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

Panduan Nasihat

BADBAZAAR dan MOONSHINE: Analisis dan mitigasi teknikal

9 April 2025

BADBAZAAR and MOONSHINE: Analisis dan mitigasi teknikal

Ringkasan

Dengan sokongan Cyber League UK, panduan nasihat ini telah dihasilkan bersama The National Cyber Security Centre (NCSC UK) dan rakan-rakan kongsi antarabangsa mereka.

- **The Australian Cyber Security Centre (Pusat Keselamatan Siber Australia) sebahagian daripada The Australian Signals Directorate (Direktorat Semboyan Australia)**
- **The Canadian Centre for Cyber Security (Pusat bagi Keselamatan Siber Kanada), sebahagian daripada The Communications Security Establishment (Pertubuhan Keselamatan Komunikasi)**
- **The German Federal Intelligence Service (Perkhidmatan Perisikan Persekutuan Jerman)**
- **The German Federal Office for the Protection of the Constitution (Pejabat Persekutuan Jerman bagi Perlindungan Perlembagaan)**
- **The New Zealand National Cyber Security Centre (Pusat Keselamatan Siber Kebangsaan New Zealand), sebahagian daripada The Government Communications Security Bureau (Biro Keselamatan Komunikasi Kerajaan)**
- **The United States Federal Bureau of Investigation (Biro Penyiasatan Persekutuan Amerika Syarikat)**
- **The United States National Security Agency (Agensi Keselamatan Kebangsaan Amerika Syarikat)**

Panduan nasihat ini menyampaikan hasil risikan yang baharu dan dikumpul bersama berkenaan dua varian spyware yang dikenali sebagai BADBAZAAR dan MOONSHINE, dan mengandungi nasihat kepada para pengendali stor app, pembangun dan syarikat media sosial untuk membantu memastikan keselamatan pengguna mereka terjaga.

Panduan nasihat ini diterbitkan selari dengan panduan nasihat bagi mangsa malware ini.

Dokumen ini menggunakan definisi kosa kata NCSC bagi spyware: "Sejenis malware yang dipasang dalam sesuatu alat peranti tanpa kebenaran pengguna, memungut data dan kemudian menghantarkannya kepada pihak ketiga".

Kajian kes satu: MOONSHINE

MOONSHINE ialah satu spyware Android spyware yang dilaporkan pada 2019 oleh Citizen Lab sebagai spyware yang menjadikan kumpulan-kumpulan Tibet sasarannya. MOONSHINE berpura-pura sebagai sebuah app sahih yang mengumpan mangsa untuk memasangnya. Ia telah dikongsi melalui saluran-saluran Telegram dan melalui pautan yang dikirim melalui WhatsApp.

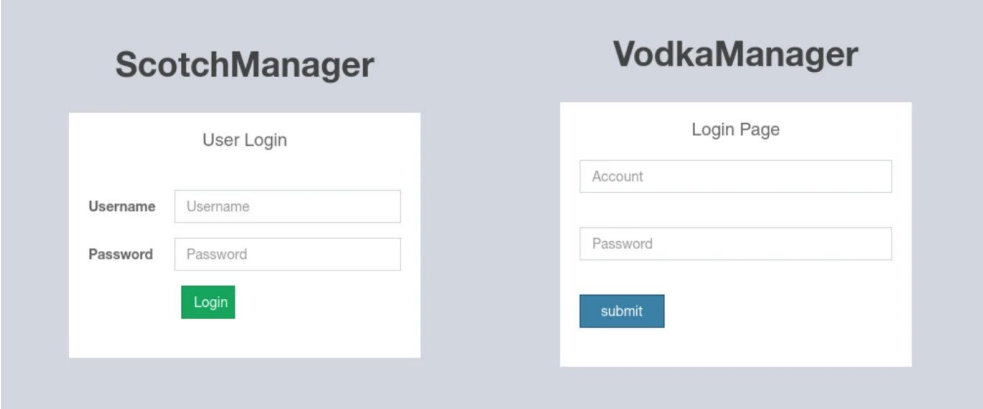
Kajian NCSC terhadap MOONSHINE menunjukkan perkara-perkara berikut:

- MOONSHINE menggunakan sebuah pengantaramuka pengurusan yang telah mengalami perubahan semenjak pertama kali ia dilaporkan.
- Pengantaramuka pengurusan itu telah mendedahkan keupayaan risikan yang meluas, termasuk keupayaan untuk menyahfiltrasikan fail daripada alat-alat peranti selain menangkap audio dan rakaman skrin yang sedang disiar langsung.
- Sebuah set pengantaramuka pengurusan MOONSHINE yang dihoskan secara maya telah ditemui. Pengantaramuka ini memiliki infrastruktur yang bertindih dengan panel-panel daftar masuk yang dikaitkan dengan UPSEC, yang menurut Intelligence Online merujuk kepada 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Pengantaramuka Pengurusan

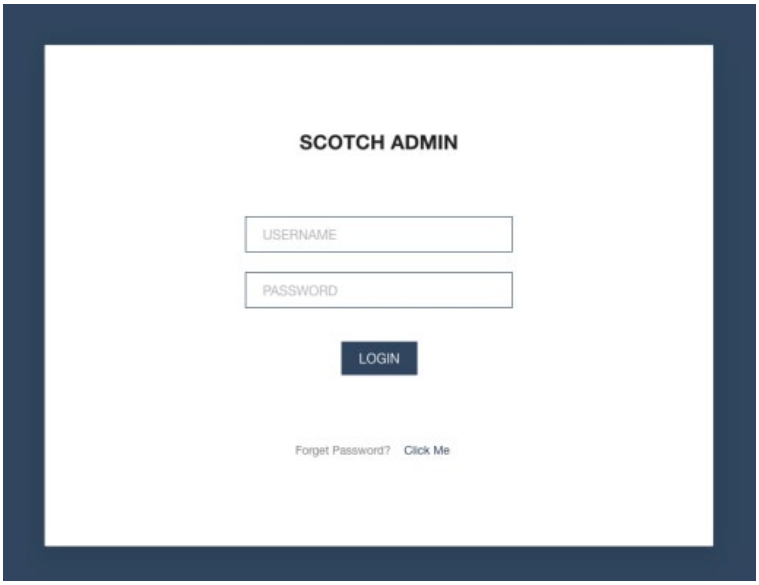
Laporan terdahulu mengenai pengantaramuka pengurusan MOONSHINE menunjukkan bahawa ia telah mengalami perubahan, yang mencadangkan ia sedang dibangunkan lagi secara berterusan.

Contoh pertama pengantaramuka pengurusan itu telah ditemui dalam laporan Citizen Lab's 2019.



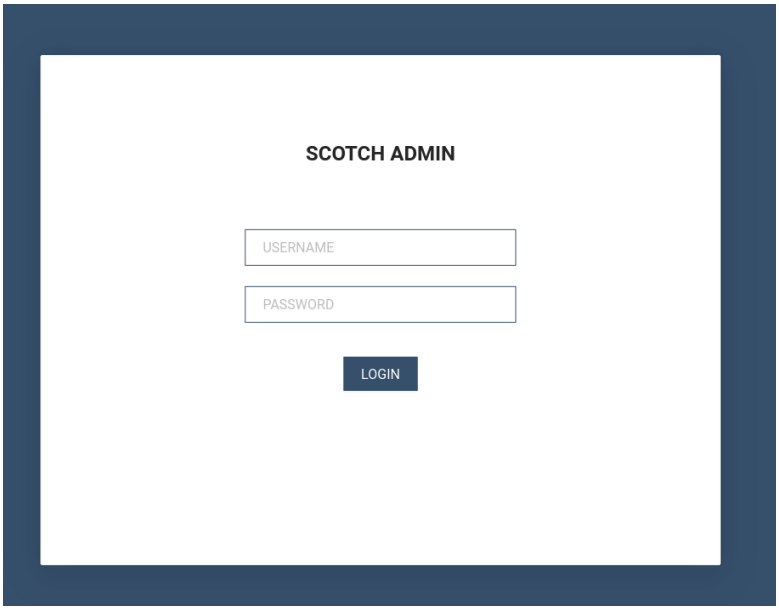
Rajah 1: Pengantaramuka pengurusan MOONSHINE yang kelihatan dalam laporan Citizen Lab's 2019 'Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits'.

Pada awal 2022, Lookout melaporkan sebuah pengantaramuka pengurusan berbeza yang telah direkabentuk semula agar ia kelihatan seperti yang ditunjukkan di bawah (yang menggantikan pengantaramuka dahulu dalam Rajah 1):



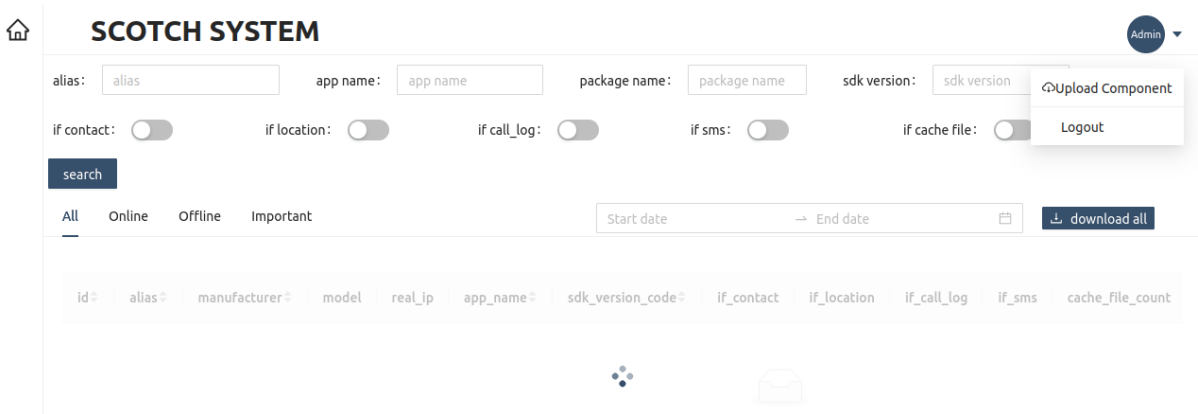
Rajah 2: Pengantaramuka pengurusan MOONSHINE yang kelihatan dalam Laporan 2022 Lookout 'MOONSHINE: Evolving Android Surveillanceware by Chinese APT POISON CARP To Target Tibetans and Uyghurs'.

Pada Ogos 2023, satu imbasan arahan dan kawalan MOONSHINE (C2) telah mendedahkan satu pengantaramuka yang serupa dengan pengantaramuka 2022 dengan fungsi '**Forget Password**' yang tidak lagi disediakan sebagai yang diberi dalam Rajah 2:



Rajah 3: Pengantaramuka pengurusan MOONSHINE yang diperhatikan pada Ogos 2023 yang tidak lagi mempunyai sebuah peringatan 'Forget Password'.

Siasatan lanjut pengantaramuka pengurusan itu menunjukkan konten di dalam panel tersebut yang mendedahkan bagaimana butir-butir alat-alat peranti yang dikompromi akan disimpan.



Rajah 4: Laman web di belakang laman daftar masuk pengantaramuka pengurusan MOONSHINE.

Kajian Lookout menunjukkan penghuluran sebuah '**score**' daripada alat peranti mangsa kepada server-server MOONSHINE C2. Nilai 'score' ini adalah berdasarkan kebenaran kelulusan sampel berniat jahat itu pada alat peranti mangsa tersebut.

Kolum 'if_contact', 'if_location', 'if_call_log' dan 'if_sms' di dalam halaman tersebut mencadangkan bukan semua sampel MOONSHINE mempunyai akses penuh kepada alat-alat peranti yang dikompromi. Pengetahuan mengenai

kolum-kolum ini dan 'score' yang dihulurkan daripada alat peranti itu kepada C2 mencadangkan pelaku ancaman ini menggunakan skor itu untuk mengkomunikasikan tahap akses yang ada pada malware itu ke atas alat peranti yang dikompromi berkenaan kepada individu yang sedang mengakses pengantaramuka pengurusan itu.

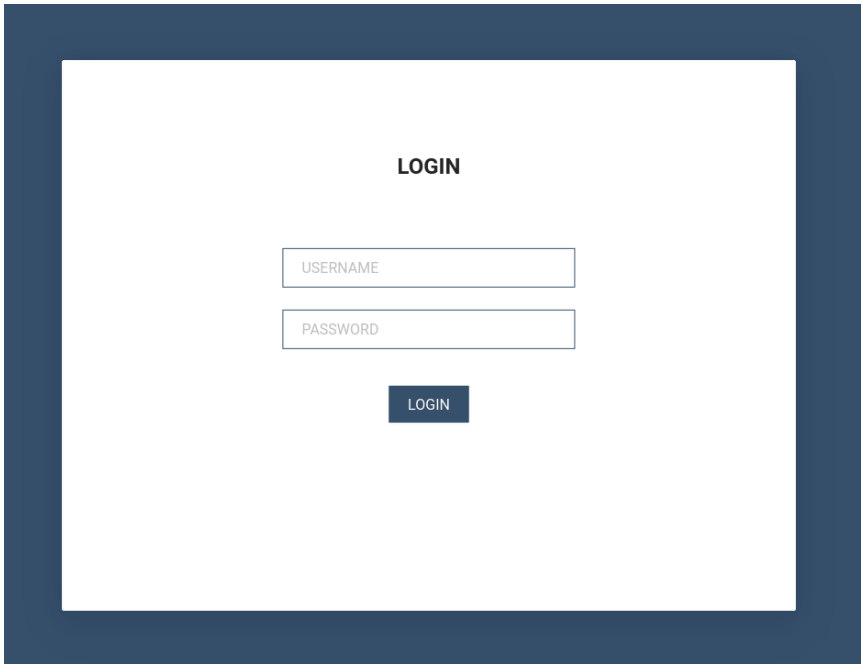
Umumnya, nasihat amalan-terbaik untuk menghalang app-app daripada memungut maklumat daripada alat peranti ialah untuk memeriksa izin app bagi apa-apa perkara yang luar biasa sebelum memuat turunkannya. Namun begitu, sampel-sampel MOONSHINE mencari izin yang relevan untuk kefungsian app tersebut, jadi ia mungkin kelihatan biasa sahaja, tetapi ia juga akan menggunakan izin ini untuk memungut maklumat daripada alat-alat peranti.

MOONSHINE juga mempunyai sebuah Pengantaramuka Pemprograman Aplikasi (Application Programming Interface) (API) yang mendedahkan cakupan keupayaannya. Versi-versi awal dokumentasi API mengandungi nama-nama API dalam Bahasa Mandarin.

Hos-hos Virtual

Dalam carian bagi panel-panel MOONSHINE, contoh-contoh yang dihos secara virtual atau maya telah ditemui. Pengehosan virtual ialah apabila satu alamat IP boleh menghoskan pelbagai laman web dengan sekaligus. Alamat-alamat IP contoh-contoh yang dihoskan secara virtual ini dan domain-domain yang dihoskan tidak diperhatikan di dalam mana-mana sampel malware yang diketahui.

Contoh-contoh pengantaramuka pengurusan ini berbeza, kerana tajuk halaman-halaman ini ialah '**LOGIN**' dan bukannya '**SCOTCH ADMIN**' yang kelihatan sebelum ini.



Rajah 5: Pengantaramuka pengurusan MOONSHINE yang menggunakan tajuk LOGIN dan bukannya SCOTCH ADMIN.

Selai itu, konten pada panel tersebut juga berbeza daripada Rajah 4, sebagaimana yang dilihat dalam Rajah 6:

Rajah 6: Laman web di belakang halaman daftar masuk pengantaramuka pengurusan MOONSHINE yang dihoskan secara virtual

Panel dalam Rajah 6 nampaknya ialah sebuah versi yang telah diringkaskan daripada panel dalam Rajah 4. Ciri-ciri bertindih dalam panel-panel ini ialah nama-nama kolum 'id', 'manufacturer' dan 'model' dalam rajah tersebut.

Contoh-contoh MOONSHINE yang dihoskan secara virtual yang ditemui ialah:

Domain	Alamat IP
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

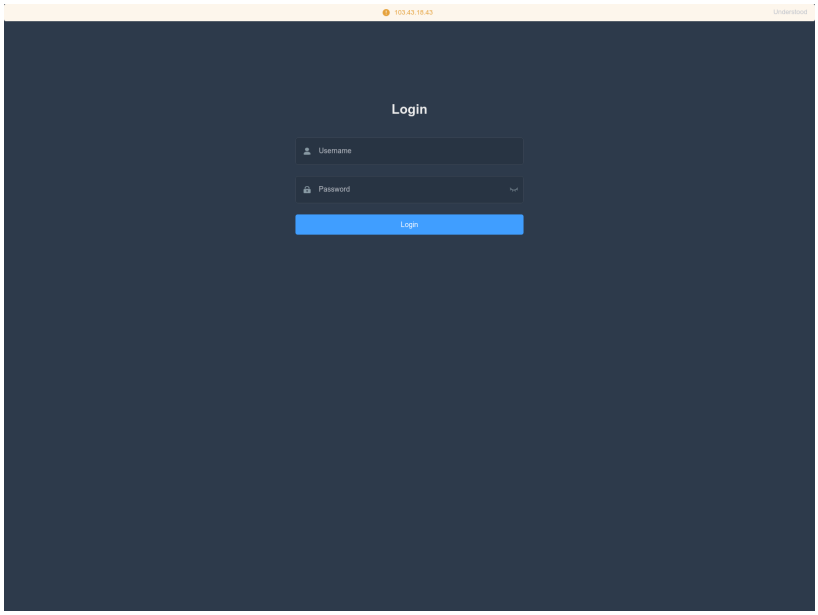
Domain-domain ini telah disenarai oleh Trend Micro sebagai kit eksploitasi MOONSHINE, yang bertanggungjawab atas pengeksploitasian kerentanan browser untuk memasang malware pada alat-alat peranti mudah alih. Trend Micro menamakan malware ini 'Dark Nimbus'.

Sebagai penjelasan, pengantaramuka pengurusan MOONSHINE ialah apa yang dikomunikasi oleh sampel-sampel malware MOONSHINE, dan ke mana data mangsa dinyahfiltrasikan. Kit pengeksploitasian MOONSHINE yang dilaporkan Trend Micro, ialah keupayaan berasingan yang mengeksploitasikan kerentanan pelayar untuk memasang sebuah malware yang dipanggil Dark Nimbus pada alat-alat peranti mudah alih. Selanjutnya, Dark Nmbus dan MOONSHINE ialah malware yang sama sekali berbeza.

Kedua-dua pengantaramuka pengurusan MOONSHINE dan kit pengeksploitasian MOONSHINE mempunyai kod yang bertindih, dan inilah sebabnya terdapat peringatan daftar masuk serupa dalam Rajah 3 dan 5 selain konten halaman dalam Rajah 4 dan 6. Mereka kedua-duanya juga mengandungi string 'webpackJsonpreact-scotchui' dalam kod sumber.

Pelaku ancaman telah menjanakan pautan URL yang dihubungkan kepada kit eksploitasi MOONSHINE dan kemudiannya diarahkan kembali kepada video-video yang relevan kepada orang Tibet dan Uyghur, yang bertindih dengan penyasaran MOONSHINE.

Di sekitar kebanyakan alamat-alamat IP yang menghoskan domain kit eksploitasi MOONSHINE, terdapat satu halaman daftar masuk bertajuk 'VLiteUI' pada port 444. Halaman ini tidak diperhatikan dengan begitu meluas dan kehadirannya pada IP-IP ini menunjukkan terdapat kemungkinan kaitannya kepada pengoperasian para pelaku itu.



Rajah 7: Panel daftar masuk dengan tajuk HTML 'VLiteUI' telah diperhatikan pada IP-IP yang juga menghoskan kit-kit pengeksploitasian MOONSHINE.

Analisis Trend Micro terhadap Dark Nimbus mendedahkan bahawa malware itu boleh memungut senarai berpanjangan maklumat yang terkandung pada alat peranti tersebut, dan bahawa ia berkomunikasi dengan C2 dengan menggunakan protokol XMPP.

Trend Micro juga mengarislakarkan bahawa di dalam sesetengah versi Dark Nimbus, mereka telah mengenalpasti prevalensi string 'DKNS'.

'**ansec[.]com**' (yang disenaraikan sebagai sebuah Dark Nimbus C2 oleh TrendMicro) juga telah diperhatikan dalam perkhidmatan-perkhidmatan XMPP bagi alamat-alamat IP lain yang berkhidmat untuk halaman-halaman web dengan DKNS dalam tajuknya:

- DKNS Android远程取证系统 (Sistem Forensik Jarak Jauh Androd DKNS) (DKNS Android Remote Forensic System)
- DKNS云网侦控平台 (Pelantar Penyiasatan dan Kawalan Awan DKNS) (DKNS Cloud Network Investigation and Control Platform)
- DKNS 云网侦控平台 (Pelantar Penyiasatan dan Kawalan Awan DKNS) (DKNS Cloud Network Investigation and Control Platform)
- DKNS远程控制侦查系统 (Sistem Penyiasatan Kawalan Jarak Jauh DKNS) (DKNS Remote Control Investigation System)

Satu lagi set alamat IP dengan '**ansec[.]com**' di dalam perkhidmatan XMPP mempunyai halaman-halaman web dengan tajuk:

- UPSEC互联网控制指挥系统 (Sistem Arahan Kawalan Internet UPSEC) (UPSEC Internet Control Command System)
- UPSEC无线侦控系统 (Sistem Pengintipan dan Kawalan Tanpa Wayar UPSEC) (UPSEC Wireless Surveillance and Control System)
- UPSEC重点人数据还原系统 (Sistem Pemulangan Kembali Data Individu Utama UPSEC) (UPSEC Key Person Data Restoration System)

Menurut Intelligence Online, 'UPSEC' yang diperhatikan dalam tajuk-tajuk halaman-halaman HTML itu merujuk kepada 'Sichuan Dianke Network Security Technology Co., Ltd'.

Kajian kes dua: BADBAZAAR

BADBAZAAR ialah sebuah malware mudah alih dengan varian-varian iOS dan Android yang telah menyasarkan individu-individu Uyghur, Tibet dan Taiwan. Spyware ini disebarkan melalui platform-platform media sosial dan stor-stor app rasmi. Laporan terkini daripada Volexity menunjukkan pelbagai varian BADBAZAAR berbeza, yang diasingkan sebagai BadSolar, BADBAZAAR dan BadSignal. Ketiga-tiga varian ini dirangkaikan bersama dengan fungsi-fungsi bertindih yang diguna untuk memungut maklumat alat peranti dan pengendali.

Kajian NCSC terhadap BADBAZAAR telah mendedahkan perkara-perkara berikut:

- Pegklusteran domain-domain C2 telah mendedahkan kaitan lanjut kepada domain-domain yang dilaporkan dalam risikan ancaman lampau.
- Server-server C2 dan sampel-sampel malware mendedahkan nama-nama hos yang dikaitkan dengan infrastruktur pelaku.
- Profil-profil lanjut yang diguna pelaku ancaman bagi penjanaan sosial untuk menyebarkan malware melangkaui stor-stor app rasmi.

Broker pengklusteran/domain WHOIS

'UJYJYUJ'

Analisis rekod-rekod WHOIS records bagi domain BADBAZAAR '**signalplus[.]org**' (dilaporkan oleh ESET) menunjukkan nilai '**UJYJYUJ**' dalam ruang '**State**'.

Carian domain lain dengan nilai sama telah mendedahkan domain-domain berikut yang patut diperhatikan:

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

(Lihat Annex A, imej 1)

Domain-domain **signalplus[.]org**, **tubevideoplus[.]org** dan **thetubeplus[.]com** ialah domain-domain BADBAZAAR C2 yang telah dilaporkan, manakala ESET melaporkan sub-domain **mail.pmumail[.]com** sebagai satu server proksi FlyGram. FlyGram ialah sebuah app BADBAZAAR yang dibangunkan oleh pelaku siber berniat jahat (lihat Lampiran untuk satu senarai app-app BADBAZAAR lain).

Nilai-nilai berjalan papan kekunci

NCSC juga telah melihat corak berjalan papan kekunci serupa dalam domain-domain BADBAZAAR C2 berdaftar lain.

Contohnya, domain-domain berikut semuanya mempunyai nilai '**REWR**' yang diperhatikan dalam ruang '**State**' (sebagaimana yang digunakan dahulu):

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

(Lihat Annex A, imej 2)

Domains dengan nilai ruang keadaan 'FSDF'

Satu lagi set domain-domain C2 BADBAZAAR C2 mempunyai nilai '**State**' '**FSDF**':

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

(Lihat Annex A, imej 3)

Laporan lampau dengan nilai-nilai berjalan papan kekunci

Penggunaan nilai-nilai berjalan papan kekunci dalam rekod-rekod domain-domain WHOIS BADBAZAAR juga boleh dilihat dalam penyasaran organisasi-organisasi Tibet yang dilaporkan dahulu oleh TA413. Recorded Future telah memperhatikan domain-domain yang dikawal-pelaku menipusamarkan ('spoofing') organisasi-organisasi Tibet dan penggunaan sebuah nilai organisasi pendaftar "**asfasf**".

clublogs[.]com

Sampel-sampel BADBAZAAR yang diperolehi Lookout mengandungi '**xle.clublogs[.]com'** sebagai domain C2. Domain root '**clublogs[.]com**' telah dihoskan pada alamat IP '**95.179.210[.]85**' dan mempunyai sebuah sijil SSL dengan subjek dan nilai pengeluar '**CN=WIN-50QO3EIRQVP**'. Nilai ini dipadankan dengan sijil-sijil SSL yang ditemui dalam sampel-sampel BADBAZAAR yang menggunakan pinning SSL untuk mengelakkan pemintasan komunikasi.

Sejarah lampau pengehosan alamat IP **95.179.210[.]85** telah memulangkan kembali domain-domain berikut yang patut diperhatikan:

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

(Lihat Annex A, imej 4)

www.voiceoftibet[.]net

Domain '**www.voiceoftibet[.]net**' nampaknya sedang menyamar sebagai stesen radio 'Voice of Tibet', serupa dengan TTP yang diguna oleh TA413.

Domain '**rewrwer[.]com**' ialah serupa dengan nilai '**State**' '**REWR**' yang dikenal pasti sebelum ini yang ditemui dalam rekod-rekod WHOIS domain-domain BADBAZAAR.

Domain-domain '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' dan '**myloughborough[.]com**' kesemuanya telah didaftar dengan alamat e-mel '**tplutalova@list[.]ru**'.

actuallys[.]com

Rekod-rekod WHOIS untuk '**actuallys[.]com**' menunjukkan sebuah contoh di mana alamat e-mel tech dan admin ialah '**tplutalova@list[.]ru**' tetapi e-mel pendaftar ialah '**ivan_s81@mail[.]ru**'.

Maklumat WHOIS lampau untuk domain '**actuallys[.]com**' mendedahkan email pendaftaran '**wangminghua6@gmail[.]com**' yang disenarai pada 24 Februari 2016. Pada 11 Mac 2016, e-mel itu kemudian ditukar kepada '**ivan_s81@mail.ru**' walaupun tarikh luput pendaftaran pendaftarnya kekal sama.

wangminghua6@gmail[.]com

Alamat e-mel '**wangminghua6@gmail[.]com**' telah diguna untuk mendaftar domain-domain yang ditemui dalam laporan risikan ancaman lampau. Pada 2015, Palo Alto telah mengenal pasti e-mel yang diguna untuk mendaftar domain-domain C2 bagi malware tersebut, Cmstar. Pada 2014, ia juga telah

diguna untuk mendaftar domain-domain yang dikenal pasti oleh Mandiant dalam kempen-kempen pancingan yang dilakukan oleh APT3. Pada 2013, ia telah diguna untuk mendaftar domain-domain yang ditemui CrowdStrike dalam dropper malware dengan laluan sebuah Pangkalan Data Program (Program Database) (PDB) yang mengandungi huruf Cina. Hal ini mencadangkan pengkompilasian pada sebuah sistem China.

taoyujun@gmail[.]com

Domain '**hcjbtt[.]com**' telah didaftar dengan alamat e-mel '**taoyujun@gmail[.]com**' tetapi e-mel pentadbirnya telah didaftar dengan '**wangminghua6@gmail[.]com**'.

Tiada aktiviti berniat jahat yang dikaitkan dengan domain '**hcjbtt[.]com**', namun begitu alamat e-mel '**taoyujun@gmail[.]com**' telah ditemui dalam laporan perisikan ancaman lampau. Pada 2014, ia telah diguna untuk mendaftarkan sebuah domain yang ditemui oleh Mandiant dalam sampel-sampel '**Cueisfry Trojan**' yang diguna untuk menyasarkan organisasi-organisasi Jepun.

Alamat e-mel itu juga telah mendaftarkan domain-domain seperti '**iaea-international[.]org**' yang nampaknya menyamar sebagai **International Atomic Energy Agency** dan '**idc-ctbto[.]org**' menyamar sebagai **International Data Centre** di **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO).**

Rekod Whois lebih awal bagi domain '**iaea-international[.]org**' menunjukkan e-mel pendaftar sebagai '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Domain '**udtglobals[.]com**' telah diperhati menggunakan '**wangminghua6@gmail[.]com**' sebagai e-mel pentadbir dan '**ocean.nio@rediffmail[.]com**' sebagai alamat e-mel pendaftar. Rekod-rekod lain WHOIS bagi domain ini, menunjukkan e-mel pendaftar sama tetapi dengan alamat e-mel pentadbir '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' nampaknya sedang menyamar sebagai '**UDT Global**' iaitu satu acara global bagi syarikat-syarikat pertahanan dan keselamatan bawah laut. Nama pengguna '**ocean.nio**' yang terkandung di dalam alamat e-mel itu mungkin meniru **National Institute of Oceanography (NIO)** yang wujud di pelbagai negara. Walapun penggunaan perkhidmatan e-mel '**Rediff**' (yang berpangkalan di India) mungkin mencadangkan penyamaran **Indian National Institute of Oceanography**.

Djibdiplomatie[.]com

Domain '**djibdiplomatie[.]com**' nampaknya menyamar sebagai perkhidmatan diplomatik Djibouti, yang mempunyai rekod WHOIS serupa dengan '**utdglobals[.]com**'**.** Satu rekod nampaknya menunjukkan pendaftar '**ocean.nio@rediffmail[.]com**' dan admin '**taoyujun@gmail[.]com**' manakala rekod-rekod lain menunjukkan '**wangminghua6@gmail[.]com**' sebagai alamat e-mel adminnya dengan '**ocean.nio@rediffmail[.]com**' sebagai e-mel pendaftar.

Kedua-dua domain ini juga mempunyai nilai jenis berjalan papan kekunci dalam rekod-rekod WHOIS. Contohnya, '**udtglobals[.]com**' mempunyai nilai '**ASDF**' sebagai bandar pendaftarannya dan '**djibdiplomatie[.]com**' mempunyai '**DAF DAGF**' sebagai nilai nama pendaftarnya. Hal ini boleh dibandingkan dengan nilai-nilai yang diperhatikan di dalam domain-domain BADBAZAAR lain.

Walaupun alamat-alamat e-mel '**wangminghua6@gmail[.]com**' dan '**taoyujun@gmail[.]com**' ditemui dalam rekod-rekod WHOIS bagi domain-domain yang menyamar sebagai sebuah **acara pertahanan bawah laut global, perkhidmatan diplomatik Dibouti** dan **International Atomic Energy Agency**, mereka juga diguna dalam rekod-rekod WHOIS bagi pelbagai domain-domain tidak berniat jahat.

Campuran penyamaran domain-domain dan domain-domain tidak berniat jahat mungkin mencadangkan kewujudan sebuah entiti pemerolehan-infrastruktur yang diguna untuk menyokong pengoperasian para pelaku siber berniat jahat.

Alamat e-mel '**ocean.nio@rediffmail[.]com**' hanya ditemui dalam domain-domain penyamar yang dijelaskan di atas. '**ivan_s81@mail[.]ru**' and '**tplutalova@list[.]ru**' telah mendaftarkan sejumlah sangat kecil domain-domain masing-masing, dan sesetengah daripada domain-domain ini telah dihoskan pada infrastruktur BADBAZAAR. Ketiga-tiga alamat e-mel ini dipercayai lebih berkait rapat dengan pengoperasian para pelaku siber berniat jahat. Ini ialah kerana bilangan tinggi domain yang dikaitkan dengan mereka adalah dikaitkan dengan aktiviti berniat jahat, berbanding e-mel '**wangminghua6@gmail[.]com**' dan '**taoyujun@gmail[.]com**'.

(Lihat Annex A, imej 5)

Kaitan kepada para pelaku ancaman lain

Satu lagi ciri biasa domain-domain yang terkait dengan BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', dan '**voiceoftibet[.]net**' adalah mereka semua telah didaftar dengan eNom dan telah 'diletakkan' di '**255.255.255[.]254**'.

Berikutan siasatan NCSC sebelum ini, domain-domain lain dengan ciri-ciri ini telah mendedahkan aktiviti berkaitan dengan **APT5** pada 2019, dan **APT14** antara 2009 dan 2011.

Domain-domain yang terkait dengan APT5-mempunyai rekod-rekod WHOIS lampau yang menyenaraikan '**taoyujun@gmail[.]com**' sebagai alamat e-mel pendaftar.

Domain-domain yang terkait kepada APT14-linked domains mempunyai domain-domain tiga-huruf yang nampaknya mewakili sasaran yang diniatkan bagi operasi berniat jahat mereka. Satu contoh perkara ini ialah '**bae.cisconline[.]net**', yang mencadangkan niat untuk menyasarkan BAE Systems dan ditemui dalam sebuah sampel '**Poison Ivy**'.

Satu ciri serupa diperhati di dalam domain-domain BADBAZAAR di mana sub-domainnya berkait kepada nama app yang ditrojankan:

Tajuk Aplikasi	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

Ia penting untuk mengambil maklum bahawa aktiviti-aktiviti berkaitan APT5 dan APT14 telah berlaku pada masa lampau dan terdapat domain-domain lain yang berdaftar dengan eNom dan telah diresolvekan ke **255.255.255.254**' yang tidak boleh dikaitkan dengan aktiviti berniat jahat. Oleh yang demikian, ia tidak dapat dipastikan bahawa pelaku-pelaku di sebalik kempen-kempen ini ialah orang yang sama atau ada kaitan antara mereka.

Nama-Nama Mesin

Analisis C2 BADBAZAAR dan sampel-sampel mendedahkan bahawa nama hos digunakan sebagai nilai 'Common Name' dalam sijil-sijil SSL. Siasatan NCSC terhadap nama hos yang diperhatikan di dalam sampel-sampel dan infrastruktur BADBAZAAR menunjukkan bahawa nama-nama hos ini telah diguna di merata-rata pelbagai alamat IP. Alamat-alamat IP ini ialah domain pengehosan yang ditemui dalam sampel-sampel BADBAZAAR. Terdapat butir-butir terperinci lanjut di dalam seksyen di bawah berkenaan nama-nama hos ini, serta alamat-alamat IP dengan nama hos yang mengehoskan domain-domain BADBAZAAR C2.

Di dalam hampir semua kes, kehadiran sijil-sijil dengan nilai nama hos bertindih dengan resolusi IP bagi nama-nama domain berniat jahat yang diperincikan, dan beberapa contoh-contoh kecil di mana ia bukannya kes ini juga telah digariskan.

WIN-EU0VLBL7TUJ

Nama hos '**WIN-EU0VLBL7TUJ**' telah diperhati dalam alamat-alamat IP berikut yang patut diperhatikan:

- '**116.203.53[.]21**' menghoskan domain-domain BADBAZAAR C2 '**uyapkfinder[.]com**' dan '**thewestuniverse[.]com**'.
- **'95.216.169[.]27**' menghoskan domain-domain BADBAZAAR C2 '**adysfunction[.]com'** dan sub-domain '**download.apkbazar[.]biz**' diperhati sebagai pautan muat turun bagi sebuah sampel BADBAZAAR.

(Lihat Annex A, imej 6)

WIN-70E59JVOB9G

Nama hos '**WIN-70E59JVOB9G**' telah diperhati dalam alamat-alamat IP berikut yang telah menarik perhatian:

- ‘**23.88.28[.]220**’ menghoskan sub-domain BADBAZAAR C2, **‘aua.rondwsign[.]com’, ‘nal.tokenmajorp[.]com’, ‘pep.rondwsign[.]com’** ‘**doa.rondwsign[.]com**’, dan **‘pls.rondwsign[.]com’.** Terdapat tempoh masa dua hari antara bila sijil dengan mesin ini kali terakhir dilihat, dan bila domain-domain berniat jahat pertama kali dilihat meresolve kepada IP.

- ‘**23.88.28[.]221**’ menghoskan sub-domain yang berkait dengan BADBAZAAR ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222**’ menghoskan domain-domain BADBAZAAR C2 ‘**tubevideoplus[.]org**’ and ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ menghoskan sub-domain BADBAZAAR C2 ‘**bat.androidupdated[.]net**’. Ia juga menghoskan sub-domain ‘**apps.androidupdated[.]net**’ yang merupakan sebuah malware C2 DoubleAgent.

- ‘**65.21.92[.]77**’ menghoskan sub-domain BADBAZAAR C2 ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ and ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ menghoskan domain-domain BADBAZAAR C2 ‘**upd.whoscaller.net**’. dan ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ menghoskan domain-domain BADBAZAAR C2 ‘**bvn.lookincategory[.]com’** dan ‘**edr.lookincategory[.]com’.** Terdapat tempoh masa sebelas hari antara bila sijil dengan mesin ini kali terakhir dilihat, dan bila domain-domain berniat jahat pertama kali dilihat meresolve kepada IP.

- **‘142.132.131[.]20’** menghoskan sub-domain ‘**son.onlinegamersgroup[.]com’** dan ‘**system.onlinegamersgroup[.]com’**, yang dipercayai merupakan C2 BADBAZAAR kerana mereka telah dihoskan sewaktu sijil-sijil SSL berkaitan BADBAZAAR telah diperhatikan pada IP tersebut.

- '**142.132.131[.]28'** menghoskan sub-domain BADBAZAAR C2 '**goldplusapp[.]net**' dan sub-domain '**who.goldplusapp[.]net**' and '**cgf.goldplusapp[.]net**'.

- '**162.55.103[.]211**' menghoskan sub-domain BADBAZAAR C2 '**oha.alpinemap[.]net**', '**aru.alpinemap[.]net'**, '**aso.alpinemap[.]net**', '**afr.alpinemap[.]net**', dan '**aar.alpinemap[.]net**'.

- '**162.55.103[.]212**' menghoskan sub-domain BADBAZAAR C2 **'pep.rondwsign[.]com', 'ckp.jkiohreh[.]com', 'aar.tokenmajorp[.]com', 'nal.tokenmajorp[.]com', 'pls.rondwsign[.]com'** dan **'aua.rondwsign[.]com'.**

- '**195.154.47[.]99**' menghoskan sub-domain BADBAZAAR C2 '**ggl.whoscaller[.]net**' dan '**upd.whoscaller.net**'. Terdapat tempoh masa tiga hari antara bila sijil dengan mesin ini kali terakhir dilihat, dan bila domain-domain berniat jahat pertama kali dilihat meresolve kepada IP.

- '**195.154.60[.]3**' menghoskan sub-domain BADBAZAAR C2 '**upd.whoscaller[.]net**' '**ggl.whoscaller[.]net**'.

- '**212.83.189[.]89**' menghoskan sub-domain BADBAZAAR C2 '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' dan '**afg.collinformations[.]com**'.

- '**212.129.21[.]168**' menghoskan sub-domain BADBAZAAR C2, '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**' '**luj.lookincategory[.]com**' dan '**bvn.lookincategory[.]com**'.

(Lihat Annex A, imej 7)

WIN-50QO3EIRQVP

Nama hos '**WIN-50QO3EIRQVP**' telah diperhati dalam alamat-alamat IP berikut yang telah menarik perhatian:

- '**45.76.132[.]91**' telah menghoskan domain-domain, '**yumoftion[.]com**', '**androidupdated[.]net**'. Kedua-dua domain yang dikaitkan dengan BADBAZAAR sebagai sub-domain '**fow.yumoftion[.]com**' dan '**bat.androidupdated[.]net**' adalah domain-domain C2 BADBAZAAR. Selain itu, sub-domain '**apps.androidupdated[.]net**' ialah sebuah domain C2 DoubleAgent C2. Ia juga mengehoskan domain '**pmstwocqn[.]com**', yang dikaitkan dengan BADBAZAAR melalui rekod-rekod WHOIS.

- '**95.179.210[.]85**' mengehoskan '**clublogs[.]com**', yang mana '**xle.clublogs[.]com**' ialah sebuah domain C2 BADBAZAAR C2 dan juga mengehoskan domain-domain yang terkait dengan BADBAZAAR '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' dan '**actuallys[.]com**'.

- '**199.247.21[.]34**' mengehoskan '**titeperformance[.]com**', dan '**collinformations[.]com'** yang merupakan sub-domain bagi domain-domain C2 BADBAZAAR.

- '**217.69.10[.]128**' menghoskan domain BADBAZAAR C2 '**uyghurdict[.]com**'.

(Lihat Annex A, imej 8)

WMSvc-WIN-50QO3EIRQVP

Nama hos '**WIN-50QO3EIRQVP**' telah diperhati dalam alamat-alamat IP berikut yang telah menarik perhatian:

- **'78.46.185[.]251'** menghoskan domain BADBAZAAR C2 **'groupgram[.]org'**, yang dilaporkan Volexity sebagai menggunakan port 4432 untuk hubungan yang berniat jahat.

- **‘65.21.92[.]69’** dan **‘163.172.205[.]207’** mengehoskan domain **‘widelygram[.]org’** yang dipercayai ialah sebuah domain BADBAZAAR C2, kerana walaupun ia sedang dihoskan oleh kedua-dua IP, port 4432 kekal terbuka.

- **‘163.172.198[.]206’** mengehoskan domain **‘maxgram[.]org’** yang dipercayai ialah sebuah domain BADBAZAAR C2, kerana walaupun ia sedang dihoskan oleh kedua-dua IP, port 4432 kekal terbuka.

(Lihat Annex A, imej 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Nama hos ‘**WMSvc-WIN-50QO3EIRQVP**’ dan ‘**WIN-7LSBB9R0F1L**’ telah diperhati serentak pada alamat IP berikut:

- ‘**148.251.87[.]245**’ menghoskan domain-domain BADBAZAAR C2 ‘**flygram[.]org**’ dan ‘**groupgram[.]org**’.

(Lihat Annex A, imej 10)

WIN-N8H8S9BG2P0

Nama hos ‘**WIN-N8H8S9BG2P0**’ telah diperhati pada alamat-alamat IP berikut:

- ‘**148.251.87[.]247**’ menghoskan domain-domain BADBAZAAR C2 ‘**omarwhatsapp[.]org**’ dan ‘**flygram[.]org**’.

(Lihat Annex A, imej 11)

WIN-I6VBN8MR92A

Nama hos ‘**WIN-I6VBN8MR92A**’ telah diperhati pada alamat-alamat IP berikut:

- ‘**148.251.87[.]197**’ menghoskan domain BADBAZAAR C2 ‘**tryhrwserf[.]com**’.

(Lihat Annex A, imej 12)

Berdasarkan data komersial sedia ada, keberhadiran nama-nama mesin ini di sekitar internet berbeza-beza. Sesetengah daripada mereka diperhatikan bertindak serentak di sekitar pelbagai alamat IP yang menandakan VM sedang direka daripada template sama. Ia penting untuk mengetahui bahawa bagi

sesetengah nama hos, tidak semua IP pada mana ia diperhatikan boleh dikaitkan dengan aktiviti berniat jahat. Ini mungkin bererti bahawa penggunaan nama-nama hos ini tidak eksklusif kepada pelaku-laku ancaman ini sahaja.

Namun begitu, keberhadian sesetengah daripada nama mesin-mesin ini di merata IP yang pernah mengehoskan domain-domain C2 BADBAZAAR, mungkin mencadangkan bahawa sebuah entiti yang memperolehi-infrastruktur sedang diguna untuk mengkonfigurasikan mesin-mesin itu untuk menyokong operasi siber pelaku-pelaku berniat jahat tersebut.

Kehadiran media sosial

Laporan lalu oleh Volexity menunjukkan bahawa video-video YouTube (yang mempromosikan penggunaan aplikasi berniat jahat) telah dicipta oleh para pelaku siber berniat jahat. Video-video ini mengandungi tutorial tentang cara bagaimana untuk menggunakan aplikasi yang telah dibangunkan.

Pihak NCSC telah menemui dua saluran YouTube lagi yang terkait dengan operasi para pelaku ancaman ini. Saluran YouTube dengan handle URL '**@josephjoey3499**' nampaknya mempromosikan penggunaan '**Maxgram**' dan sebuah saluran tambahan berdaftar dengan '**@uyghurapks3096**' mempromosikan '**Uyghur APK Finder**'.

Selain itu, video-video YouTube yang mempromosikan '**Flygram**' dan '**Signal Plus**', menunjukkan pelaku ancaman menggunakan nombor-nombor telefon yang boleh dilihat. Dalam video '**Flygram**', pada 0:36 kelihatan nombor telefon '**+1 (570) 378-7250**' dan dalam video '**Signal Plus**', nombor telefon '**+1 (267) 298 4259**' didedahkan.

Volexity melaporkan sebuah laman berita bertemakan Tibet palsu '**ignitetibet[.]net**', yang mereka temui dalam saluran-saluran Telegram yang dipercayai sedang dikendalikan oleh pelaku ancaman. Alamat e-mel '**choekyi.wangmo@ignitetibet[.]net**' diperhati meninggalkan komen pada hantaran di dalam halaman '**tibetone.org**' yang telah dilaporkan secara umum oleh Lookout sebagai sebuah halaman C2 yang diguna bagi iOS variant of BADBAZAAR.

Alamat e-mel ini dipercayai dikawal-pelaku, dengan menggunakan persona '**Choekyi Wangmo**'.

Penilaian

BADBAZAAR dan MOONSHINE menggunakan beberapa kaedah penjanaan sosial untuk menyasarkan komuniti-komuniti Uyghur, Tibet dan Taiwan secara khusus, terutamanya:

- pentrojanan app berkaitan komuniti-komuniti ini, misalnya sebuah app Quran bahasa Uyghur, yang hampir pastinya telah digubah untuk kumpulan dasar mangsa yang disasarkan.
- Penambahan app-app yang ditrojankan ini ke dalam stor-stor app rasmi barangkali memberikan rasa kesahihan, dan pengongsiannya dalam chat-chat kumpulan barangkali dibuat dengan niat untuk mengeksploitasikan hubungan yang sudah dipercayai dalam kalangan komuniti-komuniti ini.

BADBAZAAR dan MOONSHINE memungut data yang hampir pasti akan bernilai bagi negara China. Walaupun BADBAZAAR dan MOONSHINE telah diperhati menyasar individu Uyghur, Tibet dan Taiwan, terdapat malware-malware lain yang menyasarkan kumpulan-kumpulan minoriti lain di China. Warganegara daripada negara-negara pemeterai bersama, di China dan di luar negara, yang dianggap menyokong perjuangan yang mengancam kestabilan rejim, hampir sudah pastinya terancam daripada malware mudah alih seperti BADBAZAAR dan MOONSHINE. Keupayaan untuk menangkap data lokasi, audio dan foto hampir pastinya menyampaikan peluang untuk memanfaatkan pengintipan lanjut dan operasi kekacauan dengan menyampaikan maklumat masa-nyata mengenai aktiviti sasaran tersebut.

MITRE ATT&CK®

Laporan ini telah dikumpul dengan merujuk kepada kerangka kerja MITRE ATT&CK®, sebuah pangkalan pengetahuan yang boleh diakses secara global tentang taktik-taktik dan teknik-teknik musuh berdasarkan pemerhatian dunia-nyata.

Taktik	ID	Teknik	Prosedur
Pengintipan	T1593.001	Mencari Laman Web/Domain-domain Terbuka: Media Sosial	Para pelaku mencari kumpulan atau forum yang sepadan dengan mangsa yang dihasrat untuk mengongsikan malware
Pembangunan Sumber	T1583.001	Dapatkan Infrastruktur: Domain-domain	Para pelaku mendaftarkan domain-domain untuk server arahan dan kawalan mereka
Pembangunan Sumber	T1587.001	Membangunkan keupayaan: Malware	Kod berniat jahat ditulis untuk diselitkan ke dalam app-app yang ditrojankan
Pembangunan Sumber	T1608.001	Menetapkan Keupayaan: Muat naik Malware	App-app yang telah ditrojankan dimuat naik ke dalam platform-platform dalam talian termasuk stor-stor app
Pembangunan Sumber	T1585.001	Menubuhkan Akaun-akaun: Akaun-akaun Media Sosial	Para pelaku mewujudkan akaun-akaun pada laman-laman web dan media sosial untuk dikongsi dan mengiklankan malware
Pembangunan Sumber	T1585.002	Menubuhkan Akaun-akaun: Akaun-akaun e-Mel	Para pelaku menggunakan akaun-akaun e-mel yang dihoskan secara peribadi dan komersil untuk mengehos dan mengongsi malware
Akses Permulaan	T1189	Pengkompromian Pandu-Lalu (Drive-by Compromise)	Skrip-skrip berniat jahat disembunyikan di dalam app-app yang sebenarnya sahih dan dimuat naik ke dalam stor-stor app
Akses Permulaan	T1566.003	Pancingan: Pancingan Serampang	Para pelaku menghantar app-app yang ditrojankan ke

		(Spearphishing) menerusi Service	kumpulan-kumpulan sasaran menerusi media sosial termasuk Telegram
Pelaksanaan	T1204.002	Pelaksanaan oleh Pengguna: Fail Berniat Jahat	Para mangsa perlu memasang app-app yang telah ditrojankan untuk melaksanakan payloadnya
Elakan Pertahanan	T1027.009	Fail-fail atau Maklumat yang Diobfusikasikan: Payload terpendam	Payload berniat jahat itu disembunyikan di dalam app-app yang amnya sahih.
Elakan Pertahanan	T1036.005	Penyamaran Ajukan: Sepadan dengan Nama atau Lokasi Sahih	Fail-fail yang ditrojankan adalah sepadan dengan nama, rupa dan fungsi app-app sahih.
Elakan Pertahanan	T1656	Penyamaran	Pelaku akan menyamar sebagai individu-individu yang dipercayai dengan menciptakan laman web tudungan dan menggunakan nama pengguna yang dikaitkan dengan kumpulan-kumpulan sasaran.
Pemungutan	T1123	Tangkapan Audio	App yang ditrojankan mungkin akan meminta izin yang tidak diperlukan termasuk akses mikrofon
Pemungutan	T1125	Tangkapan Video	App yang ditrojankan mungkin akan meminta izin yang tidak diperlukan termasuk akses kamera
Pemungutan	T1005	Data dari Sistem Lokal	App yang ditrojankan mungkin akan meminta izin yang tidak diperlukan termasuk fail-fail lokal
Arahan dan Kawalan	T1071.001	Protokol Lapisan Aplikasi: Protokol-Protokol Web	Malware berhubung dengan C2 dengan menggunakan HTTPS dan WebSocket.
Arahan dan Kawalan	T1509	Port Bukan-Standard	Port-port bukan standard digunakan seperti port 4432 dan 2333

Penyahfiltrasian	T1041	Penyahfiltrasian Melalui Saluran C2	Malware menyahfiltrasikan data dengan menggunakan hubungan HTTPS dan WebSocket.
Impak	T1565.002	Manipulasi Data: Manipulasi Data yang Ditransmisi	Para pelaku memperolehi data daripada mangsa dengan membolehkan trafik web app yang tidak semestinya diguna bagi kefungsian app itu

Indikasi-Indikasi

MOONSHINE:

- Pada 1hb April 2025, satu carian bagi panel-panel VLiteUI telah memulangkan butiran berikut:

Alamat IP	Port	Pertama kali dilihat	Kali terakhir dilihat
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

- Pada 1hb April 2025, satu carian bagi panel-panel SCOTCH ADMIN virtual telah memulangkan butiran berikut:

Alamat IP	Port	Pertama kali dilihat	Kali terakhir dilihat
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

- Pada 14hb Mac 2024, satu carian bagi panel-panel SCOTCH ADMIN virtual telah memulangkan butiran berikut:

Domain	Alamat IP
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:

Keterangan	Sijil SSL yang diperhatikan dalam C2s BADBAZAAR
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Pada 1hb April 2025, satu carian bagi sijil BADBAZAAR di atas telah memulangkan butiran berikut:

Alamat IP	Port	Pertama kali dilihat	Kali terakhir dilihat
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

Keterangan	**Sijil SSL yang diperhatikan dalam C2s BADBAZAAR**
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62d b3db1baa

- Pada 1hb April 2025, satu carian bagi sijil BADBAZAAR di atas telah memulangkan butiran berikut:

Alamat IP	**Port**	**Pertama kali dilihat**	**Kali terakhir dilihat**
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

- Domain-domian WHOIS

Di bawah ini ialah satu rajah domain yang sedang atau pernah mempunyai rekod-rekod WHOIS dengan nilai-nilai yang sepadan dengan nilai-nilai yang diperhatikan dalam domain-domain C2 BADBAZAAR C2.

Nilai WHOIS	Domain
Negeri Pendaftar: UJYJYUJ **Negara Pendaftar: Bolivia:** **Pendaftar: 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
Negeri Pendaftar: REWR **Negara Pendaftar: CF** **Pendaftar: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com

	• tooenabled[.]com • suguestions[.]com • searching2[.]com
Negeri Pendaftar: FSDF **Negara Pendaftar: AL** **Pendaftar: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Alamat-Alamat e-Mel
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

Saluran-saluran YouTube
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

Berikut ialah pautan-pautan kepada indikasi kompromi lain (indicators of compromise) (IoCs) yang berkaitan dengan BADBAZAAR dan MOONSHINE. NCSC tidak boleh mengesahkan ketentusahan semua maklumat di dalam pautan-pautan ini dan pembaca dinasihati untuk menentusahkan ketepatan dan relevansnya secara sendiri.

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

Pemitigasian

NCSC menggalakkan pendokongan syor-syor di bawah untuk dijadikan pertahanan terhadap ancaman yang diterangkan dalam kajian-kajin kes tersebut.

- **Pengendali stor app, termasuk stor-stor app pihak ketiga, dan para pembangun patut memastikan app-app pada pelantar mereka adalah teguh dan mematuhi Kod Amalan kerajaan.** Sila lihat Panduan: 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

- **Sokongan pelbagai-bahasa**: Pembangun app patut melabur dalam usaha untuk melokalkan app-app popular bagi pengguna yang bercakap dalam bahasa kumpulan minoriti dalam kalangan kumpulan-kumpulan yang disasarkan termasuk Uyghur, Tibet, Hokkien Taiwan dan Kantonis. Panduan Apple guidance bagi pelokalan app-app: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Panduan Google bagi penterjemahan app-app: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Menjaga keteguhan pelantar media sosial anda:** Syarikat-syarikat media sosial boleh menjadikannya lebih sukar bagi pelaku siber berniat jahat untuk mencipta akaun-akaun palsu dan mengongsi fail-fail atau pautan-pautan berniat jahat pada pelantar-pelantar mereka dalam komuniti-komuniti dalam talian yang sebenarnya sahih. Sejauh mana yang boleh, syarikat-syarikat patut mengongsi indikasi berniat jahat dengan industri secara lebih meluas untuk mempertingkatkan pemahaman kolektif tentang ancaman tersebut dan untuk menolong dalam langkah-langkah perlindungan.

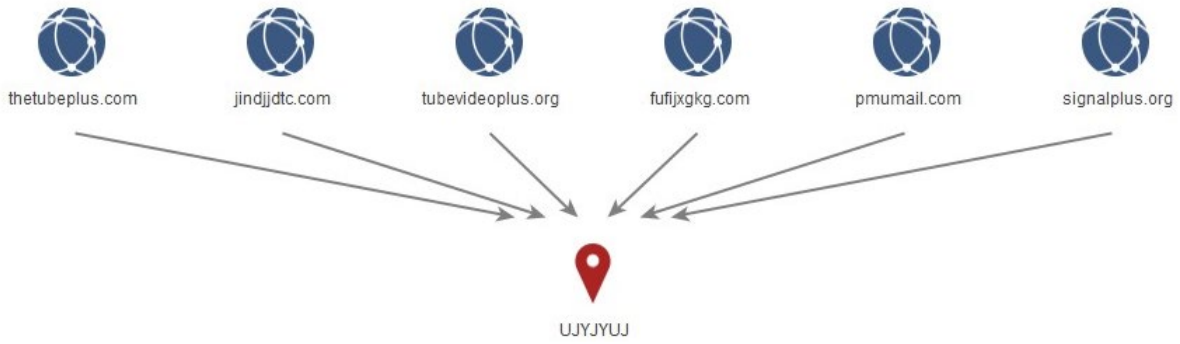
- **Pelan remediasi bagi pelanggan:** Organisasi-organisasi patut mempunyai prosedur-prosedur yang sudah ditetapkan untuk memberitahu pelanggan yang menggunakan perkhidmatan mereka yang telah memasang apps berniat jahat. Amaran-amaran ini patut menarik perhatian dan bersifat informatif. Di mana ia sesuai untuk berbuat demikian, organisasi patut menyampaikan panduan tetang cara bagaimana untuk membuang perisian tersebut dan menggalakkan mangsa untuk melaporkannya kepada pihak berkuasa, misalnya NCSC di UK.
  Untuk maklumat lanjut, sila lihat Kod Amalan Stor App (App Store Code of Practice):
  https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Kumpulan kerja untuk kolaborasi:** Syarikat-syarikat media sosial boleh membentuk kumpulan kerja, yang membenarkan pasukan-pasukan keselamatan mereka masing-masing untuk berkongsi indikasi-indikasi berniat jahat, TTPs dan pemerhatian, yang akan menjadikkannya lebih sukar bagi para pelaku untuk menggunakan pelantar-pelantar mereka untuk menyokong kempen-kempen berniat jahat.

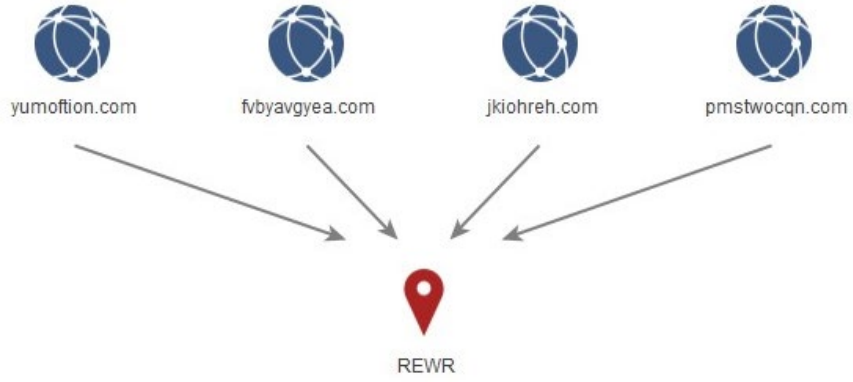
- **Mengesan app yang digubah:** Sejauh mana yang boleh, pembangun app patut memasukkan kefungsian yang memberitahu pengguna jika mereka telah memuat turunkan versi 'tidak rasmi' sesuatu app, untuk membantu melindungi mereka daripada salinan-salinan yang berniat jahat.

Lampiran A: Graf-graf maklumat broker clustering/domain BADBAZAAR WHOIS

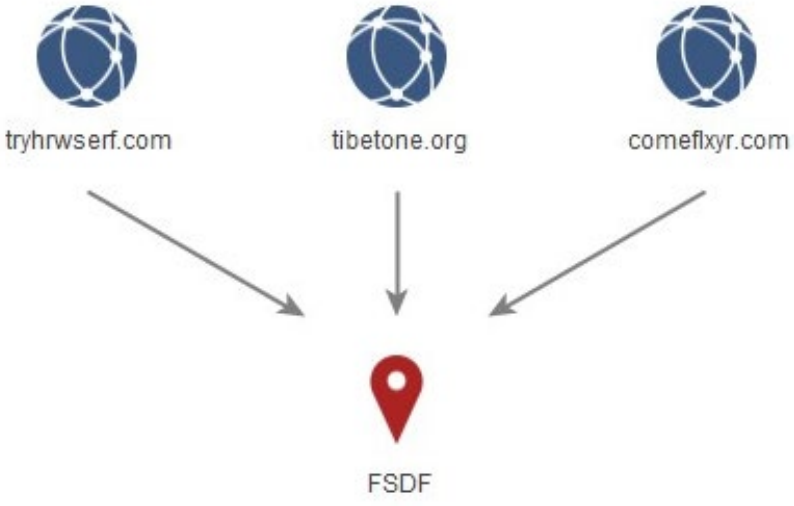
Imej 1 - 'UKYJYUJ'



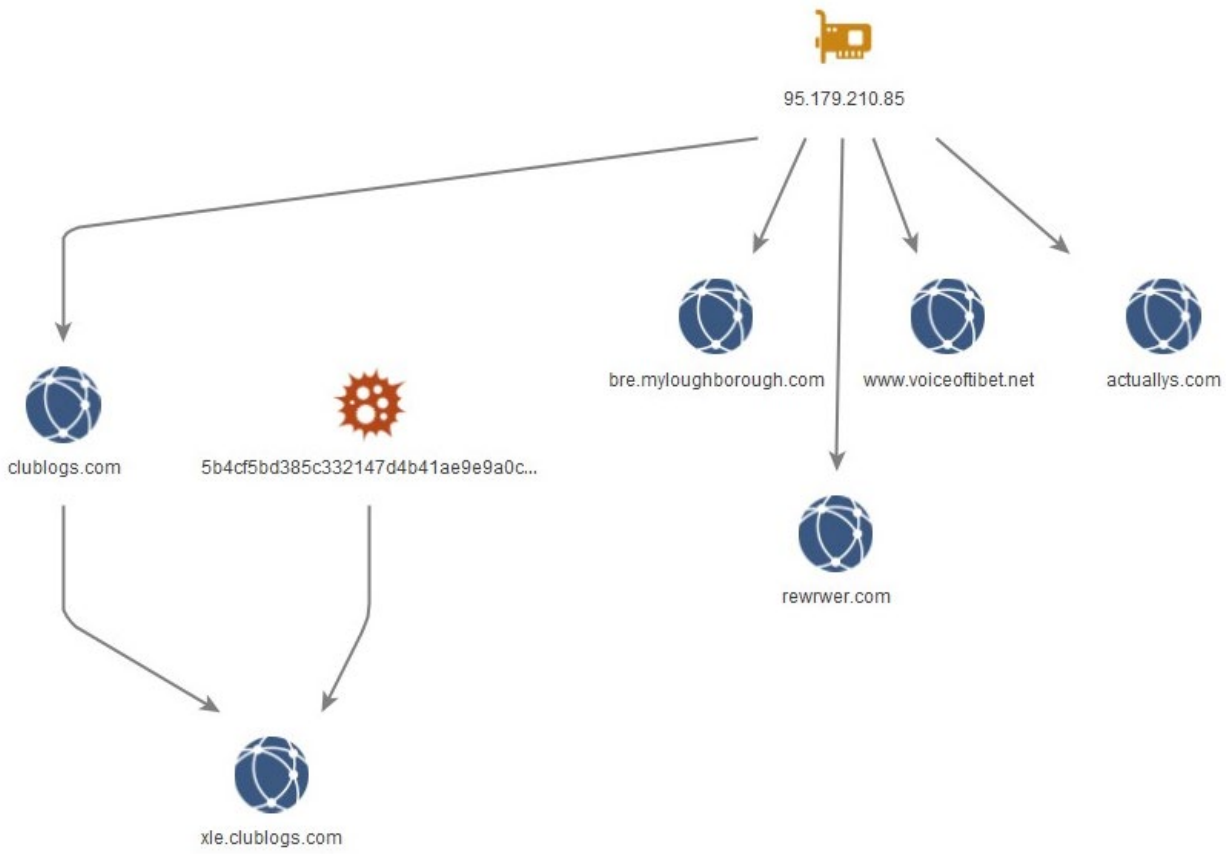
Imej 2 – Nilai-nilai papan kekunci berjalan



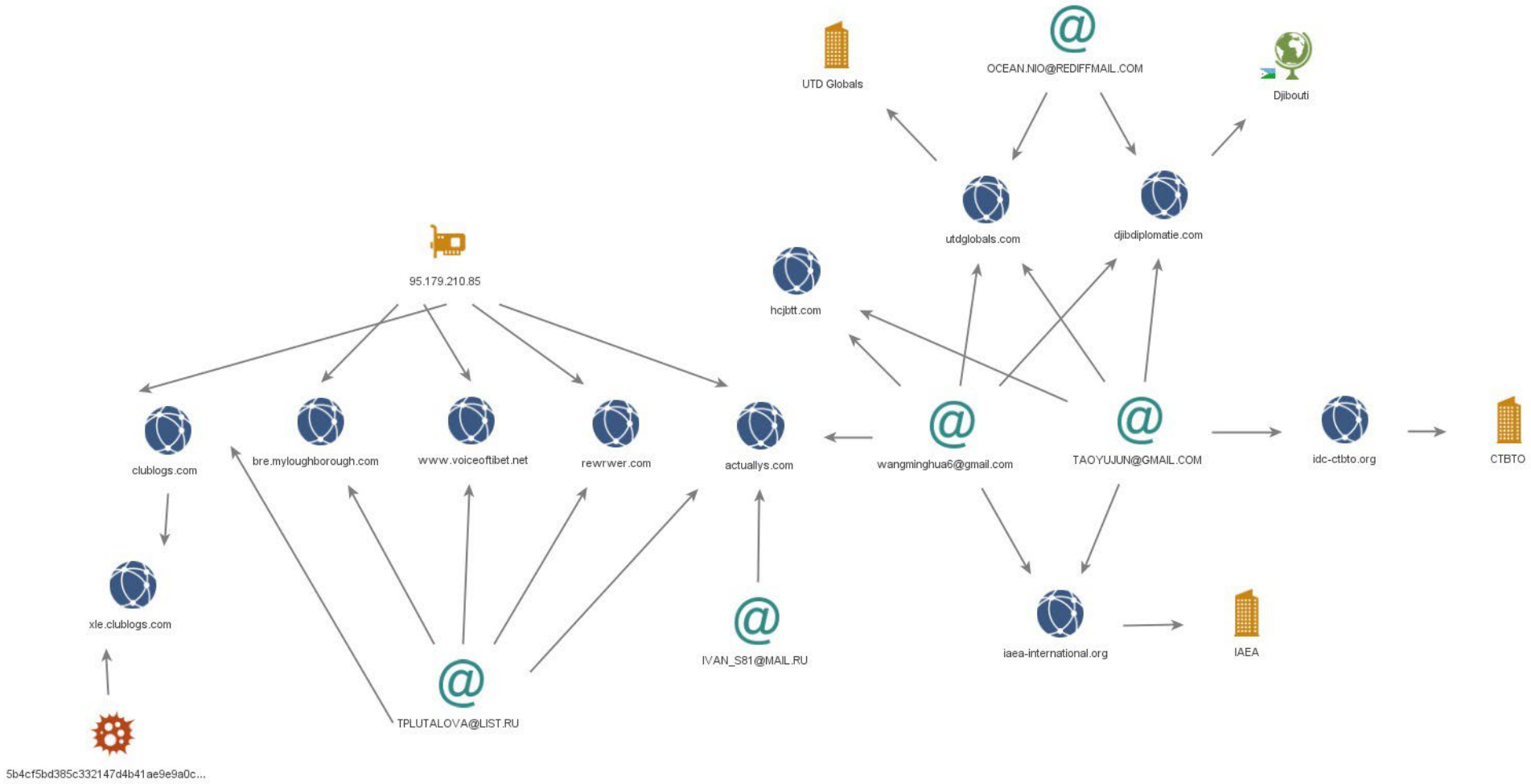
Imej 3 – Domain-domain tambahan dengan nilai ruang keadaan 'FSDF'



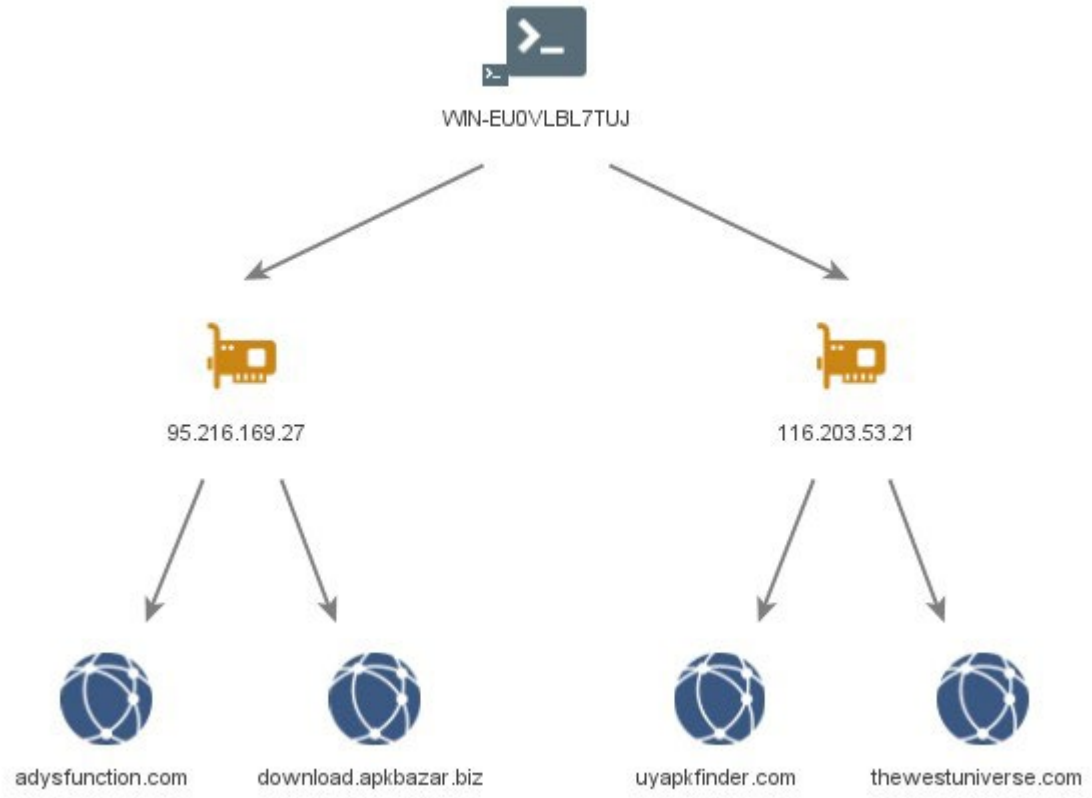
Imej 4 – **95.179.210[.]85**



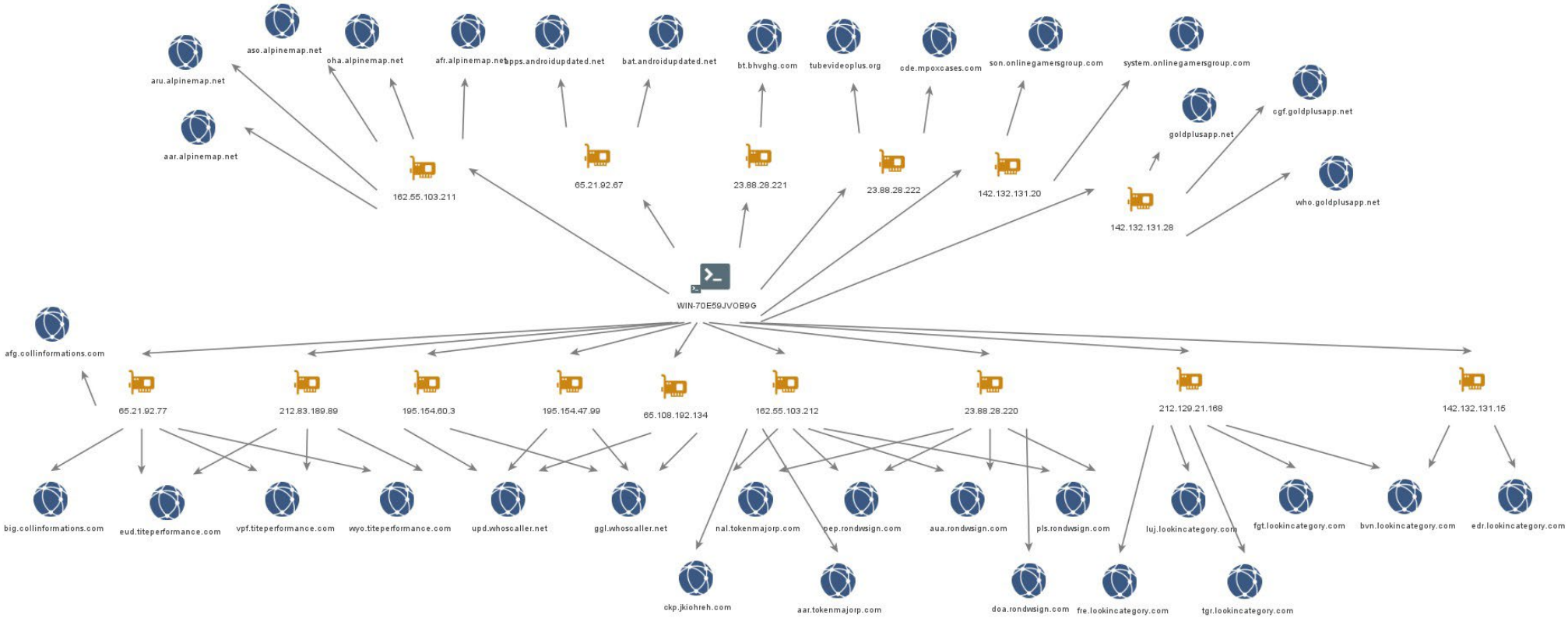
Imej 5 – Pautan-pautan WHOIS



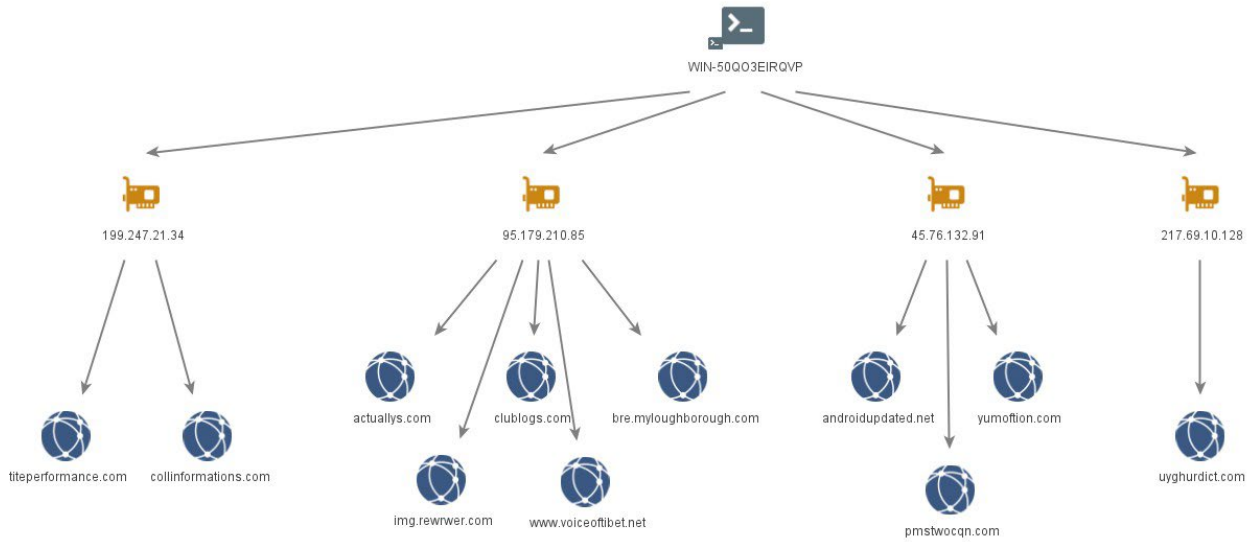
Imej 6 – **WIN-EU0VLBL7TUJ**



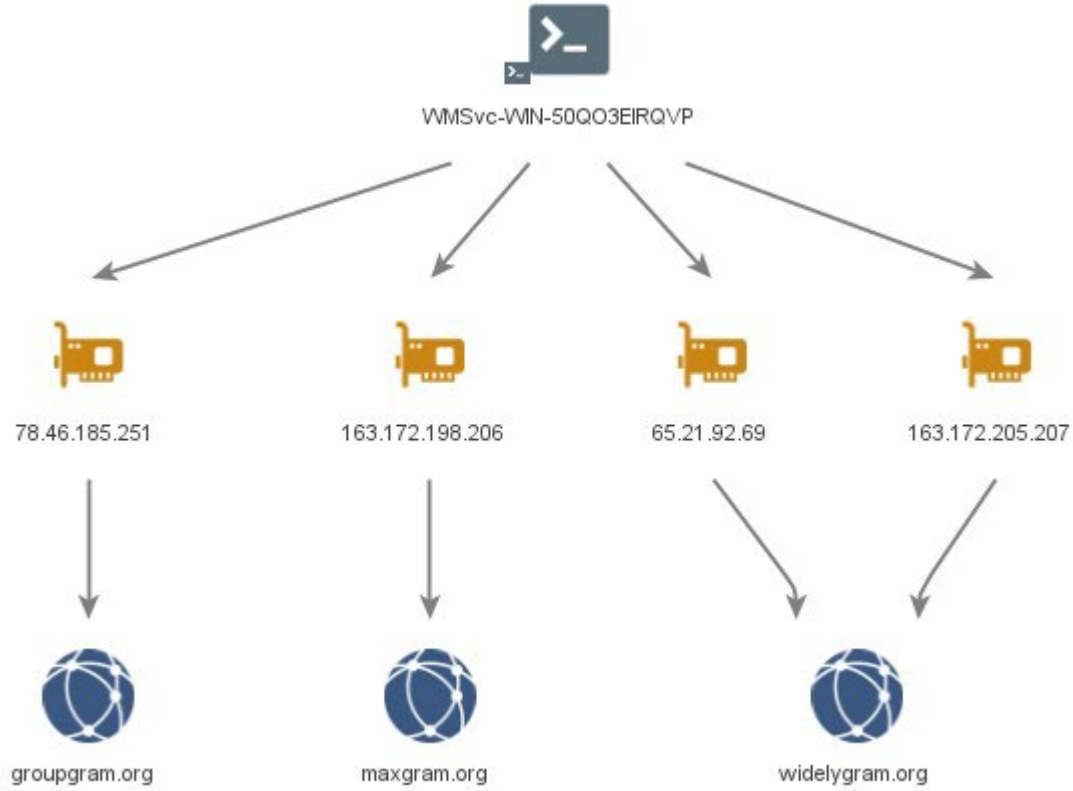
Imej 7 – **WIN-70E59JVOB9G**



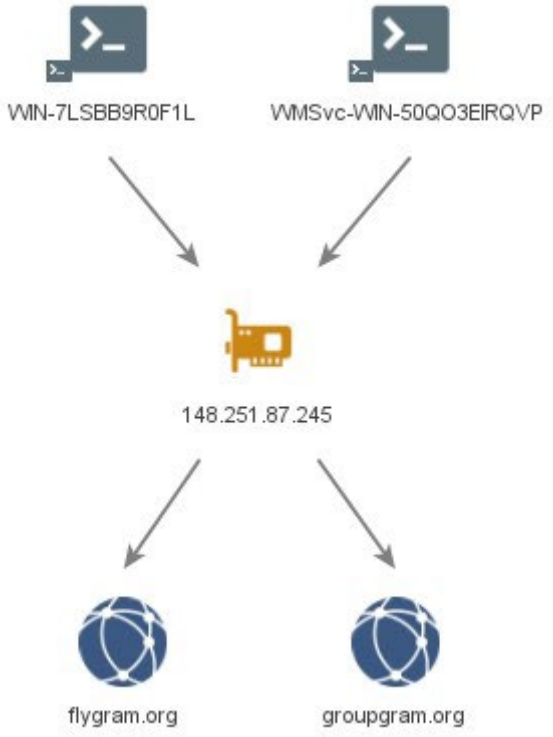
Imej 8 - **WIN-50QO3EIRQVP**



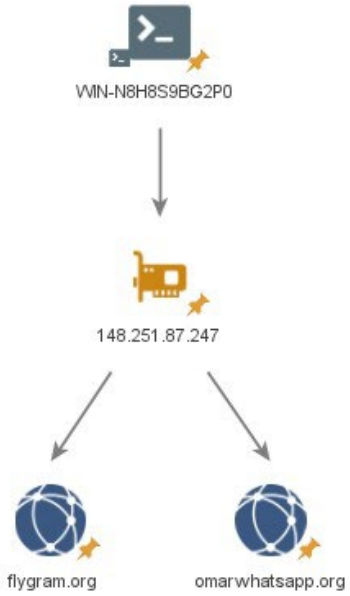
Imej 9 - **VMSvc-WIN-50QO3EIRQVP**



Imej 10 – **VMSvc-WIN-50QO3EIRQVP** dan **WIN-7LSBB9R0F1L**



Imej 11 - **WIN-N8H8S9BG2P0**



Imej 12 – **WIN-I6VBN8MR92A**

Lampiran B: Sampel-sampel MOONSHINE & BADBAZAAR yang diperhatikan

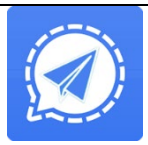
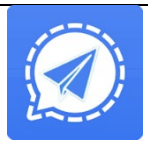
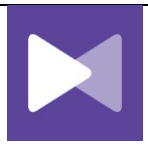
Rajah di bawah menyenaraikan app-app yang diguna dalam kempen-kempen MOONSHINE dan BADBAZAAR dalam tempoh masa dua tahun kebelakangan ini.

Sebahagian besar app ini menunjukkan persamaan dengan app-app yang sedia ada yang sudah lama ditubuhkan. Ia barangkali merupakan teknik sengaja pelaku untuk menipusamarkan ('spoof') jenama-jenama yang dikenali ramai.

Ia penting untuk mengambil tahu bahawa, tajuk app, nama pakej, dan ikon app semua boleh meniru atau kelihatan serupa dengan aplikasi sebenar dan oleh yang demikian tidak sepatutnya diguna secara eksklusif untuk mengenal pasti sama ada sesuatu alat peranti telah dijangkiti.

Tajuk App	Nama Pakej	Ikon App
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

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

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

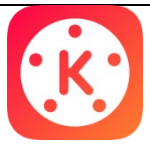
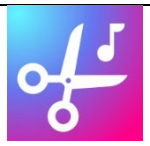
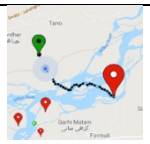
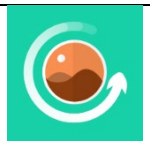
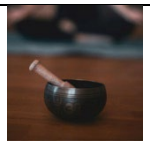
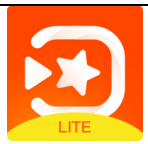
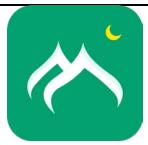
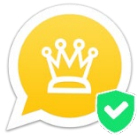
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

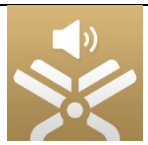
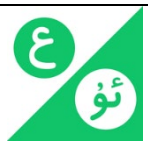
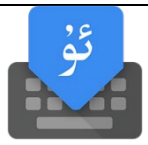
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore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

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

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

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

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

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

汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	

Bacaan lanjut

Panduan daripada Pusat Keselamatan Siber Australia (Australian Cyber Security Centre)

- Report a cybercrime, incident or vulnerability
- How to secure your devices
- Secure your mobile phone
- Phishing
- Scams
- Secure your social media
- Security tips for social media and messaging apps

Panduan daripada UK NCSC dan NPSA

- Defending Democracy
- Social Media: how to use it safely
- Device Security Guidance for organisations including mobile
- Threat report on application stores.
- Personal safety and security for high-risk individuals

Panduan daripada NSA US

- Mobile Device Best Practices

Penafian

Harap maklum bahawa panduan nasihat ini menyampaikan maklumat yang telah ditentusahkan pada waktu ia diterbitkan.

Laporan ini meraih maklumat yang diperolehi daripada agensi pengarang dan sumber-sumber industri. Sebarang hasil carian dan cadangan yang dibuat tidak disampaikan dengan niat untuk mengelakkan semua risiko dan mengikut cadangan ini tidak akan membuang semua risiko sedemikian. Pemilikan risiko maklumat berkenaan tetap ditanggung oleh pemilik sistem berkaitan pada setiap masa.

Di UK, maklumat ini dikecualikan di bawah Akta Kebebasan Maklumat 2000 (FOIA) dan mungkin dikecualikan di bawah peraturan perundangan maklumat UK lain.

Sila rujukkan sebarang pertanyaan FOIA kepada ncscinfoleg@ncsc.gov.uk.