையைப் பயன் படுத்துகிறது: “பயனரின் அனுமதியின்றி சாதனத்தில் நிறுவி, தரவைச் சேகரித்து மூன்றாம் தரப்புக்கு அனுப்பும் ஒரு வகை தீம்பொருள்.”

விரிவான ஆய்வு ஒன்று: MOONSHINE

MOONSHINE என்ற Android உளவுமென்பொருள் திபெத்திய குழுக்களை குறி வைப்பதாக 2019ஆம் ஆண்டில் Citizen Lab அறிவித்தது. முறையான செயலியாக MOONSHINE காட்டிக் கொண்டு, அதை நிறுவ பாதிக்கப்பட்டவர்களைக் கவர்ந்திழுக்கிறது. அது Telegram சேனல்கள் மூலம் பகிரப்பட்டு, அதன் இணைப்புகள் WhatsApp வழியாகப் பகிரப்பட்டுள்ளது.

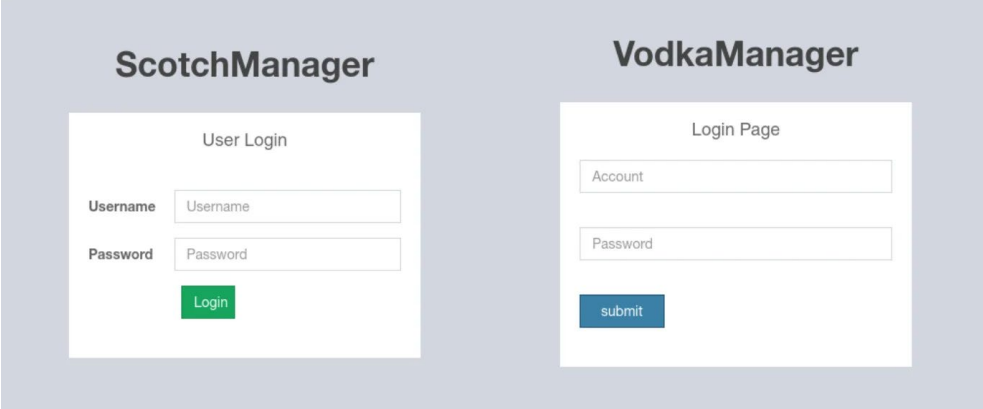
MOONSHINE பற்றிய NCSCஇன் ஆராய்ச்சி பின்வருவனவற்றைக் கண்டறிந்துள்ளது:

- ஒரு மேலாண்மை இடைமுகத்தை MOONSHINE பயன்படுத்துகிறது. முதலில் அறிமுகமானதிலிருந்து இது மாற்றங்களுக்கு உட்பட்டுள்ளது.
- விரிவான கண்காணிப்பு திறன்களை மேலாண்மை இடைமுகம் வெளிப்படுத்துகிறது. சாதனங்களிலிருந்து கோப்புகளை வெளியேற்றும் திறன் மற்றும் நேரடி ஆடியோ மற்றும் திரை பதிவுகளைப் பிடிக்கும் திறன் ஆகியவை இதில் அடங்கும்.
- மற்றவர்களால் பராமரிக்கப்படும் சேவையகங்களில் MOONSHINE மேலாண்மை இடைமுகங்களின் தொகுப்பு கண்டுபிடிக்கப்பட்டுள்ளது. இந்த இடைமுகங்கள், உள்கட்டமைப்புரீதியில் UPSECஉடன் தொடர்புடைய உள்நுழைவுப் பலகையுடன் ஒற்றுமையைக் கொண்டுள்ளன என்றும், UPSEC என்பது 'Sichuan Dianke Network Security Technology Co. Ltd' என்பதைக் குறிக்கிறது என்றும் Intelligence Online குறிப்பிடுகிறது.

மேலாண்மை இடைமுகம்

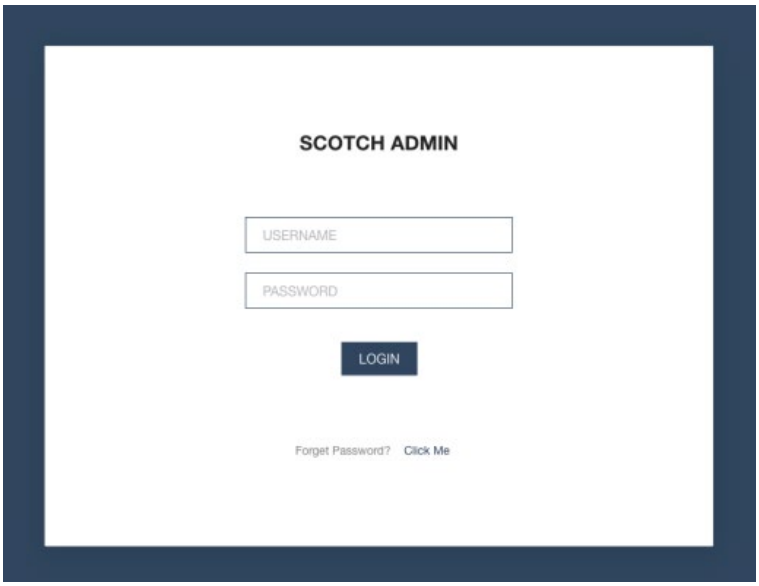
MOONSHINE மேலாண்மை இடைமுகம் மாற்றங்களுக்கு உட்பட்டுள்ளது என்பதை அது குறித்த முந்தைய அறிக்கையுடன் ஒப்பிடும் போது தெரிகிறது. அப்படியென்றால், அது தொடர்ச்சியாக மாற்றியமைக்கப்பட்டு வருவதைக் குறிக்கிறது.

மேலாண்மை இடைமுகத்தின் முதல் எடுத்துக்காட்டு 2019ஆம் ஆண்டு Citizen Lab வெளியிட்ட அறிக்கையில் காணப்படுகிறது.



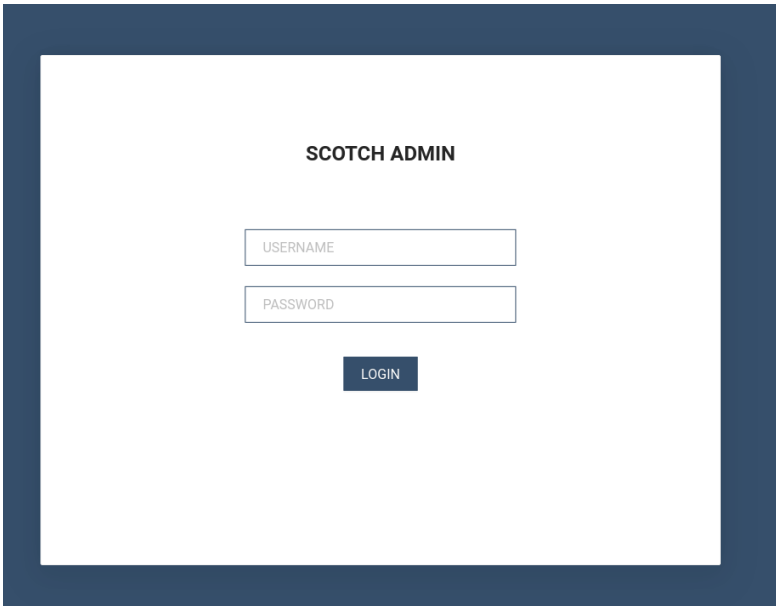
படம் *à:* 2019ஆம் ஆண்டு *Citizen Lab* வெளியிட்ட *'Missing Link Tibetan Groups Targeted with* 1-*Click Mobile Exploits'* என்ற அறிக்கையில் காணப்படும் *MOONSHINE* மேலாண்மை இடைமுகங்கள்.

2022 ஆம் ஆண்டின் தொடக்கத்தில், Lookout வேறுபட்ட மேலாண்மை இடைமுகத்தைக் காட்சிப் படுத்தியது. மறு வடிவமைப்பு செய்யப்பட்ட இடைமுகம் கீழே உள்ளபடி மாற்றப்பட்டுள்ளது (படம் 1 இல் இருந்த முந்தைய இடைமுகம் மாறியுள்ளது):



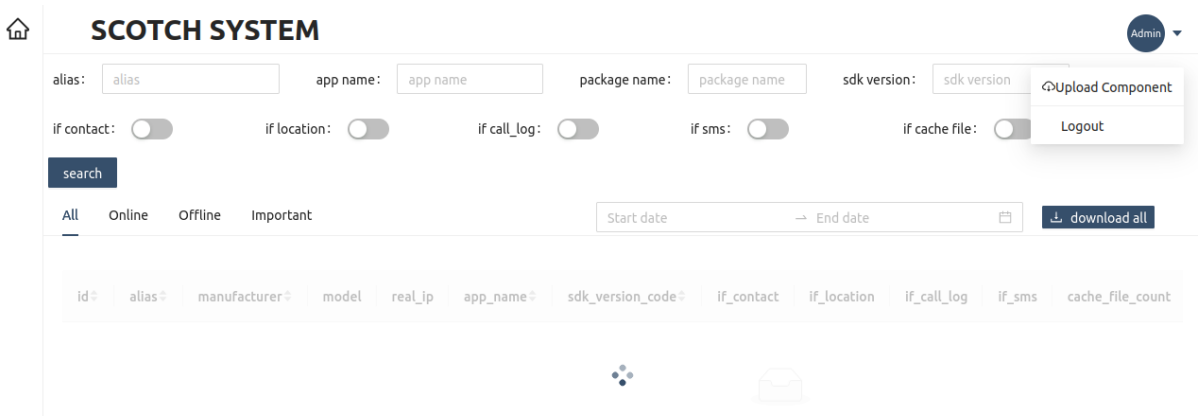
படம் *ã: Lookout 2022*ஆம் ஆண்டு வெளியிட்ட அறிக்கையில் காணப்படும் *MOONSHINE* மேலாண்மை இடைமுகம். *'MOONSHINE:* திபெத்தியர்கள் மற்றும் உய்குர்களைக் குறிவைத்து சீன *APT POISON CARP* ஆல் உருவாக்கப்பட்டு வரும் *Android* கண்காணிப்பு மென்பொருள்.*'*

2023ஆம் ஆண்டு ஆகஸ்ட் மாதத்தில் MOONSHINE கட்டளை மற்றும் கட்டுப்பாடு (C2) scan செய்யப்பட்டபோது, படம் 2 இல் உள்ளது போல, 2022ஆம் ஆண்டு இருந்த இடைமுகத்தில் இருந்த **'கடவுச்சொல்லை மறந்துவிட்டேன்'** என்ற செயல்பாடு இல்லை என்பதை வெளிப்படுத்தியது:



படம் ச: *MOONSHINE* மேலாண்மை இடைமுகம் ஆகஸ்ட் *2023* இல் அவதானிக்கப்பட்டது, அதில் 'கடவுச்சொல்லை மறந்துவிட்டேன் 'என்ற வரி இல்லை.

சமரசம் செய்யப்பட்ட சாதனங்களின் விவரங்கள் எவ்வாறு சேமிக்கப்படும் என்பது அதன் உள்ளடக்கத்திலேயே இருக்கிறது என்பதை, மேலாண்மை இடைமுகத்தின் மேலதிக விசாரணை வெளிப்படுத்தியது.



படம் *ம:* *MOONSHINE* மேலாண்மை இடைமுகத்தின் உள்நுழைவு பக்கத்தின் உள்ளடக்க வலைப் பக்கம்.

பாதிக்கப்பட்ட சாதனத்திலிருந்து MOONSHINE C2 சேவையகங்களுக்கு ஒரு '**மதிப்பெண்**' அனுப்பப்பட்டதை Lookout செய்த ஒரு ஆராய்ச்சி காட்டியது. 'மதிப்பெண்' மதிப்பு பாதிக்கப்பட்ட சாதனத்தில் தீங்கிழைக்கும் மாதிரியின் அனுமதிகளை அடிப்படையாகக் கொண்டது.

பக்கத்தில் உள்ள 'if_contact', 'if_location', 'if_call_log' மற்றும் 'if_sms' போன்ற நெடுவரிசைகள், சமரசம் செய்யப்பட்ட சாதனங்களுக்கான முழு

அணுகலை அனைத்து MOONSHINE மாதிரிகளும் பெறவில்லை என்று எடுத்துக் கூறுகின்றன. இந்த நெடுவரிசைகள் பற்றிய அறிவு மற்றும் சாதனத்திலிருந்து C2ற்கு அனுப்பப்பட்ட 'மதிப்பெண்' ஆகியவை அச்சுறுத்துபவர்கள் மேலாண்மை இடைமுகத்தை அணுகுபவர்களுக்கு தீம்பொருளின் அணுகல் அளவைத் தெரிவிக்க மதிப்பெண்ணைப் பயன்படுத்துகிறார்கள் என்பதைக் கூறுகிறது.

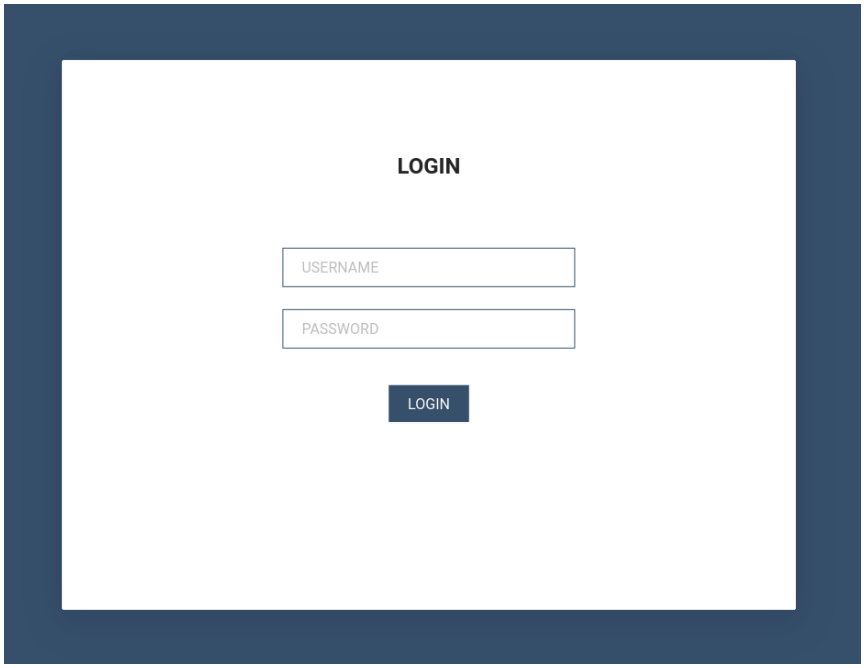
பொதுவாக, செயலியைப் பதிவிறக்குவதற்கு முன்னர் அசாதாரணமான எதற்கும் அனுமதி கொடுக்கப்பட்டிருக்கிறதா என்பதை ஆய்வு செய்வதே சாதனங்களிலிருந்து தகவல்களைச் சேகரிக்கும் செயலிகளைத் தடுப்பதற்கான சிறந்த நடைமுறை ஆலோசனையாகும். இருப்பினும், MOONSHINE மாதிரிகள் செயலியின் செயல்பாட்டுடன் தொடர்புடைய அனுமதிகளை நாடுகின்றன. எனவே அதனை சந்தேகப்படத் தேவையில்லை என்று தோன்றலாம். ஆனால் அவை, சாதனங்களிலிருந்து தகவல்களைச் சேகரிக்க இந்த அனுமதிகளைப் பயன்படுத்துகின்றன.

MOONSHINE அதன் திறன்களின் அகலத்தை வெளிப்படுத்தும் செயலி நிரலாக்க இடைமுகத்தையும் (Application Programming Interface - API) கொண்டுள்ளது. API ஆவணங்களின் ஆரம்பப் பதிப்புகள், சீன (Mandarin) மொழியில் API பெயர்களைக் கொண்டிருந்தன.

மெய்நிகர் இயந்திரம்

MOONSHINE பலகைகளுக்கான தேடல்களில், பல மெய்நிகர் இயந்திரங்கள் (virtual hosts) இதை இயக்குவது கண்டுபிடிக்கப் பட்டன. மெய்நிகர் இயந்திரங்கள் மூலம் ஒரு IP முகவரி ஒரே நேரத்தில் பல வலைத் தளங்களை இயங்கச் செய்ய முடியும். இந்த மெய்நிகர் இயந்திரங்களின் IP முகவரிகள் மற்றும் அப்படி நிர்வகிக்கப்பட்ட டொமெய்ன்கள், அறியப்பட்ட எந்த ஒரு தீம்பொருள் மாதிரிகளிலும் காணப்படவில்லை.

மேலாண்மை இடைமுகம் இங்கே வேறுபட்டுக் காணப்படுகின்றன. பக்கங்களின் தலைப்பு முன்பு பார்த்த **'SCOTCH ADMIN'** என்பதற்குப் பதிலாக '**LOGIN**' என்று இருந்தது.



படம் ii: *SCOTCH ADMIN* ற்குப் பதிலாக *LOGIN* என்ற தலைப்புடன் *MOONSHINE* மேலாண்மை இடைமுகம்.

கூடுதலாக, பலகையில் உள்ள உள்ளடக்கமும் படம் 4 இலிருந்து வேறுபட்டு, படம் 6 இல் உள்ளது போல் காணப்படுகிறது:

படம் ii: மெய்நிகர் இயந்திரத்தால் இயக்கப்படும் *MOONSHINE* மேலாண்மை இடைமுகத்தின் உள்நுழைவு பக்கத்தின் உள்ளடக்க வலைப் பக்கம்.

படம் 6 இல் உள்ள பலகையின் படம் 4 இல் உள்ள பலகையின் அகற்றப்பட்ட பதிப்பாகத் தெரிகிறது. அட்டவணையில் உள்ள id', 'உற்பத்தியாளர்' மற்றும் model' ஆகிய நெடுவரிசை பெயர்கள், இரண்டு பலகைகளிலும் ஒன்றுடன் ஒன்றுபட்டவையாக இருக்கின்றன

மெய்நிகர் இயந்திரங்களால் இயக்கப்படும் MOONSHINE என்று கண்டுபிடிக்கப்பட்டதன் அட்டவணை

களம்	IP முகவரி
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

இந்த டொமெய்ன்களைப் பயன்படுத்தி, மொபைல் சாதனங்களில் தீம்பொருளை நிறுவி, பயனர்களை MOONSHINE சுரண்டுவதாக Trend Micro பட்டியலிட்டுள்ளது. இந்தத் தீம்பொருளுக்கு, 'Dark Nimbus' என்று Trend Micro பெயரிட்டுள்ளது.

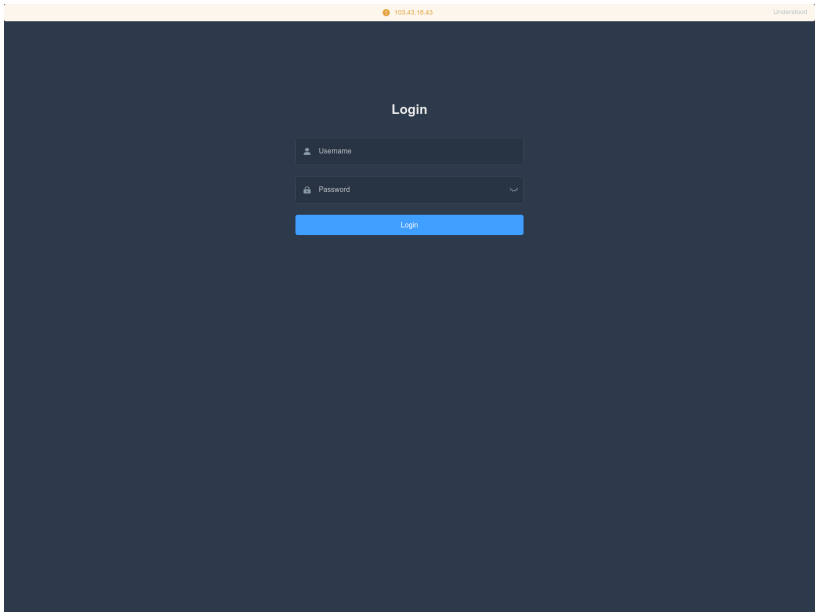
தெளிவுபடுத்துவதற்காக, MOONSHINE மேலாண்மை இடைமுகங்கள் மூலமாக MOONSHINE தீம்பொருள் மாதிரிகள் தொடர்பு கொண்டு பாதிக்கப்பட்டவரின் தரவுகளை வெளியே எடுக்கிறது. Trend Micro அறிவித்துள்ள MOONSHINE இல் இருக்கும் சுரண்டல் கருவிகள் (exploit kits), மொபைல் சாதனங்களில் Dark Nimbus எனப்படும் தீம்பொருளை நிறுவ, இணைய உலாவிகளிலுள்ள பாதிக்கப்படக்கூடிய விடயங்களைப் பயன்படுத்தும் ஒரு தனித் திறன். மேலும், Dark Nimbus மற்றும் MOONSHINE ஆகியவை முற்றிலும் மாறுபட்ட தீம்பொருட்கள்.

MOONSHINE மேலாண்மை இடைமுகம் மற்றும் MOONSHINE சுரண்டல் கருவிகள் இரண்டும் ஒரே மாதிரியாக அமைக்கப்பட்டுள்ளன, எனவே படங்கள் 3 மற்றும் 5 இல் இதேபோன்ற உள்நுழைவு இருப்பதைப் பார்க்கலாம், அத்துடன் படங்கள் 4 மற்றும் 6 இல் உள்ள பக்கத்தின் உள்ளடக்கமும் ஒரே மாதிரி உள்ளன. அவை இரண்டும் மூலக் குறியீட்டில் 'webpackJsonpreact-scotchui' என்ற சரத்தையும் கொண்டுள்ளன.

அச்சுறுத்துபவர்கள் MOONSHINE சுரண்டல் கருவிகளுடன் இணைக்கப்பட்ட URL இணைப்புகளை உருவாக்கிய பின்னர், திபெத்தியர்கள் மற்றும் உய்குர்கள் தொடர்பான வீடியோக்களை MOONSHINEஐ இலக்காகக் கொண்டு இயங்கும் தளங்களுக்குத் திருப்பி விட்டனர். அவை ஒன்றுடன் ஒன்று செயல்படுகின்றன.

MOONSHINE சுரண்டல் கருவிகளைத் தாங்கிவரும் டொமெய்னை வழங்கும் பல IP முகவரிகளில், போர்ட் 444 இல், 'VLiteUI' என்ற தலைப்பில் ஒரு

உள்நுழைவுப் பக்கம் உள்ளது. இந்த பக்கம் பரவலாகக் கவனிக்கப்படவில்லை என்றாலும், இந்த IPகளில் அது இருப்பது, தீங்கிழைப்பவர்களின் செயல்பாடுகளுக்கான சாத்தியமான தொடர்பு இருப்பதைக் குறிக்கிறது.



படம் *ii: HTML* தலைப்பு *'VLiteUI'* உடன் அமைந்திருக்கும் உள்நுழைவு பலகைகள், *MOONSHINE* சுரண்டல் கருவிகளைத் தாங்கிவரும் *IP* முகவரிகளில் காணப்பட்டது.

தீம்பொருள் சாதனத்தில் உள்ள தகவல்களின் முழுமையான பட்டியலை சேகரிக்க முடியும் என்பதையும், அது XMPP நெறிமுறையைப் பயன்படுத்தி C2 உடன் தொடர்பு கொள்வதையும் Trend Micro இன் Dark Nimbus குறித்த பகுப்பாய்வு வெளிப்படுத்தியது.

Dark Nimbusஇன் சில பதிப்புகளில், 'DKNS' என்ற சரத்தின் பரவலை அவர்கள் அடையாளம் கண்டதாகவும் Trend Micro கோடிட்டுக் காட்டுகிறது.

பிற IP முகவரிகளுக்கான XMPP சேவைகளை வழங்கும் வலைப்பக்கங்களின் தலைப்பில் DKNS காணப்பட்டது என்று **'ansec[.]com'** (அதனை TrendMicro, Dark Nimbus C2 என பட்டியலிட்டுள்ளது) அவதானித்துள்ளது.

- 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 சேவையில் **‘ansec[.]com’**ஐத் தலைப்பில் கொண்டிருந்த IP முகவரிகள் பின்வரும் வலைப் பக்கங்களில் இருந்தன:

- 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 தகவலின் படி, HTML பக்கங்களின் தலைப்புகளில் காணப்பட்ட 'UPSEC' என்பது 'Sichuan Dianke Network Security Technology Co., Ltd' எனக் குறிப்பிடப்படுகிறது.

விரிவான ஆய்வு இரண்டு: BADBAZAAR

BADBAZAAR என்பது உய்குர்கள், திபெத்தியர்கள் மற்றும் தைவானியர்களைக் குறி வைக்கும் iOS மற்றும் Android வகை மொபைல் தீம்பொருளாகும். இந்தத் தீம்பொருள் சமூக ஊடகத் தளங்கள் மற்றும் அதிகார பூர்வ App storeகள் வழியாக பரவுகிறது. BadSolar, BADBAZAAR மற்றும் BadSignal என்று வெவ்வேறு திரிபுகளாக BADBAZAAR இருப்பதாக Volexity வெளியிட்ட சமீபத்திய அறிக்கை கூறுகிறது. சாதனம் மற்றும் இணைப்பாளர் குறித்த தகவல்களைச் சேகரிக்கப் பயன்படுத்தப்படும் செயல்பாடுகளுக்கு மூன்று திரிபுகளும் ஒன்றுடன் ஒன்று இணைந்து செயல்படுகின்றன.

BADBAZAAR பற்றிய NCSC செய்த ஆராய்ச்சி பின்வருவனவற்றை வெளிப்படுத்தியது:

- C2 களங்களைக் கொத்துக்களாக்குவதன் மூலம், நுண்ணறிவில் தெரிவிக்கப்பட்ட அச்சுறுத்தல் களங்களுக்கான கூடுதல் இணைப்புகள் வெளிப்படுத்தப்பட்டன.
- C2 சேவையகங்கள் மற்றும் தீம்பொருள் மாதிரிகள் உள்கட்டமைப்புடன் தொடர்புடைய ஹோஸ்ட் பெயர்களை வெளிப்படுத்துகின்றன.
- உத்தியோகபூர்வ App storeகளுக்கு அப்பால், தங்கள் தீம்பொருளைப் பரப்ப அச்சுறுத்துபவர்கள் சமூக பொறியியலுக்குப் பயன்படுத்தும் கூடுதல் சுய விவரங்கள்.

WHOIS கொத்துக்கள் / டொமெய்ன் தரகர்

'UJYJYUJ'

'signalplus[.]org' டொமெய்னுக்கான WHOIS பதிவுகளில் BADBAZAAR இன் பகுப்பாய்வில் 'State' என்ற தரவிற்கு **'UJYJYUJ**' என்ற மதிப்பைக் காட்டுகிறது என்று ESET அறிக்கையிட்டுள்ளது.

அதே மதிப்பைக் கொண்ட பிற களங்களுக்கான தேடல் பின்வரும் ஆர்வமுள்ள களங்களை வெளிப்படுத்துகிறது:

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

(இணைப்பு Aயிலுள்ள, படம் 1ஐ பார்க்கவும்)

களங்கள் **signalplus[.]org**, **tubevideoplus[.]org** மற்றும் **thetubeplus [.]com** என்பன BADBAZAAR C2 டொமெய்ன்கள் என்றும், **mail.pmumail[.]com** ஒரு FlyGram புறொக்ஸி சேவையகமாக இயங்குகிறது என்றும் ESET கூறுகிறது. FlyGram என்பது தீங்கிழைக்கும் சைபர் குற்றவாளிகளால் உருவாக்கப்பட்ட BADBAZAAR செயலியாகும். (இது போன்ற, பிற BADBAZAAR செயலிகளின் பட்டியலுக்கு பின் இணைப்பைப் பார்க்கவும்).

விசைப்பலகை நடை மதிப்புகள்

மற்றைய பதிவு செய்யப்பட்ட BADBAZAAR C2 டொமெய்ன்களிலும் இதேபோன்ற விசைப்பலகை நடை முறைகளை NCSC கண்டுள்ளது.

எடுத்துக்காட்டாக, பின்வரும் களங்கள் அனைத்தும் '**State**' என்பதற்கு (முன்பு பயன்படுத்தப்பட்ட படி,) **'REWR'** என்ற மதிப்பைக் கொண்டுள்ளன:

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

(இணைப்பு Aயிலுள்ள, படம் 2ஐ பார்க்கவும்)

State என்பதற்கு 'FSDF' என்ற மதிப்பைக் கொண்ட டொமெய்ன்கள்

BADBAZAAR C2 களங்களின் மற்றொரு தொகுப்பு, **'State'** என்பதற்கு '**FSDF**' என்ற மதிப்பைக் கொண்டுள்ளது:

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

(இணைப்பு Aயிலுள்ள, படம் 3ஐ பார்க்கவும்)

விசைப்பலகை நடை மதிப்புகளுடன் வரலாற்று அறிக்கையிடல்

BADBAZAAR களங்களின் WHOIS பதிவுகளில் விசைப்பலகை நடை மதிப்புகளின் மூலம், அது திபெத்திய அமைப்புகளை இலக்காகக் கொண்டு இயங்குவதாக வரலாற்று ரீதியாக TA413 கண்டுள்ளது. திபெத்திய அமைப்புகளை ஏமாற்றுபவர்கள் கட்டுப்பாட்டு டொமெய்ன்கள் "**asfasf**" என்று பதிவு செய்யப்பட்ட நிறுவன பெயரைப் பயன்படுத்துவதை Recorded Future கவனித்துள்ளது.

clublogs[.]com

Lookout கண்டுபிடித்த BADBAZAAR மாதிரிகளில் '**xle.clublogs[.]com'** என்ற C2 டொமெய்ன் பயன்படுத்தப்பட்டுள்ளது. **‘clublogs[.]com’** தளம் '**95.179.210[.]85'** என்ற IP முகவரியில் மற்றும் வழங்குநர் மதிப்பு **'CN=WIN-50QO3EIRQVP'** என்றும், மற்றும் SSL சான்றிதழையும் கொண்டிருந்தது. BADBAZAAR மாதிரிகளில் காணப்படும் SSL சான்றிதழ்களின் மதிப்புடன் இந்த மதிப்பு பொருந்தியது. SSL pinning என்பதைப் பயன்படுத்தி, தகவல்தொடர்புகளின் குறுக்கீட்டைத் தவிர்ப்பதற்காக இப்படி செய்யப்படுகிறது.

95.179.210[.]85 எனும் IP முகவரியில் எந்த தளங்கள் இயங்கின என்ற வரலாறு பின்வரும் களங்களைப் பட்டியலிடுகிறது:

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

(இணைப்பு Aயிலுள்ள, படம் 4ஐ பார்க்கவும்)

www.voiceoftibet[.]net

TA413 பயன்படுத்தும் TTP யைப் போன்ற '**www.voiceoftibet[.]net'** என்ற தளம் ‘திபெத்தின் குரல்' வானொலி நிலையம் போன்று தோற்றமளிக்கிறது.

முன்னர் அடையாளம் காணப்பட்ட BADBAZAAR டொமெய்ன்களின் WHOIS பதிவுகளில் காணப்படும் **'state'** மதிப்பு **'REWR'** ஐப் போன்று '**rewrwer[.]com**' என்ற டொமெய்ன் இருக்கிறது.

‘**clublogs[.]com**’, ‘**rewrwer[.]com**’, ‘**voiceoftibet[.]net**’ மற்றும் ‘**myloughborough[.]com**’ என்ற டொமெய்ன்கள் அனைத்தும் **'tplutalova@list[.]ru** என்ற மின்னஞ்சல் முகவரியுடன் பதிவு செய்யப்பட்டிருக்கின்றன**.**

actuallys[.]com

‘**actuallys[.]com**' டொமெய்னின் WHOIS பதிவுகளில் தொழில்நுட்ப மற்றும் நிர்வாகி மின்னஞ்சல் முகவரிகள் '**tplutalova@list[.]RU**' என்று குறிப்பிடப்பட்டாலும் பதிவு செய்தவரின் மின்னஞ்சல் '**ivan_s81@mail[.]ru** ஆகும்.

WHOIS இல் பதியப்பட்டுள்ள டொமெய்னுக்கான வரலாற்று தகவலில் '**actuallys[.]com**' பதிவு செய்யப்பட்ட மின்னஞ்சல் '**wangminghua6@gmail[.]com**' என்று 2016ஆம் ஆண்டு பிப்ரவரி 24 அன்று பட்டியலிடப்பட்டுள்ளது. மின்னஞ்சல் பின்னர் 2016ஆம் ஆண்டு மார்ச் 11 அன்று, '**ivan_s81@mail.ru**' என மாற்றப்பட்டது, இருப்பினும் பதிவாளர் பதிவு காலாவதி தேதி அப்படியே இருந்தது.

wangminghua6@gmail[.]com

மின்னஞ்சல் முகவரி '**wangminghua6@gmail[.]com** வரலாற்று அச்சுறுத்தல் புலனாய்வு அறிக்கையில் காணப்படும் களங்களை பதிவு செய்யப் பயன்படுத்தப்பட்டது. 2015 ஆம் ஆண்டில், இந்த மின்னஞ்சல் தீம்பொருளுக்கான C2 களங்களை பதிவு செய்யப் பயன்படுத்தப்படுகிறது என்று Cmstar Palo Alto அடையாளம் கண்டது. 2014 இல், APT3 ஆல் நடத்தப்பட்ட மின் தூண்டிலிடல் குறித்த பிரச்சாரங்களில் Mandiant அடையாளம் கண்ட டொமெய்ன்களைப் பதிவு செய்யவும் இது பயன்படுத்தப்பட்டது. 2013 ஆம் ஆண்டில், சீன எழுத்துக்களைக் கொண்ட நிரல் தரவுத் தள (PDB) பாதையுடன் தீம்பொருள் தரவிறக்கும் களங்களைப் பதிவு செய்ய இது பயன்படுத்தப்பட்டது என்று CrowdStrike கண்டறிந்தது. இது ஒரு சீன இயங்கு தளத்தில் உருவாக்கப்பட்டது என்பதைக் காட்டுகிறது.

taoyujun@gmail[.]com

'**hcjbtt[.]com**' என்ற டொமெய்ன் '**taoyujun@gmail[.]com**' என்ற மின்னஞ்சல் முகவரியுடன் பதிவு செய்யப்பட்டுள்ளது, ஆனால் அதன் நிர்வாகி மின்னஞ்சல் '**wangminghua6@gmail[.]com**' என்று பதிவு செய்யப்பட்டுள்ளது.

'**hcjbtt[.]com**' என்ற டொமெய்னுடன் எந்த தீங்கிழைக்கும் செயற்பாடும் இணைக்கப்படவில்லை , இருப்பினும் '**taoyujun@gmail[.]com**' என்ற மின்னஞ்சல் முகவரி அச்சுறுத்தல் புலனாய்வு அறிக்கைகளில் முன்னர் காணப்பட்டது. 2014 ஆம் ஆண்டில், ஜப்பானிய நிறுவனங்களைக் குறிவைக்கப் பயன்படுத்தப்படும் '**Cueisfry Trojan**' மாதிரிகளில், ஒரு டொமெய்னைப் பதிவு செய்ய இது பயன்படுத்தப்பட்டது என்பதை Mandiant கண்டறிந்தது.

இந்த மின்னஞ்சல் முகவரி '**iaea-international[.]org'** போன்ற டொமெய்ன்களையும் பதிவு செய்யப் பயன்படுத்தப்பட்டுள்ளது. அது, பன்னாட்டு அணுசக்தி முகமை '**idc-ctbto[.]org**' மற்றும் **CTBTO** என்ற

விரிவான அணு ஆயுத சோதனை தடை ஒப்பந்த அமைப்பின் **சர்வதேச தரவு மையம்** ஆகும்**.**

‘**iaea-international[.]org**’ டொமெய்னுக்கான WHOIS பதிவு, அதனைப் பதிவு செய்தவர் மின்னஞ்சல் ‘**wangminghua6@gmail[.]com**’ என்று முந்தைய பதிவு ஒன்றில் காட்டுகிறது.

udtglobals[.]com

‘**udtglobals[.]com**’ என்ற டொமெய்ன், அதன் நிர்வாகியின் மின்னஞ்சல் ‘**wangminghua6@gmail[.]com**’ என்றும், பதிவு செய்தவர் மின்னஞ்சல் ‘**ocean.nio@rediffmail[.]com**’ என்றும் பதிவு செய்துள்ளது அவதானிக்கப்பட்டது. இந்த டொமெய்னுக்கான பிற WHOIS பதிவுகள், அதே பதிவு செய்திருப்பவரின் மின்னஞ்சலைக் காட்டுகின்றன, ஆனால் நிர்வாகி மின்னஞ்சல் முகவரியை ‘**taoyujun@gmail[.]com**’ என்று காட்டுகிறது.

‘**udtglobals[.]com**’ என்பது, கடலுக்கடியில் பாதுகாப்பு மற்றும் பாதுகாப்பு சேவை வழங்கும் நிறுவனங்களுக்கான உலகளாவிய நிகழ்வான ‘**UDT Global**’ என்ற பெயரில் தோன்றியது. மின்னஞ்சல் முகவரியில் உள்ள **'ocean.nio**' என்ற பயனர் பெயர், பல நாடுகளில் உள்ள தேசிய கடல் சார் நிறுவனம் (**National Institute of Oceanography - NIO)** என்று போலியாக உருவாக்கப்பட்டிருக்கக்கூடும். ‘**Rediff**’ மின்னஞ்சல் சேவையின் பயன்பாடு இந்தியாவை அடிப்படையாகக் கொண்டது என்றாலும் இந்திய தேசிய கடல் சார் நிறுவனம் (**Indian National Institute of Oceanography**) போன்ற தோற்றத்தை அது கொடுக்கலாம்.

Djibdiplomatie[.]com

Djibouti இராஜதந்திர சேவை போன்று ‘**djibdiplomatie[.]com**’ என்ற டொமய்ன் தோற்றமளித்தது. இது ‘**utdglobals[.]com**’ ற்கு ஒத்த WHOIS பதிவைக் கொண்டிருந்தது**.** பதிவு செய்தவர் ‘**ocean.nio@rediffmail[.]com**’ என்று ஒரு பதிவு காட்டியது, மற்றும் நிர்வாகம் செய்பவர் என்று ‘**taoyujun@gmail[.]com**’ மின்னஞ்சல் பதிவாகியுள்ளது. ஆனால், வேறு பதிவுகளில் ‘**wangminghua6@gmail[.]com**’ பெயரில் டொமெய்ன் பதிவாகியுள்ளது, மற்றும் பதிவு செய்தவரின் மின்னஞ்சலாக ‘**ocean.nio@rediffmail[.]com**’ உள்ளது.

இந்த இரண்டு களங்களும் WHOIS பதிவுகளில் விசைப்பலகை நடை வகை மதிப்புகளைக் கொண்டிருந்தன. உதாரணமாக, '**udtglobals[.]com**' அதன் பதிவு நகரமாக 'ASDF' என்றும் ‘**djibdiplomatie[.]com**’ அதனை **'DAF DAGF'**

என்ற மதிப்புடனும் பதிவு செய்யப்பட்டுள்ளது. மற்றைய BADBAZAAR களங்களில் காணப்பட்ட மதிப்புகளுடன் இது ஒப்பிடத்தக்கது.

மின்னஞ்சல் முகவரிகள் '**wangminghua6@gmail[.]com**' மற்றும் '**taoyujun@gmail[.]com**' **உலகளாவிய கடலுக்கடியில் பாதுகாப்பு நிகழ்வு, Djibouti** இராஜதந்திர சேவைகள் மற்றும் **சர்வதேச அணுசக்தி நிறுவனம் போன்ற** டொமெய்ன்களுக்கான WHOIS பதிவுகளில் காணப்படுகின்றன, அவை பல தீங்கிழைக்காத டொமெய்ன்களுக்கான WHOIS பதிவுகளிலும் உள்ளன.

மாறுவேடம் போடும் களங்கள் மற்றும் தீங்கிழைக்காத களங்களின் கலவை, தீங்கிழைப்பவர்களின் செயல்பாடுகளை ஆதரிக்கப் பயன்படுத்தப்படும் உட்கட்டமைப்பு கொள்முதல் நிறுவனம் ஒன்று இயங்குவதைக் குறிக்கலாம்.

'**ocean.nio@rediffmail[.]com**' என்ற மின்னஞ்சல் முகவரி, மேலே விவரிக்கப்பட்ட மாறுவேடம் போடும் களங்களில் மட்டுமே காணப்படுகிறது. '**ivan_s81@mail[.]ru**' மற்றும் '**tplutalova@list[.]ru**' இரண்டும் மிகக் குறைந்த எண்ணிக்கையிலான டொமெய்ன்களைப் பதிவு செய்துள்ளது. மேலும், BADBAZAAR உட்கட்டமைப்பில் இந்த களங்களில் சில இயக்கப்படுகின்றன. இந்த மூன்று மின்னஞ்சல் முகவரிகளும் தீங்கிழைக்கும் சைபர் குற்றவாளிகளின் செயற்பாடுகளுடன் மிகவும் நெருக்கமாக இணைக்கப்பட்டுள்ளன என்று நம்பப்படுகிறது. ஏனென்றால், '**wangminghua6@gmail[.]com**' மற்றும் '**taoyujun@gmail[.]com**'. என்ற மின்னஞ்சல்களுடன் ஒப்பிடுகையில், அதிக எண்ணிக்கையிலான டொமெய்ன்கள் தீங்கிழைக்கும் செயல்பாட்டுடன் இணைக்கப்பட்டுள்ளன

(இணைப்பு Aயிலுள்ள, படம் 5ஐ பார்க்கவும்)

பிற அச்சுறுத்துபவர்களது இணைப்புகள்

BADBAZAAR உடன் இணைக்கப்பட்ட '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', மற்றும் '**voiceoftibet[.]net**' என்ற களங்களின் மற்றொரு பொதுவான பண்பு, அவர்கள் அனைவரும் eNom இல் '**255.255.255[.]254**' என்ற முகவரியில் பதிவு செய்யப்பட்டுள்ளார்கள்.

முந்தைய NCSC விசாரணைகளைத் தொடர்ந்து, இந்த குணாதிசயங்களைக் கொண்ட பிற களங்கள், 2019ஆம் ஆண்டில் **APT5** உடனும், 2009 ஆம் ஆண்டிற்கும் 2011ஆம் ஆண்டிற்கும் இடைப்பட்ட காலத்தில் **APT14** உடனும் இணைக்கப்பட்ட செயல்பாட்டை வெளிப்படுத்தின**.**

APT5- உடன் இணைக்கப்பட்ட டொமெய்ன்களில், பதிவு செய்தவரின் மின்னஞ்சல் '**taoyujun@gmail[.]com**' என்று WHOIS பதிவுகள் பட்டியலிடப்பட்டதாக வரலாறு இருக்கிறது.

APT14 உடன் இணைக்கப்பட்ட டொமெய்ன்களின் மூன்றெழுத்து துணை டொமெய்ன்கள் தீங்கிழைக்கும் செயல்பாடுகளின் நோக்கம் கொண்ட இலக்கைக் குறிக்கின்றன. இதற்கு '**bae.cisconline[.]net**' ஒரு உதாரணம். BAE Systemsஐ இலக்காகக் கொண்ட இணைப்புகள் '**Poison Ivy**' மாதிரியில் காணப்பட்டது.

இதேபோன்ற பண்பு BADBAZAAR களங்களில் காணப்படுகிறது, அங்கு துணை டொமெய்ன்கள், மறைந்திருந்து தாக்கும் ட்ரோஜன் ஆக்கப்பட்ட செயலியின் பெயருடன் தொடர்புடையவை:

செயலியின் பெயர்	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 மற்றும் APT14 தொடர்பான நடவடிக்கைகள் வரலாற்று ரீதியானவை என்பதையும், eNom உடன் **'255.255.255.254'** என பதிவு செய்யப்பட்ட பிற களங்கள் இருந்தாலும் அவை தீங்கிழைக்கும் செயல்பாட்டுடன் தொடர்பில்லாதவை என்பதையும் கவனத்தில் கொள்ள வேண்டும். எனவே இந்த பிரச்சாரங்களுக்குப் பின்னால் உள்ளவர்கள் ஒரே மாதிரியானவர்கள் அல்லது தொடர்புடையவர்கள் என்பது உறுதியாகத் தெரியவில்லை.

இயந்திர பெயர்கள்

SSL சான்றிதழ்களில் 'பொதுவான பெயர்' மதிப்பாகப் பயன்படுத்தப்படும் ஹோஸ்ட் பெயர்களை, BADBAZAAR C2s மற்றும் மாதிரிகளின் பகுப்பாய்வு வெளிப்படுத்தியது. இந்த ஹோஸ்ட் பெயர்கள் பல IP முகவரிகளில் பயன்படுத்தப்படுகின்றன என்பதை BADBAZAAR மாதிரிகள் மற்றும் உட்கட்டமைப்பில் காணப்பட்ட ஹோஸ்ட் பெயர்கள் குறித்த NCSC விசாரணைகள் காட்டின. BADBAZAAR மாதிரிகளில் காணப்படும்

டொமெய்ன்களை இந்த IP முகவரிகள் ஹோஸ்டிங் செய்கின்றன. கீழேயுள்ள பகுதியில், BADBAZAAR C2 களங்களை ஹோஸ்ட் செய்யும் ஹோஸ்ட்பெயர் மற்றும் IP முகவரிகள் பற்றி கூடுதல் விவரங்கள் உள்ளன.

ஏறக்குறைய எல்லா சந்தர்ப்பங்களிலும், ஹோஸ்ட்பெயர் மதிப்புடன் சான்றிதழ்களின் இருப்பு குறிப்பிடப்பட்ட தீங்கிழைக்கும் டொமெய்ன் பெயர்களுக்கான IP முகவரித் தீர்மான நெறிமுறையில் ஒன்றுடன் ஒன்று பின்னிப் பிணைந்துள்ளது. இருந்தாலும் அப்படி இல்லாத சில நிகழ்வுகள் கோடிட்டுக் காட்டப்பட்டுள்ளன.

WIN-EU0VLBL7TUJ

'**WIN-EU0VLBL7TUJ**' என்ற ஹோஸ்ட் பெயர் பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- '**uyapkfinder[.]com**' மற்றும் '**thewestuniverse[.]com**' என்ற BADBAZAAR C2 டொமெய்ன்களை '**116.203.53[.]21**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 கொண்ட '**adysfunction[.]com'** என்ற டொமெய்ன் மற்றும் '**download.apkbazar[.]biz**' என்ற துணைடொமெய்னை '**95.216.169[.]27**' ஹோஸ்ட் செய்தது. அங்கு BADBAZAAR மாதிரிக்கான தரவிறக்க இணைப்பு காணப்பட்டது.

(இணைப்பு Aயிலுள்ள, படம் 6ஐ பார்க்கவும்)

WIN-70E59JVOB9G

'**WIN-70E59JVOB9G**' என்ற ஹோஸ்ட் பெயர் பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- BADBAZAAR C2 துணை டொமெய்ன்கள், **'aua.rondwsign[.]com', 'nal.tokenmajorp[.]com', 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**', மற்றும் **'pls.rondwsign[.]com'** என்பவற்றை '**23.88.28[.]220**' ஹோஸ்ட் செய்தது. இயந்திரத்தின் சான்றிதழ் கடைசியாக காணப்பட்டதற்கும், தீங்கிழைக்கும் களங்கள் முதன் முறையாக குறிப்பிட்ட IPற்குத்

தீர்க்கப்படுவதைக் காண்பதற்குமிடையில் இரண்டு நாள் இடைவெளி இருந்தது.

- BADBAZAAR துணை டொமெய்ன், '**bt.bhvghg[.]com**' என்பதை '**23.88.28[.]221**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 டொமெய்ன்கள், '**tubevideoplus[.]org**' மற்றும் '**cde.mpoxcases[.]com**' என்பவற்றை '**23.88.28[.]222**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன் '**bat.androidupdated[.]net**' என்பதை '**65.21.92[.]67**' ஹோஸ்ட் செய்தது. இது, DoubleAgent தீம்பொருள் C2 கொண்ட துணை டொமெய்ன் '**apps.androidupdated[.]net**' என்பதை உள்ளடக்கியது.

- BADBAZAAR C2 துணை டொமெய்ன்கள், '**wyo.titeperformance[.]com**', '**big.collinformations[.]com**' '**vpf.titeperformance[.]com**', '**eud.titeperformance[.]com**' மற்றும் '**afg.collinformations[.]com**' என்பவற்றை '**65.21.92[.]77**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள், '**upd.whoscaller.net**'. மற்றும் '**ggl.whoscaller[.]net**' என்பவற்றை '**65.108.192[.]134**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள், '**bvn.lookincategory[.]com'** மற்றும் '**edr.lookincategory[.]com'** என்பவற்றை '**142.132.131[.]15**' ஹோஸ்ட் செய்தது. இயந்திரத்தின் சான்றிதழ் கடைசியாக காணப்பட்டதற்கும், தீங்கிழைக்கும் களங்கள் முதன் முறையாக குறிப்பிட்ட IPற்குத் தீர்க்கப்படுவதைக் காண்பதற்குமிடையில் பதினொரு நாட்கள் இடைவெளி இருந்தது.

- '**142.132.131[.]20**' ஹோஸ்ட் செய்த துணை டொமெய்ன்கள் '**son.onlinegamersgroup[.]com**' மற்றும் '**system.onlinegamersgroup[.]com'**, என்பன **BADBAZAAR** C2 என நம்பப்படுகின்றன. ஏனென்றால் BADBAZAAR உடன் தொடர்புடைய SSL சான்றிதழ்கள் அந்த IP முகவரியில் காணப்பட்டன.

- BADBAZAAR C2 டொமெய்ன் '**goldplusapp[.]net**' மற்றும் துணை டொமெய்ன்கள் '**who.goldplusapp[.]net**' மற்றும் '**cgf.goldplusapp[.]net**' என்பவற்றை '**142.132.131[.]28'** ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள் '**oha.alpinemap[.]net**', '**aru.alpinemap[.]net'**, '**aso.alpinemap[.]net**', '**afr.alpinemap[.]net**', மற்றும் '**aar.alpinemap[.]net**'. என்பவற்றை '**162.55.103[.]211**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள் **'pep.rondwsign[.]com', 'ckp.jkiohreh[.]com', 'aar.tokenmajorp[.]com', 'nal.tokenmajorp[.]com', 'pls.rondwsign[.]com'** மற்றும் **'aua.rondwsign[.]com'** என்பவற்றை '**162.55.103[.]212**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள் '**ggl.whoscaller[.]net**' மற்றும் '**upd.whoscaller.net**' என்பவற்றை'**195.154.47[.]99**' ஹோஸ்ட் செய்தது. இயந்திரத்தின் சான்றிதழ் கடைசியாக காணப்பட்டதற்கும், தீங்கிழைக்கும் களங்கள் முதன் முறையாக குறிப்பிட்ட IPற்குத் தீர்க்கப்படுவதைக் காண்பதற்குமிடையில் மூன்று நாட்கள் இடைவெளி இருந்தது.

- BADBAZAAR C2 துணை டொமெய்ன் '**upd.whoscaller[.]net**' என்பதை '**195.154.60[.]3**' ஹோஸ்ட் செய்தது.
'**ggl.whoscaller[.]net**'.

- BADBAZAAR C2 துணை டொமெய்ன்கள் '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' மற்றும் '**afg.collinformations[.]com**' என்பவற்றை '**212.83.189[.]89**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 டொமெய்ன்கள் '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**' '**luj.lookincategory[.]com**' மற்றும் '**bvn.lookincategory[.]com**' என்பவற்றை '**212.129.21[.]168**' ஹோஸ்ட் செய்தது.

(இணைப்பு Aயிலுள்ள, படம் 7ஐ பார்க்கவும்)

WIN-50QO3EIRQVP

'**WIN-50QO3EIRQVP**' என்ற ஹோஸ்ட்பெயர் பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- டொமெய்ன்கள் '**yumoftion[.]com**' மற்றும், '**androidupdated[.]net**' என்பவற்றை '**45.76.132[.]91**' ஹோஸ்ட் செய்தது. இரண்டு களங்களும் BADBAZAAR உடன் துணை டொமெய்ன்களாக இணைக்கப்பட்டுள்ளன. '**fow.yumoftion[.]com**' மற்றும் '**bat.androidupdated[.]net**' என்பன BADBAZAAR C2 டொமெய்ன்கள் ஆகும். கூடுதலாக, துணை டொமெய்ன் '**apps.androidupdated[.]net**' என்பது DoubleAgent C2 டொமெய்ன். இது '**pmstwocqn[.]com**' என்ற டொமெய்னையும் ஹோஸ்ட் செய்கிறது. இது WHOIS பதிவுகள் BADBAZAAR உடன் இணைக்கப்பட்டுள்ளது.

- '**95.179.210[.]85**' என்ற முகவரி, '**clublogs[.]com**' என்பதை ஹோஸ்ட் செய்தது, அதில் '**xle.clublogs[.]com**' என்பது BADBAZAAR C2 டொமெய்ன். மற்றும், BADBAZAAR C2 டொமெய்ன்கள் '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' மற்றும் '**actuallys[.]com**' என்பவற்றையும் ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 துணை டொமெய்ன்கள் அமைந்திருக்கும் '**titeperformance[.]com**', மற்றும் '**collinformations[.]com'** என்ற டொமெய்ன்களை '**199.247.21[.]34**' ஹோஸ்ட் செய்தது.

- BADBAZAAR C2 டொமெய்ன்'**uyghurdict[.]com**' என்பதை '**217.69.10[.]128**' ஹோஸ்ட் செய்தது.

(இணைப்பு Aயிலுள்ள, படம் 8ஐ பார்க்கவும்)

WMSvc-WIN-50QO3EIRQVP

ஹோஸ்ட்பெயர் '**WMSvc-WIN-50QO3EIRQVP**' பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- BADBAZAAR C2 டொமெய்ன் **'groupgram[.]org'** என்பதை **'78.46.185[.]251'** ஹோஸ்ட் செய்தது என்றும் port 4432 வழியாக தீங்கிழைக்கும் தொடர்புகளை ஏற்படுத்துவதாகவும் Volexity அறிக்கையிட்டுள்ளது.

- BADBAZAAR C2 டொமெய்ன் **'widelygram[.]org'** என்பதை **'65.21.92[.]69'** மற்றும் **'163.172.205[.]207'** ஹோஸ்ட் செய்தன, இரண்டிலும் port 4432 திறந்திருக்கக் காணப்பட்டது.

- BADBAZAAR C2 டொமெய்ன் **'maxgram[.]org'** என்பதை **'163.172.198[.]206'**, ஹோஸ்ட் செய்தது, port 4432 திறந்திருக்கக் காணப்பட்டது.

(இணைப்பு Aயிலுள்ள, படம் 9ஐ பார்க்கவும்)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

'**WMSvc-WIN-50QO3EIRQVP**' மற்றும் '**WIN-7LSBB9R0F1L**' என்ற ஹோஸ்ட்பெயர் பின்வரும் IP முகவரியில் ஒரே நேரத்தில் காணப்பட்டன:

- BADBAZAAR C2 டொமெய்ன்கள் '**flygram[.]org**' மற்றும் '**groupgram[.]org**' என்பவற்றை '**148.251.87[.]245**' ஹோஸ்ட் செய்தது.

(இணைப்பு Aயிலுள்ள, படம் 10ஐ பார்க்கவும்)

WIN-N8H8S9BG2P0

ஹோஸ்ட் பெயர் '**WIN-N8H8S9BG2P0**' பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- BADBAZAAR C2 டொமெய்ன்கள் '**omarwhatsapp[.]org**' மற்றும் '**flygram[.]org**' என்பவற்றை '**148.251.87[.]247**' ஹோஸ்ட் செய்தது.

(இணைப்பு Aயிலுள்ள, படம் 11ஐ பார்க்கவும்)

WIN-I6VBN8MR92A

ஹோஸ்ட் பெயர் '**WIN-I6VBN8MR92A**' பின்வரும் IP முகவரிகளில் காணப்பட்டது:

- BADBAZAAR C2 டொமெய்ன் **tryhrwserf[.]com**' என்பதை '**148.251.87[.]197**' ஹோஸ்ட் செய்தது.

(இணைப்பு Aயிலுள்ள, படம் 12ஐ பார்க்கவும்)

கிடைக்கக்கூடிய வர்த்தக தரவுகளின் அடிப்படையில், இந்த இயந்திரப் பெயர்கள் இணையத்தில் காணப்படும் அளவு மாறுபடுகின்றது. அவற்றில் சில, பல IP முகவரிகளில் ஒரே நேரத்தில் இயங்குகின்றன. ஒரே 'மாதிரி அமைப்பிலிருந்து' மெய்நிகர் இயந்திரங்கள் (VMகள்) உருவாக்கப்படுவதை இது குறிக்கிறது. கவனிக்கப்பட்ட சில ஹோஸ்ட் பெயர்களுடன் தொடர்புடைய அனைத்து IPக்களும் தீங்கிழைக்கும் செயல்பாட்டுடன் இணைக்கப்பட முடியாது என்பதை கவனத்தில் கொள்ளவும். இந்த ஹோஸ்ட் பெயர்களின் பயன்பாடு, அச்சுறுத்துபவர்களுக்குப் பிரத்தியேகமானது அல்ல என்று இதை அர்த்தப்படுத்தலாம்.

இருப்பினும், BADBAZAAR C2 களங்களை ஹோஸ்ட் செய்த IP களில் இந்த இயந்திர பெயர்களில் சில பரவலாகக் காணப்படுவது, தீங்கிழைப்பவர்களின் இணைய செயல்பாடுகளை ஆதரிக்க இயந்திரங்களை உள்ளமைக்க உட்கட்டமைப்பு கொள்முதல் நிறுவனம் பயன்படுத்தப்படுகிறது என்று ஊகிக்கலாம்.

சமூக ஊடக இருப்பு

(தீங்கிழைக்கும் செயலிகளின் பயன்பாட்டை ஊக்குவிக்கும்) YouTube வீடியோக்கள், தீங்கிழைப்பவர்களால் உருவாக்கப்பட்டவை என்பதை Volexity வெளியிட்ட முந்தைய அறிக்கை, காட்டியது. இந்த வீடியோக்களில், உருவாக்கப்பட்ட செயலிகளை எவ்வாறு பயன்படுத்துவது என்பது குறித்த பயிற்சிகள் இருந்தன.

அச்சுறுத்துபவர்களின் நடவடிக்கைகளுடன் தொடர்புடைய இரண்டு கூடுதல் YouTube சேனல்களை NCSC கண்டுபிடித்துள்ளது. '**@josephjoey3499**' என்பவரின் YouTube சேனல் **Maxgram**' என்ற செயலியை ஊக்குவிப்பதாகத் தோன்றியது. அத்துடன், '**@uyghurapks3096**' என்பவருடன் பதிவு

செய்யப்பட்ட கூடுதல் சேனல் '**Uyghur APK Finder**' என்ற செயலியை பயன்படுத்த ஊக்குவிக்கிறது.

கூடுதலாக, '**Flygram**' மற்றும் '**Signal Plus**' ஆகியவற்றை விளம்பரப்படுத்தும் YouTube வீடியோக்களில், அச்சுறுத்துபவர்கள் தொலைபேசி எண்களைப் பயன்படுத்துவதைக் காணக்கூடியதாக இருந்தது. '**Flygram**' வீடியோவில், நேரம் 0:36 என்று இருக்கும் போது, '**+1 (570) 378-7250**' என்ற தொலைபேசி எண் தெரியும், அதே போல் '**Signal Plus**' வீடியோவில் தொலைபேசி எண் '**+1 (267) 298 4259**' என்று வெளிப்படும்.

ஒரு போலி திபெத்-கருப்பொருள் செய்தித் தளமான '**ignitetibet[.]net**' மிரட்டுபவர்களால் இயக்கப்படுவதாகவும், பாதிக்கப்படுபவர்களை அவர்கள் Telegram சேனல்களில் கண்டுபிடிக்கிறார்கள் என்றும் Volexity அறிக்கையிட்டுள்ளது. '**choekyi.wangmo@ignitetibet[.]net**' என்ற மின்னஞ்சல் முகவரி, '**tibetone.org**' என்ற பக்கத்திலுள்ள இடுகைகளில் பின்னூட்டங்களை இடுவதைக் காண முடிகிறது. இது, iOS திரிபிற்காகப் பயன்படுத்தப்படும் BADBAZAAR C2 பக்கம் என்று Lookout பகிரங்கமாக அறிவித்துள்ளது.

இந்த மின்னஞ்சல் முகவரி, '**Choekyi Wangmo**' என்ற ஆளுமை என்பதைப் போல ஏமாற்றுபவர்கள் பயன்படுத்துவதாக நம்பப்படுகிறது.

மதிப்பீடு

BADBAZAAR மற்றும் MOONSHINE இரண்டும், குறிப்பாக உய்குர், தைவானிய மற்றும் திபெத்திய குழுக்களைக் குறி வைக்க, பல சமூக பொறியியல் முறைகளைப் பயன்படுத்துகின்றன. அதாவது:

- இந்த சமூகங்களுக்கு ஆர்வமுள்ள செயலிகளில் மறைந்திருந்து தாக்கக்கூடிய, உய்குர் மொழி குர்ஆன் செயலி போன்றவை, கிட்டத்தட்ட நிச்சயமாக இலக்கு வைத்து பாதிக்கப்பட்டவர்களுக்கு ஏற்ற வகையில் வடிவமைக்கப்பட்டுள்ளது.
- உத்தியோக பூர்வ app storeகளில், இப்படி மறைத்து வைக்கப்பட்டுள்ள செயலிகளை சேர்ப்பதன் மூலம், அவை சட்டபூர்வமானவை என்ற உணர்வை அளிக்கிறது. மேலும் குழு அரட்டைகளில் அது குறித்துப் பகிர்வதன் மூலம், இந்த சமூகங்களுக்குள் நம்பகத்தன்மையை உருவாக்கி, அவர்களை சுரண்டுவதை நோக்கமாகக் கொண்டுள்ளது

BADBAZAAR மற்றும் MOONSHINE ஆகியவை சேகரிக்கும் தரவுகள் நிச்சயமாக சீன அரசுக்கு மதிப்பு மிக்கதாக இருக்கும். BADBAZAAR மற்றும் MOONSHINE ஆகியவை உய்குர், திபெத்திய மற்றும் தைவானியர்களைக் குறிவைத்துள்ளதாகப் பார்க்கப்பட்டாலும், சீனாவில் உள்ள பிற சிறுபான்மை குழுக்களை குறி வைக்கும் பிற தீம்பொருள்களும் உள்ளன. ஆட்சி நிலைத் தன்மையை அச்சுறுத்தும் காரணங்களை ஆதரிப்பதாகக் கருதப்படும் சீனா மற்றும் வெளிநாடுகளில் உள்ள co-sealing நாடுகளின் குடிமக்கள், BADBAZAAR மற்றும் MOONSHINE போன்ற மொபைல் தீம்பொருட்களால் நிச்சயமாக அச்சுறுத்தலுக்கு உள்ளாகியுள்ளனர். இருப்பிடம், ஆடியோ மற்றும் புகைப்படத் தரவைப் பிடிக்கும் திறன், கண்காணிக்கப்படுபவரின் செயல்பாடு குறித்த நிகழ்நேர தகவல்களை வழங்குவதன் மூலம் எதிர்காலத்தில், கண்காணிப்பு மற்றும் துன்புறுத்தல் நடவடிக்கைகளுக்கு வாய்ப்பளிக்கிறது.

MITRE ATT&CK®

சைபர் தாக்குதல்கள் மற்றும் ஊடுருவல்களை வகைப்படுத்துவதற்கும் விவரிப்பதற்கும் ஒரு வழிகாட்டுதலாக இருக்கும், நடைமுறை உலக அவதானிப்புகளை அடிப்படையாகக் கொண்ட எதிரி தந்திரோபாயங்கள் மற்றும் நுட்பங்களின் உலகளவில் அணுகக்கூடிய அறிவுத் தளமான MITRE ATT&CK® கட்டமைப்பைப் பயன்படுத்தி இந்த அறிக்கை தொகுக்கப்பட்டுள்ளது.

உத்தி	அடையாளம்	நுட்பம்	செயல்முறை
ஆய்வு	T1593. 001	திறந்த தேடல் வலைத்தளங்கள் / களங்கள்: சமூக ஊடகம்	தீம்பொருளைப் பகிரும் நோக்குடன் ஆன்லைன் குழுக்கள் மற்றும் மன்றங்களில் பாதிக்கப்படக்கூடியவர்களை, தீங்கிழைப்பவர்கள் அடையாளம் காண்கிறார்கள்
வள மேம்பாடு	T1583.001	உள்கட்டமைப்பைப் பெறுதல்: டொமெய்ன்கள்	ஏமாற்றுபவர்கள் தங்கள் கட்டளை மற்றும் கட்டுப்பாட்டு சேவையகங்களுக்காக (C2) டொமெய்ன்களைப் பதிவு செய்கிறார்கள்
வள மேம்பாடு	T1587.001	திறன்களை வளர்த்துக் கொள்ளுங்கள்: தீம்பொருள்	சட்டபூர்வமாக பதிவிறக்கம் செய்யக்கூடிய செயலிகளுக்குள் இந்த தீங்கிழைக்கும் செயல்பாடுகள் மறைத்து வைக்கப்பட்டுள்ளன.
வள மேம்பாடு	T1608.001	மேடை திறன்கள்: தீம்பொருளைப் பதிவேற்றல்	ட்ரோஜன் செய்யப்பட்ட செயலிகள் App Storeகள் உள்ளிட்ட ஆன்லைன் தளங்களில் பதிவேற்றப்படுகின்றன
வள மேம்பாடு	T1585.001	கணக்குகளை நிறுவுதல்: சமூக ஊடக கணக்குகள்	தீம்பொருளைப் பகிரவும் விளம்பரப்படுத்தவும் தீங்கிழைப்பவர்கள் வலைத்தளங்கள் மற்றும் சமூக ஊடகங்களில் கணக்குகளை உருவாக்குகிறார்கள்

வள மேம்பாடு	T1585.002	கணக்குகளை நிறுவுதல்: மின்னஞ்சல் கணக்குகள்	தீம்பொருளை ஹோஸ்ட் செய்வதற்கும் பகிர்வதற்கும் தீங்கிழைப்பவர்கள் தனிப்பட்ட முறையில் ஹோஸ்ட் செய்யப்பட்ட மற்றும் வணிக மின்னஞ்சல் கணக்குகளைப் பயன்படுத்துகின்றனர்
ஆரம்ப அணுகல்	T1189	சமரசம்	தீங்கிழைக்கும் குறியீடுகள் முறையான செயலிகளில் மறைக்கப்பட்டு App Storeகளில் பதிவேற்றப்படுகின்றன
ஆரம்ப அணுகல்	T1566.003	Phishing எனப்படும் மின் தூண்டிலிடல் சேவைகள் வழியாக மின் தூண்டிலிடல்	Telegram உள்ளிட்ட சமூக ஊடகங்கள் வழியாக இலக்கு வைக்கப்பட்ட குழுக்களுக்கு, ட்ரோஜன் செய்யப்பட்ட செயலிகளை தீங்கிழைப்பவர்கள் அனுப்புகிறார்கள்
நிறைவேற்றுதல்	T1204.002	பயனர் நிறைவேற்றுதல்: தீங்கிழைக்கும் கோப்பு	தீங்கிழைக்கும் செயலியை பாதிக்கப்பட்டவர்கள் இயக்குவதற்கு, முதலில் மறைந்திருந்து தாக்கும் (ட்ரோஜன் செய்யப்பட்ட) செயலிகளை அவர்களது சாதனத்தில் நிறுவ வேண்டும்
பாதுகாப்பு தவிர்ப்பு	T1027.009	குழப்பமான கோப்புகள் அல்லது தகவல்: உட்பொதிக்கப்பட்ட தீங்கிழைக்கும் செயலிகள்	தீங்கிழைக்கும் குறியீடுகள் முறையான செயலிகளில் மறைக்கப்பட்டிருக்கும்.
பாதுகாப்பு தவிர்ப்பு	T1036.005	**மாறுவேடம் போடுதல்:** முறையான பெயர் அல்லது இடத்தைப் பயன்படுத்தல்	ட்ரோஜன் செய்யப்பட்ட கோப்புகள் முறையான செயலிகளின் பெயர், தோற்றம் மற்றும் செயல்பாட்டுடன் பொருந்துகின்றன.
பாதுகாப்பு தவிர்ப்பு	T1656	ஆள்மாறாட்டம்	முகப்பு வலைத் தளங்களை உருவாக்குவதன் மூலமும், இலக்கு வைக்கப்பட்ட குழுக்களுடன் தொடர்புடைய பயனர் பெயர்களைப் பயன்படுத்துவதன் மூலமும்

			தீங்கிழைப்பவர்கள் நம்பகமானவர்களைப் போல ஆள்மாறாட்டம் செய்கிறார்கள்
தொகுப்பு	T1123	ஆடியோ பிடிப்பு	ட்ரோஜன் செய்யப்பட்ட செயலிகள் ஒலிவாங்கி அணுகல் உள்ளிட்ட தேவையற்ற அனுமதிகளைக் கோரலாம்
தொகுப்பு	T1125	வீடியோ பிடிப்பு	ட்ரோஜன் செய்யப்பட்ட செயலிகள் கமரா அணுகல் உள்ளிட்ட தேவையற்ற அனுமதிகளைக் கோரலாம்
தொகுப்பு	T1005	உள்ளூர் அமைப்பிலிருந்து தரவு	ட்ரோஜன் செய்யப்பட்ட செயலிகள் உள்ளூர் கோப்புகள் உட்பட தேவையற்ற அனுமதிகளைக் கோரலாம்.
கட்டளை மற்றும் கட்டுப்பாடு	T1071.001	பயன்பாட்டு அடுக்கு நெறிமுறை: வலை நெறிமுறைகள்	HTTPS மற்றும் WebSocket ஐப் பயன்படுத்தி தீம்பொருள் C2 உடன் இணைகிறது.
கட்டளை மற்றும் கட்டுப்பாடு	T1509	தரமற்ற வழி	port 4432 மற்றும் 2333 போன்ற தரமற்ற வழிகள் பயன்படுத்தப்படுகின்றன
ஊடுருவல்	T1041	C2 சேனல் வழியாக வெளியேற்றம்	HTTPS மற்றும் WebSocket இணைப்புகளைப் பயன்படுத்தி தீம்பொருள் தரவை வெளியே அனுப்புகிறது.
தாக்கம்	T1565.002	தரவு கையாளுதல்: அனுப்பப்பட்ட தரவைக் கையாளுதல்	செயலியின் செயல்பாட்டிற்கு அவசியமில்லாத செயலியின் வலை போக்குவரத்தை இயக்குவதன் மூலம் பாதிக்கப்பட்டவர்களிடமிருந்து தீங்கிழைப்பவர்கள் தரவைப் பெறுகிறார்கள்

குறிகாட்டிகள்

MOONSHINE:

- VLiteUI பலகைகளுக்கான தேடல், 2025ஆம் ஆண்டு ஏப்ரல் 1 அன்று நடத்தப்பட்ட போது, பின்வரும் தரவுகள் கிடைத்தன:

IP முகவரி	வழி	முதலில் பார்த்தது	கடைசியாகப் பார்த்தது
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

- SCOTCH ADMIN பலகைகளுக்கான தேடல், 2025ஆம் ஆண்டு ஏப்ரல் 1 அன்று நடத்தப்பட்ட போது, பின்வரும் தரவுகள் கிடைத்தன:

IP முகவரி	வழி	முதலில் பார்த்தது	கடைசியாகப் பார்த்தது
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

- மெய்நிகர் SCOTCH ADMIN பலகைகளுக்கான தேடல், 2024ஆம் ஆண்டு மார்ச்14 அன்று நடத்தப்பட்ட போது, பின்வரும் தரவுகள் கிடைத்தன:

களம்	**IP** முகவரி
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:

விளக்கம்	**BADBAZAAR C2s இல் காணப்பட்டSSL சான்றிதழ்**
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- மேலே உள்ள BADBAZAAR சான்றிதழுக்கான தேடல், 2025ஆம் ஆண்டு ஏப்ரல் 1 அன்று நடத்தப்பட்ட போது, பின்வரும் தரவுகள் கிடைத்தன:

IP முகவரி	வழி	முதலில் பார்த்தது	கடைசியாகப் பார்த்தது
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

விளக்கம்	BADBAZAAR C2s-இல் காணப்பட்ட SSL சான்றிதழ்
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- மேலே உள்ள BADBAZAAR சான்றிதழுக்கான தேடல், 2025ஆம் ஆண்டு ஏப்ரல் 1 அன்று நடத்தப்பட்ட போது, பின்வரும் தரவுகள் கிடைத்தன:

IP முகவரி	வழி	முதலில் பார்த்தது	கடைசியாகப் பார்த்தது
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 டொமெய்ன்கள்

BADBAZAAR C2 டொமெய்ன்களில் அவதானிக்கப்பட்டவற்றுடன் பொருந்தக்கூடிய மதிப்புகளைக் கொண்ட WHOIS பதிவுகளைக் கொண்ட டொமெய்ன்களின் அட்டவணை கீழே தரப்பட்டுள்ளது.

WHOIS மதிப்பு	டொமெய்ன்கள்
பதிவு செய்யும் மாநிலம்: UJYJYUJ **பதிவு செய்த நாடு: பொலிவியா** **பதிவாளர்: 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
பதிவு செய்யும் மாநிலம்: REWR **பதிவு செய்த நாடு: CF** **பதிவாளர்: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com

	• tooenabled[.]com • suguestions[.]com • searching2[.]com
பதிவு செய்யும் மாநிலம்: FSDF **பதிவு செய்த நாடு: AL** **பதிவாளர்: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

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

BADBAZAAR மற்றும் MOONSHINE உடன் தொடர்புடைய indicators of compromise என்ற சமரசக் குறிகாட்டிகளுக்கான (IoCs) இணைப்புகள் கீழே தரப்பட்டுள்ளது இந்த இணைப்புகளில் உள்ள அனைத்து தகவல்களின் உண்மைத் தன்மையை NCSC உறுதிப்படுத்த முடியாது, அத்துடன் அவற்றின் துல்லியம் மற்றும் அவை பொருத்தமானவையா என்பதை சுயாதீனமாக சரிபார்க்க வாசகர்கள் அறிவுறுத்தப்படுகிறார்கள்:

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity

- Citizen Lab

தணிப்பு நடவடிக்கை

விரிவான ஆய்வுகளில் விவரிக்கப்பட்டுள்ள அச்சுறுத்தல்களுக்கு எதிராகப் பாதுகாக்க கீழே உள்ள பரிந்துரைகளை ஏற்று நடப்பதை NCSC ஊக்குவிக்கிறது.

- **மூன்றாம் தரப்பு App Storeகள் உட்பட App store இயக்குனர்கள் மற்றும் செயலிகளைத் தயாரிப்பவர்கள் தங்கள் மேடையில் உள்ள செயலிகள் பாதுகாப்பானவை என்பதையும், அவை அரசின் நடைமுறைக் கோட்பாட்டிற்கு இணங்குவதையும் உறுதி செய்ய வேண்டும்.**
  இந்த வழிகாட்டலைப் பார்க்கவும்:
  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

- **பன்மொழி ஆதரவு:** உய்குர், திபெத்திய, தைவானிய ஹொக்கியன் மற்றும் கான்டோனீஸ் உள்ளிட்ட, இலக்கு வைக்கப்படும் சிறுபான்மை மொழிகளைப் பேசும் குழுக்களிடையே பயனர்களுக்கு பிரபலமான செயலிகளை உள்ளூர் மயமாக்கும் முயற்சிகளில் செயலிகளை உருவாக்குபவர்கள் முதலீடு செய்ய வேண்டும். செயலிகளை உள்ளூர் மயமாக்குவதற்கான Apple நிறுவனத்தின் வழிகாட்டுதல்:
  https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. செயலிகளை மொழிபெயர்ப்பதற்கான Google வழிகாட்டல்:
  https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **உங்கள் சமூக ஊடக தளத்தை பாதுகாப்பாக வைத்திருத்தல்:** தீங்கிழைப்பவர்கள் போலிக் கணக்குகளை உருவாக்குவதற்கும் மற்றும் தீங்கிழைக்கும் கோப்புகள் அல்லது இணைப்புகளை தங்கள் தளங்களில், முறையான ஆன்லைன் சமூகங்களில் பகிர்வதை சமூக ஊடக நிறுவனங்கள் மிகவும் கடினமாக்கலாம். சாத்தியமானால், அச்சுறுத்தல் பற்றிய கூட்டு புரிதலை மேம்படுத்துவதற்கும் பாதுகாப்பு நடவடிக்கைகளுக்கு உதவுவதற்கும் நிறுவனங்கள் தீங்கிழைக்கும் குறிகாட்டிகளை பரந்த தொழில் துறையுடன் பகிர்ந்து கொள்ள வேண்டும்.

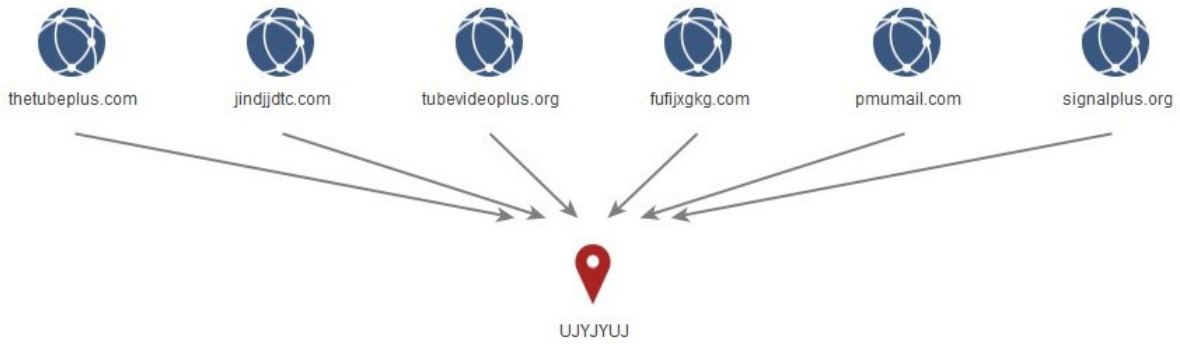
- **வாடிக்கையாளர்களுக்கான பரிகார திட்டம்:** நிறுவனங்கள் தங்கள் சேவைகளைப் பயன்படுத்தி தீங்கிழைக்கும் செயலிகளை நிறுவிய வாடிக்கையாளர்களை எச்சரிக்கவும் அது குறித்து அறிவிக்கவும் நடைமுறைகளைக் கொண்டிருக்க வேண்டும். இந்த விழிப்பூட்டல்கள் கவனத்தை ஈர்க்கும் வகையிலும் மேலதிக தகவல்களைப் பகிரும் வகையிலும் அமைந்திருக்க வேண்டும். தேவையான இடங்களில், நிறுவனங்கள் அந்த மென்பொருளை எப்படி நீக்குவது என்பதைப் பற்றிய வழிகாட்டுதலையும், பாதிக்கப்பட்டவர்கள் தங்கள் அதிகாரிகளிடம் -உதாரணத்திற்கு, இங்கிலாந்திலுள்ள NCSC போன்றவை- புகாரளிக்க வேண்டும் என்பதையும் ஊக்குவிக்க வேண்டும்.

- **ஒத்துழைப்புகான பணிக குழுகள:** சமூக ஊடக நிறுவனங்கள பணிக் குழுக்களை உருவாக்கலாம், அந்தந்த பாதுகாப்புக் குழுக்கள் தீங்கிழைக்கும் குறிகாட்டிகள், TTPக்கள் மற்றும் அவர்கள் அவதானித்தவற்றை பகிர்ந்து கொள்ள அனுமதிக்கின்றன, இதனால் தீங்கிழைப்பவர்கள் அந்தத் தளங்களைப் பயன்படுத்துவது மிகவும் கடினமாக்கப்படும்.

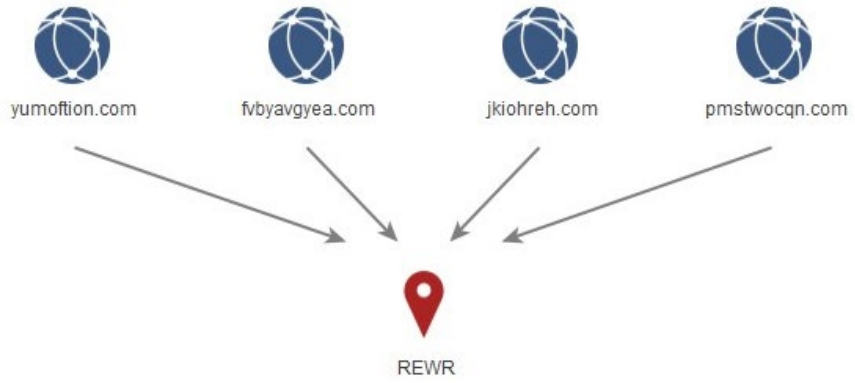
- **மாற்றப்பட்ட செயலிகளைக் கண்டறிதல்:** சாத்தியமான இடங்களில், செயலிகளைத் தயாரிப்பவர்கள் தீங்கிழைக்கும் நகல்களிலிருந்து பாதுகாக்க உதவும் வகையில், செயலியின் 'அதிகாரப்பூர்வமற்ற' பதிப்பைப் பதிவிறக்கியிருந்தால், பயனருக்குத் தெரிவிக்கும் செயல்பாட்டைச் சேர்க்க வேண்டும்.

பின் இணைப்பு A: BADBAZAAR WHOIS தொகுப்புகள் / டொமெய்ன் தரகர் தகவலின் வரைபடங்கள்

படம் 1 - 'UKYJYUUJ'

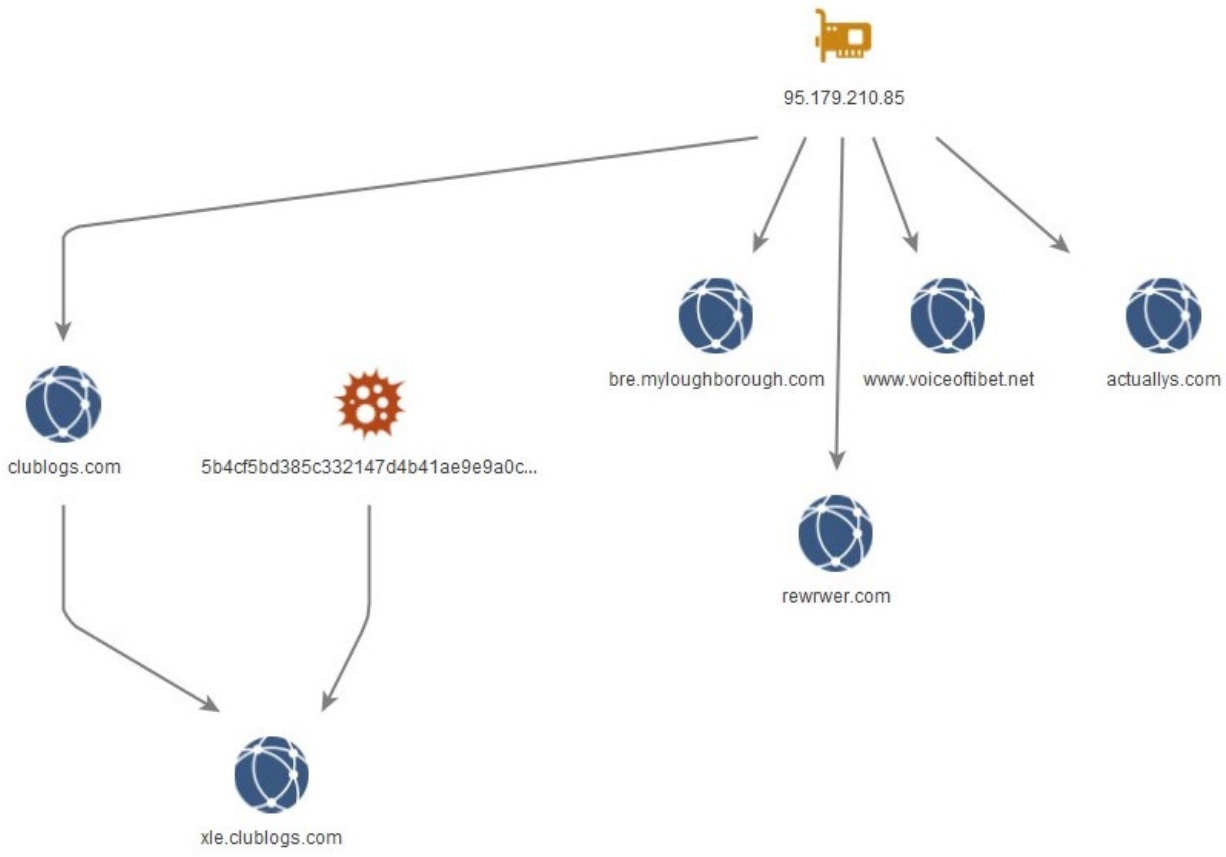


படம் 2 - விசைப்பலகை நடை மதிப்புகள்

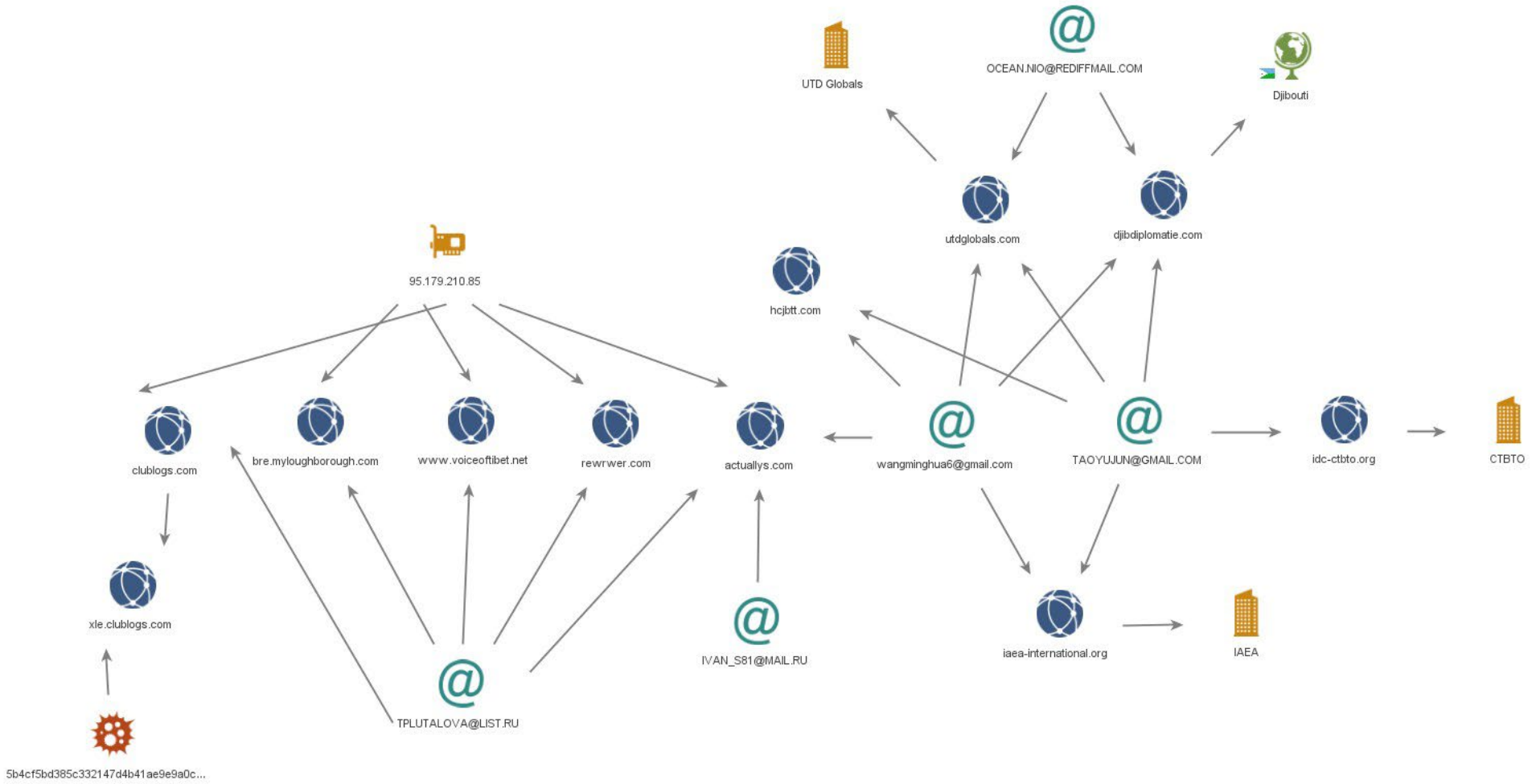


படம் 3 – state மதிப்பு 'FSDF' என்று கூறியுள்ள கூடுதல் களங்கள்

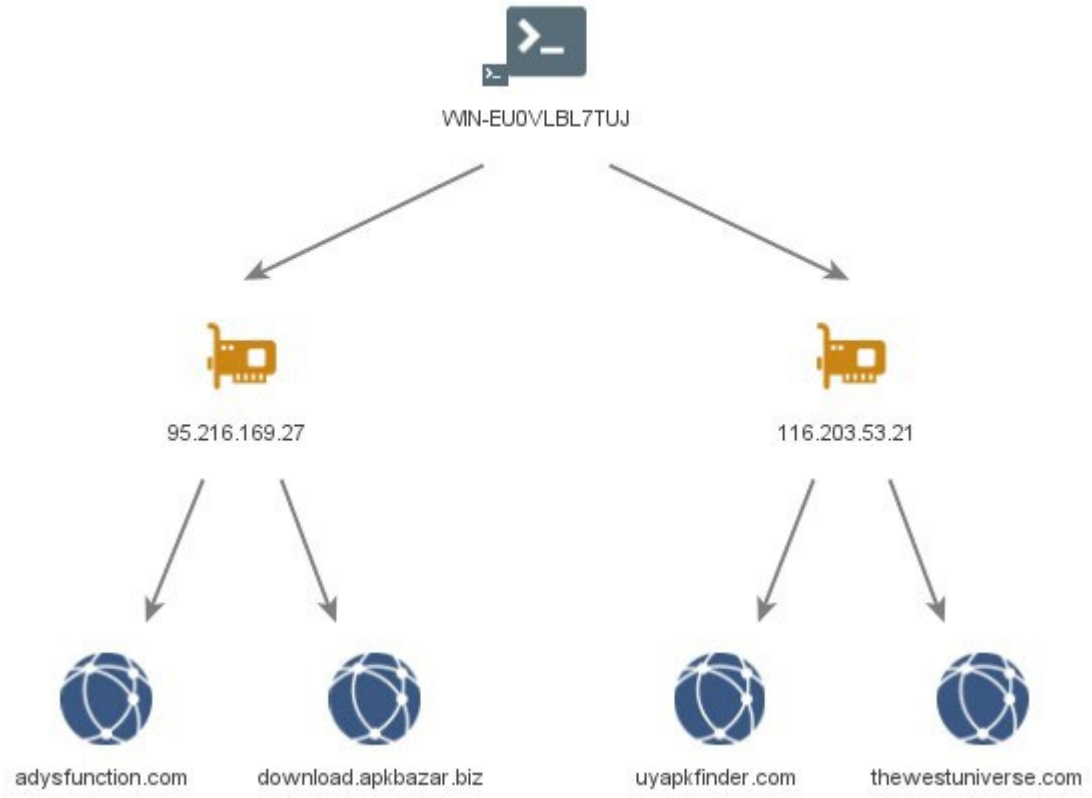
படம் 4 - **95.179.210[.]85**



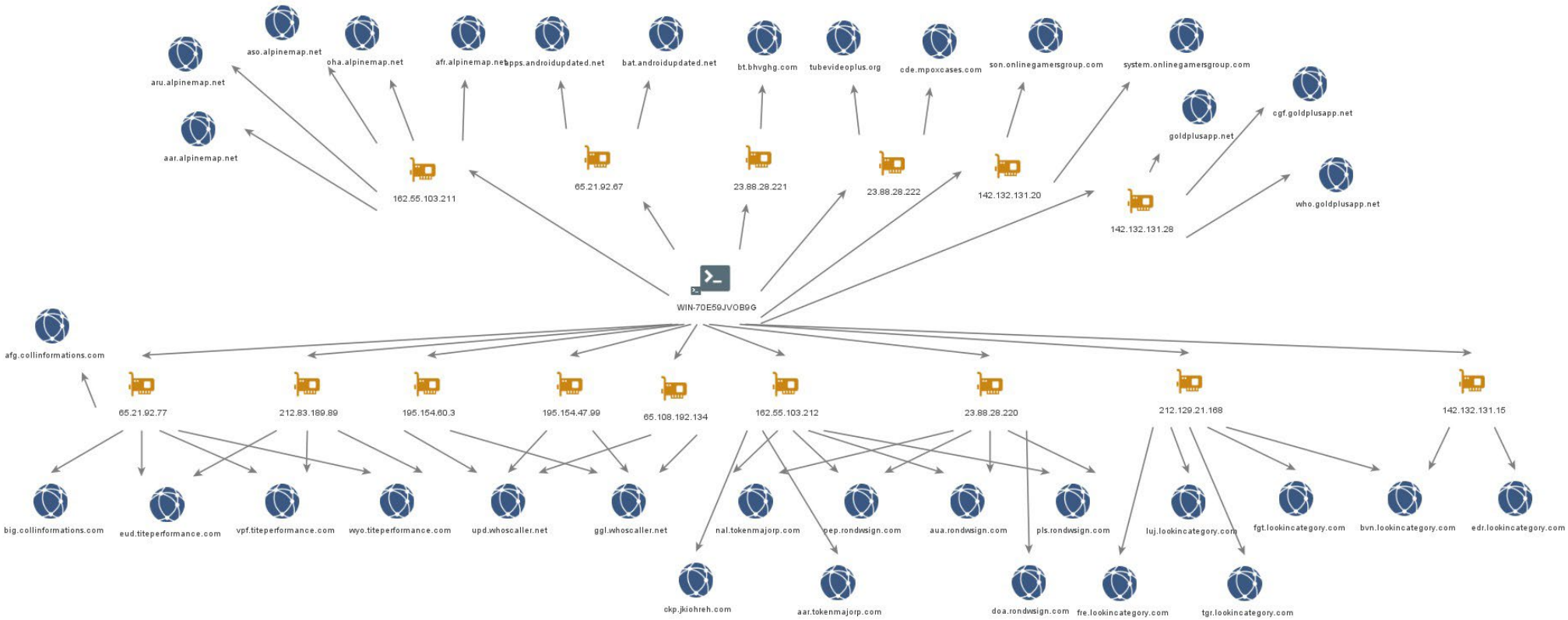
படம் 5 - WHOIS இணைப்புகள்



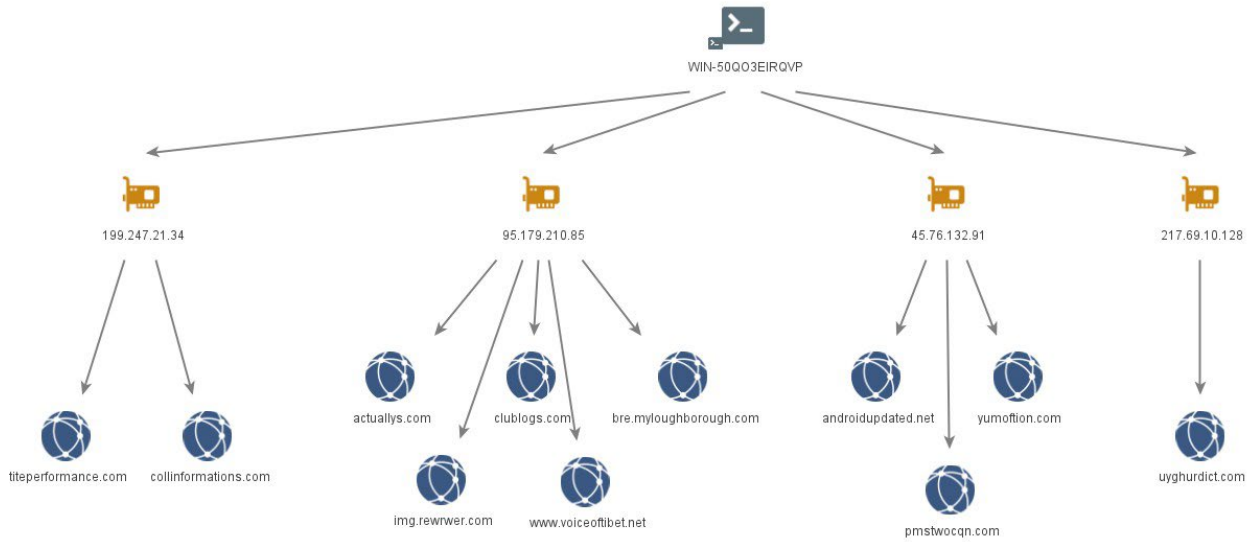
படம் 6 - **WIN-EU0VLBL7TUJ**



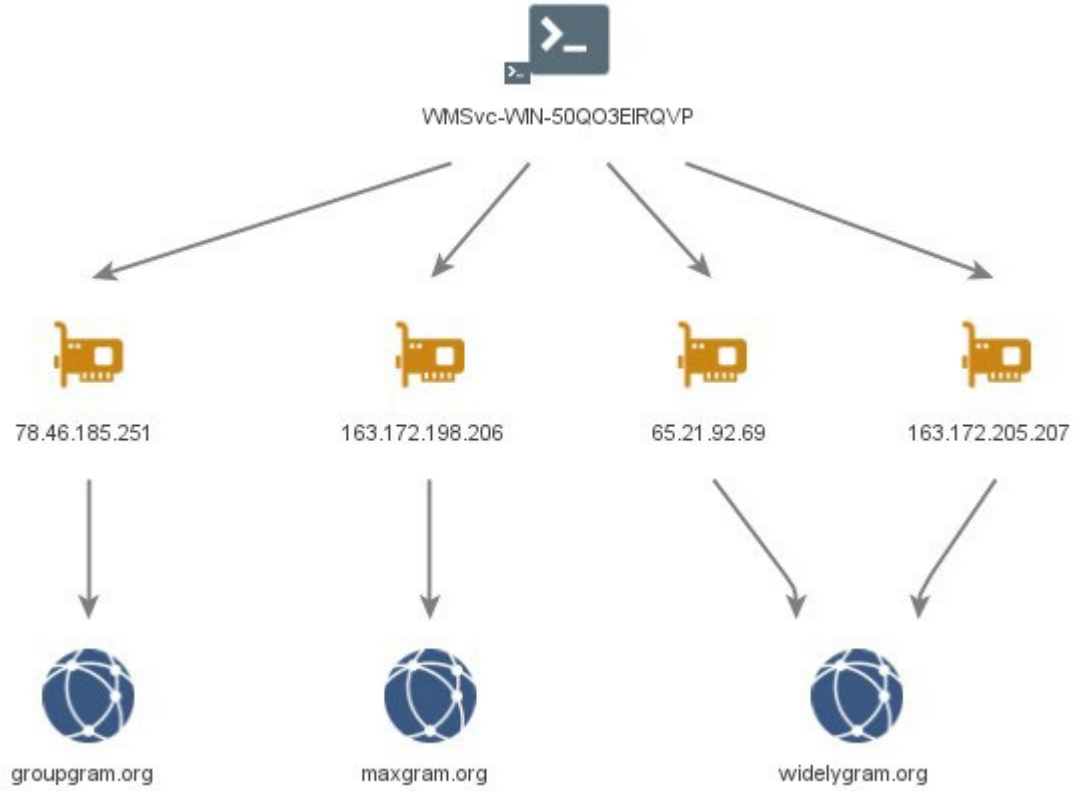
படம் 7 - **WIN-70E59JVOB9G**



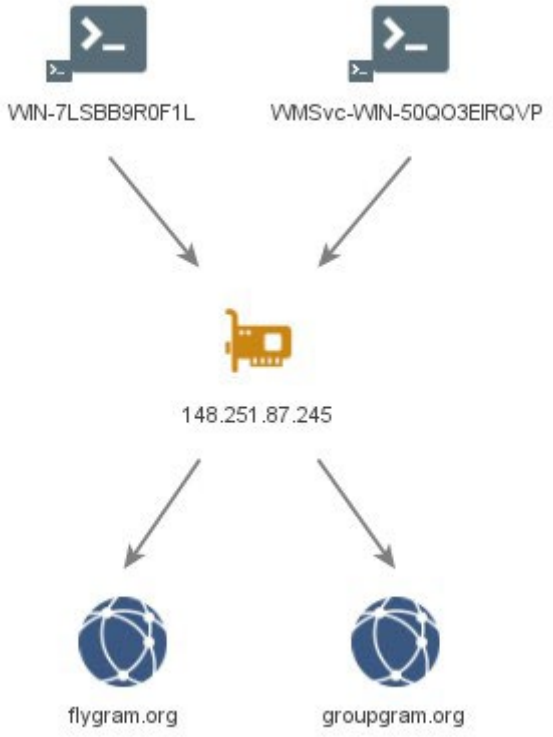
படம் 8 - **WIN-50QO3EIRQVP**



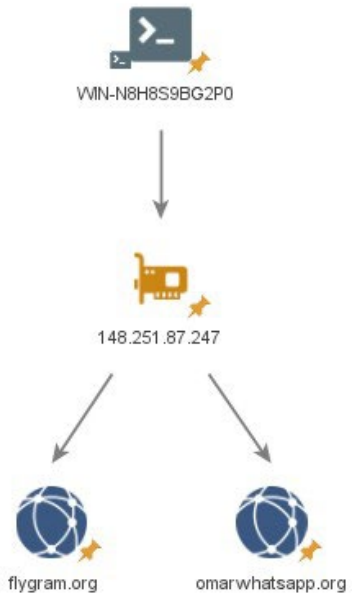
படம் 9 - **VMSvc-WIN-50QO3EIRQVP**



படம் 10 - **VMSvc-WIN-50QO3EIRQVP** மற்றும் **WIN-7LSBB9R0F1L**



படம் 11 - **WIN-N8H8S9BG2P0**



படம் 12 - **WIN-I6VBN8MR92A**

பின் இணைப்பு B: MOONSHINE & BADBAZAAR மாதிரிகள் காணப்பட்டவை

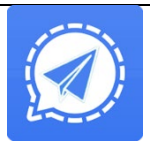
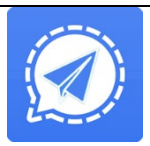
கடந்த இரண்டு ஆண்டுகளில் MOONSHINE மற்றும் BADBAZAAR பிரச்சாரங்களில் பயன்படுத்தப்பட்ட செயலிகளை கீழே உள்ள அட்டவணை பட்டியலிடுகிறது.

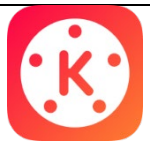
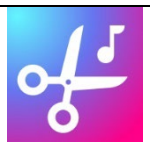
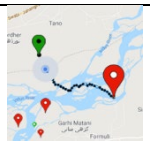
ஏற்கனவே உள்ள செயலிகளுடன் தெளிவான ஒற்றுமையை இந்த செயலிகளில் பல காட்டுகின்றன. வேண்டுமென்றே ஏமாற்றுவதற்காக, ஏற்கனவே நன்கு அறியப்பட்டவற்றைப் பயன்படுத்தும் உத்தியாக இருக்கலாம்.

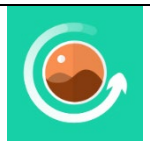
செயலியின் பெயர், அதன் தொகுப்பின் பெயர் மற்றும் குறியீட்டு சின்னம் அனைத்தும் உண்மையான செயலியைப் போன்றதாக இருக்கலாம் அல்லது பொருந்தலாம். எனவே ஒரு சாதனம் பாதிக்கப்பட்டுள்ளதா என்பதை அடையாளம் காண அதனைப் பிரத்தியேகமாகப் பயன்படுத்தப்படக்கூடாது என்பதைக் கவனத்தில் கொள்ள வேண்டும்.

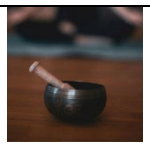
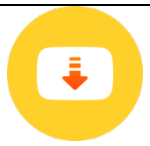
செயலியின் பெயர்	தொகுப்பின் பெயர்	செயலியின் குறியீட்டு சின்னம்
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	

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	

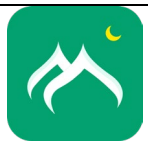
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	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	

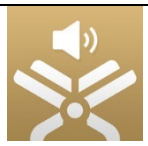
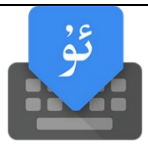
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
குர்ஆன்	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	
بقاپ لۇغىتىqكۇ	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	

மேலதிக விபரங்களுக்கு

ஆஸ்திரேலிய சைபர் பாதுகாப்பு மையத்தின் வழிகாட்டி

- சைபர் குற்றம், சம்பவம் அல்லது அதனால் ஏற்பட்ட பாதிப்பு குறித்து புகாரளிக்க
- உங்கள் சாதனங்களைப் பாதுகாக்க
- உங்கள் மொபைல் ஃபோனைப் பாதுகாக்க
- Phishing என்ற மின் தூண்டிலிடல்
- மோசடிகள்
- உங்கள் சமூக ஊடகத்தைப் பாதுகாக்க
- சமூக ஊடகங்கள் மற்றும் செய்தியிடல் செயலிகளின் பயன்பாடுகளுக்கான பாதுகாப்பு உதவிக் குறிப்புகள்

UK NCSC மற்றும் NPSA இன் வழிகாட்டுதல்

- ஜனநாயகத்தை பாதுகாத்தல்
- சமூக ஊடகம்: அதை எவ்வாறு பாதுகாப்பாக பயன்படுத்துவது
- மொபைல் உள்ளிட்ட சாதனங்களைப் பாதுகாக்க, நிறுவனங்களுக்கான வழிகாட்டல்
- Application storeகளில் ஏற்படுத்தப்படும் அச்சுறுத்தல்கள் குறித்த அறிக்கை.
- அதிக ஆபத்திலுள்ள தனிநபர்களுக்கான பாதுகாப்பு மற்றும் தனிப்பட்ட பாதுகாப்பு

அமெரிக்க NSAயின் வழிகாட்டி

- மொபைல் சாதனங்கள் குறித்த சிறந்த நடைமுறைகள்

பொறுப்புத் துறப்பு

இந்த ஆலோசனை வெளியிடப்படும் நேரத்தில் தகவல்கள் சரிபார்க்கப்பட்டன என்பதை நினைவில் கொள்க.

இந்த அறிக்கையை எழுதும் நிறுவனத்திலிருந்தும் தொழில் துறையிலிருந்தும் பெறப்பட்ட தகவல்களைக் கொண்டு இந்த அறிக்கை எழுதப்பட்டுள்ளது. அனைத்து ஆபத்துகளையும் தவிர்க்கும் நோக்கத்துடன் இதில் கூறப்பட்டுள்ள கண்டுபிடிப்புகளும் பரிந்துரைகளும் வழங்கப்படவில்லை, மேலும் பரிந்துரைகளைப் பின்பற்றுவதால் மட்டுமே அத்தகைய அனைத்து ஆபத்துகளையும் அகற்ற முடியாது. தொடர்புடைய கணினி

உரிமையாளர்களிடமே அந்த தகவல் அபாயங்களின் உரிமை எல்லா நேரங்களிலும் இருக்கும்.

இங்கிலாந்தில், தகவல் சுதந்திரச் சட்டம் 2000 (FOIA) இன் கீழ் இந்த தகவலுக்கு விலக்கு அளிக்கப்பட்டுள்ளது, மேலும் பிற UK தகவல் சட்டங்களின் கீழ் விலக்கு அளிக்கப்படலாம்.

ஏதேனும் கேள்விகள் இருந்தால், ncscinfoleg@ncsc.gov.uk என்ற மின்னஞ்சல் முகவரிக்கு அனுப்பி வைக்கவும்.