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

Saran

BADBAZAAR dan MOONSHINE: Analisis teknis dan mitigasi

9 April 2025

BADBAZAAR dan MOONSHINE: Analisis teknis dan mitigasi

Ringkasan

Dengan dukungan dari Inggris Raya Cyber League, nasihat ini telah dibuat bersama oleh Pusat Keamanan Siber Nasional (NCSC UK) dan mitra-mitra internasional:

- **Pusat Keamanan Siber Australia, bagian dari Direktorat Sinyal Australia**
- **Pusat Keamanan Siber Kanada, bagian dari Badan Keamanan Komunikasi**
- **Badan Intelijen Federal Jerman**
- **Kantor Federal Jerman untuk Perlindungan Konstitusi**
- **Pusat Keamanan Siber Nasional Selandia Baru, bagian dari Biro Keamanan Komunikasi Pemerintah**
- **Biro Investigasi Federal Amerika Serikat**
- **Badan Keamanan Nasional Amerika Serikat**

Saran ini memberikan intelijen ancaman baru dan terkumpul pada dua varian spyware yang dikenal sebagai BADBAZAAR dan MOONSHINE, dan mencakup saran bagi operator toko aplikasi, pengembang, dan perusahaan media sosial untuk membantu menjaga keamanan penggunanya.

Saran ini diterbitkan bersamaan dengan saran untuk korban malware ini.

Dokumen ini menggunakan definisi glosarium NCSC tentang spyware: "Sejenis malware yang dipasang pada perangkat tanpa persetujuan pengguna, mengumpulkan data, lalu mengirimkannya ke pihak ketiga."

Studi kasus satu: MOONSHINE

MOONSHINE adalah spyware Android yang dilaporkan pada tahun 2019 oleh Citizen Lab yang menargetkan kelompok Tibet. MOONSHINE menyamar sebagai aplikasi sah untuk memikat korban agar menginstalnya. Aplikasi ini telah dibagikan melalui saluran Telegram dan tautan yang dikirim melalui WhatsApp.

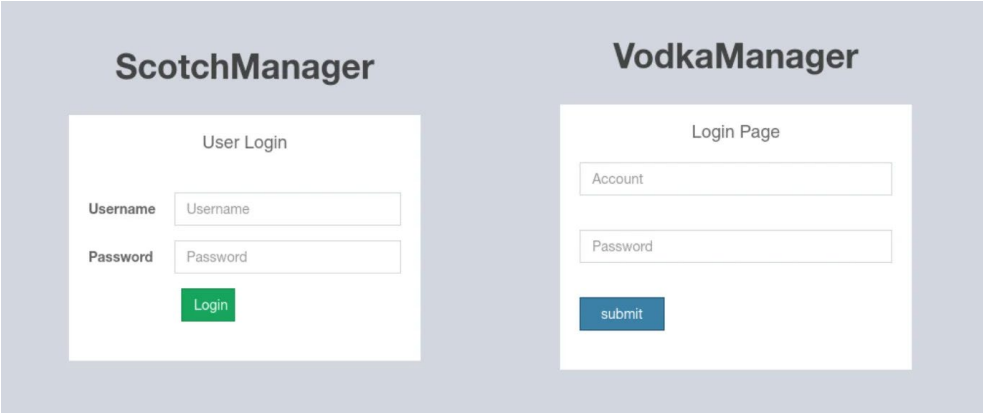
Penelitian NCSC terhadap MOONSHINE menunjukkan hal berikut:

- MOONSHINE menggunakan antarmuka manajemen yang telah mengalami perubahan sejak pertama kali dilaporkan.
- Antarmuka manajemen tersebut mengungkap kemampuan pengawasan yang luas, termasuk kemampuan untuk mengekstrak file dari perangkat serta menangkap audio langsung dan rekaman layar.
- Seperangkat antarmuka manajemen MOONSHINE yang dihosting secara virtual telah ditemukan. Antarmuka ini memiliki infrastruktur yang tumpang tindih dengan panel login yang terkait dengan UPSEC, yang menurut Intelligence Online mengacu pada 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Antarmuka manajemen

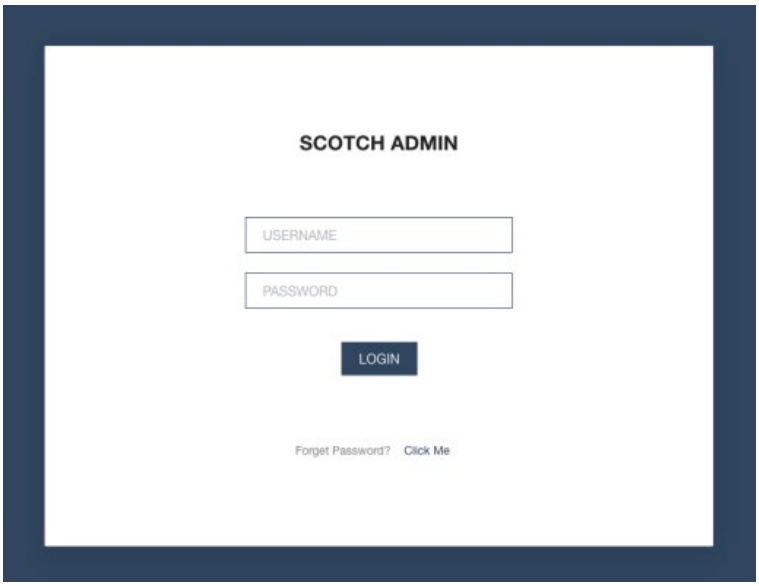
Pelaporan sebelumnya tentang antarmuka manajemen MOONSHINE menunjukkan bahwa antarmuka tersebut telah mengalami perubahan, yang menunjukkan pengembangan yang sedang berlangsung.

Contoh pertama antarmuka manajemen ditemukan dalam pelaporan Citizen Lab tahun 2019.



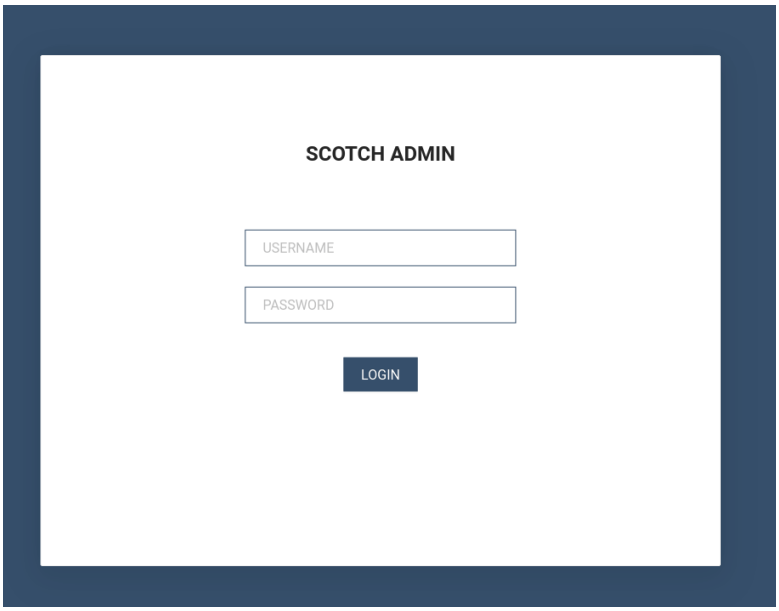
Gambar 1: Antarmuka manajemen MOONSHINE terlihat dalam laporan Citizen Lab tahun 2019 'Kelompok Tibet yang Hilang Menjadi Sasaran Eksploitasi Seluler 1-Klik'.

Pada awal tahun 2022, Lookout melaporkan antarmuka manajemen berbeda yang telah didesain ulang agar terlihat seperti di bawah ini (menggantikan antarmuka sebelumnya pada gambar 1):



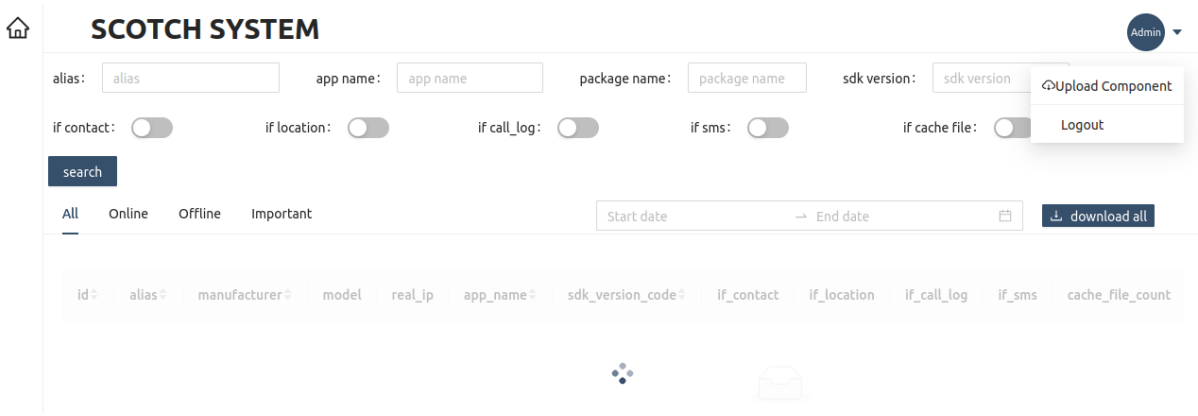
Gambar 2: Antarmuka manajemen MOONSHINE terlihat dalam laporan Lookout 2022 'MOONSHINE: Perkembangan Perangkat Lunak Pengawasan Android oleh APT POISON CARP Tiongkok Untuk Menargetkan Warga Tibet dan Uighur.

Pada bulan Agustus 2023, pemindaian perintah dan kontrol MOONSHINE (C2) mengungkapkan antarmuka yang mirip dengan antarmuka 2022 dengan fungsi **'Lupa Kata Sandi'** tidak lagi tersedia seperti pada gambar 2:



Gambar 3: Antarmuka manajemen MOONSHINE yang diamati pada bulan Agustus 2023 tidak lagi memiliki perintah 'Lupa Kata Sandi'.

Investigasi lebih lanjut terhadap antarmuka manajemen menunjukkan konten dalam panel yang mengungkapkan bagaimana detail perangkat yang disusupi akan disimpan.



Gambar 4: Halaman web di balik halaman login antarmuka manajemen MOONSHINE.

Penelitian Lookout menunjukkan adanya **'skor'** yang diteruskan dari perangkat korban ke server MOONSHINE C2. Nilai 'skor' didasarkan pada izin sampel berbahaya pada perangkat korban.

Kolom 'if_contact', 'if_location', 'if_call_log', dan 'if_sms' di dalam halaman menunjukkan bahwa tidak semua sampel MOONSHINE memiliki akses penuh ke perangkat yang disusupi. Pengetahuan tentang kolom-kolom ini dan 'skor' yang diteruskan dari perangkat ke C2 menunjukkan bahwa pelaku ancaman menggunakan skor untuk mengomunikasikan tingkat akses yang dimiliki malware ke perangkat yang disusupi kepada individu yang mengakses antarmuka manajemen.

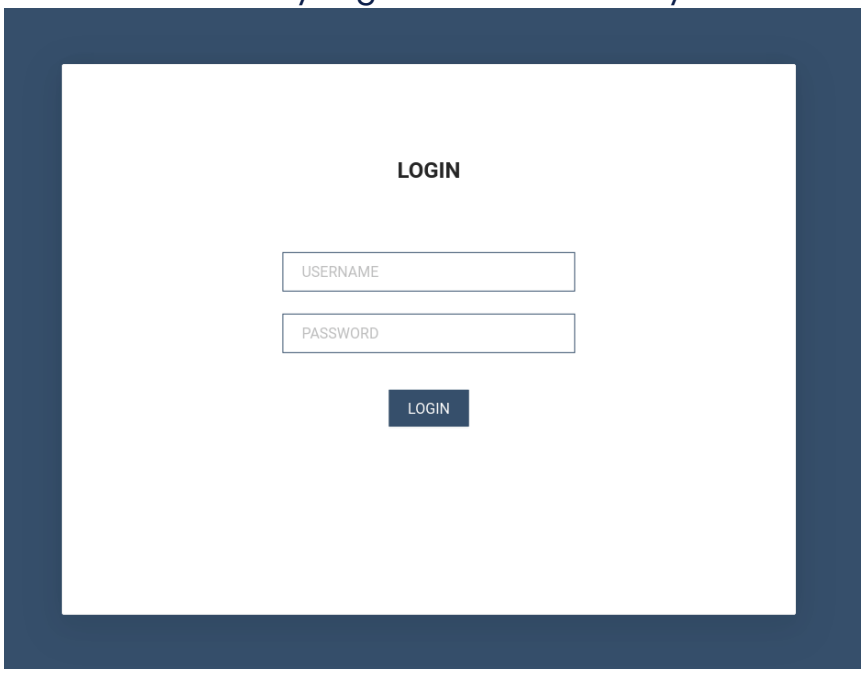
Secara umum, saran praktik terbaik untuk mencegah aplikasi mengumpulkan informasi dari perangkat adalah memeriksa izin aplikasi untuk hal-hal yang tidak biasa sebelum mengunduh. Namun, sampel MOONSHINE mencari izin yang relevan dengan fungsionalitas aplikasi, sehingga mungkin tampak tidak mencurigakan, tetapi mereka juga menggunakan izin ini untuk mengumpulkan informasi dari perangkat.

MOONSHINE juga memiliki Antarmuka Pemrograman Aplikasi (API) yang menunjukkan luasnya kemampuannya. Versi awal dokumentasi API memuat nama API dalam bahasa Mandarin.

Host virtual

Dalam penelusuran panel MOONSHINE, ditemukan contoh hosting virtual. Host virtual adalah saat satu alamat IP dapat menjadi host beberapa situs web sekaligus. Alamat IP dari contoh hosting virtual ini dan domain yang dihosting tidak ditemukan dalam sampel malware yang diketahui.

Contoh antarmuka manajemen ini berbeda, karena judul halamannya adalah **'LOGIN'**, bukan **'SCOTCH ADMIN'** yang terlihat sebelumnya.



Gambar 5: Antarmuka manajemen MOONSHINE menggunakan judul LOGIN, bukan SCOTCH ADMIN.

Selain itu, konten pada panel juga berbeda dari gambar 4, seperti yang terlihat pada gambar 6:

Gambar 6: Halaman web di balik halaman login antarmuka manajemen MOONSHINE yang dihosting secara virtual.

Panel pada gambar 6 tampak seperti versi sederhana dari panel pada gambar 4. Karakteristik panel yang tumpang tindih adalah nama kolom 'id', 'manufacturer', dan 'model' dalam tabel.

Contoh kasus MOONSHINE yang dihosting secara virtual yang ditemukan adalah:

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

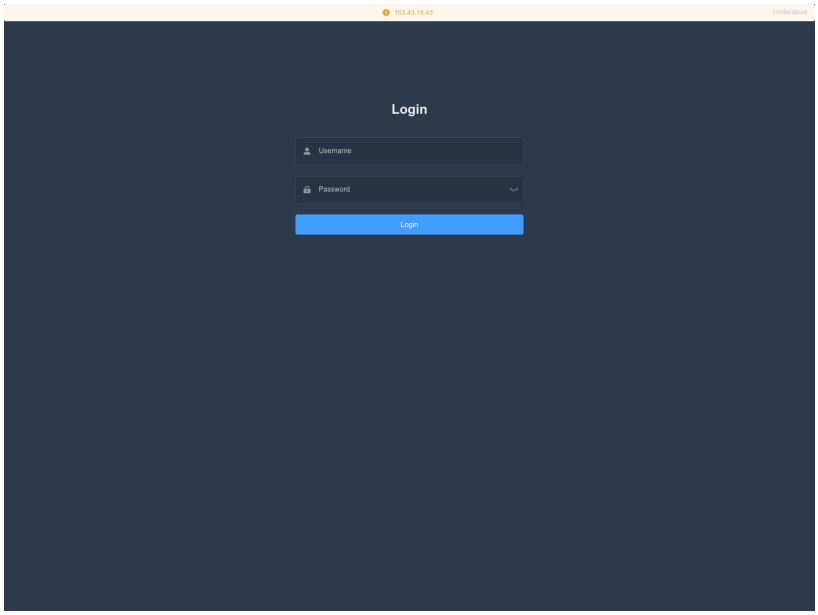
Domain-domain ini dicantumkan oleh Trend Micro sebagai kit eksploitasi MOONSHINE, yang bertanggung jawab untuk mengeksploitasi kerentanan peramban guna memasang malware pada perangkat seluler. Trend Micro menamai malware ini 'Dark Nimbus'.

Untuk klarifikasi, antarmuka manajemen MOONSHINE adalah tempat sampel malware MOONSHINE berkomunikasi, dan ke sanalah data korban diekstraksi. Kit eksploitasi MOONSHINE yang dilaporkan oleh Trend Micro, merupakan kemampuan terpisah yang mengeksploitasi kerentanan browser untuk memasang malware bernama Dark Nimbus pada perangkat seluler. Lebih jauh lagi, Dark Nimbus dan MOONSHINE merupakan malware yang sama sekali berbeda.

Antarmuka manajemen MOONSHINE dan kit eksploitasi MOONSHINE memiliki kode yang tumpang tindih sehingga perintah login serupa pada gambar 3 dan 5 serta konten halaman pada gambar 4 dan 6. Keduanya juga berisi string 'webpackJsonpreact-scotchui' dalam kode sumber.

Pelaku ancaman membuat tautan URL yang terhubung ke kit eksploitasi MOONSHINE dan kemudian dialihkan ke video yang relevan dengan orang Tibet dan Uighur, yang tumpang tindih dengan penargetan MOONSHINE.

Di banyak alamat IP yang menjadi host domain kit eksploitasi MOONSHINE, terdapat halaman login berjudul 'VLiteUI' pada port 444. Halaman ini tidak banyak terlihat dan keberadaannya pada IP ini menunjukkan kemungkinan tautan ke operasi pelaku.



Gambar 7: Panel login dengan judul HTML 'VLiteUI' terlihat pada IP yang juga menjadi host kit eksploitasi MOONSHINE.

Analisis Trend Micro terhadap Dark Nimbus mengungkap malware tersebut dapat mengumpulkan daftar informasi lengkap tentang perangkat, dan berkomunikasi dengan C2 menggunakan protokol XMPP.

Trend Micro juga menguraikan bahwa dalam beberapa versi Dark Nimbus, mereka mengidentifikasi prevalensi string 'DKNS'.

'**ansec[.]com**' (terdaftar sebagai Dark Nimbus C2 oleh TrendMicro) juga ditemukan di layanan XMPP untuk alamat IP lain yang menyajikan halaman web dengan DKNS dalam judulnya:

- 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)

Seperangkat alamat IP lain dengan '**ansec[.]com**' di layanan XMPP memiliki halaman web dengan judul:

- 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)

Menurut Intelligence Online, 'UPSEC' yang diamati pada judul halaman HTML, merujuk pada 'Sichuan Dianke Network Security Technology Co., Ltd'.

Studi kasus kedua: BADBAZAAR

BADBAZAAR adalah malware seluler dengan varian iOS dan Android yang menargetkan warga Uighur, Tibet, dan Taiwan. Spyware ini disebarkan melalui platform media sosial dan toko aplikasi resmi. Laporan terbaru dari Volexity menunjukkan berbagai varian BADBAZAAR, yang dipisahkan sebagai BadSolar, BADBAZAAR, dan BadSignal. Ketiga varian tersebut dihubungkan bersama melalui fungsi yang tumpang tindih yang digunakan untuk mengumpulkan informasi perangkat dan operator.

Penelitian NCSC terhadap BADBAZAAR mengungkapkan hal berikut:

- Pengelompokan domain C2 mengungkap tautan lebih lanjut ke domain yang dilaporkan dalam intelijen ancaman historis.
- Server C2 dan sampel malware mengungkap nama host yang terkait dengan infrastruktur pelaku.
- Profil lebih lanjut yang digunakan pelaku ancaman untuk rekayasa sosial guna menyebarkan malware mereka ke luar toko aplikasi resmi.

Pengelompokan WHOIS/perantara domain

'UJYJYUJ'

Analisis catatan WHOIS untuk domain BADBAZAAR '**signalplus[.]org**' (dilaporkan oleh ESET) menunjukkan nilai '**UJYJYUJ**' di bidang '**State**'.

Pencarian domain lain dengan nilai yang sama akan mengungkap domain yang dimaksud berikut:

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

(Lihat Lampiran A, gambar 1)

Domain **signalplus[.]org**, **tubevideoplus[.]org** dan **thetubeplus[.]com** dilaporkan sebagai domain BADBAZAAR C2, sementara ESET melaporkan sub domain **mail.pmumail[.]com** sebagai server proxy FlyGram. FlyGram adalah aplikasi BADBAZAAR yang dikembangkan oleh pelaku kejahatan siber (lihat Lampiran untuk daftar aplikasi BADBAZAAR lainnya).

Nilai-nilai keyboard walking

NCSC juga telah melihat pola keyboard walking yang serupa di domain BADBAZAAR C2 terdaftar lainnya.

Misalnya, semua domain berikut memiliki nilai '**REWR**' yang diamati di kolom '**State**' (seperti yang digunakan sebelumnya):

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

(Lihat Lampiran A, gambar 2)

Domain dengan nilai bidang status 'FSDF'

Kumpulan domain BADBAZAAR C2 lainnya memiliki nilai **'State' 'FSDF'**:

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

(Lihat Lampiran A, gambar 3)

Pelaporan historis dengan nilai keyboard walking

Penggunaan nilai keyboard walking dalam catatan WHOIS domain BADBAZAAR juga dapat dilihat dalam penargetan organisasi Tibet yang dilaporkan secara historis oleh TA413. Recorded Future telah mengamati domain yang dikendalikan aktor yang memalsukan organisasi Tibet dan penggunaan nilai organisasi pendaftar **“asfasf”**.

clublogs[.]com

Sampel BADBAZAAR yang diperoleh Lookout berisi '**xle.clublogs[.]com**' sebagai domain C2. Domain root '**clublogs[.]com'** dihosting pada alamat IP '**95.179.210[.]85**' dan memiliki sertifikat SSL dengan subjek dan nilai penerbit '**CN=WIN-50QO3EIRQVP'.** Nilai ini cocok dengan sertifikat SSL yang ditemukan dalam sampel BADBAZAAR yang menggunakan penyematan SSL untuk menghindari penyadapan komunikasi.

Riwayat hosting untuk alamat IP **95.179.210[.]85** mengembalikan domain yang diminati berikut ini:

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

(Lihat Lampiran A, gambar 4)

www.voiceoftibet[.]net

Domain '**www.voiceoftibet[.]net**' tampaknya menyamar sebagai stasiun radio 'Voice of Tibet', mirip dengan TTP yang digunakan oleh TA413.

Domain '**rewrwer[.]com**' mirip dengan nilai '**State**' yang diidentifikasi sebelumnya '**REWR**' yang ditemukan dalam catatan WHOIS domain BADBAZAAR.

Domain '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' dan '**myloughborough[.]com**' semuanya didaftarkan dengan alamat email '**tplutalova@list[.]ru**'.

actuallys[.]com

Catatan WHOIS untuk '**actuallys[.]com**' menunjukkan contoh di mana alamat email teknisi dan admin adalah '**tplutalova@list[.]ru**' tetapi email pendaftar adalah '**ivan_s81@mail[.]ru**'.

Informasi WHOIS historis untuk domain '**actuallys[.]com**' mengungkapkan email pendaftaran '**wangminghua6@gmail[.]com**' terdaftar pada tanggal 24 Februari 2016. Pada tanggal 11 Maret 2016, email tersebut kemudian diubah menjadi '**ivan_s81@mail.ru**' meskipun tanggal kedaluwarsa registrasi registrar tetap sama.

wangminghua6@gmail[.]com

Alamat email '**wangminghua6@gmail[.]com**' digunakan untuk mendaftarkan domain yang ditemukan dalam pelaporan intelijen ancaman historis. Pada tahun 2015, Palo Alto mengidentifikasi email yang digunakan untuk mendaftarkan domain C2 untuk malware, Cmstar. Pada tahun 2014, email tersebut juga

digunakan untuk mendaftarkan domain yang diidentifikasi oleh Mandiant dalam kampanye phishing yang dilakukan oleh APT3. Pada tahun 2013, kode ini digunakan untuk mendaftarkan domain yang ditemukan oleh CrowdStrike dalam dropper malware dengan jalur Program Database (PDB) yang berisi karakter bahasa Mandarin. Hal ini menunjukkan kompilasi pada sistem bahasa Mandarin.

taoyujun@gmail[.]com

Domain '**hcjbtt[.]com**' didaftarkan dengan alamat email '**taoyujun@gmail[.]com**' tetapi email administratornya didaftarkan dengan '**wangminghua6@gmail[.]com**'.

Tidak ada aktivitas jahat yang terkait dengan domain '**hcjbtt[.]com**', namun alamat email '**taoyujun@gmail[.]com**' ditemukan dalam laporan intelijen ancaman historis. Pada tahun 2014, alamat email tersebut digunakan untuk mendaftarkan domain yang ditemukan oleh Mandiant dalam sampel '**Cueisfry Trojan**' yang digunakan untuk menargetkan organisasi Jepang.

Alamat email tersebut juga mendaftarkan domain seperti '**iaea-international[.]org**' yang menyamar sebagai **Badan Tenaga Atom Internasional** dan '**idc-ctbto[.]org**' yang menyamar sebagai **Pusat Data Internasional** di **Organisasi Perjanjian Pelarangan Uji Coba Nuklir Komprehensif (CTBTO)**.

Catatan Whois sebelumnya untuk domain '**iaea-international[.]org**' menunjukkan email pendaftar adalah '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Domain '**udtglobals[.]com**' diamati menggunakan '**wangminghua6@gmail[.]com**' sebagai email administrator dan '**ocean.nio@rediffmail[.]com**' sebagai alamat email pendaftar. Catatan WHOIS lainnya untuk domain ini, menunjukkan email pendaftar yang sama tetapi dengan alamat email administrator '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' tampaknya menyamar sebagai '**UDT Global**' yang merupakan acara global untuk perusahaan pertahanan dan keamanan bawah laut. Nama pengguna '**ocean.nio**' dalam alamat email tersebut mungkin meniru **Institut Oseanografi Nasional (NIO)** yang ada di beberapa negara. Meskipun penggunaan layanan email '**Rediff**' (yang berbasis di India) dapat menunjukkan tiruan dari **Institut Oseanografi Nasional India**.

Djibdiplomatie[.]com

Domain '**djibdiplomatie[.]com**' tampaknya menyamar sebagai layanan diplomasi Djibouti, yang memiliki catatan WHOIS serupa dengan '**utdglobals[.]com**'. Satu catatan menunjukkan pendaftar '**ocean.nio@rediffmail[.]com**' dan admin '**taoyujun@gmail[.]com**' sedangkan catatan lain menunjukkan '**wangminghua6@gmail[.]com**' sebagai alamat email admin dengan '**ocean.nio@rediffmail[.]com**' sebagai email pendaftar.

Kedua domain ini juga memiliki nilai jenis pergerakan keyboard dalam catatan WHOIS. Misalnya, '**udtglobals[.]com**' memiliki nilai '**ASDF**' sebagai kota pendaftarnya dan '**djibdiplomatie[.]com**' memiliki '**DAF DAGF**' sebagai nilai nama pendaftarnya. Ini sebanding dengan nilai yang diamati di domain BADBAZAAR lainnya.

Meskipun alamat email '**wangminghua6@gmail[.]com**' dan '**taoyujun@gmail[.]com**' ditemukan dalam catatan WHOIS untuk domain yang menyamar sebagai **acara pertahanan bawah laut global**, **layanan diplomasi Djibouti**, dan **Badan Tenaga Atom Internasional**, alamat tersebut juga ditemukan dalam catatan WHOIS untuk sejumlah domain yang tidak berbahaya.

Campuran domain penyamaran dan domain yang tidak berbahaya dapat menunjukkan keberadaan entitas pengadaan infrastruktur yang digunakan untuk mendukung operasi pelaku kejahatan siber.

Alamat email '**ocean.nio@rediffmail[.]com**' hanya ditemukan di domain penyamaran yang dijelaskan di atas. '**ivan_s81@mail[.]ru**' dan '**tplutalova@list[.]ru**' masing-masing telah mendaftarkan sejumlah kecil domain, dan beberapa domain ini telah dihosting di infrastruktur BADBAZAAR. Ketiga alamat email ini diyakini lebih erat kaitannya dengan operasi pelaku kejahatan siber. Hal ini karena lebih banyak domain yang dikaitkan dengan aktivitas jahat, dibandingkan dengan email '**wangminghua6@gmail[.]com**' dan '**taoyujun@gmail[.]com**'.

(Lihat Lampiran A, gambar 5)

Tautan ke pelaku ancaman lainnya

Karakteristik umum lain dari domain terkait BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', dan '**voiceoftibet[.]net**' adalah bahwa semuanya terdaftar di eNom dan telah 'diparkir' di '**255.255.255[.]254**'.

Berdasarkan investigasi NCSC sebelumnya, domain lain dengan karakteristik ini mengungkapkan aktivitas terkait dengan **APT5** pada tahun 2019, dan **APT14** antara tahun 2009 dan 2011.

Domain yang terhubung dengan APT5- memiliki catatan WHOIS historis yang mencantumkan '**taoyujun@gmail[.]com**' sebagai alamat email pendaftar.

Domain yang terhubung dengan APT14 memiliki subdomain tiga huruf yang tampaknya mewakili target yang dituju dari operasi jahatnya. Contohnya adalah '**bae.cisconline[.]net**', yang menunjukkan target yang dituju dari BAE Systems dan ditemukan dalam sampel '**Poison Ivy**'.

Karakteristik serupa diamati di domain BADBAZAAR tempat subdomain terkait dengan nama aplikasi yang terkena trojan:

Judul 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

Penting untuk dicatat bahwa aktivitas yang terkait dengan APT5 dan APT14 bersifat historis dan ada pula domain lain yang terdaftar dengan eNom dan diselesaikan ke '**255.255.255.254**' yang tidak dapat dikaitkan dengan aktivitas jahat. Oleh karena itu, tidak dapat dipastikan bahwa pelaku di balik kampanye ini sama atau terkait.

Nama Mesin

Analisis BADBAZAAR C2 dan sampel mengungkapkan nama host yang digunakan sebagai nilai 'Nama Umum' dalam sertifikat SSL. Investigasi NCSC terhadap nama host yang diamati dalam sampel dan infrastruktur BADBAZAAR menunjukkan bahwa nama host ini digunakan di beberapa alamat IP. Alamat IP ini menjadi host domain yang ditemukan dalam sampel BADBAZAAR. Ada detail lebih lanjut di bagian di bawah ini tentang nama host, dan alamat IP dengan nama host yang menjadi host domain BADBAZAAR C2.

Dalam hampir semua kasus, keberadaan sertifikat dengan nilai nama host tumpang tindih dengan resolusi IP untuk nama domain berbahaya yang ditentukan, beberapa contoh di mana hal ini tidak terjadi telah diuraikan.

WIN-EU0VLBL7TUJ

Nama host '**WIN-EU0VLBL7TUJ**' ditemukan pada alamat IP yang dimaksud berikut:

- '**116.203.53[.]21**' menjadi host domain BADBAZAAR C2 '**uyapkfinder[.]com**' dan '**thewestuniverse[.]com**'.
- '**95.216.169[.]27**' menjadi host domain BADBAZAAR C2 '**adysfunction[.]com**' dan subdomain '**download.apkbazar[.]biz**' diamati sebagai tautan unduhan untuk sampel BADBAZAAR.

(Lihat Lampiran A, gambar 6)

WIN-70E59JVOB9G

Nama host '**WIN-70E59JVOB9G**' ditemukan pada alamat IP yang dimaksud berikut:

- '**23.88.28[.]220**' menjadi host subdomain BADBAZAAR C2, **'aua.rondwsign[.]com', 'nal.tokenmajorp[.]com', 'pep.rondwsign[.]com'** '**doa.rondwsign[.]com**', dan **'pls.rondwsign[.]com'.** Ada rentang waktu dua hari antara saat sertifikat pada mesin terakhir terlihat dan saat domain berbahaya pertama kali terlihat mengarah ke IP.

- '**23.88.28[.]221**' menjadi host subdomain yang terhubung dengan BADBAZAAR '**bt.bhvghg[.]com**'.

- **'23.88.28[.]222**' menjadi host domain BADBAZAAR C2 '**tubevideoplus[.]org**' dan '**cde.mpoxcases[.]com**'.

- '**65.21.92[.]67**' menjadi host subdomain BADBAZAAR C2 '**bat.androidupdated[.]net**'. Ia juga menjadi host subdomain '**apps.androidupdated[.]net**' yang merupakan malware DoubleAgent C2.

- '**65.21.92[.]77**' menjadi host subdomain BADBAZAAR C2 '**wyo.titeperformance[.]com**', '**big.collinformations[.]com**' '**vpf.titeperformance[.]com**', '**eud.titeperformance[.]com**' dan '**afg.collinformations[.]com**'

- '**65.108.192[.]134**' menjadi host subdomain BADBAZAAR C2 '**upd.whoscaller.net**'. dan '**ggl.whoscaller[.]net**'.

- '**142.132.131[.]15**' menjadi host subdomain BADBAZAAR C2 '**bvn.lookincategory[.]com**' dan '**edr.lookincategory[.]com**'. Ada jangka waktu sebelas hari antara saat sertifikat dengan nama mesin terakhir terlihat dan saat domain berbahaya pertama kali terlihat mengarah ke IP.

- '**142.132.131[.]20**' menjadi host subdomain '**son.onlinegamersgroup[.]com**' dan '**system.onlinegamersgroup[.]com**', diyakini sebagai BADBAZAAR C2 karena keduanya dihosting saat sertifikat SSL terkait BADBAZAAR ditemukan di IP tersebut.

- '**142.132.131[.]28**' menjadi host domain BADBAZAAR C2 '**goldplusapp[.]net**' dan subdomain '**who.goldplusapp[.]net**' dan '**cgf.goldplusapp[.]net**'.

- '**162.55.103[.]211**' menjadi host subdomain BADBAZAAR C2 '**oha.alpinemap[.]net**', '**aru.alpinemap[.]net**', '**aso.alpinemap[.]net**', '**afr.alpinemap[.]net**', dan '**aar.alpinemap[.]net**'.

- '**162.55.103[.]212**' menjadi host subdomain 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**' menjadi host subdomain BADBAZAAR C2 '**ggl.whoscaller[.]net**' dan '**upd.whoscaller.net**'. Ada jangka waktu tiga hari antara saat sertifikat dengan nama mesin pertama kali terlihat dan saat domain berbahaya terakhir kali terlihat mengarah ke IP.

- '**195.154.60[.]3**' menjadi host subdomain BADBAZAAR C2 '**upd.whoscaller[.]net**'**ggl.whoscaller[.]net**'.

- '**212.83.189[.]89**' menjadi host subdomain BADBAZAAR C2 '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' dan '**afg.collinformations[.]com**'.

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

(Lihat Lampiran A, gambar 7)

WIN-50QO3EIRQVP

Nama host '**WIN-50QO3EIRQVP**' ditemukan pada alamat IP yang dimaksud berikut:

- '**45.76.132[.]91**' menjadi host domain, '**yumoftion[.]com**', '**androidupdated[.]net**'. Kedua domain tersebut terhubung ke BADBAZAAR sebagai subdomain '**fow.yumoftion[.]com**' dan '**bat.androidupdated[.]net**' adalah domain BADBAZAAR C2. Selain itu subdomain '**apps.androidupdated[.]net**' adalah domain DoubleAgent C2. Alamat ini juga menjadi host domain '**pmstwocqn[.]com**', yang terhubung ke BADBAZAAR melalui catatan WHOIS.

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

- '**199.247.21[.]34**' menjadi host '**titeperformance[.]com**', dan '**collinformations[.]com**' yang subdomainnya adalah domain BADBAZAAR C2.

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

(Lihat Lampiran A, gambar 8)

WMSvc-WIN-50QO3EIRQVP

Nama host '**WMSvc-WIN-50QO3EIRQVP**' ditemukan pada alamat IP yang dimaksud berikut:

- '**78.46.185[.]251**' menjadi host domain BADBAZAAR C2 '**groupgram[.]org**', dilaporkan oleh Volexity menggunakan port 4432 untuk koneksi berbahaya.

- '**65.21.92[.]69**' dan '**163.172.205[.]207**' menjadi host domain '**widelygram[.]org**' yang diyakini sebagai domain BADBAZAAR C2, karena meskipun dihosting di kedua IP tersebut, port 4432 terbuka.

- **'163.172.198[.]206'** menjadi host domain **'maxgram[.]org'** yang diyakini sebagai domain BADBAZAAR C2, karena saat dihosting port 4432 terbuka.

(Lihat Lampiran A, gambar 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Nama host '**WMSvc-WIN-50QO3EIRQVP**' dan '**WIN-7LSBB9R0F1L**' diamati pada alamat IP berikut secara bersamaan:

- '**148.251.87[.]245**' menjadi host domain BADBAZAAR C2 '**flygram[.]org**' dan '**groupgram[.]org**'.

(Lihat Lampiran A, gambar 10)

WIN-N8H8S9BG2P0

Nama host '**WIN-N8H8S9BG2P0**' ditemukan pada alamat IP berikut:

- '**148.251.87[.]247**' menjadi host domain BADBAZAAR C2 '**omarwhatsapp[.]org**' dan '**flygram[.]org**'.

(Lihat Lampiran A, gambar 11)

WIN-I6VBN8MR92A

Nama host '**WIN-I6VBN8MR92A**' terpantau pada alamat IP berikut:

- '**148.251.87[.]197**' menjadi host domain BADBAZAAR C2 '**tryhrwserf[.]com**'.

(Lihat Lampiran A, gambar 12)

Berdasarkan data komersial yang tersedia, prevalensi nama-nama mesin ini di internet bervariasi. Beberapa di antaranya diamati secara bersamaan di beberapa alamat IP yang menunjukkan bahwa VM dibuat dari templat yang sama. Penting untuk dicatat bahwa untuk beberapa nama host, tidak semua IP

tempat nama-nama tersebut diamati dapat dikaitkan dengan aktivitas jahat. Ini dapat berarti bahwa penggunaan nama host tidak eksklusif untuk pelaku ancaman ini.

Namun, prevalensi beberapa nama mesin ini di seluruh IP yang telah menjadi host domain BADBAZAAR C2, dapat menunjukkan bahwa entitas pengadaan infrastruktur digunakan untuk mengonfigurasi mesin guna mendukung operasi siber pelaku kejahatan.

Kehadiran di media sosial

Pelaporan sebelumnya oleh Volexity menunjukkan bahwa video YouTube (yang mempromosikan penggunaan aplikasi berbahaya) dibuat oleh pelaku kejahatan siber. Video ini menyertakan tutorial tentang cara menggunakan aplikasi yang dikembangkan.

NCSC telah menemukan dua saluran YouTube tambahan yang terkait dengan operasi pelaku kejahatan siber. Saluran YouTube dengan pegangan URL '**@josephjoey3499**' tampaknya mempromosikan penggunaan '**Maxgram**' dan saluran tambahan yang terdaftar dengan '**@uyghurapks3096**' mempromosikan '**Uyghur APK Finder**'.

Selain itu, video YouTube yang mempromosikan '**Flygram**' dan '**Signal Plus**', menunjukkan pelaku ancaman menggunakan nomor telepon yang terlihat. Dalam '**Flygram**' video, pada menit ke 0:36 nomor telepon '**+1 (570) 378-7250**' terlihat dan selama '**Signal Plus**' video, nomor telepon '**+1 (267) 298 4259**' terlihat.

Volexity melaporkan situs berita palsu bertema Tibet '**ignitetibet[.]net**', yang mereka temukan di saluran Telegram yang diyakini dioperasikan oleh pelaku ancaman. Alamat email '**choekyi.wangmo@ignitetibet[.]net**' terlihat meninggalkan komentar pada posting di halaman '**tibetone.org**' yang telah dilaporkan secara publik oleh Lookout sebagai halaman C2 yang digunakan untuk varian iOS dari BADBAZAAR.

Alamat email ini diyakini dikendalikan oleh aktor, menggunakan persona '**Choekyi Wangmo**'.

Penilaian

BADBAZAAR dan MOONSHINE menggunakan beberapa metode rekayasa sosial untuk secara khusus menargetkan komunitas Uighur, Tibet, dan Taiwan, yaitu:

- trojanisasi aplikasi yang menarik bagi komunitas ini, seperti aplikasi Al-Qur'an berbahasa Uighur, hampir pasti disesuaikan dengan basis korban yang menjadi target
- penambahan aplikasi Trojan ini ke toko aplikasi resmi sangat mungkin memberikan kesan legitimasi, dan berbagi dalam obrolan grup sangat mungkin dimaksudkan untuk mengeksploitasi hubungan tepercaya dalam komunitas ini

BADBAZAAR dan MOONSHINE mengumpulkan data yang hampir pasti akan berharga bagi negara Tiongkok. Meskipun BADBAZAAR dan MOONSHINE telah diamati menargetkan orang Uighur, Tibet, dan Taiwan, ada malware lain yang menargetkan kelompok minoritas lain di Tiongkok. Warga negara dari negara-negara yang ikut menyegel, di Tiongkok dan luar negeri, yang dianggap mendukung gerakan yang mengancam stabilitas rezim, hampir pasti terancam oleh malware seluler seperti BADBAZAAR dan MOONSHINE. Kemampuan untuk menangkap data lokasi, audio, dan foto hampir pasti memberikan peluang untuk menginformasikan operasi pengawasan dan pelecehan di masa mendatang dengan memberikan informasi waktu nyata tentang aktivitas target.

MITRE ATT&CK®

Laporan ini telah disusun dengan mengacu pada kerangka kerja MITRE ATT&CK®, basis pengetahuan yang dapat diakses secara global tentang taktik dan teknik musuh berdasarkan pengamatan di dunia nyata.

Taktik	ID	Teknik	Prosedur
Pengintaian	T1593.001	Cari Situs Web/Domain Terbuka: Media Sosial	Pelaku menemukan grup dan forum daring yang cocok dengan korban yang dituju untuk menyebarkan malware
Pengembangan Sumber Daya	T1583.001	Memperoleh Infrastruktur: Domain	Pelaku mendaftarkan domain untuk server perintah dan kontrol mereka
Pengembangan Sumber Daya	T1587.001	Kemampuan Pengembangan: Malware	Kode berbahaya ditulis untuk dimasukkan ke dalam aplikasi yang terinfeksi Trojan
Pengembangan Sumber Daya	T1608.001	Kemampuan Tahap: Mengunggah Malware	Aplikasi yang terkena Trojan diunggah ke platform daring termasuk toko aplikasi
Pengembangan Sumber Daya	T1585.001	Membuat Akun: Akun Media Sosial	Pelaku membuat akun di situs web dan media sosial untuk berbagi dan mengiklankan malware
Pengembangan Sumber Daya	T1585.002	Membuat Akun: Akun Email	Pelaku menggunakan akun email yang dihosting secara pribadi dan komersial untuk menjadi host dan berbagi malware
Akses Awal	T1189	Menyusupkan: Drive-by	Skrip berbahaya disembunyikan di aplikasi yang sah dan diunggah ke toko aplikasi
Akses Awal	T1566.003	Phishing: Spearphishing melalui Layanan	Pelaku mengirim aplikasi trojan ke grup yang ditargetkan melalui media sosial termasuk Telegram
Eksekusi	T1204.002	Eksekusi Pengguna: File Berbahaya	Korban harus memasang aplikasi Trojan untuk mengeksekusi payload

Penghindaran Pertahanan	T1027.009	File atau Informasi yang Disamarkan: Muatan Tertanam	Muatan berbahaya disembunyikan dalam aplikasi yang sah
Penghindaran Pertahanan	T1036.005	Penyamaran: Mencocokkan Nama atau Lokasi yang Sah	File yang terkena trojan akan mencocokkan nama, tampilan, dan fungsi aplikasi yang sah.
Penghindaran Pertahanan	T1656	Peniruan	Pelaku meniru individu tepercaya dengan membuat situs web palsu dan menggunakan nama pengguna yang terkait dengan kelompok target.
Koleksi	T1123	Perekaman Audio	Aplikasi yang terkena virus trojan mungkin meminta izin yang tidak diperlukan termasuk akses mikrofon
Koleksi	T1125	Perekaman Video	Aplikasi yang terkena virus trojan mungkin meminta izin yang tidak diperlukan termasuk akses kamera
Koleksi	T1005	Data dari Sistem Lokal	Aplikasi yang terkena virus Trojan mungkin meminta izin yang tidak diperlukan termasuk file lokal.
Perintah dan Kontrol	T1071.001	Protokol Lapisan Aplikasi: Protokol Web	Malware terhubung ke C2 menggunakan HTTPS dan WebSocket.
Perintah dan Kontrol	T1509	Port Non-Standar	Port nonstandar digunakan seperti port 4432 dan 2333
Eksfiltrasi	T1041	Eksfiltrasi Melalui Saluran C2	Malware mengeksfiltrasi data menggunakan koneksi HTTPS dan WebSocket.
Dampak	T1565.002	Manipulasi Data: Manipulasi Data yang Ditransmisikan	Pelaku memperoleh data dari korban dengan mengaktifkan lalu lintas web aplikasi yang tidak diperlukan untuk fungsionalitas aplikasi

Indikator

MOONSHINE:

- Pada tanggal 1 April 2025, pencarian panel VLiteUI menghasilkan hal berikut:

Alamat IP	Port	Pertama Kali Dilihat	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 tanggal 1 April 2025, penelusuran panel SCOTCH ADMIN menghasilkan hal berikut:

Alamat IP	Port	Pertama Kali Dilihat	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 tanggal 14 Maret 2024, penelusuran panel SCOTCH ADMIN virtual menghasilkan hal 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:

Deskripsi	Sertifikat SSL diamati pada BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Pada tanggal 1 April 2025, pencarian sertifikat BADBAZAAR di atas menghasilkan hal berikut:

Alamat IP	Port	Pertama Kali Dilihat	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

Deskripsi	Sertifikat SSL diamati pada BADBAZAAR C2
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Pada tanggal 1 April 2025, pencarian sertifikat BADBAZAAR di atas menghasilkan hal berikut:

Alamat IP	Port	Pertama Kali Dilihat	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 WHOIS

Di bawah ini adalah tabel domain yang saat ini atau secara historis memiliki catatan WHOIS dengan nilai yang cocok dengan yang diamati di domain BADBAZAAR C2.

Nilai WHOIS	Domain
Negara 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
Negara 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
Negara 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 Email
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

Berikut ini adalah tautan ke indikator kompromi (IoC) lain yang terkait dengan BADBAZAAR dan MOONSHINE. NCSC tidak dapat mengonfirmasi validitas semua informasi dalam tautan ini dan pembaca disarankan untuk memverifikasi keakuratan dan relevansinya secara independen:

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

Mitigasi

NCSC menganjurkan penerapan rekomendasi di bawah ini untuk mempertahankan diri dari ancaman yang dijelaskan dalam studi kasus.

- **Operator toko aplikasi, termasuk toko aplikasi pihak ketiga, dan pengembang harus memastikan bahwa aplikasi di platform mereka aman dan mematuhi Kode Praktik pemerintah.** 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

- **Dukungan multibahasa:** Pengembang aplikasi harus berinvestasi dalam upaya melokalkan aplikasi populer bagi pengguna yang berbicara dalam bahasa minoritas di antara kelompok sasaran termasuk Uyghur, Tibet, Hokkien Taiwan, dan Kanton. Panduan Apple untuk melokalkan dalam aplikasi: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Panduan Google tentang aplikasi penerjemahan: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Menjaga keamanan platform media sosial Anda:** Perusahaan media sosial dapat mempersulit pelaku kejahatan siber untuk membuat akun palsu dan membagikan berkas atau tautan berbahaya di platform mereka di komunitas daring yang sah. Jika memungkinkan, perusahaan harus membagikan indikator berbahaya dengan industri yang lebih luas untuk meningkatkan pemahaman kolektif tentang ancaman tersebut dan membantu langkah-langkah perlindungan.

- **Rencana perbaikan untuk pelanggan:** Organisasi harus memiliki prosedur untuk memberi tahu pelanggan yang telah memasang aplikasi berbahaya menggunakan layanan mereka. Peringatan ini harus menarik perhatian dan informatif. Jika sesuai, organisasi harus memberikan panduan tentang cara menghapus perangkat lunak dan mendorong

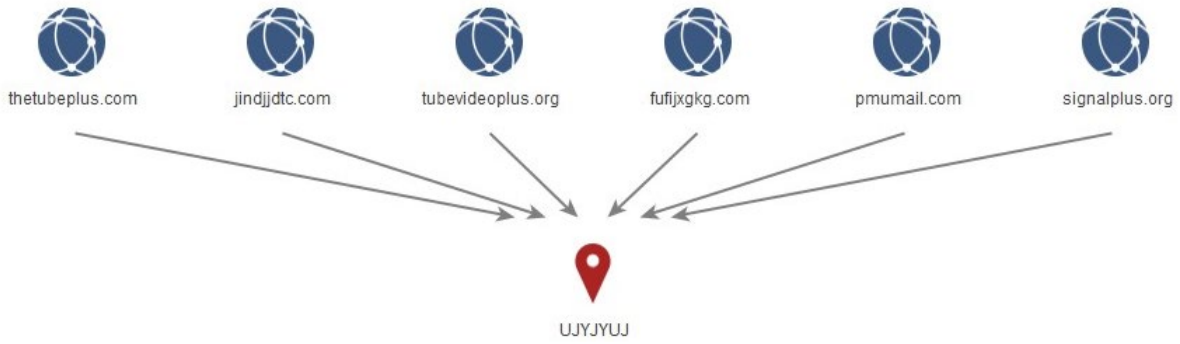
korban untuk melaporkannya kepada pihak berwenang, seperti NCSC di Inggris Raya.
Lihat Kode Praktik App Store untuk informasi lebih lanjut: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Kelompok kerja untuk kolaborasi:** Perusahaan media sosial dapat membentuk kelompok kerja, yang memungkinkan tim keamanan masing-masing untuk berbagi indikator berbahaya, TTP, dan pengamatan, sehingga mempersulit pelaku kejahatan untuk menggunakan platform mereka guna mendukung kampanye berbahaya.

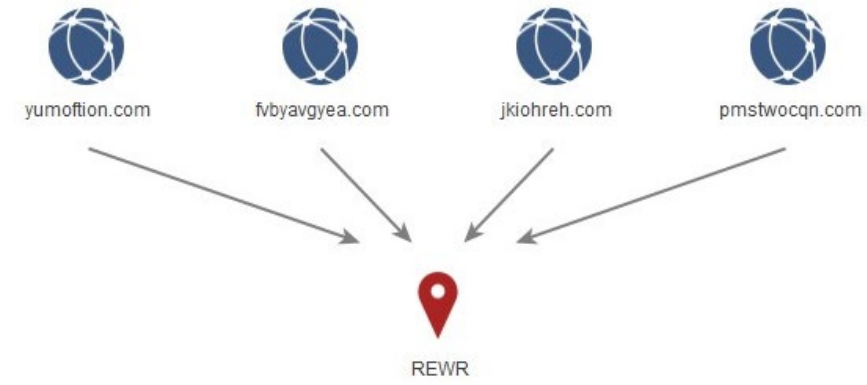
- **Mendeteksi aplikasi yang diubah:** Jika memungkinkan, pengembang aplikasi harus menyertakan fungsi yang memberi tahu pengguna jika mereka telah mengunduh versi aplikasi yang 'tidak resmi', untuk membantu melindungi dari salinan berbahaya.

Lampiran A: Grafik informasi pengelompokan WHOIS BADBAZAAR / pialang domain

Gambar 1 - 'UKYJYUJ'

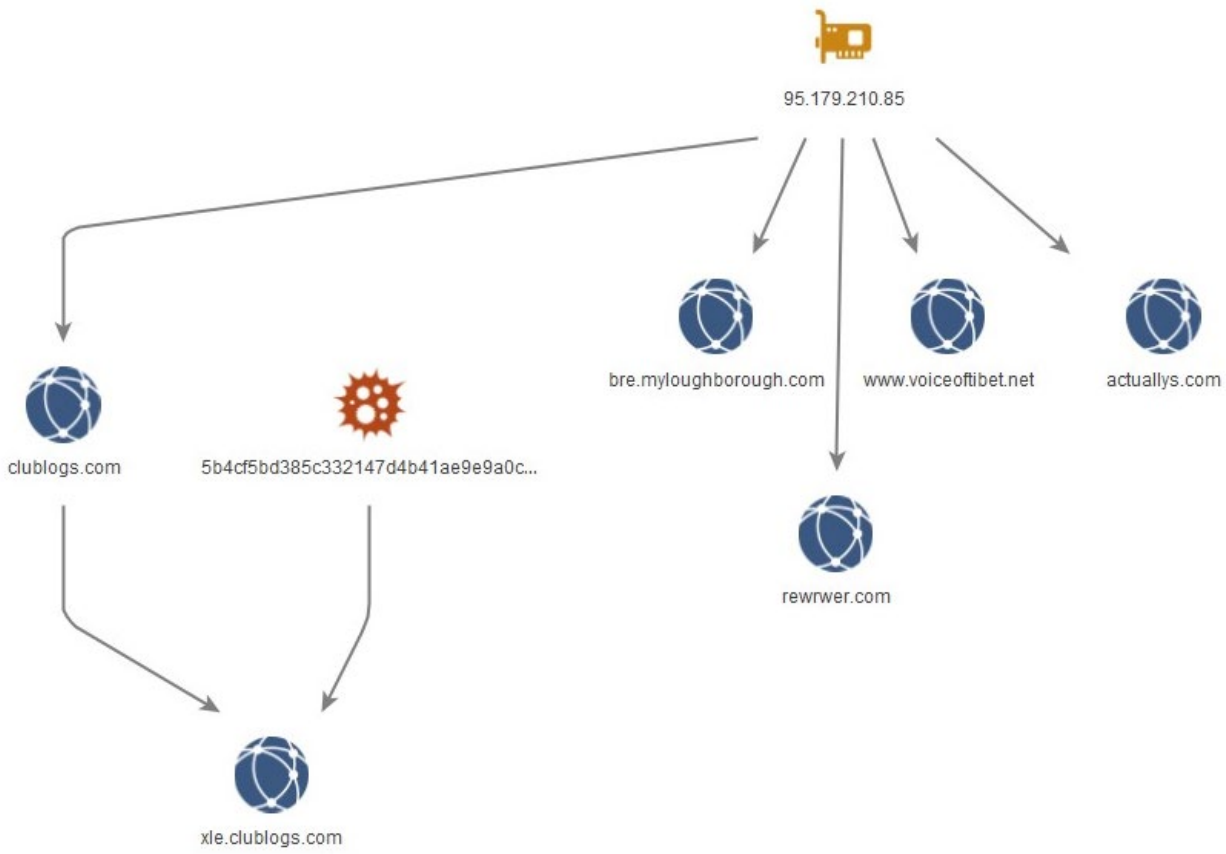


Gambar 2 – Nilai keyboard walking

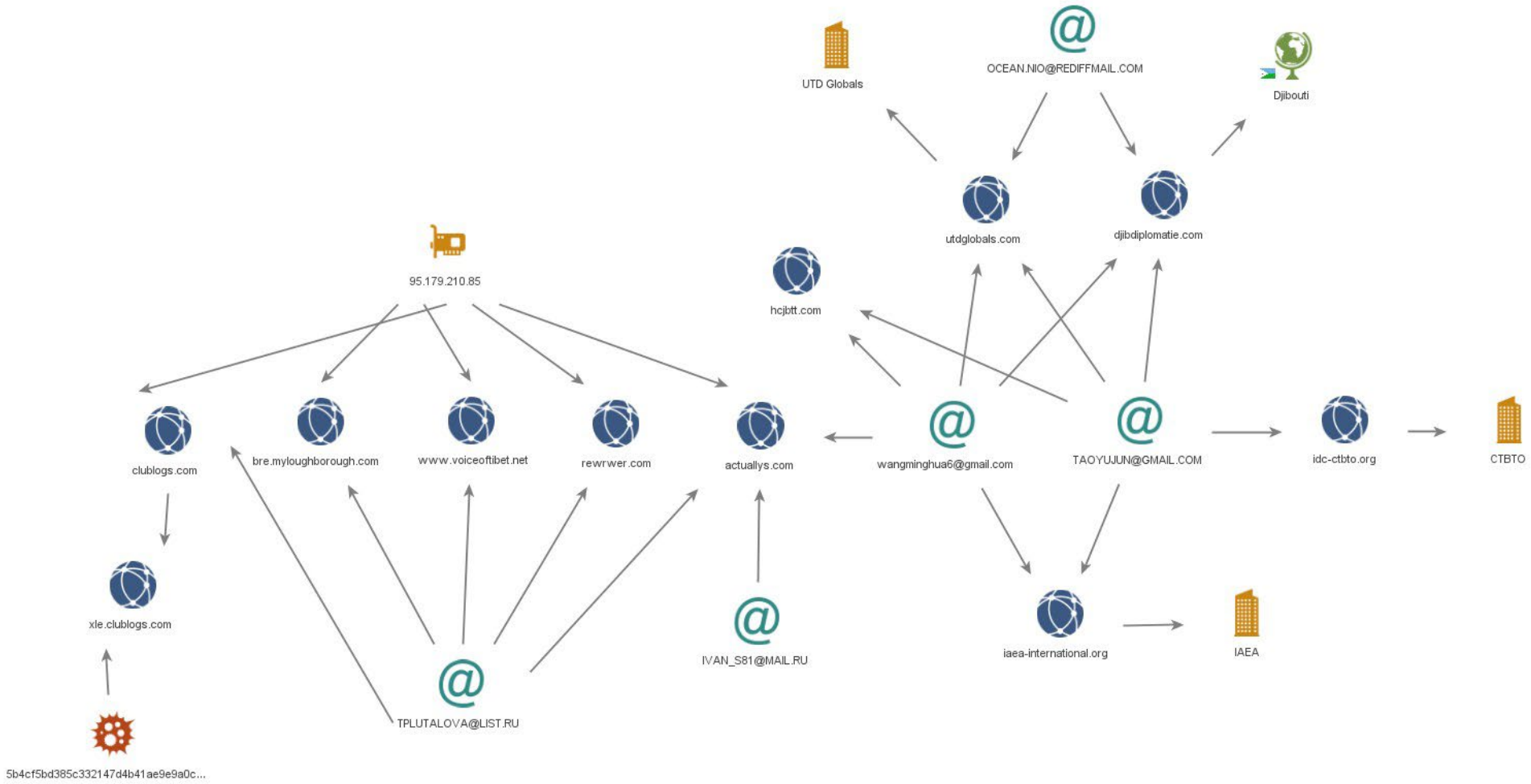


Gambar 3 – Domain tambahan dengan nilai bidang status 'FSDF'

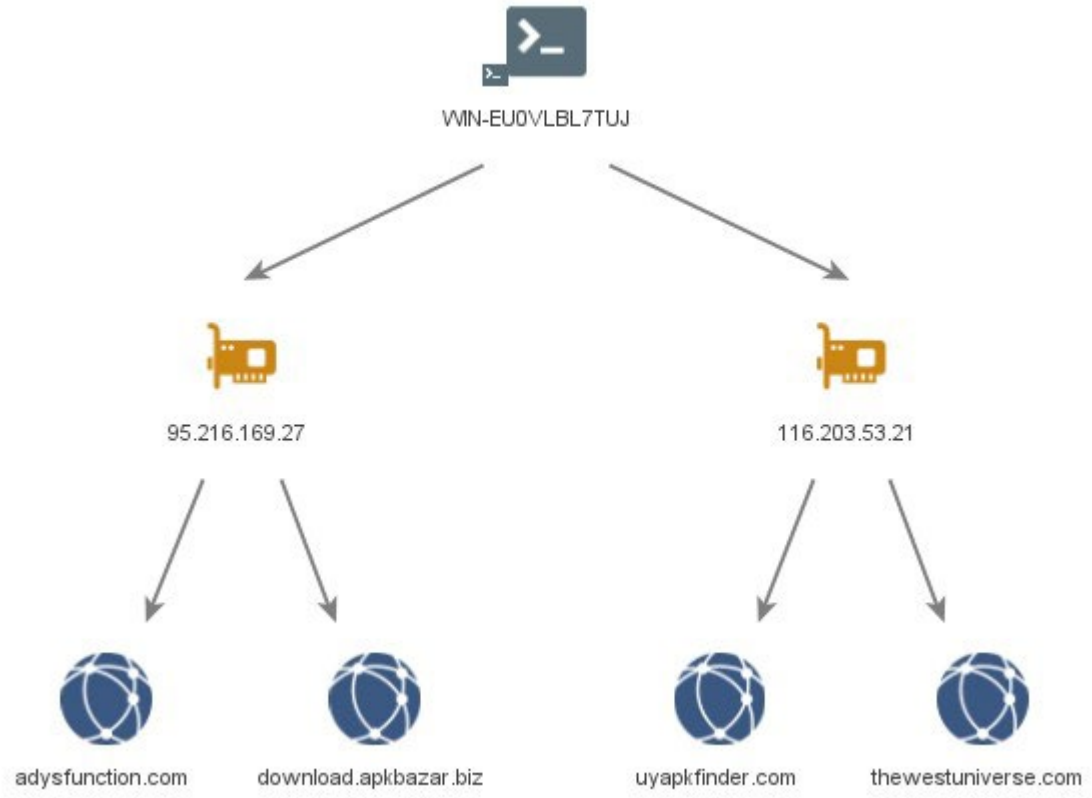
Gambar 4 – **95.179.210[.]85**



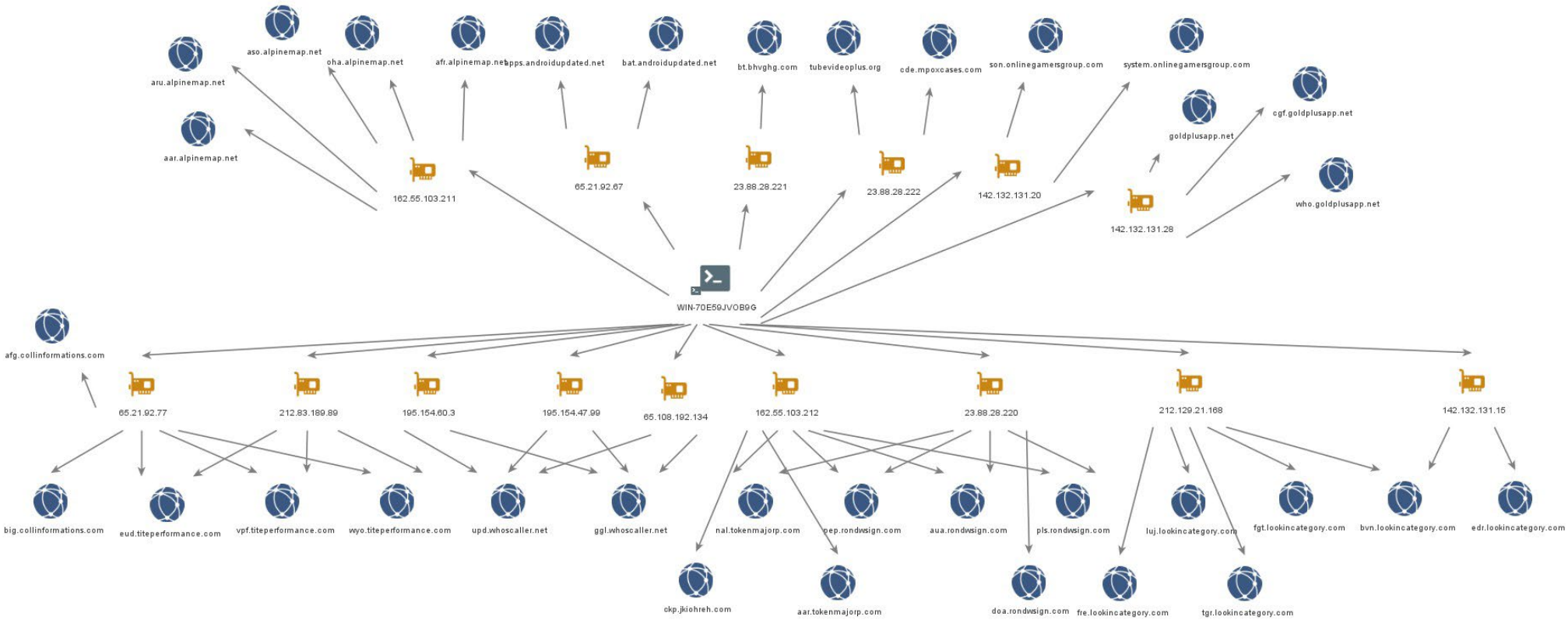
Gambar 5 – Tautan WHOIS



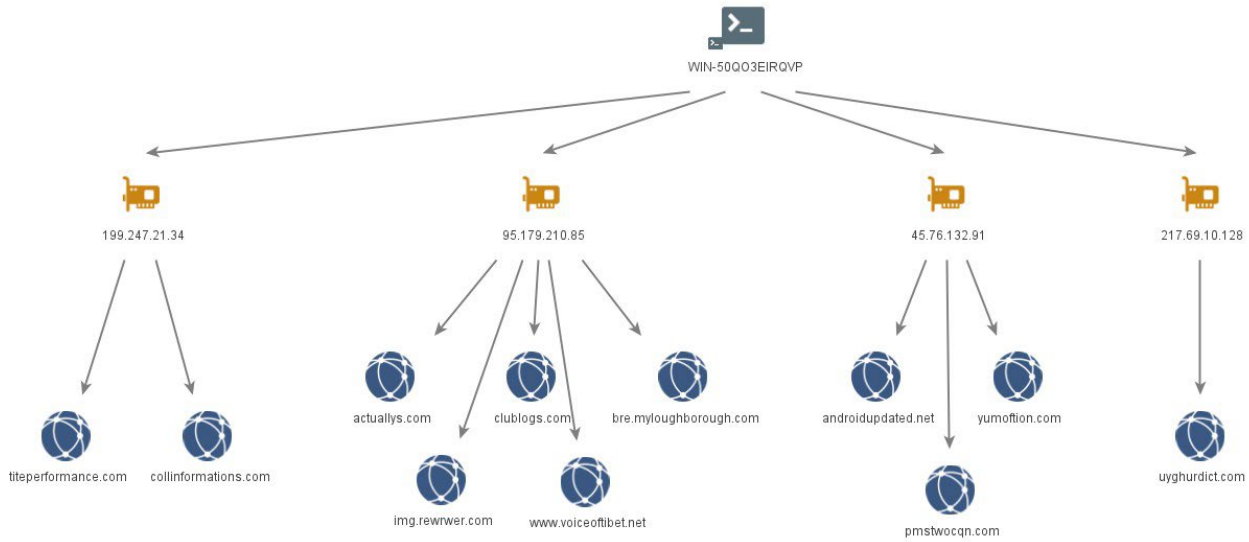
Gambar 6 – **WIN-EU0VLBL7TUJ**



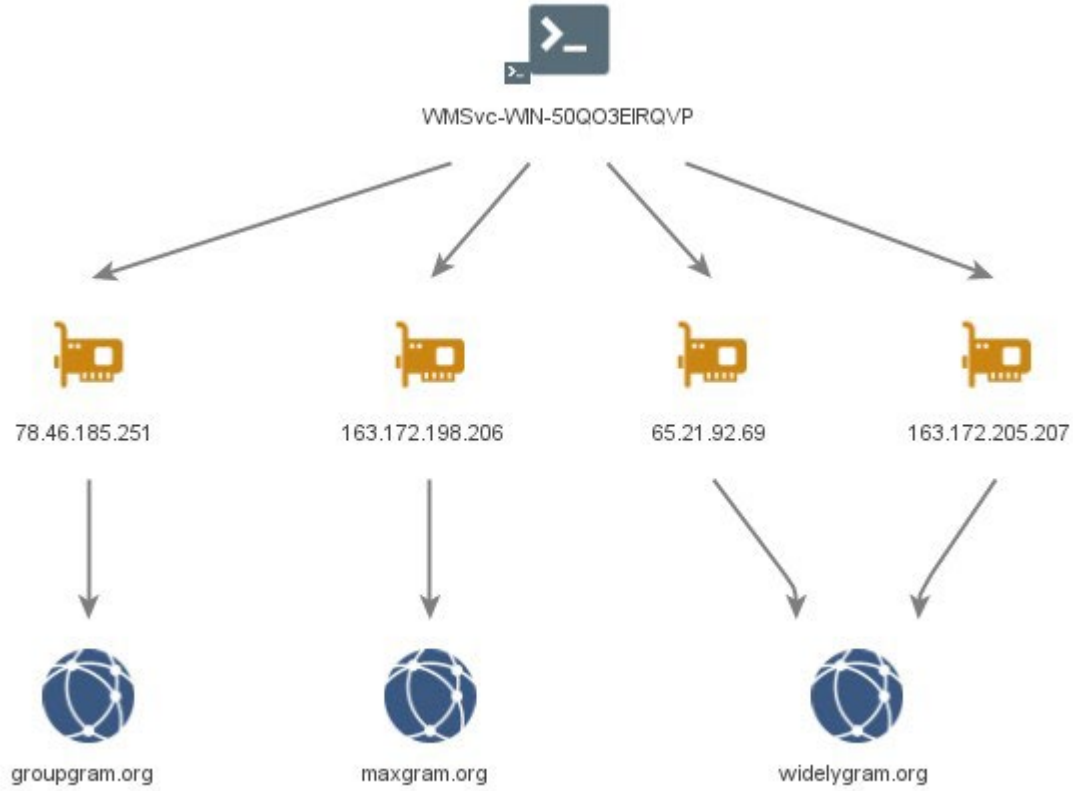
Gambar 7 – **WIN-70E59JVOB9G**



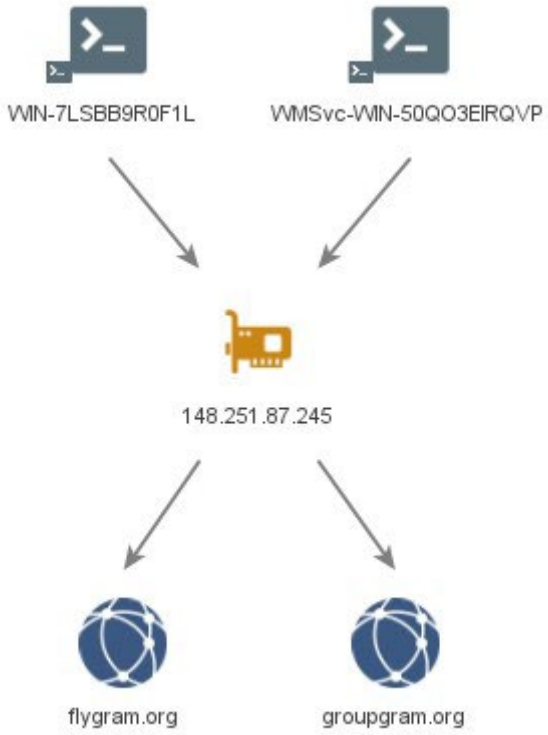
Gambar 8 - **WIN-50QO3EIRQVP**



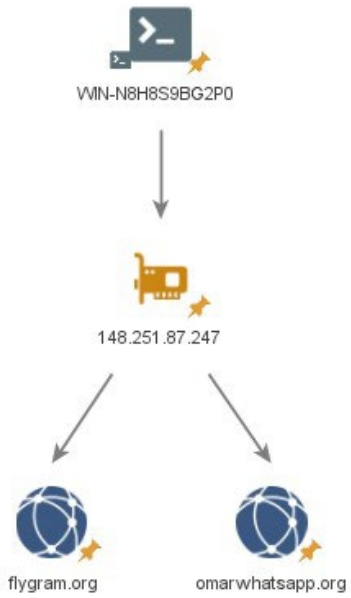
Gambar 9 - **VMSvc-WIN-50QO3EIRQVP**



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



Gambar 11 - **WIN-N8H8S9BG2P0**



Gambar 12 – **WIN-I6VBN8MR92A**

Lampiran B: Contoh MOONSHINE & BADBAZAAR yang diamati

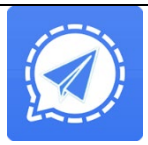
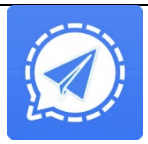
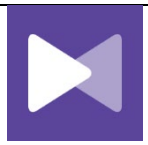
Tabel ini mencantumkan aplikasi yang digunakan dalam kampanye MOONSHINE dan BADBAZAAR dalam dua tahun terakhir.

Banyak dari aplikasi ini menunjukkan kemiripan yang jelas dengan aplikasi yang sudah ada. Ini kemungkinan merupakan teknik yang disengaja oleh aktor untuk 'meniru' merek terkenal.

Penting untuk dicatat, judul aplikasi, nama paket, dan ikon aplikasi semuanya dapat meniru atau menyamai aplikasi sebenarnya dan karenanya tidak boleh digunakan secara eksklusif untuk mengidentifikasi apakah suatu perangkat terinfeksi.

Judul aplikasi	Nama paket	Ikon aplikasi
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	
Keyboard Bahasa Arab	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.buddhistssongs1	
Kalkulator	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	

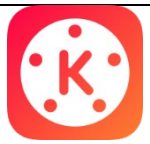
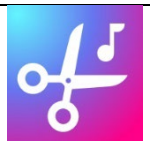
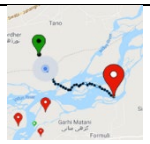
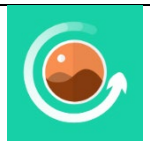
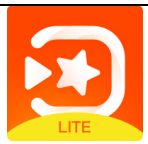
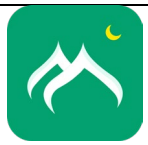
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime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

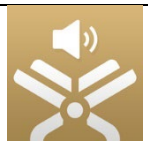
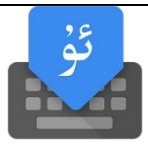
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore 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	
Papan Ketik SwiftKey	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	
Papan Ketik Uighur	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter	com.inverseai.video_converter	
Video Cutter	com.naing.cutter	
Video Downloader	downloader.video.download.free	
Video Maker	com.bstech.slideshow.videomaker	

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

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

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

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

Bacaan lebih lanjut

Panduan dari Pusat Keamanan Siber Australia

- Laporkan kejahatan siber, insiden, atau kerentanan
- Cara mengamankan perangkat Anda
- Amankan ponsel Anda
- Phishing
- Penipuan
- Amankan media sosial Anda
- Tip keamanan untuk media sosial dan aplikasi perpesanan

Panduan dari NCSC UK dan NPSA

- Mempertahankan Demokrasi
- Media Sosial: cara menggunakannya dengan aman
- Panduan Keamanan Perangkat untuk organisasi termasuk seluler
- Laporan ancaman pada toko aplikasi.
- Keamanan dan keselamatan pribadi untuk individu berisiko tinggi

Panduan dari NSA AS

- Praktik Terbaik Perangkat Seluler

Penafian

Harap perhatikan bahwa saran ini memberikan informasi yang divalidasi pada saat publikasi.

Laporan ini mengacu pada informasi yang diperoleh dari badan penyusun dan sumber industri. Segala temuan dan rekomendasi yang dibuat tidak diberikan dengan maksud untuk menghindari semua risiko dan mengikuti rekomendasi tidak akan menghilangkan semua risiko tersebut. Kepemilikan risiko informasi tetap berada di tangan pemilik sistem yang relevan setiap saat.

Di Inggris Raya, informasi ini dikecualikan berdasarkan Freedom of Information Act 2000 (FOIA) (Undang-Undang Kebebasan Informasi) dan mungkin dikecualikan berdasarkan undang-undang informasi Inggris Raya lainnya.

Ajukan pertanyaan FOIA apa pun ke ncscinfoleg@ncsc.gov.uk.