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

সতর্কতামূলক পরামর্শ

BADBAZAAR এবং MOONSHINE: প্রযুক্তিগত বিশ্লেষণ এবং ঝুঁকি হ্রাস

৯ এপ্রিল ২০২৫

BADBAZAAR এবং MOONSHINE: প্রযুক্তিগত বিশ্লেষণ এবং ঝুঁকি হ্রাস

সারসংক্ষেপ

যুক্তরাজ্যের সাইবার লীগ এর সহায়তায় ন্যাশনাল সাইবার সিকিউরিটি সেন্টার (NCSC UK) এবং আন্তর্জাতিক অংশীদাররা যৌথভাবে এই নির্দেশিকাটি তৈরি করেছে:

- **অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টার, অস্ট্রেলিয়ান সিগন্যালস ডিরেক্টরেটের অংশ**
- **কানাডিয়ান সেন্টার ফর সাইবার সিকিউরিটি, কমিউনিকেশনস সিকিউরিটি এস্টাবলিশমেন্টের অংশ**
- **জার্মান ফেডারেল ইন্টেলিজেন্স সার্ভিস**
- **জার্মান ফেডারেল অফিস ফর দ্য প্রোটেকশন অফ দ্য কনস্টিটিউশন**
- **নিউজিল্যান্ড ন্যাশনাল সাইবার সিকিউরিটি সেন্টার, সরকারি যোগাযোগ নিরাপত্তা ব্যুরোর অংশ**
- **মার্কিন যুক্তরাষ্ট্রের ফেডারেল ব্যুরো অফ ইনভেস্টিগেশন**
- **মার্কিন যুক্তরাষ্ট্রের জাতীয় নিরাপত্তা সংস্থা**

এই নির্দেশিকাটি BADBAZAAR এবং MOONSHINE নামে পরিচিত স্পাইওয়্যার বা নজরদারি সফটওয়্যারের দুটি রূপের বিষয়ে নতুন ও সংকলিত হুমকির তথ্য তুলে ধরেছে। এটি অ্যাপ স্টোর অপারেটর, অ্যাপ ডেভেলপার এবং সামাজিক যোগাযোগমাধ্যম কোম্পানিগুলোর জন্য পরামর্শও দিয়েছে যাতে তারা ব্যবহারকারীদের নিরাপদ রাখতে কার্যকর পদক্ষেপ নিতে পারে।

এই নির্দেশিকা যেসব ব্যবহারকারী ইতোমধ্যে এই ম্যালওয়্যারের শিকার হয়েছেন, তাদের জন্য প্রস্তুতকৃত আরেকটি নির্দেশিকার পাশাপাশি প্রকাশ করা হচ্ছে।

এই নথিতে স্পাইওয়্যার শব্দটি NCSC (ন্যাশনাল সাইবার সিকিউরিটি সেন্টার) এর শব্দকোষে যেভাবে সংজ্ঞায়িত, ঠিক সেই অর্থেই ব্যবহার করা হয়েছে। "এটি এমন এক ধরনের ক্ষতিকর ম্যালওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়াই কোনো ডিভাইসে নিজে থেকে ইনস্টল হয়ে যায়। এরপর এটি ব্যক্তিগত তথ্য সংগ্রহ করে তৃতীয় কোনো পক্ষের কাছে পাঠিয়ে দেয়।"

কেস স্টাডি ১ MOONSHINE

MOONSHINE হল একটি অ্যান্ড্রয়েড স্পাইওয়্যার যা তিব্বতি গোষ্ঠীগুলির উপর নজরদারি করছিল বলে ২০১৯ সালে Citizen Lab রিপোর্ট করেছিল। MOONSHINE একটি বৈধ অ্যাপ হিসেবে ছদ্মবেশ ধারণ করে যাতে এটি ইনস্টল করার জন্য ভুক্তভোগীদের প্রলুব্ধ করা যায়। টেলিগ্রাম চ্যানেল ও হোয়াটসঅ্যাপ লিংকের মাধ্যমে এটি ছড়ানো হয়েছে।

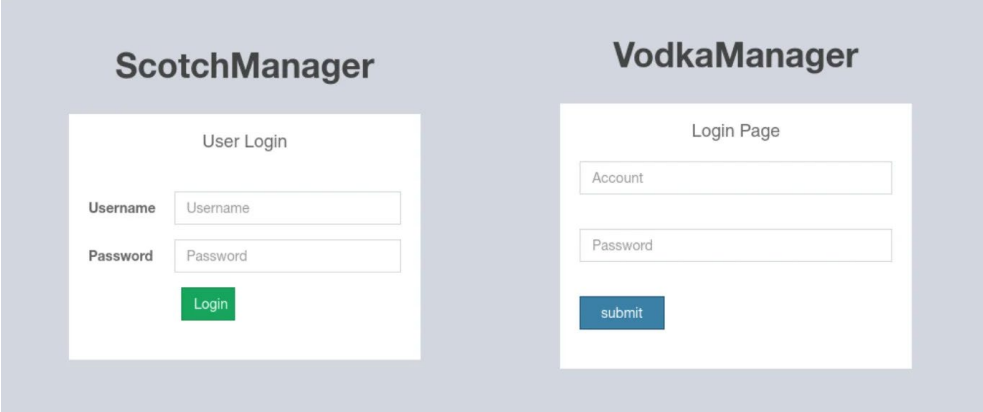
MOONSHINE সম্পর্কে NCSC গবেষণা নিম্নলিখিত বিষয়গুলি নির্দেশ করে:

- MOONSHINE একটি ব্যবস্থাপনা ইন্টারফেস ব্যবহার করে যা প্রথম রিপোর্ট করার পর থেকে পরিবর্তিত হয়েছে।
- ম্যানেজমেন্ট ইন্টারফেসটির ব্যাপক নজরদারি ক্ষমতা রয়েছে, যার মধ্যে রয়েছে ডিভাইস থেকে ফাইল চুরি করার ক্ষমতা। তাছাড়া এটি রিয়েল-টাইমে অডিও রেকর্ড এবং স্ক্রিনের ভিডিও ধারণ করতেও সক্ষম।
- ভার্চুয়ালি হোস্ট করা একাধিক MOONSHINE ম্যানেজমেন্ট ইন্টারফেসের সন্ধান পাওয়া গেছে। এই ইন্টারফেসগুলো এমন কিছু লগইন প্যানেলের সঙ্গে একই অবকাঠামো ব্যবহার করছে, যেগুলো UPSEC এর সঙ্গে যুক্ত বলে মনে করা হয়। আর Intelligence Online এর সূত্র অনুসারে, UPSEC হচ্ছে 'সিচুয়ান ডিয়াঙ্কে নেটওয়ার্ক সিকিউরিটি টেকনোলজি কোং লিমিটেড' নামের একটি প্রতিষ্ঠান।

ব্যবস্থাপনা ইন্টারফেস

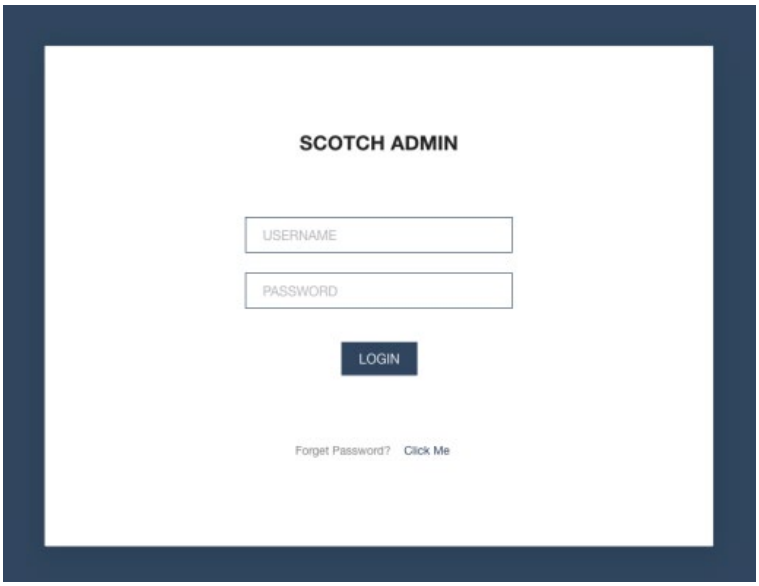
MOONSHINE ম্যানেজমেন্ট ইন্টারফেসের পূর্ববর্তী প্রতিবেদন ইঙ্গিত দেয় যে এতে পরিবর্তন এসেছে, যা চলমান উন্নয়নের ইঙ্গিত দেয়।

ম্যানেজমেন্ট ইন্টারফেসের প্রথম উদাহরণ সিটিজেন ল্যাবের ২০১৯ সালের প্রতিবেদনে পাওয়া যায়।



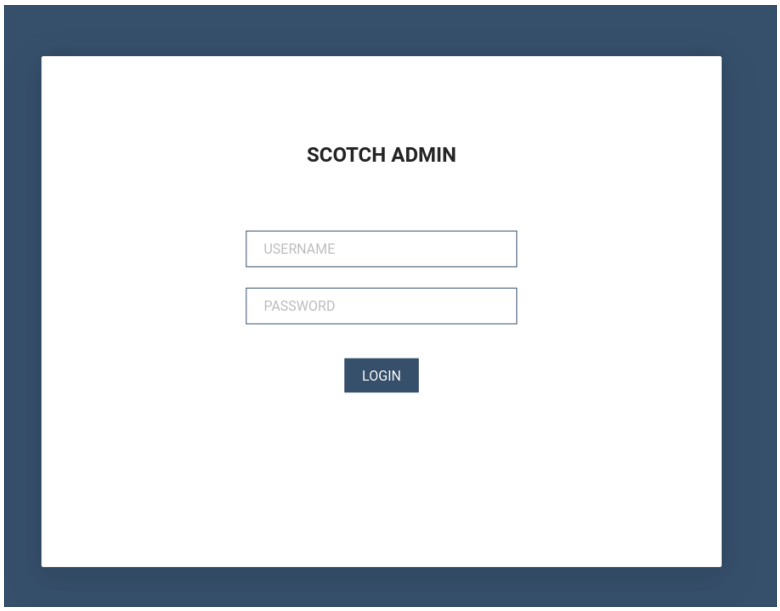
চিত্র 1: *MOONSHINE ম্যানেজমেন্ট ইন্টারফেসগুলি সিটিজেন ল্যাবের ২০১৯ সালের প্রতিবেদন 'মিসিং লিংক টিবেটান গ্রুপস টার্গেটেড উইথ 1-ক্লিক মোবাইল এক্সপ্লয়েটস'-এ দেখা গেছে।*

২০২২ সালের গোড়ার দিকে, লুকআউট এক প্রতিবেদনে উল্লেখ করে যে, MOONSHINE স্পাইওয়্যারের ব্যবস্থাপনা ইন্টারফেসটি নীচের মতো দেখতে পুনরায় ডিজাইন করা হয়েছিল (চিত্র ১-এ দেখানো পূর্ববর্তী ইন্টারফেসগুলিকে প্রতিস্থাপন করে):



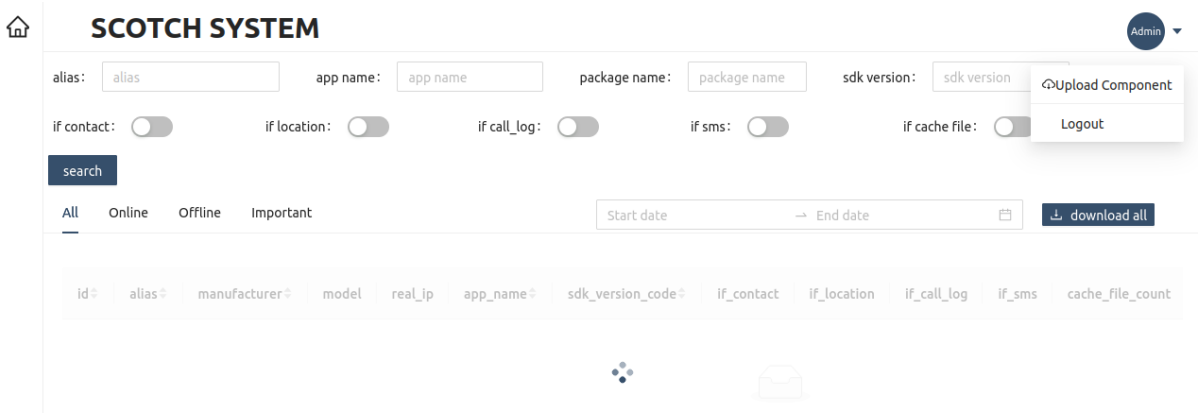
চিত্র 2: লুকআউটের ২০২২ রিপোর্টে 'MOONSHINE: টিবেটান এবং উইগুরদের টার্গেট করে চীনা APT POISON CARP দ্বারা তৈরি অ্যান্ড্রয়েড সারভেইলেন্সওয়্যার'-এ MOONSHINE ব্যবস্থাপনা ইন্টারফেস দেখা গেছে।

২০২৩ সালের আগস্টে, MOONSHINE কমান্ড অ্যান্ড কন্ট্রোল (C2) এর একটি স্ক্যান প্রকাশ করে যে ২০২২ সালের ইন্টারফেসের মতো একটি ইন্টারফেস ছিল যেখানে **'পাসওয়ার্ড ভুলে গেছেন '** ফাংশনটি আর বিদ্যমান ছিল না যেমনটি চিত্র ২-এ দেখানো হয়েছে:



চিত্র 3: ২০২৩ সালের আগস্টে MOONSHINE ম্যানেজমেন্ট ইন্টারফেস পর্যবেক্ষণ করা হয়েছিল যেখানে আর 'পাসওয়ার্ড ভুলে গেছেন' প্রম্পটটি ছিল না।

ব্যবস্থাপনা ইন্টারফেসের আরও তদন্তে দেখা গেছে যে, সেই প্যানেলের ভেতরে এমন কিছু তথ্য রয়েছে যা স্পষ্ট করে দেয়—সংক্রমিত বা আক্রান্ত ডিভাইসগুলোর বিস্তারিত তথ্য কীভাবে সংরক্ষণ করা হবে।



চিত্র 4: MOONSHINE ম্যানেজমেন্ট ইন্টারফেসের লগইন পেজ এর পিছনের ওয়েবপেজ।

লুকআউট গবেষণায় দেখা গেছে যে ভুক্তভোগীর ডিভাইস থেকে MOONSHINE C2 সার্ভারে একটি **'স্কোর'** স্থানান্তরিত হচ্ছে। 'স্কোর' বা পয়েন্টের যে মান প্রদর্শিত হয়, তা নির্ভর করে আক্রান্ত ডিভাইসে ম্যালিশাস বা ক্ষতিকর সফটওয়্যারটির যেসব অনুমতি রয়েছে তার ওপর।

পৃষ্ঠার মধ্যে 'if_contact', 'if_location', 'if_call_log' এবং 'if_sms' কলামগুলি ইঙ্গিত দেয় যে সব MOONSHINE স্যাম্পলেরই সংক্রমিত ডিভাইসগুলিতে সম্পূর্ণ অ্যাক্সেস নেই। কলামগুলোর সংশ্লিষ্ট তথ্য এবং ডিভাইস থেকে C2 তে পাঠানো 'স্কোর' বিশ্লেষণে বোঝা যায়—হ্যাকাররা এই স্কোর ব্যবহার করে ম্যানেজমেন্ট ইন্টারফেসে যুক্ত ব্যক্তিদের জানায়, সংক্রমিত ডিভাইসটিতে সেই ম্যালওয়্যারটি কতটা নিয়ন্ত্রণ বা প্রবেশাধিকার অর্জন করেছে।

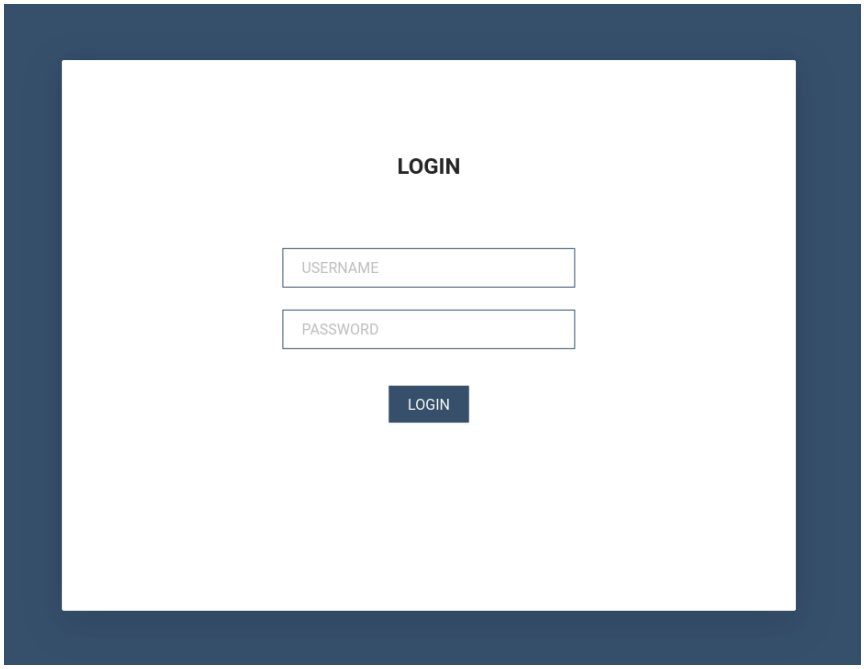
সাধারণভাবে, ডিভাইস থেকে তথ্য সংগ্রহ প্রতিরোধে সেরা উপায়টি হলো অ্যাপ ডাউনলোডের আগে তার অনুমতি বা পারমিশনগুলো খতিয়ে দেখা, যাতে কোনো অস্বাভাবিক অনুমতি চাওয়া হচ্ছে কি না সেটা বোঝা যায়। তবে, MOONSHINE স্পাইওয়্যারের যেসব নমুনা পাওয়া গেছে, সেগুলো এমন অনুমতি (permission) চায় যেগুলো দেখতে অ্যাপের স্বাভাবিক কার্যকারিতার জন্য প্রাসঙ্গিক মনে হতে পারে। এই কারণে, ব্যবহারকারীদের কাছে এগুলো সন্দেহজনক না-ও লাগতে পারে, কিন্তু আসলে এই অনুমতিগুলো ব্যবহার করেই অ্যাপটি ডিভাইস থেকে তথ্য সংগ্রহ করে থাকে।

MOONSHINE-এর একটি অ্যাপ্লিকেশন প্রোগ্রামিং ইন্টারফেস (API)ও রয়েছে যার মাধ্যমে এর বিস্তৃত কার্যক্ষমতা সম্পর্কে জানা যায়। MOONSHINE স্পাইওয়্যারের API ডকুমেন্টেশনের প্রাথমিক সংস্করণে দেখা গেছে, অনেক API-এর নাম ম্যানডারিন ভাষাতে লেখা ছিল।

ভার্চুয়ালহোস্ট

MOONSHINE প্যানেলের তদন্তে ভার্চুয়াল হোস্টিং প্ল্যাটফর্ম শনাক্ত করা হয়েছে। ভার্চুয়াল হোস্টিং বলতে বোঝায় যখন একটি মাত্র IP ঠিকানা ব্যবহার করে একাধিক ওয়েবসাইট বা অনলাইন পরিষেবা চালানো যায়। যেসব আইপি ঠিকানা ও ডোমেইন MOONSHINE এর এই ভার্চুয়াল হোস্টিংয়ে ব্যবহৃত হয়েছে, সেগুলোর কোনোটি কোনো পূর্বপরিচিত ম্যালওয়্যারের নমুনায় পাওয়া যায়নি।

এই ব্যবস্থাপনা ইন্টারফেসগুলোর মধ্যে পার্থক্য ছিল, কারণ এসব পেজের শিরোনামে **'LOGIN'** লেখা ছিল, যেখানে আগের সংস্করণগুলোতে **'SCOTCH ADMIN'** শিরোনাম ব্যবহার করা হয়েছিল।



চিত্র 5: *MOONSHINE ব্যবস্থাপনা ইন্টারফেস SCOTCH ADMIN এর পরিবর্তে LOGIN শিরোনাম ব্যবহার করে।*

এছাড়াও, প্যানেলের বিষয়বস্তু চিত্র ৪ থেকেও আলাদা, যেমন চিত্র ৬-এ দেখা যাচ্ছে:

চিত্র ৬: ভার্চুয়ালি হোস্ট করা MOONSHINE ব্যবস্থাপনা ইন্টারফেসের লগইন পেজ এর পিছনের ওয়েবপেজ।

চিত্র ৬-এ থাকা প্যানেলটি চিত্র ৪-এ থাকা প্যানেলের একটি সরলীকৃত সংস্করণ বলে মনে হচ্ছে। বিভিন্ন ব্যবস্থাপনা ইন্টারফেসের মধ্যে যে মিল বা সাদৃশ্য দেখা যায় সেগুলি হল টেবিলে কলামের নাম যেমন 'আইডি', 'নির্মাতা' এবং 'মডেল'।

আবিষ্কৃত ভার্চুয়ালি হোস্ট করা MOONSHINE উদাহরণগুলি ছিল:

ডোমেইন	আইপি ঠিকানা
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

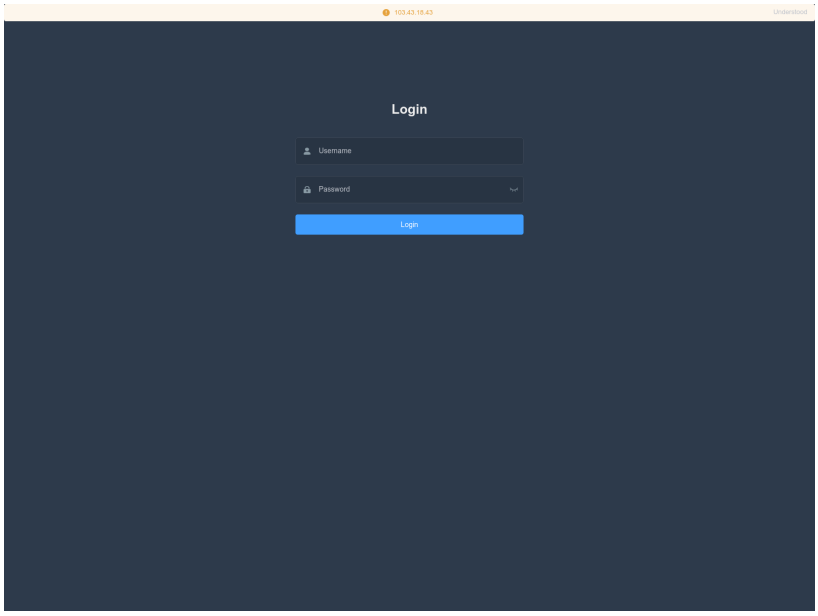
এই ডোমেইনগুলোকে ট্রেন্ড মাইক্রো তাদের বিশ্লেষণে MOONSHINE এক্সপ্লয়েট কিট হিসেবে তালিকাভুক্ত করেছে। এগুলোর কাজ হলো মোবাইল ডিভাইসের ব্রাউজারে থাকা দুর্বলতাগুলো (ভালনারেবিলিটি) কাজে লাগিয়ে স্বয়ংক্রিয়ভাবে ম্যালওয়্যার ইনস্টল করে দেওয়া। ট্রেন্ড মাইক্রো এই ম্যালওয়্যারটির নাম দিয়েছে 'ডার্ক নিম্বাস'।

সুস্পষ্ট করে বলা যায়— MOONSHINE ব্যবস্থাপনা ইন্টারফেসগুলোর সঙ্গে ম্যালওয়্যারের নমুনাগুলো নিয়মিত যোগাযোগ করে থাকে এবং সংক্রমিত বা আক্রান্ত ডিভাইস থেকে ব্যবহারকারীর তথ্য সংগ্রহ করে ঠিক এই ইন্টারফেসেই পাঠানো হয়। ট্রেন্ড মাইক্রো -এর প্রতিবেদন অনুযায়ী, MOONSHINE এক্সপ্লয়েট কিটগুলো একটি স্বতন্ত্র সক্ষমতা বহন করে যেগুলো মোবাইল ডিভাইসের ব্রাউজারে থাকা নিরাপত্তার দুর্বলতা (ভালনারেবিলিটি) কাজে লাগিয়ে ডার্ক নিম্বাস নামের এক ধরনের ম্যালওয়্যার ইনস্টল করে। এছাড়া ডার্ক নিম্বাস এবং MOONSHINE একে অপরের থেকে সম্পূর্ণ আলাদা ধরণের ম্যালওয়্যার।

MOONSHINE ম্যানেজমেন্ট ইন্টারফেস এবং MOONSHINE এক্সপ্লয়েট কিট উভয়েরই কোড ওভারল্যাপ রয়েছে, তাই চিত্র ৩ এবং ৫-এ দেখানো লগইন প্রম্পট এবং চিত্র ৪ এবং ৬-এ দেখানো পৃষ্ঠার বিষয়বস্তু একই রকম। উভয়টিতে সোর্স কোডে 'webpackJsonpreact-scotchui' স্ট্রিং রয়েছে।

হ্যাকাররা এমন কিছু URL লিঙ্ক তৈরি করেছিল, যেগুলো প্রথমে MOONSHINE এক্সপ্লয়টেশন কিটের সঙ্গে সংযুক্ত হতো এবং সেখান থেকে আবার এমন কিছু ভিডিওতে রিডাইরেক্ট করত—যেগুলোর বিষয়বস্তু ছিল তিব্বতীয় ও উইঘুর জনগণের সঙ্গে সম্পর্কিত, যা MOONSHINE এর পূর্বের টার্গেটিং কৌশলের সঙ্গে মিল খুঁজে পাওয়া যায়।

MOONSHINE এক্সপ্লয়েট কিট ডোমেইন হোস্ট করা অনেক IP ঠিকানায়, পোর্ট ৪৪৪-এ 'VLiteUI' শিরোনামের একটি লগইন পেজ রয়েছে। এই পৃষ্ঠাটি ব্যাপকভাবে দেখা যায় না এবং এই IP গুলিতে এর উপস্থিতি অ্যাক্টরদের ক্রিয়াকলাপের সম্ভাব্য লিঙ্ক নির্দেশ করে।



চিত্র 7: একই IP ঠিকানায়, যেখানে MOONSHINE এক্সপ্লয়েট কিট হোস্ট করা ছিল, সেখানে একটি লগইন প্যানেল শনাক্ত করা হয়েছে যার HTML শিরোনাম ছিল 'VLiteUI'।

ট্রেন্ড মাইক্রো-এর বিশ্লেষণে দেখা গেছে, ডার্ক নিম্বাস ম্যালওয়্যারটি ডিভাইস থেকে অত্যন্ত বিস্তৃত পরিমাণে তথ্য সংগ্রহ করতে পারে এবং XMPP প্রোটোকল ব্যবহার করে C2 সার্ভারের সঙ্গে যোগাযোগ স্থাপন করে।

ট্রেন্ড মাইক্রো - এর বিশ্লেষণে বলা হয়েছে, কিছু নির্দিষ্ট সংস্করণের ডার্ক নিম্বাস ম্যালওয়্যারে 'DKNS' নামে একটি স্ট্রিং এর অস্তিত্ব পাওয়া গেছে।

'ansec[.]com', (যেটিকে Trend Micro তাদের বিশ্লেষণে Dark Nimbus-এর C2 সার্ভার হিসেবে চিহ্নিত করেছে) অন্যান্য কিছু IP ঠিকানার জন্য XMPP পরিষেবায়ও ব্যবহৃত হতে দেখা গেছে— যেগুলোতে এমন ওয়েব পেজ হোস্ট করা ছিল যেখানে শিরোনামে 'DKNS' লেখা ছিল।

- DKNS অ্যান্ড্রয়েড রিমোট ফরেনসিক সিস্টেম (DKNS অ্যান্ড্রয়েড রিমোট ফরেনসিক সিস্টেম)
- 云网侦控平台 (DKNS ক্লাউড নেটওয়ার্ক ইনভেস্টিগেশন এবং কন্ট্রোল প্ল্যাটফর্ম)
- 云网侦控平台 (DKNS ক্লাউড নেটওয়ার্ক ইনভেস্টিগেশন এবং কন্ট্রোল প্ল্যাটফর্ম)
- DKNS远程控制侦查系统 (DKNS রিমোট কন্ট্রোল ইনভেস্টিগেশন সিস্টেম)

XMPP পরিষেবায় 'ansec[.]com' সহ আরও একটি IP ঠিকানার ওয়েব পেজ ছিল যার শিরোনাম ছিল:

- UPSEC互联网控制指挥系统 (UPSEC ইন্টারনেট কন্ট্রোল কমান্ড সিস্টেম)
- UPSEC无线侦控系统 (UPSEC ওয়্যারলেস সারভেইলেন্স কন্ট্রোল সিস্টেম)
- UPSEC重点人数据还原系统 (UPSEC কী পার্সন ডেটা রিস্টোরেশন সিস্টেম)

ইন্টেলিজেন্স অনলাইন অনুসারে, HTML পেজগুলির শিরোনামে 'UPSEC' লক্ষ্য করা গিয়েছিল, যা 'সিচুয়ান ডিয়াঙ্কে নেটওয়ার্ক সিকিউরিটি টেকনোলজি কোং, লিমিটেড' হিসাবে উল্লেখ করা ছিল।

কেস স্টাডি দুইঃ BADBAZAAR

BADBAZAAR হল iOS এবং Android ভেরিয়েন্ট সহ একটি মোবাইল ম্যালওয়্যার যা উইঘুর, তিব্বতি এবং তাইওয়ানিজ ব্যক্তিদের লক্ষ্যবস্তু করেছে। এই স্পাইওয়্যারটি সোশ্যাল মিডিয়া প্ল্যাটফর্ম এবং অফিসিয়াল অ্যাপ স্টোরের মাধ্যমে ছড়িয়ে পড়েছে। Volexity থেকে সাম্প্রতিক প্রতিবেদনে BADBAZAAR -এর বিভিন্ন ভেরিয়েন্ট দেখানো হয়েছে, যেগুলিকে ব্যাডসোলার, BADBAZAAR,এবং ব্যাডসিগন্যাল হিসাবে আলাদা আলাদা করে দেখানো হয়েছে। তিনটি ভেরিয়েন্টই ডিভাইস এবং অপারেটরের তথ্য সংগ্রহের জন্য ব্যবহৃত একি ধরণের ফাংশন দ্বারা একসাথে সংযুক্ত।

BADBAZAAR -এর উপর NCSC গবেষণায় নিম্নলিখিতগুলি ফলাফল পাওয়া গেছে:

- C2 ডোমেইনগুলোর ক্লাস্টারিং বা গ্রুপিং বিশ্লেষণ করে দেখা গেছে—এগুলোর কিছু ডোমেইনের সঙ্গে পূর্বের সাইবার হুমকি বিষয়ক গোয়েন্দা রিপোর্টে উল্লিখিত ডোমেইনের মিল রয়েছে।
- C2 সার্ভার এবং ম্যালওয়্যার নমুনাগুলোর বিশ্লেষণে এমন কিছু হোস্টনেম শনাক্ত হয়েছে যেগুলো সংশ্লিষ্ট হ্যাকার গ্রুপের অবকাঠামোর সঙ্গে যুক্ত।
- এই হ্যাকাররা নির্ভরযোগ্য অ্যাপ স্টোরের বাইরে তাদের ম্যালওয়্যার ছড়াতে মানুষকে ধোঁকা দেয়ার জন্য বিভিন্ন প্রোফাইল বা পরিচয় ব্যবহার করে।

WHOIS ক্লাস্টারিং / ডোমেইন ব্রোকার

'UJYJYUJ'

BADBAZAAR-এর ডোমেইন **'signalplus[.]org'**-এর WHOIS রেকর্ড বিশ্লেষণে (যা ESET কর্তৃক রিপোর্টকৃত) দেখা গেছে, এতে **'State'** ফিল্ডে **'UJYJYUJ'** মানটি উল্লেখ ছিল।

অন্যান্য ডোমেইনের মধ্যে যেগুলোর একই মান বা নির্দিষ্ট বৈশিষ্ট্য রয়েছে—তদন্তে সেগুলোর মধ্যে নিম্নলিখিত ডোমেইনগুলি শনাক্ত হয়েছে।

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

(পরিশিষ্ট A, চিত্র ১ দেখুন)

signalplus[.]org, tubevideoplus[.]org এবং **thetubeplus[.]com** ডোমেইনগুলিকে BADBAZAAR C2 ডোমেইন হিসাবে রিপোর্ট করা হয়েছে, অন্যদিকে ESET এর রিপোর্ট অনুযায়ী **mail.pmumail[.]com** সাব ডোমেইনটি FlyGram এর প্রক্সি সার্ভার হিসাবে রিপোর্ট করেছে। FlyGram হচ্ছে সাইবার অপরাধীদের তৈরি BADBAZAAR নামক ম্যালওয়্যারের একটি অ্যাপ। (অ্যাপেন্ডিক্সে BADBAZAAR-এর অন্যান্য অ্যাপের তালিকা দেওয়া আছে।)

কীবোর্ড ওয়াকিং মান

NCSC অন্যান্য নিবন্ধিত BADBAZAAR C2 ডোমেনেও একই রকম কীবোর্ড ওয়াকিং প্যাটার্ন দেখেছে।

উদাহরণস্বরূপ, নিম্নলিখিত ডোমেইনগুলির **'State'** ফিল্ডে **'REWR'** মান পরিলক্ষিত হয়েছে (যেমনটি আগে ব্যবহৃত হয়েছিল):

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

(পরিশিষ্ট A, চিত্র ২ দেখুন)

'FSDF' ফিল্ড মান সহ ডোমেইন

BADBAZAAR C2 ডোমেইনের আরেকটি সেটের **'State'** মান '**FSDF**':

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

(পরিশিষ্ট A, চিত্র ৩ দেখুন)

কীবোর্ড ওয়াকিং মান সহ ঐতিহাসিক প্রতিবেদন

BADBAZAAR ডোমেইনের WHOIS রেকর্ডে কী–বোর্ড ওয়াকিং মানের ব্যবহার দেখা গেছে, যা পূর্বে তিব্বতি সংগঠনগুলোর ওপর TA413 নামক হ্যাকার গ্রুপের সাইবার আক্রমণের সময়ও লক্ষ্য করা হয়েছিল। রেকর্ডেড ফিউচার নামক একটি সাইবার গোয়েন্দা প্রতিষ্ঠান দেখতে পেয়েছে যে, হ্যাকারদের দ্বারা পরিচালিত কিছু ডোমেইন তিব্বতি সংগঠনগুলোর নাম নকল করে তৈরি করা হয়েছে, এবং সেখানে নামক একটি সংস্থার নাম রেজিস্ট্র্যান্ট অর্গানাইজেশন এর মান হিসেবে **"asfasf"** ব্যবহার করা হয়েছে।

clublogs[.]com

Lookout কর্তৃক সংগ্রহ করা BADBAZAAR ম্যালওয়্যারের নমুনাগুলোর মধ্যে **'xle.clublogs.com'** C2 ডোমেইন হিসেবে ব্যবহৃত হচ্ছিল। **'clublogs[.]com'** রুট ডোমেইনটি **'95.179.210[.]85'** আইপি ঠিকানায় হোস্ট করা হয়েছিল এবং এর একটি SSL সার্টিফিকেট ছিল যার বিষয় এবং ইস্যুকারী মান ছিল **'CN=WIN-50QO3EIRQVP'**। এই মানটি BADBAZAAR এর নমুনাগুলিতে পাওয়া SSL সার্টিফিকেটের সাথে মিলে গেছে যেগুলি যোগাযোগের বাধা এড়াতে SSL পিনিং প্রযুক্তি ব্যবহার করেছিল।

IP ঠিকানা **95.179.210[.]85** এর হোস্টিং ইতিহাস যাচাই করে যেসব গুরুত্বপূর্ণ ডোমেইন পাওয়া গেছে, তা নিচে উল্লেখ করা হলো:

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

(পরিশিষ্ট A, চিত্র ৪ দেখুন)

www.voiceoftibet[.]net

'**www.voiceoftibet[.]net**' ডোমেইনটি 'Voice of Tibet' নামের প্রকৃত রেডিও স্টেশনের ছদ্মবেশ ধারণ করেছে বলে মনে হচ্ছে, যা TA413 কর্তৃক ব্যবহৃত পূর্বের কৌশলগুলোর (TTP) মতোই।

'**rewrwer[.]com**' ডোমেইনটি BADBAZAAR ডোমেইনের WHOIS রেকর্ডে পূর্বে শনাক্ত করা **'REWR'** নামক **'State'** মানটির সঙ্গে সাদৃশ্যপূর্ণ।

'clublogs[.]com', 'rewrwer[.]com', 'voiceoftibet.net' এবং 'myloughborough[.]com'— এই ডোমেইনগুলো '**tplutalova@list.ru**' ইমেইল ঠিকানা ব্যবহার করে রেজিস্টার করা হয়েছে।

actuallys[.]com

'**actuallys[.]com**' ডোমেইনের WHOIS রেকর্ডে দেখা গেছে যে, টেকনিক্যাল ও অ্যাডমিন ইমেইল ঠিকানা ছিল **'tplutalova@list.ru'**, কিন্তু রেজিস্ট্র্যান্ট (মূল রেজিস্ট্রার) ইমেইল ঠিকানা ছিল **'ivan_s81@mail.ru'**।

'**actuallys[.]com**' ডোমেইনের অতীতের WHOIS তথ্য অনুযায়ী, ২৪ ফেব্রুয়ারি ২০১৬ তারিখে এই ডোমেইনের রেজিস্ট্রেশন ইমেইল ছিল **'wangminghua6@gmail[.]com'**। ২০১৬ সালের ১১ই মার্চ তারিখে ডোমেইনটির রেজিস্ট্রেশন ইমেইল **'ivan_s81@mail.ru'** তে পরিবর্তন করা হয়, যদিও রেজিস্ট্রারের রেজিস্ট্রেশন মেয়াদ শেষ হওয়ার তারিখ অপরিবর্তিত ছিল।

wangminghua6@gmail[.]com

'wangminghua6@gmail[.]com' ইমেইল ঠিকানাটি অতীতের হুমকি বিশ্লেষণ প্রতিবেদনে পাওয়া কিছু ডোমেইন রেজিস্ট্রেশনের ক্ষেত্রে ব্যবহৃত হয়েছিল। ২০১৫ সালে Palo Alto একটি ইমেইল ঠিকানা শনাক্ত করে, যা Cmstar ম্যালওয়্যারের C2 ডোমেইন রেজিস্ট্রেশনের জন্য ব্যবহার করা হয়েছিল। ২০১৪ সালে একই ইমেইল ঠিকানাটি ব্যবহার করে কিছু ডোমেইন রেজিস্টার করা হয়েছিল, যেগুলোকে Mandiant APT3 দ্বারা ফিশিং প্রচারণায় যুক্ত হিসেবে শনাক্ত করেছিল। ২০১৩ সালে একই ইমেইল ঠিকানা ব্যবহার করে কিছু ডোমেইন রেজিস্টার করা হয়েছিল, যেগুলো CrowdStrike একটি ম্যালওয়্যার ড্রপারে শনাক্ত করে—যার প্রোগ্রাম ডেটাবেস (PDB) পাথে চীনা অক্ষর অন্তর্ভুক্ত ছিল। এটি ইঙ্গিত করে যে, কম্পাইল বা প্রোগ্রাম তৈরি করা হয়েছিল একটি চীনা সিস্টেমে।

taoyujun@gmail[.]com

‘**hcjbtt[.]com**’ ডোমেইনটি **‘taoyujun@gmail[.]com’** ইমেইল ঠিকানা ব্যবহার করে রেজিস্টার করা হয়েছে, তবে এর অ্যাডমিনিস্ট্রেটর ইমেইল হিসেবে **‘wangminghua6@gmail[.]com’** ব্যবহার করা হয়েছে।

‘**hcjbtt[.]com**’ডোমেইনটির সঙ্গে কোনো ক্ষতিকর কার্যকলাপের প্রমাণ পাওয়া যায়নি, তবে **‘taoyujun@gmail[.]com’** ইমেইল ঠিকানাটি অতীতের হুমকি বিশ্লেষণ প্রতিবেদনে পাওয়া গেছে। ২০১৪ সালে, একই ইমেইল ঠিকানা ব্যবহার করে এমন একটি ডোমেইন রেজিস্টার করা হয়েছিল, যা Mandiant **‘Cueisfry Trojan’** নমুনায় খুঁজে পেয়েছিল—যেটি জাপানি প্রতিষ্ঠানগুলোর ওপর আক্রমণের জন্য ব্যবহৃত হয়েছিল।

উক্ত ইমেইল ঠিকানাটি আরও কিছু ডোমেইন রেজিস্টার করতে ব্যবহার করা হয়েছে, যেমন **‘iaea-international[.]org’**’—যা **আন্তর্জাতিক পারমাণবিক শক্তি সংস্থার** ছদ্মবেশে তৈরি হয়েছিল, এবং **‘idc-ctbto[.]org’**’—যেটি পারমাণবিক পরীক্ষা নিষিদ্ধকরণ সংক্রান্ত আন্তর্জাতিক সংস্থা **Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO)**-এর **International Data Centre** এর ছদ্মবেশে তৈরি হয়েছিল।

‘iaea-international[.]org’ ডোমেইনের পূর্ববর্তী একটি WHOIS রেকর্ডে দেখা যায় যে, রেজিস্ট্র্যান্ট ইমেইল ঠিকানা ছিল **‘wangminghua6@gmail[.]com’**।

udtglobals[.]com

‘udtglobals.com’ ডোমেইনটি অ্যাডমিনিস্ট্রেটর ইমেইল হিসেবে **‘wangminghua6@gmail[.]com’** এবং রেজিস্ট্র্যান্ট ইমেইল হিসেবে **‘ocean.nio@rediffmail[.]com’** ব্যবহার করে রেজিস্টার করা হয়েছিল। এই ডোমেইনের অন্যান্য WHOIS রেকর্ডে একই রেজিস্ট্র্যান্ট ইমেইল ঠিকানা দেখা গেলেও, অ্যাডমিনিস্ট্রেটর ইমেইল ঠিকানা ছিল **‘taoyujun@gmail[.]com’**।

‘**udtglobals[.]com**’ ডোমেইনটি ‘**UDT Global**’ নামক একটি আন্তর্জাতিক আন্ডারসি (জলতলের) প্রতিরক্ষা ও নিরাপত্তা কোম্পানিগুলোর ইভেন্টের ছদ্মবেশ ধারণ করেছে বলে মনে হয়। ‘**ocean.nio**’ নামটি যে ইমেইল ঠিকানায় ব্যবহার করা হয়েছে, তা বিভিন্ন দেশে থাকা **ন্যাশনাল ইন্সটিটিউট অব ওসিয়ানোগ্রাফি (NIO)**-কে অনুকরণ করে থাকতে পারে। যদিও **‘Rediff’** ইমেইল পরিষেবাটি (যা ভারতের ভিত্তিক) ব্যবহার করা হয়েছে, এটি ভারতীয় **ন্যাশনাল ইন্সটিটিউট অব ওসিয়ানোগ্রাফি (NIO)**-এর ছদ্মবেশ ধারণের ইঙ্গিত দিতে পারে।

Djibdiplomatie[.]com

‘**djibdiplomatie[.]com**’ ডোমেইনটি জিবুতি সরকারের কূটনৈতিক সেবা বা প্রতিষ্ঠানগুলোর ছদ্মবেশ ধারণ করেছে বলে মনে হয়, যার WHOIS রেকর্ড ‘**utdglobals[.]com**’ ডোমেইনের মতোই ছিল। একটি রেকর্ডে দেখা গেছে, রেজিস্ট্র্যান্ট হিসেবে ছিল ‘**ocean.nio@rediffmail[.]com**’ এবং অ্যাডমিন হিসেবে ছিল ‘**taoyujun@gmail[.]com**’; তবে অন্যান্য রেকর্ডে অ্যাডমিন ইমেইল হিসেবে দেখা গেছে ‘**wangminghua6@gmail[.]com**’ এবং রেজিস্ট্র্যান্ট হিসেবে আবার ছিল ‘**ocean.nio@rediffmail[.]com**’।

এই দুটি ডোমেইনের WHOIS রেকর্ডেও 'কীবোর্ড ওয়াকিং' ধাঁচের মান ব্যবহার করা হয়েছিল। উদাহরণস্বরূপ, '**udtglobals[.]com**' ডোমেইনের WHOIS রেকর্ডে রেজিস্ট্র্যান্ট সিটি হিসেবে **'ASDF'** এবং '**djibdiplomatie[.]com**' ডোমেইনে রেজিস্ট্র্যান্ট নেম হিসেবে **'DAF DAGF'** উল্লেখ করা হয়েছে। এটি অন্যান্য BADBAZAAR ডোমেইনে পর্যবেক্ষণ করা মানসমূহের সঙ্গে তুলনাযোগ্য।

যদিও '**wangminghua6@gmail[.]com**' এবং '**taoyujun@gmail[.]com**' এই দুটি ইমেইল ঠিকানা এমন কিছু ডোমেইনের WHOIS রেকর্ডে দেখা গেছে, যেগুলো একটি **বৈশ্বিক সমুদ্রতল প্রতিরক্ষা সম্মেলন, জিবুতি কূটনৈতিক সেবা,** এবং **আন্তর্জাতিক পারমাণবিক শক্তি সংস্থার (IAEA)** ছদ্মবেশ ধারণ করেছে, এই ইমেইল ঠিকানাগুলো একাধিক নিরীহ বা ক্ষতিকর নয় এমন ডোমেইনের WHOIS রেকর্ডেও পাওয়া গেছে।

ছদ্মবেশী ডোমেইন ও নিরীহ ডোমেইনের মিশ্রতা ইঙ্গিত দিতে পারে যে, একটি অবকাঠামো সংগ্রহকারী গোষ্ঠী (infrastructure-procuring entity) বিদ্যমান রয়েছে যা ক্ষতিকর সাইবার হামলাকারীদের কার্যক্রমে সহায়তা করার জন্য ব্যবহৃত হয়ে থাকে।

'**ocean.nio@rediffmail[.]com**' এই ইমেইল ঠিকানাটি শুধুমাত্র পূর্বে বর্ণিত ছদ্মবেশী ডোমেইনগুলিতেই পাওয়া গেছে। অন্যদিকে '**ivan_s81@mail[.]ru**' এবং '**tplutalova@list[.]ru**' এই ইমেইল ঠিকানাদুটি খুব অল্প সংখ্যক ডোমেইন রেজিস্ট্রেশনে ব্যবহৃত হয়েছে, এবং তাদের কিছু ডোমেইন BADBAZAAR অবকাঠামোতে হোস্ট করা হয়েছিল। এই তিনটি ইমেইল ঠিকানাকে ক্ষতিকর সাইবার হামলাকারীদের কার্যক্রমের সঙ্গে ঘনিষ্ঠভাবে যুক্ত বলে মনে করা হয়। এর কারণ হলো—এই ইমেইল ঠিকানাগুলোর সঙ্গে যুক্ত অধিকাংশ ডোমেইন অপরাধমূলক কার্যকলাপের সঙ্গে সংযুক্ত, বিশেষত '**wangminghua6@gmail[.]com**' and '**taoyujun@gmail[.]com**'. ইমেইল ঠিকানার তুলনায়।

(পরিশিষ্ট A, চিত্র ৫ দেখুন)

অন্যান্য সাইবার অপরাধীদের লিঙ্ক

BADBAZAAR-লিঙ্কযুক্ত ডোমেইন **'actuallys[.]com', 'clublogs[.]com', 'myloughborough[.]com', 'rewrwer[.]com',** এবং **'voiceoftibet[.]net'**-এর আরেকটি সাধারণ বৈশিষ্ট্য হল যে এগুলি সবই eNom-এ নিবন্ধিত ছিল এবং '255.255.255[.]254'-এ 'পার্ক' করা হয়েছিল।

পূর্ববর্তী NCSC তদন্তের পর, এই বৈশিষ্ট্যযুক্ত অন্যান্য ডোমেইনগুলিতে ২০১৯ সালে **APT5** এবং ২০০৯ থেকে ২০১১ সালের মধ্যে **APT14**-এর কার্যকলাপের প্রমাণ পাওয়া গেছে।

APT5-লিঙ্কযুক্ত ডোমেনগুলির অতীতের WHOIS রেকর্ডে নিবন্ধক ইমেল ঠিকানা হিসাবে **'taoyujun@gmail[.]com'** তালিকাভুক্ত ছিল।

APT14-লিঙ্কযুক্ত ডোমেনগুলির তিন-অক্ষরের সাবডোমেন ছিল যেগুলি সম্ভবত তাদের অপরাধমূলক ক্রিয়াকলাপের লক্ষ্যবস্তুকে নির্দেশ করেছিল। এর একটি উদাহরণ হল **'bae.cisconline[.]net'**, যা BAE সিস্টেমগুলিকে টার্গেট করার ইঙ্গিত প্রদান করে এবং এটি একটি **'পয়জন আইভি'** নমুনায় পাওয়া গেছে।

BADBAZAAR ডোমেইনগুলোর মধ্যেও একটি অনুরূপ বৈশিষ্ট্য দেখা যায়—যেখানে সাবডোমেইনগুলো সাধারণত সেই ট্রোজান ইনস্টল করা অ্যাপের নামের সঙ্গে সম্পর্কিত থাকেঃ

অ্যাপ্লিকেশন টাইটেল	C2 URL
মুসলিম প্রো	**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

এটা মনে রাখা গুরুত্বপূর্ণ যে **APT5** এবং **APT14** এর সাথে সম্পর্কিত কার্যকলাপগুলি ঐতিহাসিক ছিল এবং eNom-এ নিবন্ধিত ও **'255.255.255.254'**-এ রূপান্তরিত আরও কিছু ডোমেইন রয়েছে যেগুলির সঙ্গে ক্ষতিকর কার্যকলাপের কোনো সংযোগ পাওয়া যায়নি। সুতরাং, এই সমস্ত কার্যকলাপের পেছনে যে একই বা সম্পর্কিত সাইবার অপরাধী গোষ্ঠী রয়েছে—তা নিশ্চিতভাবে বলা যায় না।

মেশিন নাম

BADBAZAAR-এর C2 সার্ভার এবং স্যাম্পল বিশ্লেষণে দেখা গেছে যে, SSL সার্টিফিকেটে 'কমন নেইম' হিসেবে কিছু হোস্টনেম ব্যবহার করা হয়েছে। BADBAZAAR-এর স্যাম্পল ও অবকাঠামোতে পর্যবেক্ষণ করা হোস্টনেমগুলোর ওপর NCSC-এর তদন্তে দেখা গেছে—এই হোস্টনেমগুলো একাধিক আইপি ঠিকানায় ব্যবহৃত হয়েছে। এই আইপি ঠিকানাগুলোতে BADBAZAAR স্যাম্পলে পাওয়া ডোমেইনগুলো হোস্ট করা হচ্ছে। নিচের অংশে BADBAZAAR C2 ডোমেইন হোস্ট করা হোস্টনেম এবং সংশ্লিষ্ট আইপি ঠিকানাগুলোর বিষয়ে আরও বিস্তারিত তথ্য দেওয়া হয়েছে।

প্রায় সব ক্ষেত্রেই দেখা গেছে যে, SSL সার্টিফিকেটে থাকা হোস্টনেম মান এবং ক্ষতিকর ডোমেইনের IP রেজল্যুশনের মধ্যে মিল রয়েছে; তবে যেসব ক্ষেত্রে এই মিল পাওয়া যায়নি, সেগুলোর ব্যাখ্যা আলাদাভাবে দেওয়া হয়েছে।

WIN-EU0VLBL7TUJ

'WIN-EU0VLBL7TUJ' হোস্টনেমটি নিচে উল্লেখিত গুরুত্বপূর্ণ কিছু আইপি ঠিকানায় দেখা গেছেঃ

- **'116.203.53[.]21'** এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন **'uyapkfinder[.]com'** এবং **'thewestuniverse[.]com'**।

- **‘95.216.169[.]27’** এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন **‘adysfunction[.]com’** এবং সাব-ডোমেইন **‘download.apkbazar[.]biz’** BADBAZAAR নমুনার জন্য ডাউনলোড লিঙ্ক হিসেবে পর্যবেক্ষণ করা হয়েছে।

(পরিশিষ্ট A, চিত্র ৬ দেখুন)

WIN-70E59JVOB9G

WIN-70E59JVOB9G’ হোস্টনেমটি নিচে উল্লেখিত গুরুত্বপূর্ণ কিছু আইপি ঠিকানায় দেখা গেছেঃ

- ‘**23.88.28[.]220**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 sub-domains, **‘aua.rondwsign[.]com’, ‘nal.tokenmajorp[.]com’, ‘pep.rondwsign[.]com’** ‘**doa.rondwsign[.]com**’, and **‘pls.rondwsign[.]com’.** যে মেশিনটির সঙ্গে সার্টিফিকেটটি যুক্ত ছিল, সেটি সর্বশেষ দেখা যাওয়ার সময়ের সঙ্গে ক্ষতিকর ডোমেইনগুলো ওই আইপি ঠিকানায় রূপান্তরিত হতে শুরু করার সময়ের মধ্যে দুই দিনের ব্যবধান ছিল।

- ‘**23.88.28[.]221**’ এ হোস্ট করা হয়েছে BADBAZAAR লিঙ্ক যুক্ত সাব-ডোমেইন ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন ‘**tubevideoplus[.]org**’ এবং ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**bat.androidupdated[.]net**’. এটি ‘**apps.androidupdated[.]net**’ নামের একটি সাবডোমেইনও হোস্ট করেছিল, যা DoubleAgent ম্যালওয়্যারের একটি C2।

- ‘**65.21.92[.]77**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ এবং ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**upd.whoscaller.net**’. এবং ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**bvn.lookincategory[.]com’** এবং ‘**edr.lookincategory[.]com’.** যে মেশিনটির সঙ্গে সার্টিফিকেটটি যুক্ত ছিল, সেটি সর্বশেষ দেখা যাওয়ার সময়ের সঙ্গে ক্ষতিকর ডোমেইনগুলো ওই আইপি ঠিকানায় রূপান্তরিত হতে শুরু করার সময়ের মধ্যে এগার দিনের ব্যবধান ছিল।

- **‘142.132.131[.]20’** এ হোস্ট করা হয়েছে সাব-ডোমেইন ‘**son.onlinegamersgroup[.]com’** এবং ‘**system.onlinegamersgroup[.]com’**, যেগুলিকে BADBAZAAR C2 সার্ভার হিসেবে মনে করা হয় কারন এই ডোমেইনগুলো হোস্ট করা হচ্ছিল সেই সময়েই, যখন BADBAZAAR-সংশ্লিষ্ট SSL সার্টিফিকেটগুলো ওই IP ঠিকানায় দেখা গিয়েছিল।

- ‘**142.132.131[.]28’** এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন ‘**goldplusapp[.]net**’ এবং সাব-ডোমেইন ‘**who.goldplusapp[.]net**’ and ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, এবং ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** এবং **‘aua.rondwsign[.]com’.**

- ‘**195.154.47[.]99**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**ggl.whoscaller[.]net**’ এবং ‘**upd.whoscaller.net**’. যে মেশিনটির সঙ্গে সার্টিফিকেটটি যুক্ত ছিল, সেটি সর্বশেষ দেখা যাওয়ার সময়ের সঙ্গে ক্ষতিকর ডোমেইনগুলো ওই আইপি ঠিকানায় রূপান্তরিত হতে শুরু করার সময়ের মধ্যে তিন দিনের ব্যবধান ছিল।

- ‘**195.154.60[.]3**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**upd.whoscaller[.]net**’
‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ এবং ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ এ হোস্ট করা হয়েছে BADBAZAAR C2 সাব-ডোমেইন, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ এবং ‘**bvn.lookincategory[.]com**’.

(পরিশিষ্ট A, চিত্র ৭ দেখুন)

WIN-50QO3EIRQVP

হোস্টনেম '**WIN-50QO3EIRQVP**' দেখা গিয়েছিল নিম্নলিখিত IP ঠিকানায়:

- '**45.76.132[.]91**' এ হোস্ট করা হয়েছে ডোমেইন, '**yumoftion[.]com**', '**androidupdated[.]net**'. উভয় ডোমেইন BADBAZAAR-এর সঙ্গে যুক্ত, কারণ '**fow.yumoftion[.]com**' এবং '**bat.androidupdated[.]net**' সাবডোমেইন দুটি BADBAZAAR-এর C2 ডোমেইন হিসেবে ব্যবহৃত হয়েছে। এছাড়াও '**apps.androidupdated[.]net**' সাবডোমেইনটি DoubleAgent ম্যালওয়্যারের একটি C2 ডোমেইন হিসেবে ব্যবহৃত হয়েছে। এটি '**pmstwocqn[.]com**' ডোমেইনটিও হোস্ট করে, যা WHOIS রেকর্ডের মাধ্যমে BADBAZAAR-এর সঙ্গে যুক্ত।

- **'95.179.210[.]85'** এ হোস্ট করা হয়েছে **'clublogs[.]com'**, যার মধ্যে **'xle.clublogs[.]com'** একটি BADBAZAAR C2 ডোমেইন এবং এটি BADBAZAAR লিঙ্কযুক্ত ডোমেইন **'bre.myloughborough[.]com', 'img.rewrwer[.]com', 'www.voiceoftibet[.]net'** এবং **'actuallys[.]com'** হোস্ট করেছে।

- **'199.247.21[.]34'** এ হোস্ট করা হয়েছে **'titeperformance[.]com'**, এবং **'collinformations[.]com'** যার সাবডোমেনগুলি হল BADBAZAAR C2 ডোমেন।

- **'217.69.10[.]128'** এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন **'uyghurdict[.]com'**।

(পরিশিষ্ট A, চিত্র ৮ দেখুন)

WMSvc-WIN-50QO3EIRQVP

হোস্টনেম '**WMSvc-WIN-50QO3EIRQVP**' দেখা গিয়েছিল নিম্নলিখিত IP ঠিকানায়:

- **'78.46.185[.]251'** এ হোস্ট করা হয়েছে BADBAZAAR C2 ডোমেইন **'groupgram[.]org'**, যা Volexity রিপোর্ট করেছে যে এটি ক্ষতিকারক সংযোগের জন্য পোর্ট ৪৪৩২ ব্যবহার করছে।

- **'65.21.92[.]69'** এবং **'163.172.205[.]207'** এ হোস্ট করা হয়েছে ডোমেইন **'widelygram[.]org'** যেটিকে একটি BADBAZAAR C2 ডোমেইন বলে মনে করা হয়, কারণ উভয় আইপিতেই হোস্ট করা থাকলেও, পোর্ট ৪৪৩২ খোলা ছিল।

- **'163.172.198[.]206'** এ হোস্ট করা হয়েছে ডোমেইন **'maxgram[.]org'** যেটিকে একটি BADBAZAAR C2 ডোমেইন বলে মনে করা হয়, কারণ এটি হোস্ট করার সময় পোর্ট ৪৪৩২ খোলা ছিল।

(পরিশিষ্ট A, চিত্র ৯ দেখুন)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

নিম্নলিখিত IP ঠিকানায় একই সাথে হোস্টনেম **'WMSvc-WIN-50QO3EIRQVP'** এবং **'WIN-7LSBB9R0F1L'** দেখা গেছে:

- **'148.251.87[.]245'** এ BADBAZAAR C2 ডোমেইন **'flygram[.]org'** এবং **'groupgram[.]org'** হোস্ট করা হয়েছে।

(পরিশিষ্ট A, চিত্র ১০ দেখুন)

WIN-N8H8S9BG2P0

হোস্টনেম '**WIN-N8H8S9BG2P0**' দেখা গিয়েছিল নিম্নলিখিত IP ঠিকানায়:

- **'148.251.87[.]247'** এ BADBAZAAR C2 ডোমেইন **'omarwhatsapp[.]org'** এবং **'flygram[.]org'** হোস্ট করা হয়েছে।

(পরিশিষ্ট A, চিত্র ১১ দেখুন)

WIN-I6VBN8MR92A

হোস্টনেম '**WIN-I6VBN8MR92A**' দেখা গিয়েছিল নিম্নলিখিত IP ঠিকানায়:

- '**148.251.87[.]197**' এ BADBAZAAR C2 ডোমেইন '**tryhrwserf[.]com**' হোস্ট করা হয়েছে।

(পরিশিষ্ট A, চিত্র ১২ দেখুন)

বাণিজ্যিকভাবে প্রাপ্ত ডেটা অনুযায়ী, এই মেশিন নামগুলো ইন্টারনেটে কতটা ছড়ানো রয়েছে তা ভিন্ন ভিন্ন হয়ে থাকে। এদের মধ্যে কিছু মেশিনকে একসাথে একাধিক আইপি ঠিকানায় দেখা গেছে, যা ইঙ্গিত করে যে এগুলো একই টেমপ্লেট ব্যবহার করে তৈরি করা কিছু ভার্চুয়াল মেশিন (VM)। বুঝে রাখা দরকার, কিছু হোস্টনেমের ক্ষেত্রে যেসব আইপি ঠিকানায় এদের দেখা গেছে, সেগুলোর সবগুলোই যে ক্ষতিকর কার্যক্রমের সঙ্গে জড়িত—তা নয়। এর মানে হতে পারে, এই হোস্টনেমগুলো শুধুমাত্র ওই নির্দিষ্ট সাইবার অপরাধীদের ব্যবহারের মধ্যেই সীমাবদ্ধ নয়।

তবে এই মেশিন নামগুলোর কিছু যদি এমন আইপি ঠিকানায় নিয়মিতভাবে দেখা যায়, যেগুলো BADBAZAAR-এর C2 ডোমেইন হোস্ট করেছে, তাহলে এটা বোঝা যেতে পারে যে কোনো অবকাঠামো সরবরাহকারী পক্ষ হয়তো দুষ্কৃতিকারীদের সাইবার অপারেশন চালাতে মেশিন কনফিগার করাতে সহায়তা করছে।

সামাজিক মাধ্যমে উপস্থিতি

Volexity এর পূর্ববর্তী প্রতিবেদনে দেখা গেছে যে YouTube ভিডিওগুলি (ক্ষতিকারক অ্যাপ্লিকেশনগুলির ব্যবহার প্রচার করে) সাইবার অপরাধীদের দ্বারা তৈরি করা হয়েছিল। তৈরি করা অ্যাপ্লিকেশনগুলোর ব্যবহারবিধি এই ভিডিওগুলোতে শেখানো হয়েছে।

NCSC আরও দুটি ইউটিউব চ্যানেল শনাক্ত করেছে, যেগুলো ওই সাইবার অপরাধী গ্রুপের কার্যক্রমের সঙ্গে যুক্ত। **'@josephjoey3499'** URL হ্যান্ডেল সম্বলিত ইউটিউব চ্যানেল '**ম্যাক্সগ্রাম**' ব্যবহারের প্রচার করছে বলে মনে হচ্ছে এবং **'@uyghurapks3096'**-এ নিবন্ধিত আরেকটি চ্যানেল **'উইঘুর APK ফাইন্ডার'** প্রচার করছে।

অতিরিক্তভাবে, '**Flygram**' এবং '**Signal Plus**' প্রচারকারী ইউটিউব ভিডিওগুলোতে সাইবার অপরাধী গ্রুপের ব্যবহার করা ফোন নম্বরগুলো খোলাখুলিভাবে দেখা গেছে। '**Flygram**' ভিডিওর ০:৩৬ মিনিটে '**+1 (570) 378-7250**' নম্বরটি দেখা যায়, এবং '**Signal Plus**' ভিডিওতে দেখা যায় '**+1 (267) 298 4259**' নম্বরটি।

Volexity- তাদের প্রতিবেদনে '**ignitetibet[.]net**' নামে একটি ভুয়া তিব্বত-ভিত্তিক সংবাদ সাইটের কথা উল্লেখ করেছে, যা সাইবার অপরাধীদের দ্বারা পরিচালিত টেলিগ্রাম চ্যানেলগুলোর মাধ্যমে ছড়ানো হচ্ছিল বলে ধারণা করা হচ্ছে। **choekyi.wangmo@ignitetibet[.]net'** ইমেইল ঠিকানাটি **'tibetone.org'** পেজে বিভিন্ন পোস্টে মন্তব্য করেছে, যা Lookout-এর উন্মুক্ত প্রতিবেদনে BADBAZAAR-এর iOS সংস্করণের C2 পেজ হিসেবে চিহ্নিত হয়েছে।

এই ইমেইল ঠিকানাটি সম্ভবত সাইবার অপরাধী গ্রুপের নিয়ন্ত্রণে রয়েছে, যারা '**Choekyi Wangmo**' নামের ছদ্মপরিচয় ব্যবহার করছে।

মুল্যায়ন

BADBAZAAR এবং MOONSHINE গ্রুপগুলো বিভিন্ন ধরণের 'সোশ্যাল ইঞ্জিনিয়ারিং' কৌশল ব্যবহার করে বিশেষভাবে উইঘুর, তিব্বতি ও তাইওয়ানিজ জনগোষ্ঠীকে টার্গেট করে। যেমনঃ

- এই জনগোষ্ঠীগুলোর আগ্রহের বিষয়ভিত্তিক অ্যাপ—যেমন উইঘুর ভাষার কোরআন অ্যাপ—কে ট্রোজানাইজ করা হয়েছে, যা প্রায় নিশ্চিতভাবে সুনির্দিষ্ট ভুক্তভোগীদের লক্ষ্য করে তৈরি।
- এই ট্রোজানযুক্ত অ্যাপগুলোকে অফিসিয়াল অ্যাপ স্টোরে যুক্ত করার উদ্দেশ্য হল খুব সম্ভবত ব্যবহারকারীদের কাছে এগুলোর প্রতি বিশ্বাসযোগ্যতা তৈরি করা, আর এগুলোকে গ্রুপ চ্যাটে শেয়ার করা সম্ভবত ওই সম্প্রদায়ের ভেতরের পারস্পরিক আস্থাকে কাজে লাগানোর উদ্দেশ্যে করা হয়।

BADBAZAAR এবং MOONSHINE এমন ধরনের তথ্য সংগ্রহ করে, যা প্রায় নিশ্চিতভাবে চীনা রাষ্ট্রের জন্য গুরুত্বপূর্ণ হতে পারে। BADBAZAAR এবং MOONSHINE যদিও উইঘুর, তিব্বতি এবং তাইওয়ানিজ ব্যক্তিদের টার্গেট করেছে, একইভাবে আরও কিছু ম্যালওয়্যার রয়েছে যেগুলি চীনের অন্যান্য সংখ্যালঘু গোষ্ঠীকেও টার্গেট করে। চীন ও বিদেশে অবস্থানরত সহ-স্বাক্ষরকারী দেশগুলোর নাগরিকরা, যাদেরকে চিন সরকারের শাসনের স্থিতিশীলতার জন্য হুমকি বলে মনে করা হয়, তারা প্রায় নিশ্চিতভাবেই BADBAZAAR ও MOONSHINE-এর মতো মোবাইল ম্যালওয়্যারগুলির ঝুঁকির মধ্যে রয়েছে। অবস্থান, অডিও ও ছবি সংগ্রহের সক্ষমতা প্রায় নিশ্চিতভাবে টার্গেটকৃত ব্যক্তির গতিবিধি সম্পর্কে তাৎক্ষণিক তথ্য দিয়ে ভবিষ্যতের নজরদারি ও হয়রানিমূলক কার্যক্রম পরিচালনায় সহায়তা করতে পারে।

MITRE ATT&CK®

এই প্রতিবেদনটি MITRE ATT&CK® ফ্রেমওয়ার্ক অনুসরণ করে তৈরি করা হয়েছে, যা বাস্তব ঘটনার ভিত্তিতে সাইবার আক্রমণকারীদের কৌশল ও পদ্ধতির একটি বৈশ্বিকভাবে উন্মুক্ত জ্ঞানভাণ্ডার।

পন্থা	আইডি	কৌশল	পদ্ধতি
তদন্ত	T1593.001	ওপেন ওয়েবসাইট/ডোমেন অনুসন্ধান করুন: সামাজিক মাধ্যম	হ্যাকাররা তাদের আকাঙ্ক্ষিত ভুক্তভোগীর সঙ্গে মিলে এমন অনলাইন গ্রুপ ও ফোরাম খুঁজে বের করে, যেখানে তারা ম্যালওয়্যার শেয়ার করতে পারে।
রিসোর্স উন্নয়ন	T1583.001	অবকাঠামো সংগ্রহঃ ডোমেইন	সাইবার অপরাধীরা তাদের কমান্ড এবং কন্ট্রোল সার্ভারের জন্য ডোমেইন রেজিস্টার করে।
রিসোর্স উন্নয়ন	T1587.001	সক্ষমতা তৈরিঃ ম্যালওয়্যার	ট্রোজানযুক্ত অ্যাপে প্রবেশ করানোর জন্য ক্ষতিকর কোড লেখা হয়।
রিসোর্স উন্নয়ন	T1608.001	সক্ষমতা প্রস্তুত রাখাঃ ম্যালওয়্যার আপলোড করা	ট্রোজানযুক্ত অ্যাপগুলো অনলাইন প্ল্যাটফর্ম, এমনকি অফিসিয়াল অ্যাপ স্টোরেও আপলোড করা হয়।
রিসোর্স উন্নয়ন	T1585.001	অ্যাকাউন্ট খোলাঃ সামাজিক মাধ্যমে অ্যাকাউন্ট	সাইবার অপরাধীরা ম্যালওয়্যার শেয়ার ও প্রচারের জন্য বিভিন্ন ওয়েবসাইট ও সামাজিক যোগাযোগমাধ্যমে অ্যাকাউন্ট তৈরি করে।
রিসোর্স উন্নয়ন	T1585.002	অ্যাকাউন্ট খোলাঃ ইমেইল অ্যাকাউন্ট	সাইবার অপরাধীরা ম্যালওয়্যার হোস্ট ও শেয়ার করার জন্য ব্যক্তিগতভাবে হোস্ট করা এবং বাণিজ্যিক ইমেইল অ্যাকাউন্ট ব্যবহার করে।
প্রাথমিক অ্যাক্সেস	T1189	ড্রাইভ-বাই কম্প্রোমাইজ	ক্ষতিকর স্ক্রিপ্ট এমন বৈধ অ্যাপে লুকিয়ে রাখা হয়, এবং সেগুলো অ্যাপ স্টোরে আপলোড করা হয়।
প্রাথমিক অ্যাক্সেস	T1566.003	ফিশিংঃ সার্ভিসের মাধ্যমে স্পিয়ারফিশিং	সাইবার অপরাধীরা টার্গেট করা গোষ্ঠীগুলোর কাছে টেলিগ্রাম সহ সামাজিক যোগাযোগমাধ্যম ব্যবহার করে ট্রোজানযুক্ত অ্যাপ পাঠায়।
আক্রমণ চালানো	T1204.002	**ব্যবহারকারীর মাধ্যমে আক্রমণ চালানো** ক্ষতিকর ফাইল	পেলোড চালু করতে ভুক্তভোগীদের ট্রোজানযুক্ত অ্যাপ ইনস্টল করতে হয়।
নিরাপত্তা ব্যবস্থা এড়ানোর কৌশল	T1027.009	রূপান্তরিত ফাইল বা তথ্যঃ লুক্কায়িত পেলোড	ক্ষতিকর পেলোড সাধারণত বৈধ অ্যাপের ভেতরে লুকিয়ে রাখা হয়।
নিরাপত্তা ব্যবস্থা এড়ানোর কৌশল	T1036.005	ছদ্মবেশঃ বৈধ নাম বা অবস্থানকে অনুকরণ করে	ট্রোজানযুক্ত ফাইলগুলো বৈধ অ্যাপের নাম, চেহারা ও কার্যকারিতা অনুকরণ করে।

নিরাপত্তা ব্যবস্থা এড়ানোর কৌশল	T1656	ব্যক্তিগত পরিচয় নকল করা	সাইবার অপরাধীরা টার্গেটিকৃত গোষ্ঠীর সঙ্গে সম্পর্কযুক্ত ইউজারনেম ব্যবহার করে এবং ছদ্মনামে ওয়েবসাইট তৈরি করে বিশ্বাসযোগ্য ব্যক্তিদের ছদ্মবেশ ধারণ করে।
সংগ্রহ	T1123	অডিও ধারণ	ট্রোজানযুক্ত অ্যাপগুলো এমন অনুমতি চায় যা তাদের কাজের জন্য দরকার নেই—যেমন মাইক্রোফোন ব্যবহারের অনুমতি।
সংগ্রহ	T1125	ভিডিও ধারণ	ট্রোজানযুক্ত অ্যাপগুলো এমন অনুমতি চায় যা তাদের কাজের জন্য দরকার নেই—যেমন ক্যামেরা ব্যবহারের অনুমতি।
সংগ্রহ	T1005	লোকাল সিস্টেম থেকে ডেটা সংগ্রহ	ট্রোজানযুক্ত অ্যাপগুলো এমন অনুমতি চায় যা তাদের কাজের জন্য দরকার নেই—যেমন লোকাল ফাইলগুলিতে প্রবেশের অনুমতি।
কম্যান্ড এবং কন্ট্রোল	T1071.001	অ্যাপ্লিকেশন লেয়ার প্রটোকল ওয়েব প্রটোকল	ম্যালওয়্যার HTTPS এবং WebSocket's ব্যবহার করে এর C2 সাথে যুক্ত হয়।
কম্যান্ড এবং কন্ট্রোল	T1509	অপ্রচলিত পোর্ট	4432 বা 2333-এর মতো অপ্রচলিত পোর্টগুলো ব্যবহৃত হয়
গোপনে তথ্য বাইরে পাঠানো	T1041	C2 চ্যানেল ব্যবহার করে গোপনে ডেটা বাইরে পাঠানো	ম্যালওয়্যার HTTPS এবং WebSocket's সংযোগ ব্যবহার করে ডেটা বাইরে পাঠায়।
প্রভাব	T1565.002	ডেটা পরিবর্তনঃ স্থানান্তরিত ডেটা পরিবর্তন	অ্যাপের কার্যকারিতার জন্য প্রয়োজন নেই এমন ওয়েব ট্র্যাফিক চালু করে সাইবার অপরাধীরা ভুক্তভোগীদের কাছ থেকে তথ্য সংগ্রহ করে।

নির্দেশক

MOONSHINE

- ১লা এপ্রিল ২০২৫ তারিখে, VLiteUI প্যানেল অনুসন্ধানের সময় নিম্নলিখিত তথ্য পাওয়া যায়:

IP ঠিকানা	পোর্ট	প্রথম দেখা গিয়েছিল	শেষ দেখা গিয়েছিল
103.254.108[.]87	৮৮৮	২০২৪-১০-১৭	২০২৫-০২-১৪
43.159.192[.]7	444	২০২৪-১১-২১	২০২৫-০২-১৩
103.27.109[.]109	444	২০২৪-০৭-১১	২০২৫-০২-০৭
45.119.99[.]83	444	২০২৪-১২-২৬	২০২৫-০১-২৪
103.254.108[.]76	444	২০২৪-০৯-১২	২০২৪-১২-০৫
194.71.107[.]160	444	২০২৩-১২-১০	২০২৪-১১-০১
103.254.108[.]108	444	২০২৩-১১-১২	২০২৪-০৯-২৫
103.56.17[.]194	444	২০২৪-০৪-০৩	২০২৪-০৮-২৩
103.254.108[.]87	444	২০২৩-১১-১৪	২০২৪-০৮-১৫
62.72.58[.]168	444	২০২৪-০১-২৯	২০২৪-০৮-০৭
103.43.18[.]43	444	২০২৪-০২-১২	২০২৪-০৭-১৯
77.91.123[.]208	444	২০২৪-০২-০৪	২০২৪-০৪-০৯
46.246.98[.]229	444	২০২৪-০৩-০৭	২০২৪-০৩-২৬
2.58.15[.]101	444	২০২৪-০২-২৩	২০২৪-০২-২৭
46.246.98[.]209	444	২০২৪-০১-০৮	২০২৪-০২-১৪
103.254.108[.]87	৮০০০	২০২৩-১০-১৭	২০২৩-১০-১৭
103.254.108[.]87	৮০৮০	২০২৩-০৪-১৫	২০২৩-১০-১৬
103.254.108[.]108	৯০৯০	২০২৩-০৪-১৩	২০২৩-১০-১৬
103.45.66[.]123	৯০৯০	২০২৩-০৩-০২	২০২৩-০৪-০৮
103.45.66[.]32	৮০৮০	২০২২-০৭-২৯	২০২৩-০৪-০৬
27.124.20[.]23	৯০৯০	২০২২-০৫-২৮	২০২৩-০৩-২৪
27.124.20[.]22	৯০৯০	২০২২-০৫-২৮	২০২৩-০৩-২৩
27.124.20[.]24	৯০৯০	২০২২-০৫-২৭	২০২৩-০৩-১৭
69.176.94[.]148	৯০৯০	২০২৩-০৩-০৪	২০২৩-০৩-১০
69.176.94[.]228	৯০৯০	২০২২-১২-২৪	২০২৩-০২-২৫
103.253.40[.]137	৮০০০	২০২২-০৬-২৪	২০২২-০৯-০২
27.124.4[.]80	৮০৮০	২০২২-০২-২৫	২০২২-০৬-২৩
27.124.4[.]81	৮০৮০	২০২২-০২-২৫	২০২২-০৬-২৩
47.242.46[.]79	৮০৮০	২০২১-০৫-০৩	২০২২-০৬-১৭
27.124.4[.]82	৮০৮০	২০২২-০২-২৪	২০২২-০৬-১৫
27.124.4[.]165	৯০৯০	২০২২-০৫-১৪	২০২২-০৫-২৮

27.124.4[.]184	৯০৯০	২০২২-০৫-১৪	২০২২-০৫-২৭
27.124.4[.]178	৯০৯০	২০২২-০৫-১৩	২০২২-০৫-২৬
103.15.28[.]165	৮০৮০	২০২২-০৩-০৫	২০২২-০৫-২৫
69.176.94[.]226	৮০৮০	২০২২-০৩-০৫	২০২২-০৪-২২
27.124.4[.]3	৮০৮০	২০২২-০৩-১১	২০২২-০৪-০২
103.140.238[.]235	৮০৮০	২০২২-০৩-০৪	২০২২-০৪-০১
27.124.4[.]2	৮০৮০	২০২২-০৩-১২	২০২২-০৪-০১
165.84.180[.]107	৮০০০	২০২২-০২-২৫	২০২২-০৩-১৯
69.176.94[.]156	৮০০০	২০২২-০২-২৫	২০২২-০৩-০৫
141.98.212[.]70	৯০৯০	২০২১-১০-০৫	২০২২-০৩-০৪
5.188.33[.]50	৮০০০	২০২২-০২-১৫	২০২২-০৩-০৪
5.188.70[.]193	৮০০০	২০২২-০২-১৫	২০২২-০৩-০৪
69.176.94[.]140	৮০৮০	২০২২-০২-২৪	২০২২-০২-২৪
27.124.20[.]83	৮০০০	২০২২-০২-১৪	২০২২-০২-১৮
208.87.200[.]106	৮০০০	২০২২-০১-০২	২০২২-০১-০২
121.127.241[.]37	৮০০০	২০২১-১২-০৮	২০২১-১২-০৮
156.255.2[.]211	৪৪৩	২০২১-১০-০৫	২০২১-১০-০৫
156.255.2[.]211	৮০০০	২০২১-১০-০৪	২০২১-১০-০৪
156.255.2[.]203	৮০০০	২০২১-১০-০৩	২০২১-১০-০৩
47.243.43[.]248	৮০০০	২০২১-০৭-০৫	২০২১-০৭-০৫
45.115.236[.]6	৮০৮০	২০২১-০৫-০৩	২০২১-০৩-০১
43.251.118[.]97	৮০০০	২০২১-০১-০৩	২০২১-০৩-০১
185.243.43[.]138	৮০০০	২০২১-০১-০৪	২০২১-০২-০২
47.245.59[.]33	৮০০০	২০২১-০১-০৫	২০২১-০১-০৫

- ১লা এপ্রিল ২০২৫ তারিখে, SCOTCH অ্যাডমিন প্যানেল অনুসন্ধানের সময় নিম্নলিখিত তথ্য পাওয়া যায়:

IP ঠিকানা	পোর্ট	প্রথম দেখা	শেষ দেখা
104.194.152[.]24	২৩৩৩	২০২৫-০২-০৬	২০২৫-০২-২৭
172.86.80[.]126	২৩৩৩	২০২৫-০২-০৭	২০২৫-০২-২৭
154.90.59[.]62	২৩৩৩	২০২৪-০৬-২০	২০২৪-০৯-২০
154.90.59[.]88	২৩৩৩	২০২৪-০৬-২১	২০২৪-০৯-২০
154.90.58[.]210	২৩৩৩	২০২৪-০৫-১৬	২০২৪-০৬-১৪
154.90.59[.]225	২৩৩৩	২০২৪-০৫-১৭	২০২৪-০৬-১৩
38.60.199[.]208	২৩৩৩	২০২৩-১১-২৬	২০২৪-০১-০৯
38.60.199[.]254	২৩৩৩	২০২৩-১১-২৮	২০২৪-০১-০৯
38.60.199[.]99	২৩৩৩	২০২৩-০৮-২৬	২০২৩-১১-২১

38.60.199[.]44	২৩৩৩	২০২৩-০৭-২০	২০২৩-০৯-১১
194.163.34[.]23	৪৪৩	২০২২-০৯-৩০	২০২৩-০৪-১৪
45.32.125[.]112	১০৪৪৩	২০২২-১০-০১	২০২৩-০৩-১৭

- ১৪ই মার্চ ২০২৪ তারিখে, ভার্চুয়াল SCOTCH অ্যাডমিন প্যানেল অনুসন্ধানের সময় নিম্নলিখিতগুলি পাওয়া গেছে:

ডোমেইন	আইপি ঠিকানা
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:

বিবরণ	BADBAZAAR C2s-এ SSL সার্টিফিকেট পর্যবেক্ষণ করা হয়েছে।
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- ১লা এপ্রিল ২০২৫ তারিখে, উপরের BADBAZAAR সার্টিফিকেটের অনুসন্ধানে নিম্নলিখিত ফলাফল পাওয়া গেছে:

আইপি ঠিকানা	পোর্ট	প্রথম দেখা	শেষ দেখা
65.108.192[.]173	৩১২৩৭	২০২৫-০৩-১৪	২০২৫-০৩-২৮
65.108.192[.]173	৩১২৩৬	২০২৫-০৩-১৪	২০২৫-০৩-২৮
65.108.192[.]173	৩১২৩৫	২০২৫-০৩-১৪	২০২৫-০৩-২৮
157.90.129[.]73	৩১২৩৬	২০২৫-০৩-২৭	২০২৫-০৩-২৭
142.132.131[.]15	৩১২৩৬	২০২৪-০৭-২৪	২০২৫-০৩-২৭

142.132.131[.]15	৩১২৩৫	২০২৪-০৭-২৬	২০২৫-০৩-২৭
142.132.131[.]20	৩১২৩৭	২০২৩-০৮-১১	২০২৫-০৩-২৭
142.132.131[.]15	৩১২৩৭	২০২৪-০৭-২৪	২০২৫-০৩-২৭
142.132.131[.]20	৩১২৩৬	২০২৩-০৯-২৭	২০২৫-০৩-২৬
142.132.131[.]20	৩১২৩৫	২০২৩-১০-১৮	২০২৫-০৩-২৬
65.108.192[.]155	৩১২৩৬	২০২৪-১২-০৫	২০২৫-০২-২০
65.108.192[.]155	৩১২৩৭	২০২৪-১২-০৫	২০২৫-০২-২০
65.108.192[.]155	৩১২৩৫	২০২৪-১২-০৫	২০২৫-০২-১৯
23.88.28[.]222	৩১২৩৭	২০২৪-০৪-২৫	২০২৪-১১-২৯
23.88.28[.]222	৩১২৩৫	২০২৪-০৫-০২	২০২৪-১১-২৮
23.88.28[.]222	৩১২৩৬	২০২৪-০৫-০১	২০২৪-১১-২৮
212.129.21[.]168	৩১২৩৫	২০২৩-১০-১৬	২০২৪-০৩-১৭
212.129.21[.]168	৩১২৩৭	২০২৩-০৮-২৪	২০২৪-০৩-১৭
212.129.21[.]168	৩১২৩৬	২০২৩-০৯-২৬	২০২৪-০৩-১৪

বর্ণনা	BADBAZAAR C2s-এ পর্যবেক্ষণ করা SSL সার্টিফিকেট
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62d b3db1baa

- ১লা এপ্রিল ২০২৫ তারিখে, উপরের BADBAZAAR সার্টিফিকেটের অনুসন্ধানে নিম্নলিখিত ফলাফল পাওয়া গেছে:

আইপি ঠিকানা	পোর্ট	প্রথম দেখা	শেষ দেখা
162.55.103[.]211	২০১২২	২০২৩-০১-১২	২০২৫-০৩-২৮
162.55.103[.]212	২০১২১	২০২২-০৬-৩০	২০২৫-০৩-২৮
162.55.103[.]212	২০১২২	২০২৩-০৭-১৪	২০২৫-০৩-২৮
162.55.103[.]211	২০১২১	২০২২-০৬-০৩	২০২৫-০৩-২৮
162.55.103[.]211	২০১২৩	২০২৩-০৭-২২	২০২৫-০৩-২৭
162.55.103[.]212	২০১২৩	২০২৩-০৭-২২	২০২৫-০৩-২৭
212.83.162[.]152	৯০৯০	২০২২-১০-১৩	২০২৫-০৩-২৭
23.88.28[.]221	২০৪২২	২০২৩-০৭-২৮	২০২৩-০৯-৩০
23.88.28[.]221	২০৪২১	২০২৩-০৫-১৮	২০২৩-০৯-২৮
23.88.28[.]221	২০৪২৩	২০২৩-০৭-২৮	২০২৩-০৯-২৮
162.55.103[.]210	২০১২১	২০২২-০৯-৩০	২০২৩-০২-২৩

65.21.92[.]67	২০১২১	২০২১-১১-০২	২০২২-১০-১৩
65.21.92[.]67	২০১২২	২০২২-০৮-১০	২০২২-১০-১৩
23.88.28[.]220	২০১২১	২০২১-১২-০৮	২০২২-০৫-১৩
94.130.92[.]230	২০১২১	২০২১-০১-০৪	২০২১-১০-০৫
88.99.150[.]246	২০১২১	২০২১-০৪-০৬	২০২১-০৯-০৮
45.76.132[.]91	২০১২১	২০২১-০২-০২	২০২১-০৩-০১

- WHOIS ডোমেইন

নিচে এমন কিছু ডোমেইনের একটি তালিকা দেওয়া হলো, যেগুলোর বর্তমান বা অতীত WHOIS রেকর্ডে এমন কিছু তথ্য রয়েছে যা BADBAZAAR C2 ডোমেইনগুলিতে পর্যবেক্ষণ করা মানগুলির সাথে মেলে।

WHOIS মূল্য	ডোমেইন
নিবন্ধক রাষ্ট্র: UJYJYUJ **নিবন্ধক দেশ: বলিভিয়া** **নিবন্ধক: 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
নিবন্ধক স্টেট: REWR **নিবন্ধকের দেশ: CF** **নিবন্ধক: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
নিবন্ধক স্টেট: FSDF	• tryhrwserf[.]com

নিবন্ধকের দেশ: AL **নিবন্ধক: eNom**	• tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

ইউটিউব চ্যানেল
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

BADBAZAAR এবং MOONSHINE-এর সাথে সম্পর্কিত সমঝোতার অন্যান্য সূচকের (IoCs) লিঙ্কগুলি নীচে দেওয়া হল। NCSC এই লিঙ্কগুলিতে থাকা সমস্ত তথ্যের বৈধতা নিশ্চিত করতে পারে না এবং পাঠকদেরকে নিজ দায়িত্বে তথ্যগুলোর যথার্থতা ও প্রাসঙ্গিকতা যাচাই করার পরামর্শ দেওয়া হচ্ছে:

- ESET
- ট্রেন্ড মাইক্রো
- লুকআউট
- লুকআউট
- ভলেক্সিটি
- সিটিজেনস ল্যাব

ঝুঁকি হ্রাস

কেস স্টাডিতে উল্লিখিত হুমকাগুলোর বিরুদ্ধে প্রতিরক্ষা গড়তে নিচে দেওয়া সুপারিশগুলো গ্রহণ করার জন্য NCSC উৎসাহিত করছে।

- **অ্যাপ স্টোর পরিচালকদের—যাদের মধ্যে তৃতীয় পক্ষের অ্যাপ স্টোরও অন্তর্ভুক্ত—এবং অ্যাপ ডেভেলপারদের নিশ্চিত করতে হবে যে তাদের প্ল্যাটফর্মে থাকা অ্যাপগুলো নিরাপদ এবং সরকারি 'কোড অব প্র্যাকটিস'-এর সাথে সামঞ্জস্যপূর্ণ।** নির্দেশাবলী দেখুনঃ 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

- **বহু-ভাষায় সহায়তা:** অ্যাপ ডেভেলপারদের উইঘুর, তিব্বতি, তাইওয়ানিজ হোক্কিয়েন এবং ক্যান্টোনিজ সহ টার্গেট করা গোষ্ঠীর মধ্যে সংখ্যালঘু ভাষাভাষী ব্যবহারকারীদের জন্য জনপ্রিয় অ্যাপগুলিকে স্থানীয়করণের প্রচেষ্টায় বিনিয়োগ করা উচিত। অ্যাপগুলিতে স্থানীয়করণের জন্য অ্যাপলের নির্দেশিকা: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. অ্যাপ অনুবাদ করার বিষয়ে গুগলের নির্দেশিকা: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **আপনার সোশ্যাল মিডিয়া প্ল্যাটফর্মকে সুরক্ষিত রাখা:** সোশ্যাল মিডিয়া কোম্পানিগুলি সাইবার অপরাধীদের জন্য জাল অ্যাকাউন্ট তৈরি করা এবং তাদের প্ল্যাটফর্মে বৈধ অনলাইন সম্প্রদায়গুলিতে ক্ষতিকর ফাইল বা লিঙ্ক শেয়ার করা আরও কঠিন করে তুলতে পারে। যেখানে সম্ভব, হুমকি সম্পর্কে সম্মিলিত ধারণা উন্নত করতে এবং সুরক্ষা ব্যবস্থা গ্রহণে সহায়তা করার জন্য কোম্পানিগুলির উচিত বৃহত্তর শিল্পের সাথে ক্ষতিকর সূচকগুলি শেয়ার করা।

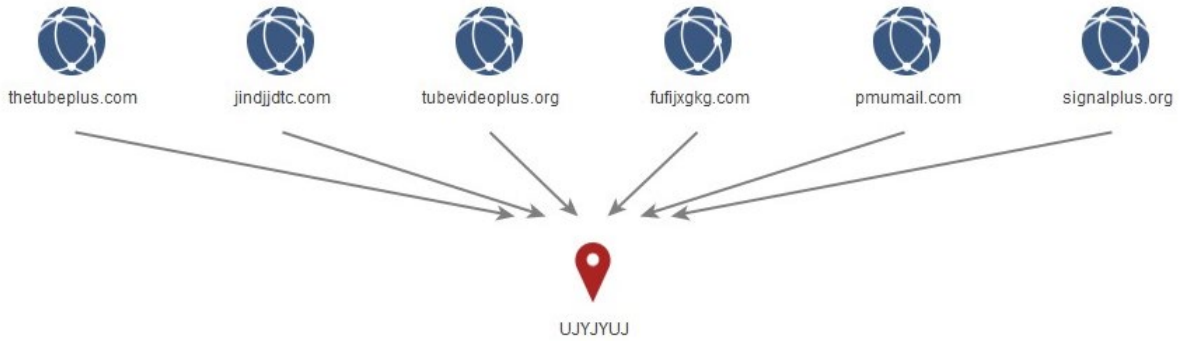
- **গ্রাহকদের জন্য প্রতিকার পরিকল্পনা:** সংস্থাগুলির এমন পদ্ধতি থাকা উচিত যাতে গ্রাহকরা তাদের পরিষেবা ব্যবহার করে ক্ষতিকারক অ্যাপ ইনস্টল করেছেন তা অবহিত করা যায়। এই সতর্কতাগুলি মনোযোগ আকর্ষণকারী এবং তথ্যবহুল হওয়া উচিত। যেখানে প্রযোজ্য, সেখানে প্রতিষ্ঠানগুলোর উচিত সফটওয়্যারটি কীভাবে সরাতে হবে সে বিষয়ে দিকনির্দেশনা প্রদান করা এবং ভুক্তভোগীদের যথাযথ কর্তৃপক্ষের—যেমন যুক্তরাজ্যে NCSC—কাছে রিপোর্ট করার জন্য উৎসাহ দেওয়া।
  আরও তথ্যের জন্য অ্যাপ স্টোর কোড অব প্র্যাকটিস দেখুন: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **সহযোগিতার জন্য কর্মী গোষ্ঠী:** সোশ্যাল মিডিয়া কোম্পানিগুলি তাদের নিজ নিজ নিরাপত্তা দলগুলিকে ক্ষতিকারক সূচক, TTP এবং পর্যবেক্ষণ শেয়ার করার অনুমতি দিয়ে ওয়ার্কিং গ্রুপ গঠন করতে পারে, যা সাইবার অপরাধীদের জন্য তাদের প্ল্যাটফর্মগুলিকে সাইবার হামলার জন্য ব্যবহার করা আরও কঠিন করে তোলে।

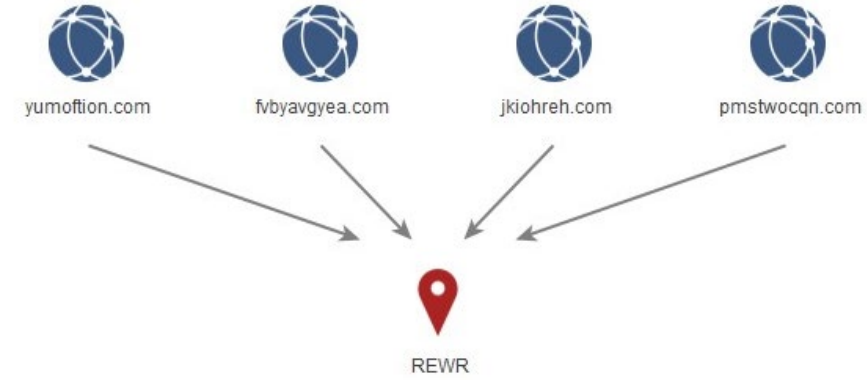
- **পরিবর্তিত অ্যাপ সনাক্তকরণ:** যেখানে সম্ভব, অ্যাপ ডেভেলপারদের এমন কার্যকারিতা অন্তর্ভুক্ত করা উচিত যা ব্যবহারকারীকে অবহিত করে যে তারা কোনও অ্যাপের 'অনানুষ্ঠানিক' সংস্করণ ডাউনলোড করেছে কিনা, যাতে তারা ক্ষতিকারক অ্যাপ থেকে নিজেদের রক্ষা করতে পারে।

পরিশিষ্ট A: BADBAZAAR WHOIS ক্লাস্টারিং / ডোমেইন ব্রোকার তথ্যের গ্রাফ

ছবি 1 - 'UKYJYUJ'

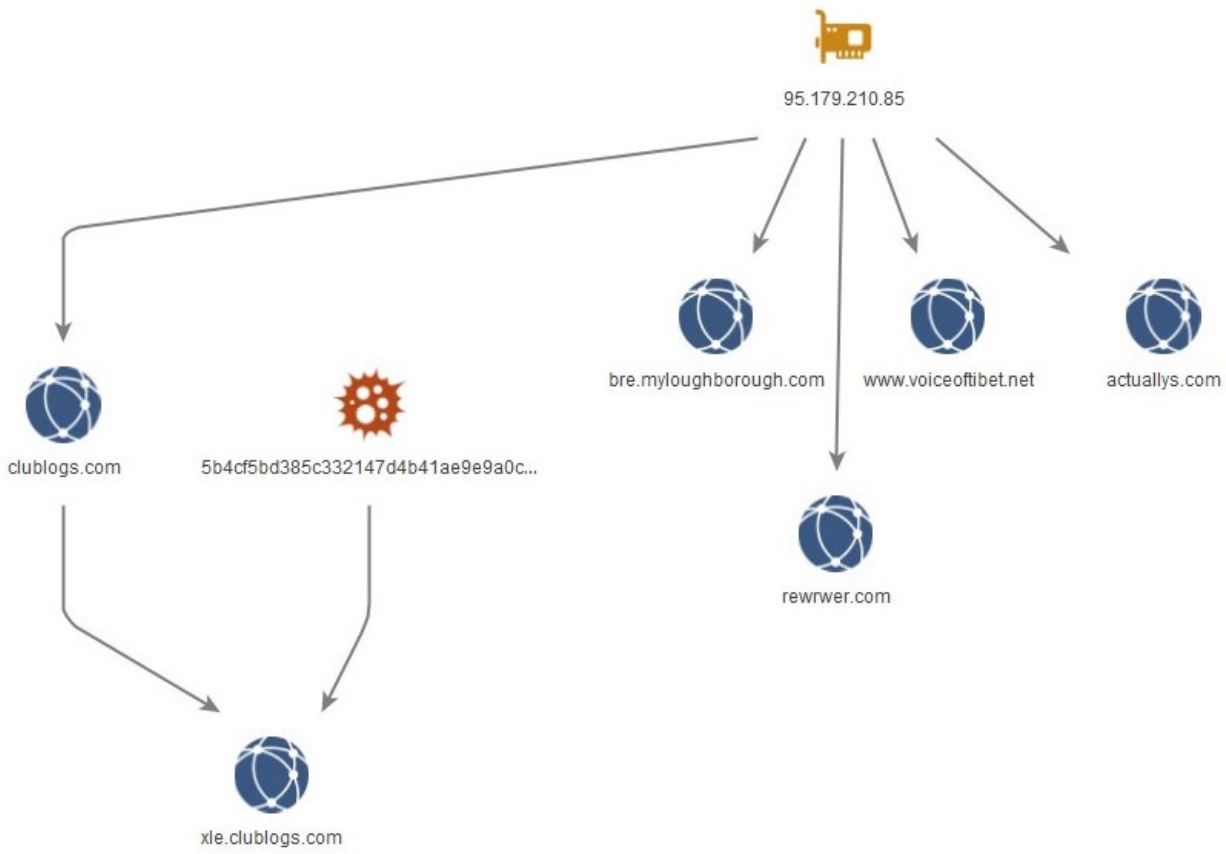


ছবি 2 – কীবোর্ড ওয়াকিং মান

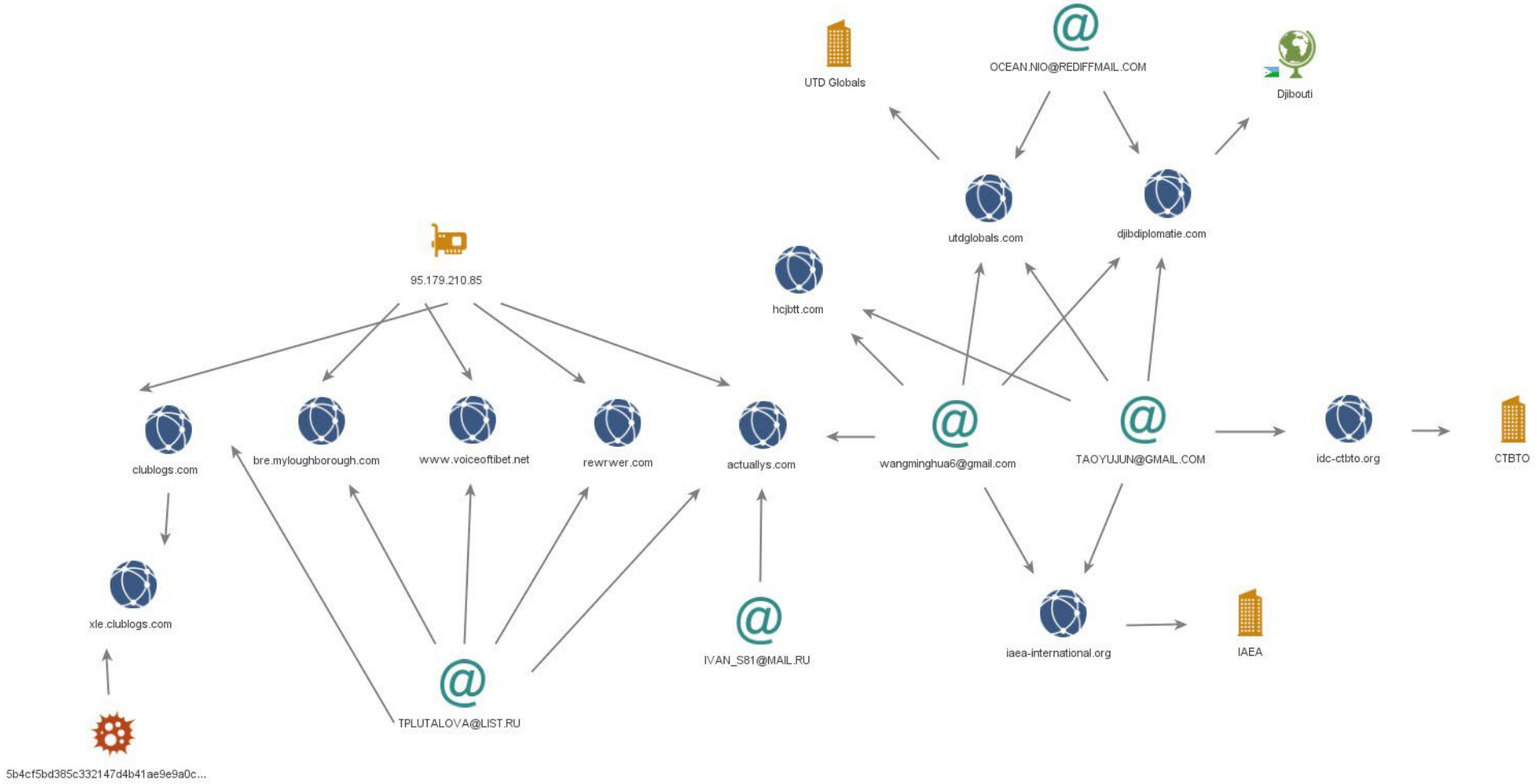


ছবি 3 – 'FSDF' স্টেট ফিল্ড মান সহ অতিরিক্ত ডোমেইন

ছবি 4 – 95.179.210[.]85

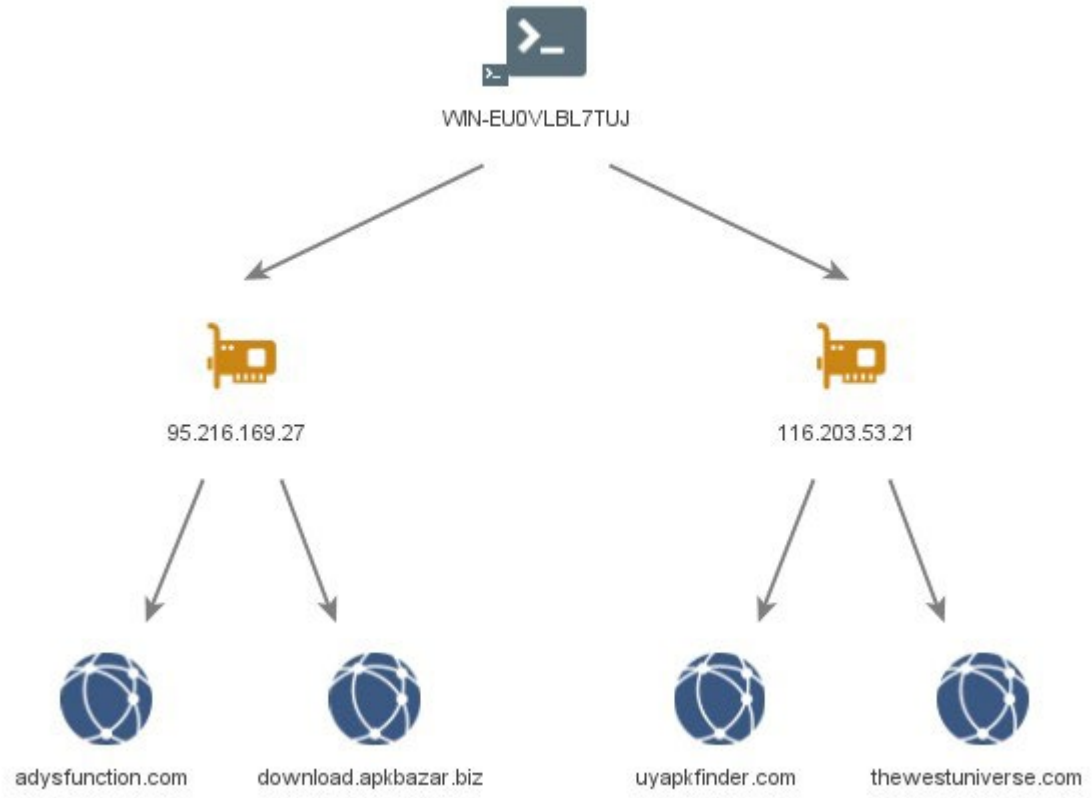


ছবি 5 – WHOIS লিঙ্ক

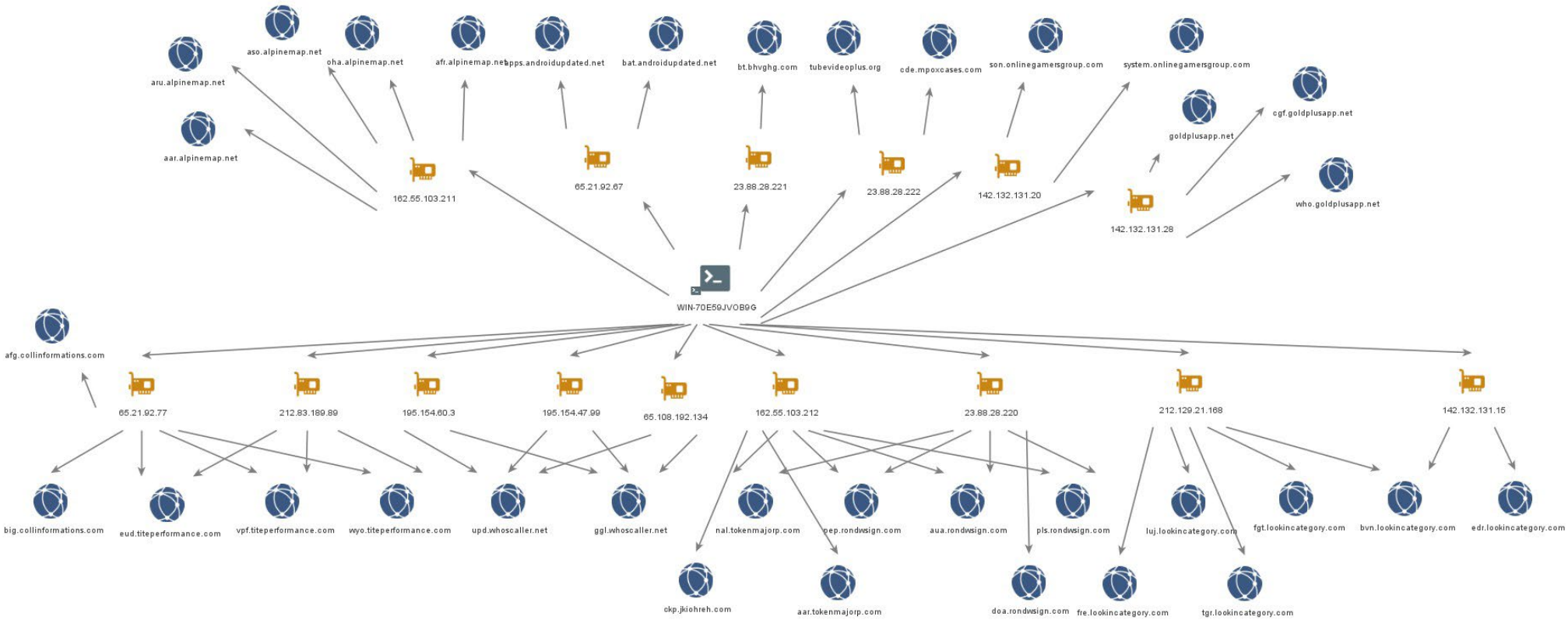


পৃষ্ঠা 33 এর মধ্যে 34

ছবি 6 – WIN-EU0VLBL7TUJ

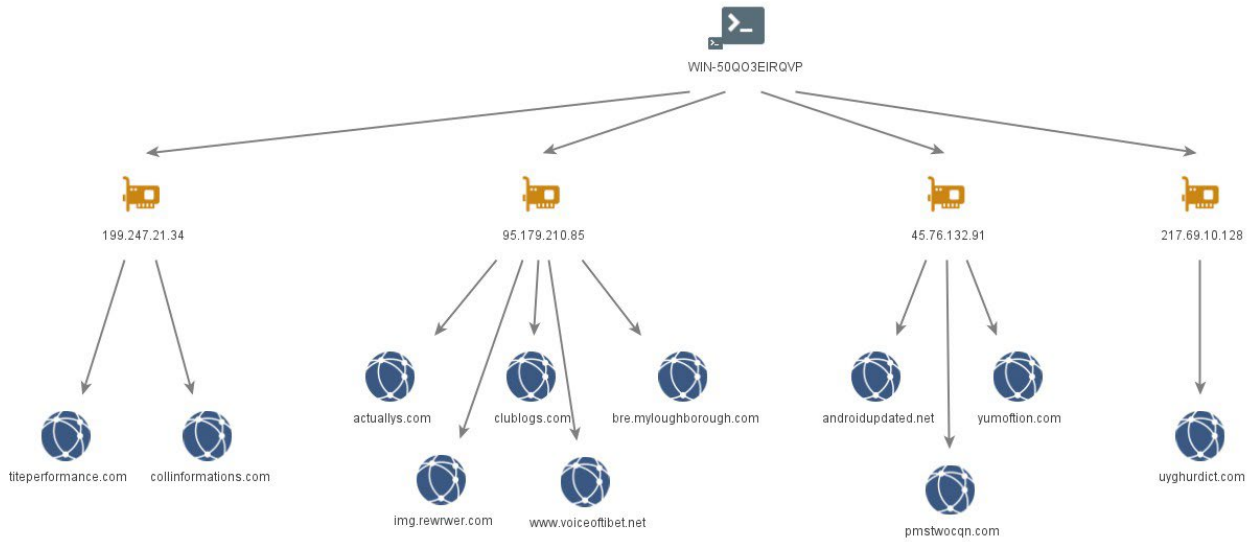


ছবি 7 – WIN-70E59JVOB9G

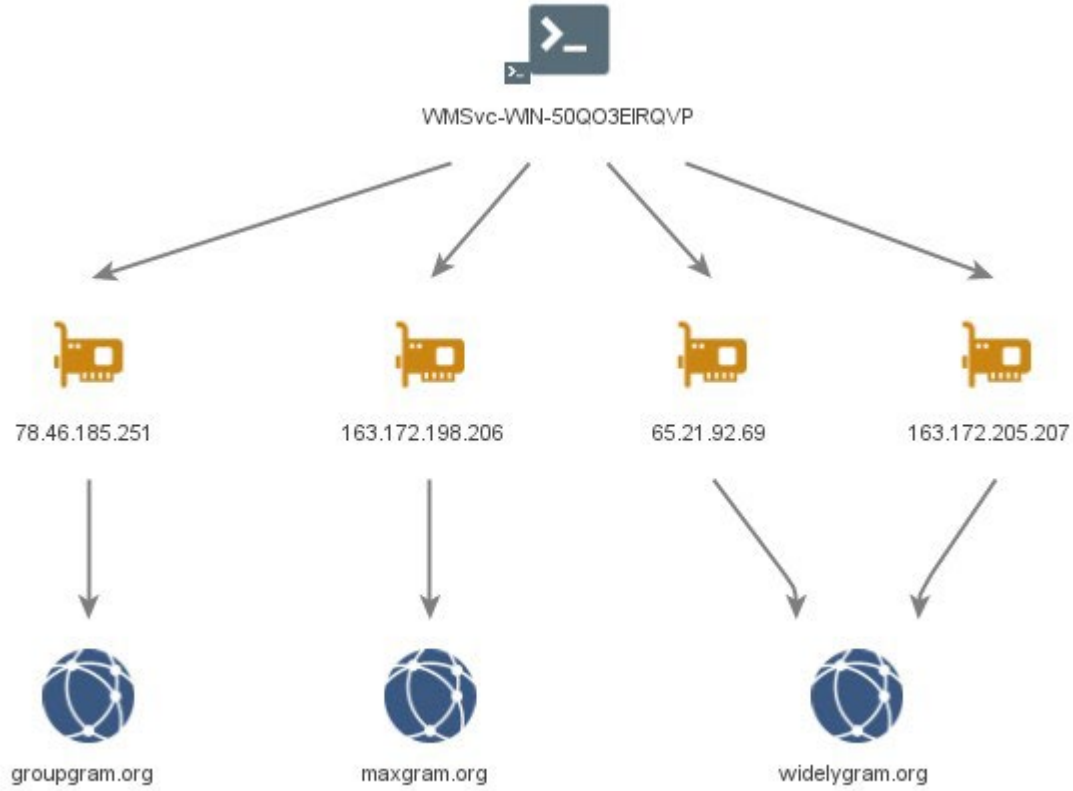


পৃষ্ঠা 35 এর মধ্যে 36

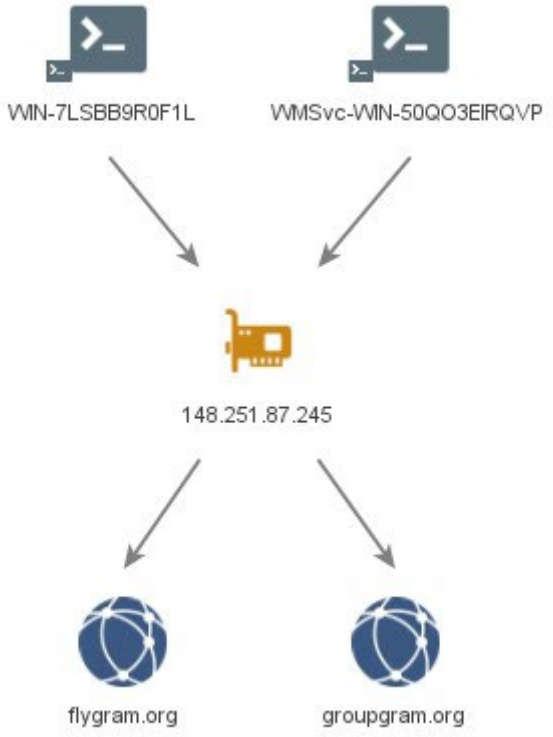
ছবি 8 - WIN-50QO3EIRQVP



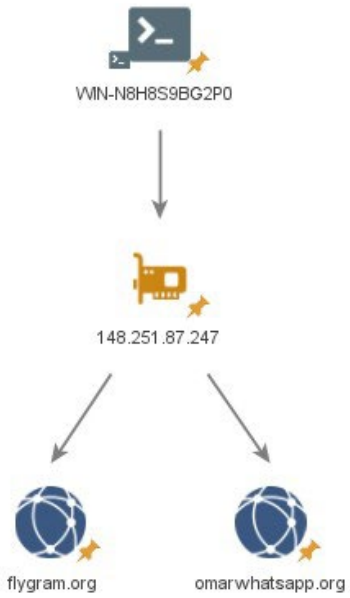
ছবি 9 - VMSvc-WIN-50QO3EIRQVP



ছবি 10 – VMSvc-WIN-50QO3EIRQVP এবং WIN-7LSBB9R0F1L



ছবি 11 - WIN-N8H8S9BG2P0



ছবি 12 – WIN-I6VBN8MR92A

পরিশিষ্ট B: MOONSHINE এবং BADBAZAAR নমুনা পর্যবেক্ষণ করা হয়েছে

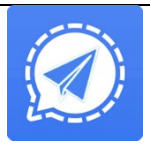
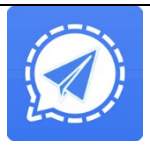
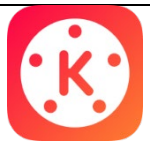
নীচের সারণীতে গত দুই বছরে MOONSHINE এবং BADBAZAAR প্রচারণায় ব্যবহৃত অ্যাপগুলির তালিকা দেওয়া হয়েছে।

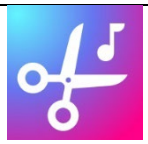
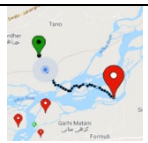
এই অ্যাপগুলির অনেকগুলিই দেখতে প্রতিষ্ঠিত অ্যাপের মতো। এটি সম্ভবত সুপরিচিত ব্র্যান্ডগুলিকে 'নকল' করার জন্য একটি ইচ্ছাকৃত কৌশল।

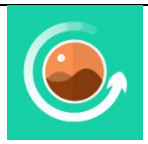
এটি মনে রাখা গুরুত্বপূর্ণ যে অ্যাপের নাম, প্যাকেজের নাম বা আইকন—এই তিনটি জিনিসই আসল অ্যাপের মতো দেখাতে পারে, তাই শুধু এগুলো দেখে বোঝা যাবে না যে ডিভাইসটি আক্রান্ত হয়েছে কি না।

অ্যাপের নাম	প্যাকেজ নাম	অ্যাপ আইকন
আল্লাহর ৯৯টি নাম	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
অ্যাডোবি অ্যাক্রোব্যাট	com.adobe.reader	
অ্যালপাইন(پښتو)	psyberia.pa.full	
অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার	psyberia.alpinequest.full	
অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার	psyberia.alpinequest.full	
অ্যালপাইন কোয়েস্ট অফ-রোড এক্সপ্লোরার (লাইট)	psyberia.alpinequest.free	

AppLock	com.alpha.applock	
অ্যারাবিক কিবোর্ড	com.arabic.keyboard.arabic.language.keyboard.app	
অডিও ভিডিও ক্লাটার	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
বাদাম维语输入法	com.ziipin.softkeyboard	
বৌদ্ধ সংগীত (1)	com.bigkidsapps.buddhistsongs1	
ক্যালকুলেটর	com.android2.calculator3	
কম্পাস ৩৬০ প্রো	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	

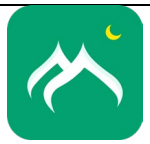
ফাইল ম্যানেজার +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
ফ্রি ওয়াইফাই পাস	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
হেফজ কোরআন	com.golap.hefzquran	
হিজরি ক্যালেন্ডার	com.ibrahim.hijricalendar	
ইনশট	com.camerasideas.instashot	
KMপ্লেয়ার	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	

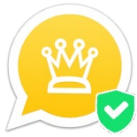
কাটার এবং রিংটোন মেকার	ringtone.maker.mp3.cutter.audio	
ম্যালক	com.mallocprivacy.antistalkerfree	
ম্যাপ ডিসটেন্স ক্যালকুলেটর	com.routemap.mapdownload.gpsrouteplanner	
মিডিয়া রিকোভারি	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
নুর输入法	com.nur.ime	
OGহোয়াটসঅ্যাপ	com.gbwhatsapp3	
PDF এক্সট্রা	com.mobisystems.mobiscanner	
PDF রিডার	pdf.pdfreader.pdfviewer.pdfeditor	
PDF রিডার	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo এডিটর	com.iudesk.android.photo.editor	

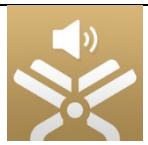
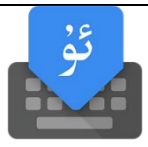
ফটো রিকভারি	recover.restore.undelete.photo.video.file	
ফটো স্টুডিও	com.kvadgroup.photostudio	
প্লাস	org.telegram.pluspro	
প্রেয়ার বুক	com.arashpayan.prayerbook	
কোয়ার্কVPN	com.speedy.vpn	
কোরআন	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
মুছে যাওয়া ছবি আবার ফিরিয়ে আনুন	com.restore.deleted.pictures.video	
সিগন্যাল	org.thoughtcrime.securesms	
সিগন্যাল প্লাস	org.thoughtcrime.securesmsplus	
সিগন্যাল প্লাস	org.thoughtcrime.securesmsplus	

সিগন্যাল বোল সাউন্ডস HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
স্কাইপ	com.skype.raider	
স্ন্যাপটিউব	com.snaptube.premium	
স্ন্যাপটিউব প্লাস	com.snaptube.gold	
সুইফটকি কিবোর্ড	com.touchtype.swiftkey	
টারটীল	com.mmmoussa.iqra	
টেলিগ্রাম	org.zhifeijihj.messenger	
টেলিগ্রাম	org.telegramfbo.messenger	
টেলিগ্রাম X	org.thunderdog.challegram	
তিবেতান ডিভাইনেশন সিস্টেম MO	net.rhombapp.mo	
তিবেতান প্রেয়ার	com.chorig.tibetanprayer	

ট্রান্সলেটর AR-TR	free_translator.artr	
ট্রুকলার	com.truecaller	
টিউবপ্লাস	com.techshop.videocraft	
আলট্রাসার্ফ	us.ultrasurf.mobile.ultrasurf	
উইগুর কিবোর্ড	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
উইগুরচি কিরগুজগুচ	com.ziipin.softkeyboard	
ভিডিও কনভার্টার	com.inverseai.video_converter	
ভিডিও ক্লাটার	com.naing.cutter	
ভিডিও ডাউনলোডার	downloader.video.download.free	
ভিডিও মেকার	com.bstech.slideshow.videomaker	
অ্যান্ডয়েড এর জন্য ভিডিও প্লেয়ার	com.zgz.supervideo	

ভিয়েকা	com.prime.story.android	
ভিভাভিডিও লাইট	com.quvideo.vivavideo.lite	
ভিভাভিডিও প্রো	com.quvideo.xiaoying.pro	
ভিমুসলিম	com.alhiwar	
ভিডিও রেকর্ডার	com.media.bestrecorder.audiorecorder	
ভক্সার	com.rebelvox.voxer	
আবহাওয়ার পূর্বাভাষ	com.graph.weather.forecast.channel	
হোয়াটসঅ্যাপ	com.whatsapp	
হোয়াটসঅ্যাপ	com.whatsapp	
হোয়াটসঅ্যাপ	com.WhatsApp3Plus	

হোয়াটসঅ্যাপ	com.whatsapp	
হোয়াটসঅ্যাপ	com.WhatsApp2Plus	
হুজকল	gogolook.callgogolook2	
ওয়াইফাই পাসওয়ার্ড মাস্টার_ v1.4	com.example.dat.a8andoserverx	
উইন্ডি	com.windyty.android	
ওয়াইজ	com.transferwise.android	
ইওহোয়াটসঅ্যাপ	com.yowhatsapp	
ইউটিউব ডাউনলোডার	dentex.youtube.downloader	
জম	im.zom.messenger	
আইকোরআন লাইট	com.guidedways.iQuran	

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

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

আরও পড়ুন

অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টারের নির্দেশিকা

- সাইবার অপরাধ, ঘটনা বা ঝুঁকি রিপোর্ট করুন
- আপনার ডিভাইসগুলি কীভাবে সুরক্ষিত করবেন
- আপনার মোবাইল ফোন সুরক্ষিত করুন
- ফিশিং
- স্ক্যাম
- আপনার সোশ্যাল মিডিয়া সুরক্ষিত করুন
- সোশ্যাল মিডিয়া এবং মেসেজিং অ্যাপের জন্য নিরাপত্তা টিপস

যুক্তরাজ্যের NCSC এবং NPSA এর নির্দেশিকা

- গণতন্ত্র রক্ষা
- সামাজিক মাধ্যম: কীভাবে এটি নিরাপদে ব্যবহার করবেন
- সংস্থাগুলির জন্য মোবাইল সহ ডিভাইস সুরক্ষা নির্দেশিকা
- অ্যাপ্লিকেশন স্টোরগুলিতে হুমকি রিপোর্ট করুন।
- যাদের ঝুঁকি বেশি তাদের জন্য ব্যক্তিগত নিরাপত্তা ও সুরক্ষা

যুক্তরাষ্ট্র NSA এর নির্দেশিকা

- মোবাইল ডিভাইসের সর্বোত্তম ব্যবহার

দাবিত্যাগ

অনুগ্রহ করে মনে রাখবেন যে এই নির্দেশিকাটি এমন তথ্য প্রদান করে যা প্রকাশের সময় যাচাই করা হয়েছে।

এই প্রতিবেদনটি প্রতিবেদন প্রদানকারী সংস্থা এবং শিল্প উৎস থেকে প্রাপ্ত তথ্যের উপর ভিত্তি করে তৈরি। যে তথ্য ও পরামর্শ দেওয়া হয়েছে, তা সব ধরনের ঝুঁকি এড়ানোর জন্য নয়—এবং এসব পরামর্শ মেনে চললেও সব ঝুঁকি পুরোপুরি দূর হবে না। তথ্য-সম্পর্কিত ঝুঁকির দায়িত্ব সব সময় সংশ্লিষ্ট সিস্টেম মালিকের উপরেই থাকে।

যুক্তরাজ্যে এই তথ্য ফ্রিডম অব ইনফরমেশন অ্যাক্ট 2000 (FOIA) এর আওতায় অব্যাহতিপ্রাপ্ত এবং যুক্তরাজ্যের অন্যান্য কিছু তথ্য সম্পর্কিত আইনের আওতায় অব্যাহতিপ্রাপ্ত হতে পারে।

যেকোনো FOIA সম্পর্কিত প্রশ্ন ncscinfoleg@ncsc.gov.uk ঠিকানায় পাঠান।