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

परामर्श-सूचना

BADBAZAAR और MOONSHINE तकनीकी विश्लेषण और मिटिगेशन्स

9 अप्रैल 2025

BADBAZAAR और MOONSHINE तकनीकी विश्लेषण और मिटिगेशन्स

सारांश

यूके साइबर लीग के समर्थन से यह परामर्श-सूचना राष्ट्रीय साइबर सुरक्षा केंद्र (एनसीएससी यूके) और निम्नलिखित अंतर्राष्ट्रीय भागीदारों द्वारा संयुक्त रूप से तैयार की गई है:

- **ऑस्ट्रेलियन साइबर सिक्योरिटी सेंटर (एसीएससी), जो ऑस्ट्रेलियन सिग्नल्स डायरेक्टोरेट का हिस्सा है**
- **कैनेडियन सेंटर फॉर साइबर सिक्योरिटी, जो संचार सुरक्षा प्रतिष्ठान का हिस्सा है**
- **जर्मन संघीय खुफिया सेवा**
- **जर्मन संविधान संरक्षण संघीय कार्यालय**
- **न्यू ज़ीलैंड नैशनल साइबर सिक्योरिटी सेंटर, जो सरकारी संचार सुरक्षा ब्यूरो का हिस्सा है**
- **संयुक्त राज्य अमेरिका फेडरल ब्यूरो ऑफ इन्वेस्टिगेशन**
- **संयुक्त राज्य अमेरिका नैशनल सिक्योरिटी एजेंसी**

यह परामर्श-सूचना BADBAZAAR और MOONSHINE के नाम से जाने जाने वाले स्पाइवेयर के दो प्रकारों पर नए और एकत्रित खतरे के बारे में खुफिया जानकारी प्रदान करती है, और इसमें ऐप स्टोर ऑपरेटर्स, डेवलपर्स और सोशल मीडिया कंपनियों को अपने उपयोगकर्ताओं को सुरक्षित रखने में सहायता देने के लिए परामर्श-सूचना शामिल है।

यह परामर्श-सूचना इन मैलवेयर द्वारा लक्षित लोगों के लिए एक परामर्श-सूचना के समानांतर प्रकाशित की जा रही है।

यह दस्तावेज़ एनसीएससी शब्दावली के अनुसार स्पाइवेयर की परिभाषा का उपयोग करता है: "उपयोगकर्ता की सहमति के बिना डिवाइस पर इंस्टॉल होने वाले मैलवेयर का एक प्रकार, जो डेटा एकत्र करता है और फिर इसे किसी तीसरे पक्ष को भेजता है।"

मामला अध्ययन एक: MOONSHINE

MOONSHINE एक एंड्रॉयड स्पाइवेयर है जिसके बारे में 2019 में सिटीज़न लैब द्वारा तिब्बती समूहों को लक्षित करने के रूप में रिपोर्ट की गई थी। MOONSHINE इंस्टॉल किए जाने के उद्देश्य से शिकारों को लुभाने के लिए इसे एक वैध ऐप के रूप में पेश करती है। इसे टेलीग्राम चैनलों और व्हॉट्सएप से भेजे गए लिंक्स के माध्यम से साझा किया गया है।

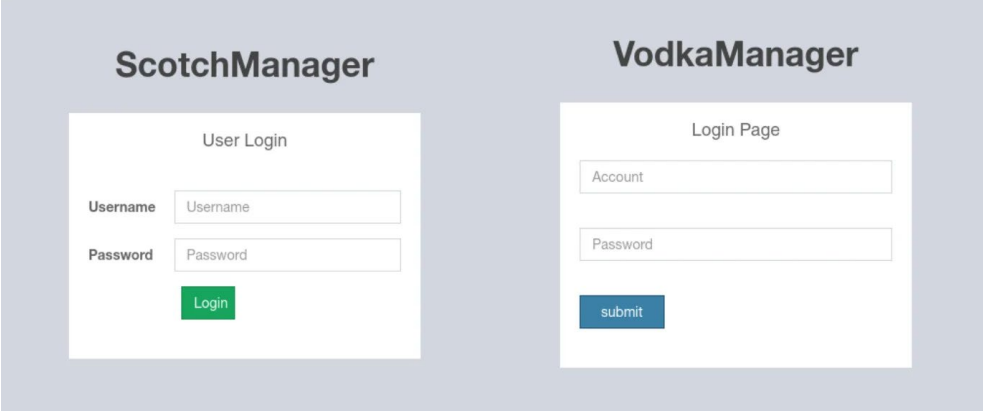
एनसीएससी का अनुसंधान MOONSHINE के बारे में निम्नलिखित इंगित करता है:

- MOONSHINE एक मैनेजमेंट इंटरफेस का उपयोग करता है, जिसमें पहली बार रिपोर्ट किए जाने के बाद से परिवर्तन हुए हैं।
- मैनेजमेंट इंटरफेस व्यापक निगरानी क्षमताओं को प्रकट करता है, जिसमें डिवाइसेज़ से फाइलों को निकालने के साथ-साथ लाइव ऑडियो और स्क्रीन रिकॉर्डिंग्स को कैप्चर करने की क्षमता भी शामिल है।
- वर्चुअल तरीके से होस्ट किए गए MOONSHINE मैंजमेंट इंटरफेसेज़ का एक सेट पाया गया है। इन इंटरफेसेज़ में यूपीएसईसी से जुड़े लॉगिन पैनल के साथ इंफ्रास्ट्रक्चर का ओवरलैप है, जिसका संदर्भ इंटेलिजेंस ऑनलाइन के अनुसार 'सिचुआन डाएन्क नेटवर्क सिक्योरिटी टेक्नोलॉजी को. लि.' से है।

मैनेजमेंट इंटरफेस

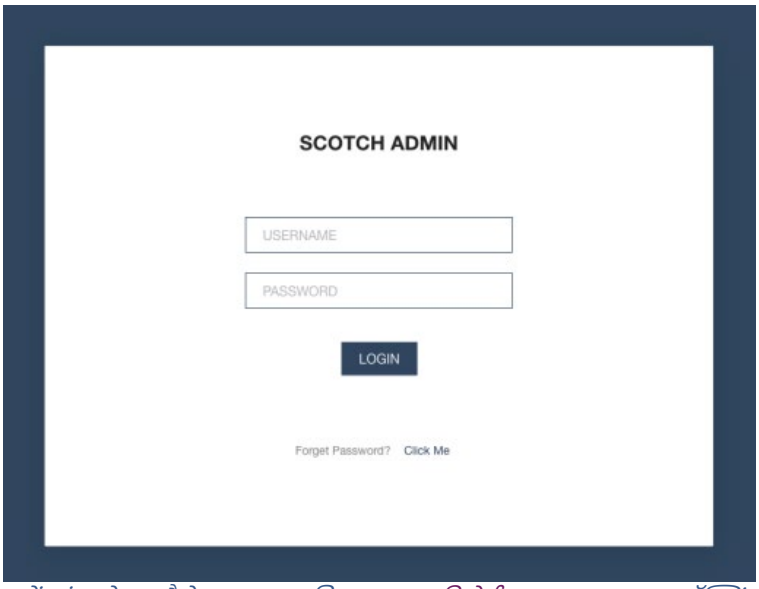
MOONSHINE मैनेजमेंट इंटरफेस की पिछली रिपोर्टिंग इंगित करती है कि इसमें बदलाव हुए हैं, जो लगातार रूप से किए जा रहे विकास का सुझाव देता है।

इस मैनेजमेंट इंटरफेस का सबसे पहला उदाहरण सिटिज़न लैब की 2019 रिपोर्टिंग में देखने को मिलता है।



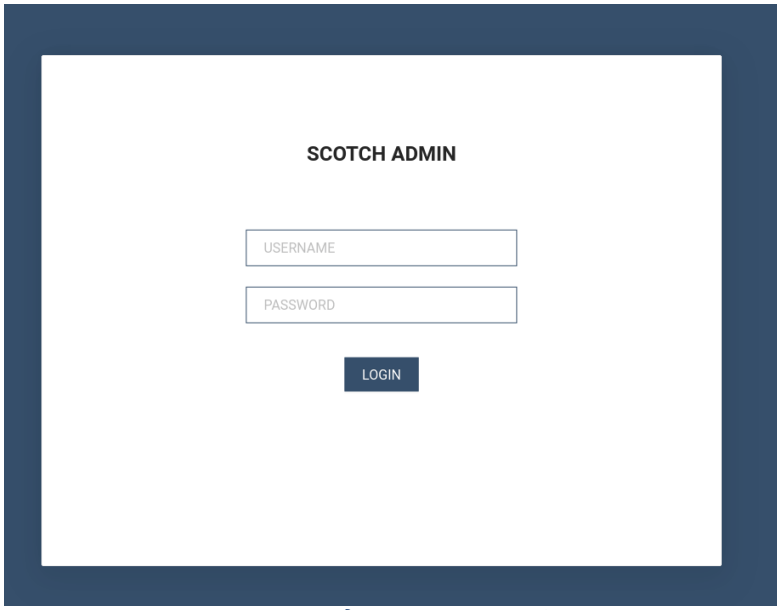
चित्र 1: MOONSHINE मैनेजमेंट इंटरफेसेज़, जिन्हें सिटीजन लैब की 2019 रिपोर्ट 'मिसिंग लिंक तिब्बतेन ग्रुप्स टार्गेट विद 1-क्लिक मोबाइल एक्सप्लॉइट्स' में देखा गया है।

2022 की शुरुआत में Lookout ने एक अलग मैनेजमेंट इंटरफेस की सूचना दी, जिसे निम्नानुसार दिखने के लिए फिर से डिज़ाइन किया गया था (चित्र 1 में पूर्व इंटरफेसेज़ के स्थान पर):



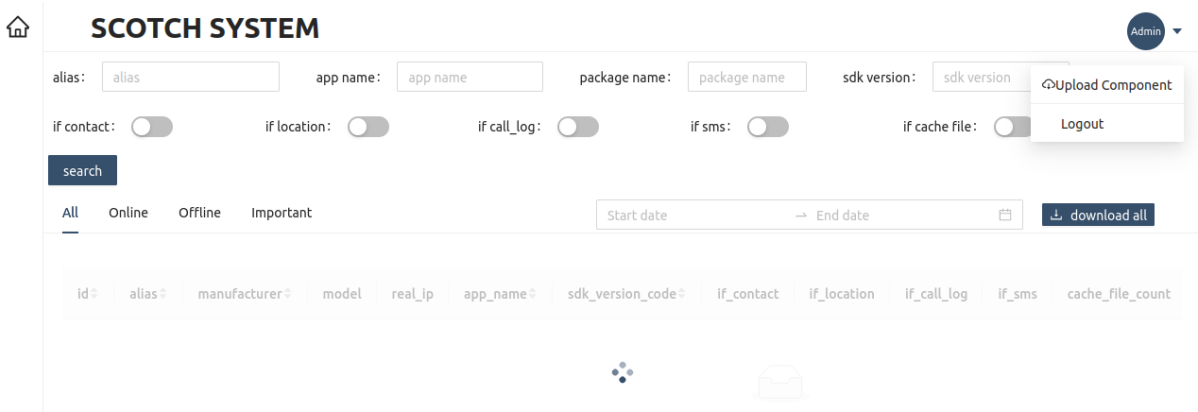
चित्र 2: MOONSHINE मैनेजमेंट इंटरफेस, जैसे Lookout की यह 2022 रिपोर्ट 'MOONSHINE: इवॉल्विंग एंड्रॉयड सर्विलांसवेयर बाय चाइनीज़ एपीटी पॉइज़न कार्प टु टार्गेट टिबटेन्स एंड उइगर्स' में देखा गया है।

अगस्त 2023 में, MOONSHINE कमान और नियंत्रण (C2) के एक स्कैन ने 2022 इंटरफेस के समान एक अन्य इंटरफेस का खुलासा किया, जिसमें अब 'फॉर्गेट पासवर्ड' फंक्शन उपलब्ध नहीं है, जैसेकि चित्र 2 में दिखाया गया है:



चित्र 3: अगस्त 2023 में देखा गया MOONSHINE मैनेजमेंट इंटरफेस, जिसमें अब 'फॉर्गेट पासवर्ड' प्रॉम्प्ट नहीं है।

मैनेजमेंट इंटरफेस की आगे की जांच में पैनल के अंदर सामग्री दिखाई दी, जिससे पता चला कि भंग किए गए डिवाइसेज़ का विवरण कैसे स्टोर किया जाएगा।



चित्र 4: MOONSHINE मैनेजमेंट इंटरफेस के लॉगिन पृष्ठ के पीछे वेबपेज।

Lookout के अनुसंधान ने लक्षित व्यक्ति के डिवाइस से MOONSHINE के C2 सर्वर्स तक एक **'स्कोर'** भेजा जाना प्रदर्शित किया। इस 'स्कोर' का वैल्यू लक्षित व्यक्ति के डिवाइस पर दुर्भावनापूर्ण नमूने की पर्मिशन्स पर आधारित है।

पेज के अंदर के कॉलम 'if_contact', 'if_location', 'if_call_log' और 'if_sms' यह सुझाव देते हैं कि MOONSHINE के सभी नमूनों के पास भंग किए गए डिवाइसेज़ की संपूर्ण एक्सेस नहीं है। इन कॉलम्स का खुलासा व डिवाइस से C2 को भेजे गए 'स्कोर' से पता चलता है कि जो व्यक्ति-विशेष मैनेजमेंट इंटरफेस को एक्सेस रहे हैं, हमलावर उन व्यक्ति-विशेषों के स्कोर के उपयोग से भंग किए गए डिवाइस में मैलवेयर की एक्सेस का स्तर संचरित कर रहे हैं।

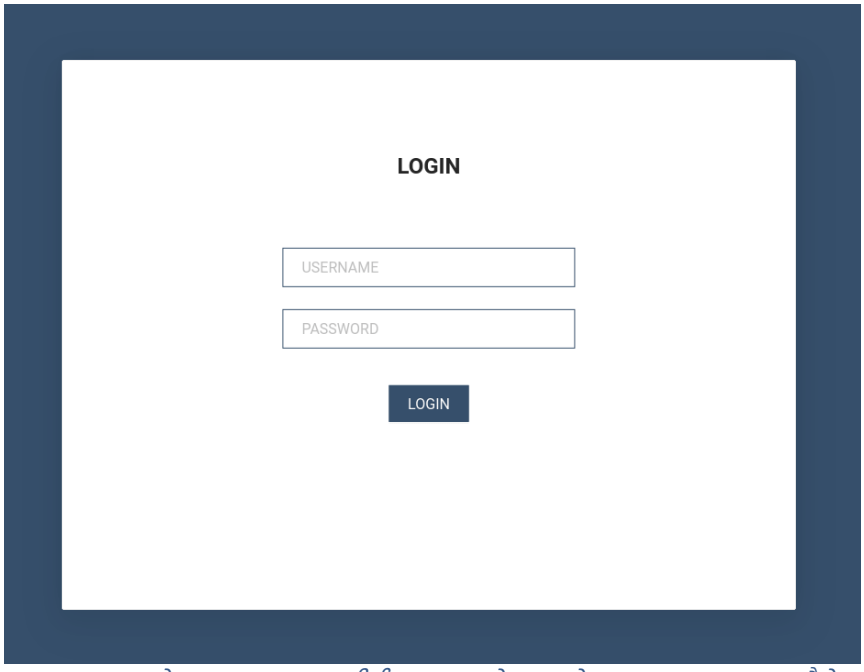
आम तौर पर ऐप्स द्वारा डिवाइसेज़ से जानकारी एकत्र किए जाने की रोकथाम के लिए सर्वोत्तम कार्यप्रथा सलाह यह है कि ऐप को डाउनलोड करने से पहले किसी भी असामान्य बात के लिए ऐप की पर्मिशन्स का निरीक्षण किया जाए। चूंकि MOONSHINE के नमूने ऐप की फंक्शनैलिटी के लिए प्रासंगिक पर्मिशन्स की तलाश करते हैं, इसलिए वे असंदिग्ध दिखाई दे सकते हैं, लेकिन वे इन पर्मिशन्स का उपयोग करके डिवाइसेज़ से जानकारी भी एकत्र करते हैं।

MOONSHINE में एक एप्लिकेशन प्रोग्रामिंग इंटरफेस (एपीआई) भी है, जो इसकी क्षमताओं की व्यापकता का खुलासा करता है। एपीआई प्रलेखन के शुरुआती संस्करणों में मंदारिन में एपीआई नेम्स शामिल थे।

वर्चुअल होस्ट्स

MOONSHINE पैनलों की खोजों में वर्चुअली होस्ट किए गए इंस्टैंसेज़ पाए गए। जब एक आईपी एड्रेस साथ में कई वेबसाइटों को होस्ट कर सकता है, तो यह वर्चुअल होस्टिंग होती है। इन वर्चुअली होस्ट किए गए इंस्टैंसेज़ के आईपी एड्रेसेज़ और होस्ट किए गए डोमेन्स को किसी भी ज्ञात मैलवेयर नमूनों में नहीं देखा गया था।

मैनेजमेंट इंटरफेस के ये इंस्टैंसेज़ अलग-अलग थे, क्योंकि पेजों का शीर्षक पहले देखे गए '**SCOTCH ADMIN**' के बजाय '**LOGIN**' था।



चित्र 5: 'SCOTCH ADMIN' के बजाय 'LOGIN' शीर्षक का उपयोग करने वाला MOONSHINE मैनेजमेंट इंटरफेस।

इसके अलावा, पैनल में शामिल सामग्री भी चित्र 4 से अलग है, जैसा कि चित्र 6 में प्रदर्शित है:

चित्र *6:* वर्चुअली होस्ट किए गए *MOONSHINE* मैनेजमेंट इंटरफेस के लॉगिन पृष्ठ के पीछे वेबपेज।

चित्र 4 में दिखाए गए पैनल की तुलना में चित्र 6 में प्रदर्शित पैनल एक स्ट्रिप्ड-डाउन संस्करण प्रतीत होता है। पैनलों में ओवरलैप करने वाली विशेषताएं हैं – तालिका में कॉलम्स के नाम 'id', 'manufacturer' और 'model'।

वर्चुअली होस्ट किए गए MOONSHINE इंस्टैंसेज़, जिन्हें पाया गया था, वे हैं:

डोमेन	आईपी एड्रेस
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

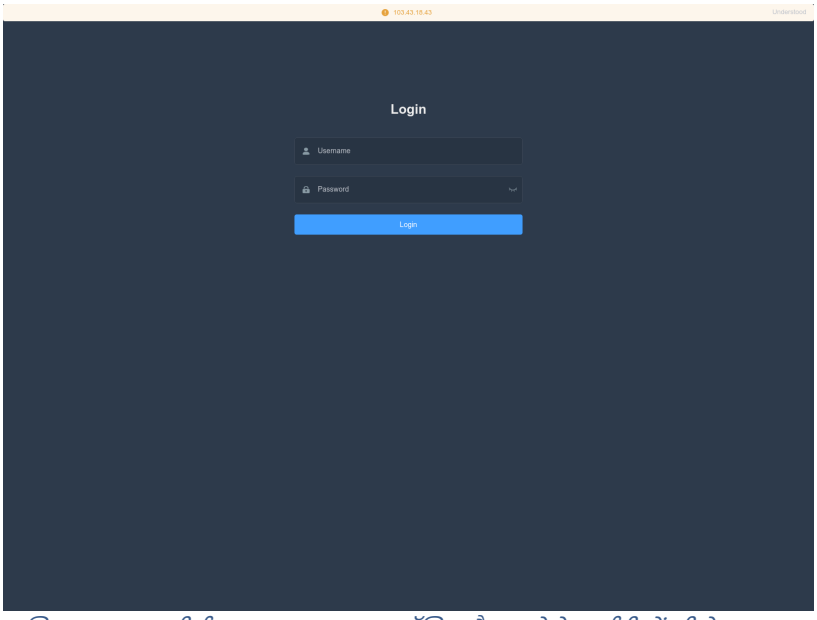
इन डोमेन्स को ट्रेंड माइक्रो द्वारा MOONSHINE एक्सप्लॉयट किट्स के रूप में सूचीबद्ध किया गया है, जो मोबाइल डिवाइसेज़ पर मैलवेयर इंस्टॉल करने के लिए ब्राउज़र की कमजोरियों का फायदा उठाने के लिए जिम्मेदार है। ट्रेंड माइक्रो ने इस मैलवेयर को 'डार्क निंबस' नाम दिया है।

स्पष्टीकरण के लिए, MOONSHINE मैनेजमेंट इंटरफेसेज़ वे होते हैं जो MOONSHINE मैलवेयर नमूने के साथ संचार करते हैं और जिनके पास लक्षित व्यक्ति के डेटा को बाहर निकाला जाता है। ट्रेंड माइक्रो द्वारा रिपोर्ट किए गए MOONSHINE एक्सप्लॉयट किट्स एक अलग क्षमता होते हैं, जो मोबाइल डिवाइसेज़ पर डार्क निंबस नाम के मैलवेयर को इंस्टॉल करने के लिए ब्राउज़र की कमजोरियों का फायदा उठाते हैं। इसके अलावा, डार्क निंबस व MOONSHINE पूरी तरह से अलग-अलग मैलवेयर हैं।

MOONSHINE मैनेजमेंट इंटरफेस और MOONSHINE एक्सप्लॉयट किट्स, इन दोनों के बीच कोड ओवरलैप होता है इसलिए चित्र 3 और 5 में लॉगिन प्रॉम्प्ट्स और साथ ही चित्र 4 और 6 में पेज की सामग्री भी एक-समान है। इन दोनों के सोर्स कोड में 'webpackJsonpreact-scotchui' स्ट्रिंग भी शामिल है।

हमलावरों ने यूआरएल लिंक जेनरेट किए जो MOONSHINE एक्सप्लॉयटेशन किट से कनेक्ट करके फिर तिब्बतियों और उइगरों से संबंधित वीडियो पर रिडायरेक्ट हो गए। यह MOONSHINE के लक्ष्यीकरण के साथ ओवरलैप में है।

MOONSHINE एक्सप्लॉयट किट डोमेन को होस्ट करने वाले कई आईपी एड्रेसेज़ में पोर्ट 444 पर 'VLiteUI' शीर्षक का एक लॉगिन पेज है। इस पेज को व्यापक रूप से नहीं देखा गया है और इन आईपी पर इसकी उपस्थिति हमलावरों के परिचालन के लिए एक संभावित लिंक की ओर इंगित करती है।



चित्र 7: HTML शीर्षक 'VLiteUI' वाला लॉगिन पैनल ऐसे आईपी में भी देखा गया, जो MOONSHINE एक्सप्लॉयट किट्स को होस्ट कर रहे थे।

ट्रेंड माइक्रो द्वारा डार्क निंबस के विश्लेषण से पता चला कि यह मैलवेयर डिवाइस में मौजूद विस्तृत जानकारी एकत्र कर सकता है, और यह एक्सएमपीपी प्रोटोकॉल का उपयोग करके C2 के साथ संचार करता है।

ट्रेंड माइक्रो इस बात को रेखांकित भी करता है कि डार्क निंबस के कुछ संस्करणों में उन्होंने 'डीकेएनएस' स्ट्रिंग की व्यापक पहचान की।

'**ansec[.]com**' (ट्रेंड माइक्रो द्वारा डार्क निंबस C2 के रूप में सूचीबद्ध) को ऐसे अन्य आईपी एड्रेसेज़ के लिए एक्सएमपीपी सेवाओं में भी देखा गया था, जिनमें डीकेएनएस शीर्षक वाले वेब पेज थे:

- 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)

आईपी एड्रेसेज़ के एक अन्य सेट में एक्सएमपीपी सेवाओं में '**ansec[.]com**' के साथ निम्नलिखित शीर्षकों वाले वेब पेज शामिल थे:

- 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)

इंटेलिजेंस ऑनलाइन के अनुसार एचटीएमएल पेजों के शीर्षकों में देखे गए 'यूपीएसईसी' का संदर्भ 'सिचुआन डाएन्क नेटवर्क सिक्योरिटी टेक्नोलॉजी को. लि.' से है।

मामला अध्ययन दो: BADBAZAAR

BADBAZAAR एक मोबाइल मैलवेयर है, जिसके आईओएस और एंड्रॉयड वेरिएंट्स मौजूद हैं। इसने उइगर, तिब्बतियों और ताइवान के व्यक्ति-विशेषों को लक्षित किया है। इस स्पाइवेयर को सोशल मीडिया प्लेटफॉर्म्स और आधिकारिक ऐप स्टोर्स के माध्यम से फैलाया गया है। Volexity की हालिया रिपोर्टिंग में BADBAZAAR के विभिन्न स्वरूपों को दिखाया गया है, जिन्हें BadSolar, BADBAZAAR और BadSignal के रूप में अलग-अलग किया गया है। ये सभी तीन वेरिएंट्स डिवाइस और ऑपरेटर के बारे में जानकारी एकत्र करने के लिए उपयोग किए जाने वाले ओवरलैपिंग फंक्शन्स के माध्यम से एक-साथ जुड़े हुए हैं।

एनसीएससी द्वारा BADBAZAAR के बारे में अनुसंधान से निम्नलिखित का पता चला:

- क्लस्टरिंग C2 डोमेन्स आगे के डोमेन लिंक्स प्रकट करते हैं, जिन्हें ऐतिहासिक रूप से खतरे की खुफिया जानकारी में रिपोर्ट किया गया है।
- C2 सर्वर्स और मैलवेयर नमूने हमलावर के इन्फ्रास्ट्रक्चर से जुड़े होस्टनेम्स प्रकट करते हैं।
- हमलावरों द्वारा सोशल इंजीनियरिंग के लिए उपयोग की जाने वाली अन्य प्रोफाइलें, ताकि वे अपने मैलवेयर को आधिकारिक ऐप स्टोर्स से परे फैला सकें।

WHOIS क्लस्टरिंग / डोमेन ब्रोकर

'UJYJYUJ'

BADBAZAAR डोमेन '**signalplus[.]org**' के WHOIS रिकॉर्ड्स विश्लेषण (ESET की रिपोर्ट) में '**State**' फील्ड में वैल्यू '**UJYJYUJ**' दिखाई गई है।

समान वैल्यू वाले अन्य डोमेन्स की खोज से निम्नलिखित रुचिकर डोमेन्स का पता चलता है:

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

(परिशिष्ट A, चित्र 1 देखें)

signalplus[.]org, **tubevideoplus[.]org** और **thetubeplus[.]com** – इन तीन डोमेन्स को BADBAZAAR के C2 डोमेन्स के रूप में, जबकि ESET सब डोमेन **mail.pmumail[.]com** को एक FlyGram प्रॉक्सी सर्वर के रूप में सूचित किया जाता है। FlyGram दुर्भावनापूर्ण साइबर अपराधियों द्वारा विकसित एक BADBAZAAR ऐप है (अन्य BADBAZAAR ऐप्स की सूची के लिए परिशिष्ट देखें)।

कीबोर्ड वॉकिंग वैल्यूज़

एनसीएससी ने अन्य पंजीकृत BADBAZAAR C2 डोमेन्स में भी इसी तरह के कीबोर्ड वॉकिंग पैटर्न देखे हैं।

उदाहरण के लिए, निम्नलिखित सभी डोमेन्स में '**State**' फील्ड में वैल्यू '**REWR**' देखी गई है (जैसे कि पहले उपयोग किया गया था):

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

(परिशिष्ट A, चित्र 2 देखें)

state फील्ड में 'FSDF' वैल्यू वाले डोमेन्स

BADBAZAAR C2 डोमेन्स के '**State**' फील्ड में '**FSDF**' वैल्यू वाला एक अन्य सेट:

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

(परिशिष्ट A, चित्र 3 देखें)

कीबोर्ड वॉकिंग मानों की ऐतिहासिक रिपोर्टिंग

BADBAZAAR डोमेन्स के WHOIS रिकॉर्ड में कीबोर्ड वॉकिंग वैल्यू के उपयोग को TA413 द्वारा तिब्बती संगठनों के ऐतिहासिक रूप से रिपोर्ट किए गए लक्ष्यीकरण में भी देखा जा सकता है। रिकॉर्डेड फ्यूचर ने तिब्बती संगठनों की स्पूफिंग करने वाले हमलावर-नियंत्रित डोमेन्स और रजिस्ट्रेंट संगठन के लिए **"asfasf"** वैल्यू का उपयोग देखा है।

clublogs[.]com

Lookout द्वारा प्राप्त BADBAZAAR के नमूनों में C2 डोमेन के रूप में '**xle.clublogs[.]com**' का उपयोग शामिल था। रूट डोमेन '**clublogs[.]com**' को आईपी एड्रेस '**95.179.210[.]85**' पर होस्ट किया गया था और इसमें एक SSL सर्टिफिकेट शामिल था, जिसमें subject और issuer की वैल्यू '**CN=WIN-50QO3EIRQVP**' थी। यह वैल्यू BADBAZAAR के नमूनों में पाए गए SSL सर्टिफिकेट्स से मेल खाती है, जो संचार में अवरोध से बचने के लिए SSL पिनिंग का उपयोग करते हैं।

आईपी एड्रेस **95.179.210[.]85** की होस्टिंग हिस्ट्री निम्नलिखित रुचिकर डोमेन्स रिटर्न करती है:

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

(परिशिष्ट A, चित्र 4 देखें)

www.voiceoftibet[.]net

डोमेन '**www.voiceoftibet[.]net**' 'वॉयस ऑफ तिब्बत' रेडियो स्टेशन के रूप में प्रतीत होता है, जोकि TA413 द्वारा इस्तेमाल किए गए TTP के समान है।

डोमेन '**rewrwer[.]com**' अतीत में पहचाने गई 'state' वैल्यू '**REWR**' के समान है, जिसे BADBAZAAR डोमेन्स के WHOIS रिकॉर्ड में पाया गया था।

ये सभी डोमेन्स - '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' और '**myloughborough[.]com**' ईमेल एड्रेस '**tplutalova@list[.]ru**' के साथ पंजीकृत थे।

actuallys[.]com

'**actuallys[.]com**' के WHOIS रिकॉर्ड ने एक इंस्टैंस प्रदर्शित किया जहां टेक और एड्मिन के ईमेल एड्रेसेज़ '**tplutalova@list[.]ru**' थे, किंतु रजिस्ट्रेंट की ईमेल '**ivan_s81@mail[.]ru**' थी।

डोमेन '**actuallys[.]com**' की ऐतिहासिक WHOIS जानकारी ने रजिस्ट्रेंट ईमेल के रूप में '**wangminghua6@gmail[.]com**' का खुलासा, जिसे 24 फरवरी 2016 को सूचीबद्ध किया गया। बाद में 11 मार्च 2016 को ईमेल को '**ivan_s81@mail.ru**' में बदल दिया गया था, किंतु रजिस्ट्रार की रजिस्ट्रेंट समाप्ति तिथि वही बनी रही।

wangminghua6@gmail[.]com

ईमेल एड्रेस '**wangminghua6@gmail[.]com**' का उपयोग ऐतिहासिक खतरे की खुफिया रिपोर्टिंग में पाए जाने वाले डोमेन्स के पंजीकरण के लिए किया गया था। 2015 में पालो ऑल्टो ने मैलवेयर Cmstar के C2 डोमेन्स पंजीकृत करने के लिए उपयोग की जाने वाली ईमेल की पहचान की. 2014 में इसका उपयोग APT3 द्वारा आयोजित फ़िशिंग अभियानों में Mandiant द्वारा पहचाने गए डोमेन्स को पंजीकृत करने के लिए भी किया गया था। 2013 में इसे CrowdStrike द्वारा खोजे गए डोमेन्स को मैलवेयर ड्रॉपर में एक प्रोग्राम डेटाबेस (पीडीबी) पथ के साथ रजिस्टर करने के लिए इस्तेमाल किया गया था, जिसमें चीनी अक्षर शामिल थे। इससे किसी चीनी सिस्टम पर कंपाइलेशन किए जाने का सुझाव मिलता है।

taoyujun@gmail[.]com

डोमेन '**hcjbtt[.]com**' ईमेल एड्रेस '**taoyujun@gmail[.]com**' के साथ पंजीकृत है, लेकिन इसकी एडमिनिस्ट्रेटर ईमेल '**wangminghua6@gmail[.]com**' के रूप में पंजीकृत है।

डोमेन '**hcjbtt[.]com**' के साथ कोई भी दुर्भाविनापूर्ण गतिविधि नहीं जुड़ी हुई है, किंतु ईमेल एड्रेस '**taoyujun@gmail[.]com**' को ऐतिहासिक खतरे की खुफिया रिपोर्टों में पाया गया था। 2014 में इसका उपयोग जापानी संगठनों के लक्ष्यीकरण में इस्तेमाल किए जाने वाले '**Cueisfry Trojan**' नमूनों में Mandiant द्वारा पाए गए एक डोमेन के पंजीकरण के लिए किया गया था।

इस ईमेल एड्रेस के साथ '**iaea-international[.]org**' जैसे डोमेन्स भी पंजीकृत थे, जो **अंतर्राष्ट्रीय परमाणु ऊर्जा एजेंसी** का प्रतिरूपण करता है और '**idc-ctbto[.]org**' व्यापक परमाणु-परीक्षण-प्रतिबंध संधि संगठन (सीटीबीटीओ) के **अंतर्राष्ट्रीय आंकड़ा केन्द्र** का प्रतिरूपण करता है।

डोमेन '**iaea-international[.]org**' के पूर्व Whois रिकॉर्ड ने रजिस्ट्रेंट ईमेल '**wangminghua6@gmail[.]com**' प्रदर्शित हुई।

udtglobals[.]com

डोमेन '**udtglobals[.]com**' में एडमिनिस्ट्रेटर ईमेल के रूप में

'**wangminghua6@gmail[.]com**' का उपयोग और रजिस्ट्रेंट ईमेल एड्रेस के रूप में '**ocean.nio@rediffmail[.]com**' का उपयोग देखा गया था। इस डोमेन के अन्य WHOIS रिकॉर्ड्स में वही रजिस्ट्रेंट ईमेल दिखाई दी, किंतु एडमिनिस्ट्रेटर ईमेल एड्रेस के रूप में '**taoyujun@gmail[.]com**' दिखाई दी।

'**udtglobals[.]com**' को '**यूडीटी ग्लोबल**' का प्रतिरूपण करते हुए पाया गया, जोकि समुद्र के नीचे रक्षा और सुरक्षा कंपनियों का एक वैश्विक आयोजन है। ईमेल एड्रेस में '**ocean.nio**' उपयोगकर्ता का मौजूद होना **राष्ट्रीय समुद्र-विज्ञान संस्थान (एनआईओ)** का प्रतिरूपण करते हुए हो सकता है, जो कई देशों में उपस्थित है। किंतु '**रेडिफ**' ईमेल सेवा का प्रयोग (जोकि भारत में आधारित है) भारत के **राष्ट्रीय समुद्र-विज्ञान संस्थान** के प्रतिरूपण का सुझाव दे सकता है।

Djibdiplomatie[.]com

डोमेन '**djibdiplomatie[.]com**' जिबूती की राजनीति सेवाओं का प्रतिरूपण प्रतीत होता है, जिसका WHOIS रिकॉर्ड '**utdglobals[.]com**' के समान था। एक रिकॉर्ड में रजिस्ट्रेंट के रूप में '**ocean.nio@rediffmail[.]com**' और एडमिन के रूप में '**taoyujun@gmail[.]com**' दिखाई दिया, जबकि अन्य रिकॉर्ड्स में एडमिन ईमेल पते के रूप में '**wangminghua6@gmail[.]com**' और रजिस्ट्रेंट ईमेल पते के रूप में '**ocean.nio@rediffmail[.]com**' दिखाई दिया।

इन दोनों डोमेन्स के WHOIS रिकॉर्ड्स में कीबोर्ड वॉकिंग टाइप वैल्यूज़ भी थीं। उदाहरण के लिए, '**udtglobals[.]com**' के रजिस्ट्रेंट शहर की वैल्यू '**ASDF**' है और '**djibdiplomatie[.]com**' के रजिस्ट्रेंट नेम की वैल्यू '**DAF DAGF**' है। यह BADBAZAAR के अन्य डोमेन्स में देखी गई वैल्यूज़ के बराबर तुलनात्मक है।

हालांकि WHOIS रिकॉर्ड्स में ईमेल पतों '**wangminghua6@gmail[.]com**' और '**taoyujun@gmail[.]com**' को एक वैश्विक समुद्र के नीचे रक्षा आयोजन, जिबूती राजनीति सेवाओं और अंतर्राष्ट्रीय परमाणु ऊर्जा एजेंसी के डोमेन्स के रूप में पाया जाता है, किंतु ये अनेक गैर-दुर्भावनापूर्ण डोमेन्स के WHOIS रिकॉर्ड में भी हैं।

प्रतिरूपण करने वाले डोमेन्स और गैर-दुर्भाविनापूर्ण डोमेन्स का मिश्रण दुर्भाविनापूर्ण साइबर अपराधियों के परिचालनों को समर्थन देने के लिए उपयोग की जाने वाली इंफ्रास्ट्रक्चर-खरीद इकाई के मौजूद होने का सुझाव दे सकता है।

ईमेल पता '**ocean.nio@rediffmail[.]com**' केवल ऊपर वर्णित प्रतिरूपण करने वाले डोमेन में पाया जाता है। '**ivan_s81@mail[.]ru**' और '**tplutalova@list[.]ru**' ने क्रमशः बहुत कम संख्या में डोमेन्स पंजीकृत किए हैं, और इनमें से कुछ डोमेन्स BADBAZAAR के इंफ्रास्ट्रक्चर पर होस्ट किए गए हैं। ऐसा माना जाता है कि ये तीन ईमेल पते दुर्भाविनापूर्ण साइबर अपराधियों के परिचालनों से अधिक निकटता से जुड़े हुए हैं। ऐसा इसलिए है क्योंकि ईमेल पतों '**wangminghua6@gmail**' और '**taoyujun@gmail[.]com**' की तुलना में इन तीन ईमेल पतों से जुड़े डोमेन्स को कहीं अधिक संख्या में दुर्भाविनापूर्ण गतिविधियों से लिंक किया गया है।

(परिशिष्ट A, चित्र 5 देखें)

अन्य हमलावरों के लिंक्स

BADBAZAAR से जुड़े इन डोमेन्स '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', और '**voiceoftibet[.]net**' की एक और सामान्य विशेषता यह है कि वे सभी eNom के साथ पंजीकृत थे और वे '**255.255.255[.]254**' पर 'पार्क' किए गए थे।

एनसीएससी द्वारा अतीत में की गई जांचों के बाद इन विशेषताओं वाले अन्य डोमेन्स के लिए 2019 में **APT5** तथा 2009 और 2011 के बीच **APT14** से जुड़ी गतिविधि का खुलासा हुआ।

APT5 से जुड़े डोमेन्स में ऐसे ऐतिहासिक WHOIS रिकॉर्ड थे, जिनमें रजिस्ट्रेंट ईमेल पते के रूप में '**taoyujun@gmail[.]com**' सूचीबद्ध था।

APT14 से जुड़े डोमेन्स में तीन-अक्षर वाले सबडोमेन्स थे, जो उनके दुर्भाविनापूर्ण परिचालनों के इच्छित लक्ष्य का प्रतिनिधित्व करते हुए प्रतीत होते थे। इसका एक उदाहरण '**bae.cisconline[.]net**' है, जिससे बीएई सिस्टम्स को लक्षित करने के इरादे का सुझाव मिला और इसे '**पॉइज़न आइवी**' के एक नमूने में पाया गया।

इसी तरह की एक अन्य विशेषता BADBAZAAR डोमेन्स में भी देखी जाती है, जहां सबडोमेन्स ट्रोज़नाइज़्ड ऐप के नाम से संबंधित हैं:

एप्लिकेशन का शीर्षक	C2 यूआरएल
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

इस बात का ध्यान रखना महत्वपूर्ण है कि APT5 और APT14 से संबंधित गतिविधियाँ ऐतिहासिक थीं और eNom के साथ पंजीकृत तथा '**255.255.255.254**' से जुड़े अन्य डोमेन्स भी मौजूद थे, जिन्हें दुर्भावनापूर्ण गतिविधि से नहीं जोड़ा जा सकता है। इसलिए यह सुनिश्चित नहीं है कि इन अभियानों के पीछे वही हमलावर हैं या वे उन्हीं हमलावरों से संबंधित हैं।

मशीनों के नाम

BADBAZAAR के C2 और नमूनों के विश्लेषण से एसएसएल सर्टिफिकेट्स में 'Common Name' वैल्यू के रूप में उपयोग किए जाने वाले होस्टनेम्स का पता चला। BADBAZAAR के नमूनों और इंफ्रास्ट्रक्चर में देखे गए होस्टनेम्स की एनसीएससी जांच से पता चला है कि इन होस्टनेम्स का उपयोग एक से अधिक आईपी एड्रेसेज़ में किया जाता है। ये आईपी एड्रेसेज़ BADBAZAAR के नमूनों में पाए जाने वाले डोमेन्स को होस्ट कर रहे हैं। आगे उपलब्ध अनुभाग में होस्टनेम्स और आईपी एड्रेसेज़ के बारे में और अधिक विवरण दिया गया है, जिसमें BADBAZAAR के C2 डोमेन्स को होस्ट करने वाले होस्टनेम्स भी शामिल हैं।

लगभग सभी मामलों में होस्टनेम्स वैल्यू के साथ सर्टिफिकेट्स की उपस्थिति निर्दिष्ट दुर्भावनापूर्ण डोमेन नेम्स के लिए आईपी रिज़ॉल्यूशन के साथ ओवरलैप होती है। ऐसे कुछ उदाहरणों को रेखांकित किया गया है, जहां ऐसा नहीं था।

WIN-EU0VLBL7TUJ

होस्टनेम '**WIN-EU0VLBL7TUJ**' को निम्नलिखित आईपी एड्रेसेज़ पर देखा गया, जो रुचिकर हो सकते हैं:

- '**116.203.53[.]21**' ने BADBAZAAR के C2 डोमेन्स '**uyapkfinder[.]com**' और '**thewestuniverse[.]com**' को होस्ट किया।

- '**95.216.169[.]27**' ने BADBAZAAR के C2 डोमेन्स '**adysfunction[.]com**' और सब-डोमेन '**download.apkbazar[.]biz**' को होस्ट किया, जिन्हें BADBAZAAR के एक नमूने के लिए डाउनलोड लिंक के रूप में देखा गया।

(परिशिष्ट A, चित्र 6 देखें)

WIN-70E59JVOB9G

होस्टनेम '**WIN-70E59JVOB9G**' को निम्नलिखित आईपी एड्रेसेज़ का उपयोग करते हुए देखा गया, जो रुचिकर हो सकते हैं:

- '**23.88.28[.]220**' ने BADBAZAAR के C2 सब-डोमेन्स '**aua.rondwsign[.]com**', '**nal.tokenmajorp[.]com**' , '**pep.rondwsign[.]com**', '**doa.rondwsign[.]com**', और '**pls.rondwsign[.]com**' को होस्ट किया। मशीन के साथ सर्टिफिकेट को अंतिम बार देखे जाने और मैलिशियस डोमेन्स को पहली बार आईपी रिज़ॉल्व करते हुए देखे जाने के बीच दो दिनों की अवधि थी।

- '**23.88.28[.]221**' ने BADBAZAAR से जुड़े सब-डोमेन '**bt.bhvghg[.]com**' को होस्ट किया।

- '**23.88.28[.]222**' ने BADBAZAAR के C2 डोमेन्स '**tubevideoplus[.]org**' और '**cde.mpoxcases[.]com**' को होस्ट किया।

- '**65.21.92[.]67**' ने BADBAZAAR के C2 सब-डोमेन्स '**bat.androidupdated[.]net**' को होस्ट किया। इसने सब-डोमेन '**apps.androidupdated[.]net**' को भी होस्ट किया, जोकि डबल एजेंट मैलवेयर C2 है

- '**65.21.92[.]77**' ने BADBAZAAR के C2 सब-डोमेन्स '**wyo.titeperformance[.]com**', '**big.collinformations[.]com**' , '**vpf.titeperformance[.]com**', '**eud.titeperformance[.]com**' और '**afg.collinformations[.]com**' को होस्ट किया।

- '**65.108.192[.]134**' ने BADBAZAAR के C2 सब-डोमेन्स '**upd.whoscaller.net**' और '**ggl.whoscaller[.]net**' को होस्ट किया।

- '**142.132.131[.]15**' ने BADBAZAAR के C2 सब-डोमेन्स '**bvn.lookincategory[.]com**' और '**edr.lookincategory[.]com**' को होस्ट किया। मशीन नेम के साथ सर्टिफिकेट को अंतिम बार देखे जाने और मैलिशियस डोमेन्स को पहली बार आईपी रिज़ॉल्व करते हुए देखे जाने के बीच ग्यारह दिनों की अवधि थी।

- '**142.132.131[.]20**' ने सब-डोमेन्स '**son.onlinegamersgroup[.]com**' और '**system.onlinegamersgroup[.]com**' को होस्ट किया, जिन्हें BADBAZAAR का C2 माना जाता है क्योंकि वे BADBAZAAR से जुड़े एसएसएल सर्टिफिकेट्स के आईपी पर देखे जाने के समय होस्ट किए गए थे।

- '**142.132.131[.]28**' ने BADBAZAAR के C2 डोमेन '**goldplusapp[.]net**' और सब-डोमेन्स '**who.goldplusapp[.]net**' और '**cgf.goldplusapp[.]net**' को होस्ट किया।

- '**162.55.103[.]211**' ने BADBAZAAR के C2 सब-डोमेन्स '**oha.alpinemap[.]net**', '**aru.alpinemap[.]net**', '**aso.alpinemap[.]net**', '**afr.alpinemap[.]net**', और '**aar.alpinemap[.]net**' को होस्ट किया।

- '**162.55.103[.]212**' ने BADBAZAAR के C2 सब-डोमेन्स '**pep.rondwsign[.]com**', '**ckp.jkiohreh[.]com**', '**aar.tokenmajorp[.]com**', '**nal.tokenmajorp[.]com**', '**pls.rondwsign[.]com**' और '**aua.rondwsign[.]com**' को होस्ट किया।

- '**195.154.47[.]99**' ने BADBAZAAR के C2 सब-डोमेन्स '**ggl.whoscaller[.]net**' और '**upd.whoscaller.net**' को होस्ट किया। मशीन नेम के साथ सर्टिफिकेट को पहली बार देखे जाने और मैलिशियस डोमेन्स को अंतिम बार आईपी रिज़ॉल्व करते हुए देखे जाने के बीच तीन दिनों की अवधि थी।

- '**195.154.60[.]3**' ने BADBAZAAR के C2 सब-डोमेन्स '**upd.whoscaller[.]net**' और '**ggl.whoscaller[.]net**' को होस्ट किया।

- '**212.83.189[.]89**' ने BADBAZAAR के C2 सब-डोमेन्स '**wyo.titeperformance[.]com**', '**eud.titeperformance[.]com**', '**vpf.titeperformance[.]com**' और '**afg.collinformations[.]com**' को होस्ट किया।

- '**212.129.21[.]168**' ने BADBAZAAR के C2 डोमेन्स '**fre.lookincategory[.]com**', '**tgr.lookincategory[.]com**', '**fgt.lookincategory[.]com**', '**luj.lookincategory[.]com**' और '**bvn.lookincategory[.]com**' को होस्ट किया।

(परिशिष्ट A, चित्र 7 देखें)

WIN-50QO3EIRQVP

होस्टनेम '**WIN-50QO3EIRQVP**' को निम्नलिखित आईपी एड्रेसेज़ पर देखा गया, जो रुचिकर हो सकते हैं:

- '**45.76.132[.]91**' ने डोमेन्स '**yumoftion[.]com**', '**androidupdated[.]net**' को होस्ट किया। ये दोनों डोमेन्स BADBAZAAR से सब-डोमेन्स '**fow.yumoftion[.]com**' और '**bat.androidupdated[.]net**' के रूप में जुड़े हुए हैं। इसके अतिरिक्त सब-डोमन '**apps.androidupdated[.]net**' DoubleAgent का एक C2 डोमेन है। यह डोमेन '**pmstwocqn[.]com**' को भी होस्ट करता है, जोकि WHOIS रिकॉर्ड्स के अनुसार BADBAZAAR से जुड़ा हुआ है।

- '**95.179.210[.]85**' ने '**clublogs[.]com**' को होस्ट किया, जिनमें से '**xle.clublogs[.]com**' BADBAZAAR का एक C2 डोमेन है और इसने BADBAZAAR से जुड़े डोमेन्स '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' और '**actuallys[.]com**' को भी होस्ट किया।

- '**199.247.21[.]34**' ने '**titeperformance[.]com**' और '**collinformations[.]com**' को होस्ट किया, जिनके सब-डोमेन्स BADBAZAAR के C2 डोमेन्स हैं।

- '**217.69.10[.]128**' ने BADBAZAAR C2 के डोमेन '**uyghurdict[.]com**' को होस्ट किया।

(परिशिष्ट A, चित्र 8 देखें)

WMSvc-WIN-50QO3EIRQVP

होस्टनेम '**WMSvc-WIN-50QO3EIRQVP** को निम्नलिखित आईपी एड्रेसेज़ पर देखा गया, जो रुचिकर हो सकते हैं:

- '**78.46.185[.]251**' ने BADBAZAAR के C2 डोमेन '**groupgram[.]org**' को होस्ट किया, जिसके बारे में Volexity ने सूचना दी है कि यह दुर्भावनापूर्ण कनेक्शन्स के लिए पोर्ट 4432 का उपयोग करता था।

- '**65.21.92[.]69**' और '**163.172.205[.]207**' ने डोमेन '**widelygram[.]org**' को होस्ट किया, जिसे BADBAZAAR का एक C2 डोमेन माना जाता है, क्योंकि जब इसे होस्ट किया जा रहा था तो पोर्ट 4432 खुला था।

- '**163.172.198[.]206**' ने डोमेन '**maxgram[.]org**' को होस्ट किया, जिसे BADBAZAAR का एक C2 डोमेन माना जाता है, क्योंकि जब इसे होस्ट किया जा रहा था तो पोर्ट 4432 खुला था।

(परिशिष्ट A, चित्र 9 देखें)

WMSvc-WIN-50QO3EIRQVP और WIN-7LSBB9R0F1L

होस्टनेम्स '**WMSvc-WIN-50QO3EIRQVP**' और '**WIN-7LSBB9R0F1L**' को निम्नलिखित आईपी एड्रेसेज़ पर एक-साथ देखा गया:

- '**148.251.87[.]245**' ने BADBAZAAR के C2 डोमन्स '**flygram[.]org**' और '**groupgram[.]org**' को होस्ट किया।

(परिशिष्ट A, चित्र 10 देखें)

WIN-N8H8S9BG2P0

होस्टनेम '**WIN-N8H8S9BG2P0**' को निम्नलिखित आईपी एड्रेस पर देखा गया:

- '**148.251.87[.]247**' ने BADBAZAAR के C2 डोमेन्स '**omarwhatsapp[.]org**' और '**flygram[.]org**' को होस्ट किया।

(परिशिष्ट A, चित्र 11 देखें)

WIN-I6VBN8MR92A

होस्टनेम '**WIN-I6VBN8MR92A**' को निम्नलिखित आईपी एड्रेस पर देखा गया:

- '**148.251.87[.]197**' ने BADBAZAAR के C2 डोमेन '**tryhrwserf[.]com**' को होस्ट किया।

(परिशिष्ट A, चित्र 12 देखें)

उपलब्ध कमर्शियल डेटा के आधार पर इंटरनेट पर इन मशीन नेम्स की व्यापकता भिन्न-भिन्न होती है। इनमें से कुछ को एक से अधिक आईपी एड्रेसेज़ में एक साथ देखा जाता है, जो एक ही टेम्पलेट से बनाई जा रही वीएम की ओर इंगित करता है। इस बात का ध्यान रखना महत्वपूर्ण है कि कुछ होस्टनेम्स के लिए उन सभी आईपी को दुर्भाविनापूर्ण गतिविधि से नहीं जोड़ा जा सकता है, जिनपर उन्हें देखा गया था। इसका मतलब यह हो सकता है कि होस्टनेम्स का उपयोग इन हमलावरों के लिए अनन्य नहीं है।

किंतु BADBAZAAR के C2 डोमेन्स को होस्ट करने वाले एक से अधिक आईपी में इनमें से कुछ मशीन नेम्स की व्यापकता यह सुझाव दे सकती है कि दुर्भाविनापूर्ण हमलावरों के साइबर परिचालनों के समर्थन के लिए मशीनों को कॉन्फ़िग्युर करने के उद्देश्य से एक इंफ्रास्ट्रक्चर-खरीद निकाय का उपयोग किया जा रहा है।

सोशल मीडिया पर उपस्थिति

अतीत में Volexity की रिपोर्टिंग से पता चला है कि दुर्भाविनापूर्ण साइबर अपराधियों द्वारा यूट्यूब (दुर्भाविनापूर्ण एप्लिकेशन्स के उपयोग को बढ़ावा देने वाले) वीडियोज़ बनाए गए थे। इन वीडियोज़ में विकसित की गई एप्लिकेशन्स का उपयोग करने के तरीकों के बारे में ट्यूटोरियल्स शामिल थे।

एनसीएससी ने हमलावरों के परिचालनों से जुड़े दो अतिरिक्त यूट्यूब चैनलों की खोज की है। यूआरएल हैंडल **'@josephjoey3499'** वाला यूट्यूब चैनल '**Maxgram**' के उपयोग को बढ़ावा देता हुआ दिखाई दिया और **'@uyghurapks3096'** के साथ पंजीकृत एक अतिरिक्त चैनल '**Uyghur APK Finder**' को बढ़ावा देता है।

इसके अतिरिक्त '**Flygram**' और '**Signal Plus**' को बढ़ावा देने वाले यूट्यूब वीडियोज़ में अपराधियों को दृश्य फोन नंबरों का उपयोग करते हुए दिखाया गया है। '**Flygram**' वीडियो में 0:36 पर फोन नंबर '**+1 (570) 378-7250**' दिखाई देता है और '**Signal Plus**' वीडियो के दौरान फोन नंबर '+1 (267) 298 4259' का पता चलता है।

Volexity ने तिब्बत के विषय पर एक नकली समाचार साइट '**ignitetibet[.]net**' के बारे में रिपोर्ट की, जो उन्हें टेलीग्राम चैनलों में मिली है। इसे अपराधियों द्वारा संचालित किए जाते हुए माना जाता है। ईमेल पते '**choekyi.wangmo@ignitetibet[.]net**' को पेज '**tibetone.org**' पर एक पोस्ट के ऊपर टिप्पणी लिखते हुए देखा गया है, जिसे Lookout द्वारा सार्वजनिक रूप से BADBAZAAR के अईओएस संस्करण के लिए उपयोग किए जाने वाले C2 पेज के रूप में रिपोर्ट किया गया है।

ऐसा माना जाता है कि यह ईमेल पता '**चोएक्यी वांगमो**' के व्यक्तित्व का उपयोग करते हुए हमलावर द्वारा नियंत्रित किया जाता है।

आकलन

BADBAZAAR और MOONSHINE विशेष रूप से उइगर, तिब्बती और ताइवानी समुदायों को निशाना बनाने के लिए कई सोशल इंजीनियरिंग तरीकों का उपयोग करते हैं, विशेषकर:

- इन समुदायों के लिए रुचिकर ऐप्स में ट्रोजन्स को जोड़ना, जैसे उइगर भाषा में कुरान ऐप, लगभग निश्चित रूप से शिकार आधारों को लक्षित करने के लिए अनुरूपित किया गया है
- आधिकारिक ऐप स्टोर में इन ट्रोज़न-युक्त ऐप्स को जोड़ने से वैधता का एहसास पैदा होने की संभावना है, और सामूहिक चैट में इन्हें साझा करने का उद्देश्य इन समुदायों के अंदर विश्वसनीय संबंधों का फायदा उठाना है

BADBAZAAR और MOONSHINE ऐसा डेटा एकत्र करते हैं, जो लगभग निश्चित रूप ही से चीनी राष्ट्र के लिए महत्वपूर्ण होगा। BADBAZAAR और MOONSHINE को उइगर, तिब्बती और ताइवान के व्यक्ति-विशेषों को लक्षित करते हुए देखा गया है, लेकिन चीन में अन्य अल्पसंख्यक समूहों को लक्षित करने वाले अन्य मैलवेयर्स भी हैं। चीन और विदेशों में को-सीलिंग देशों के नागरिकों को, जिन्हें प्रशासन की स्थिरता के लिए खतरा पैदा करने वाले कारणों को समर्थन देने के रूप में माना जाता है, लगभग निश्चित रूप से ही BADBAZAAR और MOONSHINE जैसे मोबाइल मैलवेयर से खतरा है। स्थान, ऑडियो और फोटो डेटा को कैप्चर करने की क्षमता लक्ष्य की गतिविधि पर वास्तविक समय में जानकारी देकर भविष्य में निगरानी और उत्पीड़न कार्रवाइयों को सूचित करने का अवसर लगभग निश्चित रूप से ही उपलब्ध कराती है।

MITRE ATT&CK®

इस रिपोर्ट को MITRE ATT&CK® इंफ्रास्ट्रक्चर के संबंध में संकलित किया गया है, जो वास्तविक दुनिया के अवलोकनों के आधार पर प्रतिकूल चालबाजियों और तकनीकों का विश्व-स्तर पर सुलभ एक ज्ञान आधार है।

चालबाजी	आईडी	तकनीक	प्रक्रिया
रिकॉनायसेन्स	T1593.001	खुली वेबसाइटें/डोमेन्स खोजना: सोशल मीडिया	मैलवेयर को साझा करने के लिए हमलावर अपने इच्छित लक्षित लोगों से मेल खाने वाले ऑनलाइन समूह और फोरम्स ढूंढते हैं
संसाधन का विकास	T1583.001	इन्फ्रास्ट्रक्चर की प्राप्ति: डोमेन्स डोमेन्स	हमलावर अपने कमान और नियंत्रण सर्वर के लिए डोमेन्स को पंजीकृत करते हैं
संसाधन का विकास	T1587.001	क्षमताओं का विकास: मैलवेयर	दुर्भावनापूर्ण कोड लिखा जाता है, ताकि इसे ट्रोज़नाइज़्ड ऐप्स में डाला जा सके
संसाधन का विकास	T1608.001	क्षमताओं की स्टेजिंग: मैलवेयर अपलोड	ट्रोज़नाइज़्ड ऐप्स को ऑनलाइन प्लेटफॉर्म्स पर अपलोड किया जाता है, जिसमें ऐप स्टोर्स भी शामिल हैं
संसाधन का विकास	T1585.001	खाते बनाना: सोशल मीडिया खाते	मैलवेयर को साझा और विज्ञापित करने के लिए हमलावर वेबसाइटों और सोशल मीडिया पर खाते बनाते हैं
संसाधन का विकास	T1585.002	खाते बनाना: ईमेल खाते	मैलवेयर को होस्ट और साझा करने के लिए हमलावर निजी तौर पर होस्ट किए जाने वाले और कमर्शियल ईमेल खातों का उपयोग करते हैं
आरंभिक एक्सेस	T1189	ड्राइव-बाय कॉम्प्रोमाइज़	दुर्भावनापूर्ण स्क्रिप्ट्स को अन्यथा वैध ऐप्स में छिपाया जाता है और ऐप स्टोर्स पर अपलोड किया जाता है
आरंभिक एक्सेस	T1566.003	फिशिंग: सेवा के माध्यम से स्पियरफिशिंग	हमलावर सोशल मीडिया के माध्यम से लक्षित समूहों को ट्रोज़नाइज़्ड ऐप्स भेजते हैं, जिसमें टेलीग्राम भी शामिल है
एक्ज़िक्यूशन	T1204.002	उपयोगकर्ता एक्ज़िक्यूशन: मैलिशियस फाइल	लक्षित लोगों को पेलोड एक्ज़िक्यूट करने के लिए ट्रोज़नाइज़्ड ऐप्स को इंस्टॉल करना होता है
सुरक्षा से बचाव	T1027.009	फाइलों या जानकारी को अस्पष्ट बनाना: एंबेडेड पेलोड्स	दुर्भावनापूर्ण पेलोड को अन्यथा वैध ऐप्स के अंदर छिपाया जाता है

सुरक्षा से बचाव	T1036.005	प्रतिरूपण: वैध नेम या लोकेशन का मिलान	ड्रोज़नाइज़्ड फाइलें वैध ऐप्स के नाम, प्रकटन और फंक्शन से मिलान करती हैं।
सुरक्षा से बचाव	T1656	प्रतिरूपण	हमलावर कवर वेबसाइटें बनाकर और लक्षित समूहों से जुड़े उपयोगकर्ता नामों को इस्तेमाल करके विश्वसनीय व्यक्ति-विशेषों का प्रतिरूपण करते हैं
संग्रह	T1123	ऑडियो कैप्चर	ड्रोज़नाइज़्ड ऐप्स अनावश्यक पर्मिशन्स के लिए निवेदन कर सकती हैं, जिसमें माइक्रोफोन एक्सेस शामिल है
संग्रह	T1125	वीडियो कैप्चर	ड्रोज़नाइज़्ड ऐप्स अनावश्यक पर्मिशन्स के लिए निवेदन कर सकती हैं, जिसमें कैमरा एक्सेस शामिल है
संग्रह	T1005	लोकल सिस्टम से डेटा	ड्रोज़नाइज़्ड ऐप्स अनावश्यक पर्मिशन्स के लिए निवेदन कर सकती हैं, जिसमें लोकल फाइलें शामिल हैं
कमान और नियंत्रण	T1071.001	एप्लिकेशन लेयर प्रोटोकॉल: वेब प्रोटोकॉल्स	मैलवेयर HTTPS और WebSocket का उपयोग करके C2 से जुड़ता है।
कमान और नियंत्रण	T1509	गैर-मानक पोर्ट	गैर-मानक पोर्ट्स का इस्तेमाल किया जाता है, जैसे पोर्ट 4432 और 2333
एक्सिफिल्ट्रेशन	T1041	C2 चैनल से एक्सफिल्ट्रेशन	मैलवेयर HTTPS और WebSocket कनेक्शन्स का उपयोग करके डेटा को बाहर निकालता है।
प्रभाव	T1565.002	डेटा मैनिप्युलेशन: प्रेषित डेटा का मैनिप्युलेशन	ऐप की फंक्शनैलिटी के लिए अनावश्यक ऐप वेब ट्रैफ़िक को सक्षम बनाकर हमलावर लक्षित लोगों से डेटा प्राप्त करते हैं

संकेतक

MOONSHINE

- 1 अप्रैल 2025 को VLiteUI पैनलों की खोज करने पर निम्नलिखित जानकारी प्राप्त हुई:

आईपी पता	पोर्ट	पहली बार देखा गया	अंतिम बार देखा गया
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	2024-03-26	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

- 1 अप्रैल 2025 को SCOTCH ADMIN पैनलों की खोज करने पर निम्नलिखित जानकारी प्राप्त हुई:

आईपी पता	पोर्ट	पहली बार देखा गया	अंतिम बार देखा गया
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

- 14 मार्च 2024 को वर्चुअल SCOTCH ADMIN पैनलों की खोज करने पर निम्नलिखित जानकारी प्राप्त हुई:

डोमेन	आईपी पता
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:

विवरण	BADBAZAAR के C2 पर एसएसएल सर्टिफिकेट देखा गया
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- 1 अप्रैल 2025 को उपरोक्त BADBAZAAR सर्टिफिकेट की खोज करने पर निम्नलिखित जानकारी प्राप्त हुई:

आईपी पता	पोर्ट	पहली बार देखा गया	अंतिम बार देखा गया
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

विवरण	BADBAZAAR के C2 पर एसएसएल सर्टिफिकेट देखा गया
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62d b3db1baa

- 1 अप्रैल 2025 को," उपरोक्त BADBAZAAR सर्टिफिकेट्स की खोज से निम्नलिखित परिणाम प्राप्त हुए:

आईपी पता	पोर्ट	पहली बार देखा गया	अंतिम बार देखा गया
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28

162.55.103[.]210	20121	2022-09-30	2023-02-23
65.21.92[.]67	20121	2021-11-02	2022-10-13
65.21.92[.]67	20122	2022-08-10	2022-10-13
23.88.28[.]220	20121	2021-12-08	2022-05-13
94.130.92[.]230	20121	2021-01-04	2021-10-05
88.99.150[.]246	20121	2021-04-06	2021-09-08
45.76.132[.]91	20121	2021-02-02	2021-03-01

- WHOIS डोमेन्स

नीचे डोमेन्स की तालिका दी गई है, जिनमें वर्तमान या ऐतिहासिक रूप से ऐसे WHOIS रिकॉर्ड्स शामिल हैं जिनकी वैल्यूज़ BADBAZAAR के C2 डोमेन्स में देखी गई वैल्यूज़ से मेल खाती हैं।

WHOIS वैल्यू	डोमेन्स
रजिस्ट्रेंट State: UJYJYUJ **रजिस्ट्रेंट देश: बोलिविया** **रजिस्ट्रार: 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
रजिस्ट्रेंट State: REWR **रजिस्ट्रेंट देश: CF** **रजिस्ट्रार: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

रजिस्ट्रेंट State: FSDF **रजिस्ट्रेंट देश: AL** **रजिस्ट्रार: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

यूट्यूब चैनल्स
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

BADBAZAAR और MOONSHINE से जुड़े इंडिकेटर्स ऑफ कॉम्प्रोमाइज़ (IoCs) के लिंक्स नीचे दिए गए हैं। इन लिंक्स में दी गई सभी जानकारी की वैधता की पुष्टि एनसीएससी नहीं कर सकती है और पाठकों को सलाह दी जाती है कि वे स्वतंत्र रूप से इनकी सटीकता और प्रासंगिकता सत्यापित करें:

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

मिटिगेशन

मामला अध्ययनों में बताए गए खतरों से बचाव के लिए एनसीएससी नीचे दी गई संस्तुतियाँ अपनाने को प्रोत्साहित करती है।

- **ऐप स्टोर ऑपरेटर्स और डेवलपर्स को यह सुनिश्चित करना चाहिए कि उनके प्लेटफॉर्म पर ऐप्स सुरक्षित हैं और वे सरकारी आचार संहिता के अनुपालन में हैं। इसमें तीसरे पक्ष के ऐप स्टोर्स भी शामिल हैं।** मार्गदर्शन देखें: 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

  एक से अधिक भाषाओं में समर्थन: ऐप डेवलपर्स को लक्षित समूहों में अल्पसंख्यक भाषाएं बोलने वाले उपयोगकर्ताओं के लिए लोकप्रिय ऐप्स के लोकलाइज़ेशन प्रयासों में निवेश करना चाहिए, जिनमें उइगर, तिब्बती, ताइवानी होक्किएन और कैंटोनीज़ भाषाएं शामिल हैं। ऐप्स में लोकलाइज़िंग के लिए एप्पल का मार्गदर्शन: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app.
  अनुवाद करने वाली ऐप्स के बारे में गूगल का मर्गदर्शन: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **अपने सोशल मीडिया को सुरक्षित बनाए रखें:** सोशल मीडिया कम्पनियां दुर्भावनापूर्ण साइबर अपराधियों के लिए फर्जी खाते बनाना तथा वैध ऑनलाइन समुदायों में अपने प्लेटफॉर्म्स पर दुर्भावनापूर्ण फाइलें या लिंक साझा करना अधिक कठिन बना सकती हैं। जहां संभव हो, कम्पनियों को खतरे की सामूहिक समझ के बेहतरीकरण तथा सुरक्षा उपायों में सहायता के लिए व्यापक उद्योग के साथ दुर्भावनापूर्ण संकेतकों को साझा करना चाहिए।

- **ग्राहकों के लिए सुधार योजना:** संगठनों के पास ऐसे सेवार्थियों को सूचित करने के लिए प्रक्रियाएँ होनी चाहिए, जिन्होंने उनकी सेवाओं का उपयोग करते हुए दुर्भावनापूर्ण ऐप्स इंस्टॉल की हैं। ये एलर्ट्स ध्यान आकर्षित करने वाले और जानकारीपूर्ण होने चाहिए। जहां उपयुक्त हो, संगठनों को सॉफ्टवेयर हटाने के बारे में मार्गदर्शन प्रदान करना चाहिए तथा लक्षित बने लोगों को अपने-अपने प्राधिकारियों के पास रिपोर्ट करने के लिए प्रोत्साहन देना चाहिए, जैसे यूके में एनसीएससी।

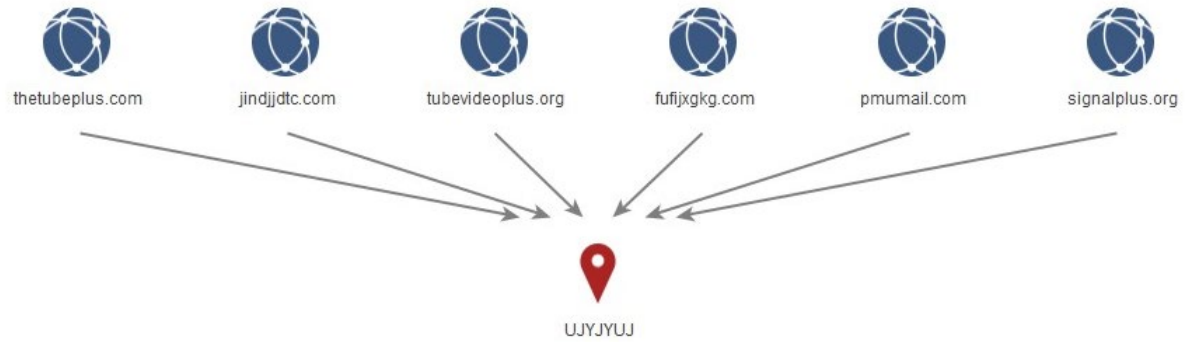
और अधिक जानकारी के लिए ऐप स्टोर आचार संहिता देखें:
https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **सहयोग के लिए कार्य समूह:** सोशल मीडिया कंपनियाँ कार्य समूह बना सकती हैं, जिससे उनकी संबंधित सुरक्षा टीमों को दुर्भावनापूर्ण संकेतक, टीटीपी और देखी जाने वाली बातें साझा करने की अनुमति मिलती है। इससे हमलावरों के लिए दुर्भावनापूर्ण अभियानों के समर्थन के उद्देश्य से अपने प्लेटफॉर्म्स का उपयोग करना अधिक कठिन हो जाता है।

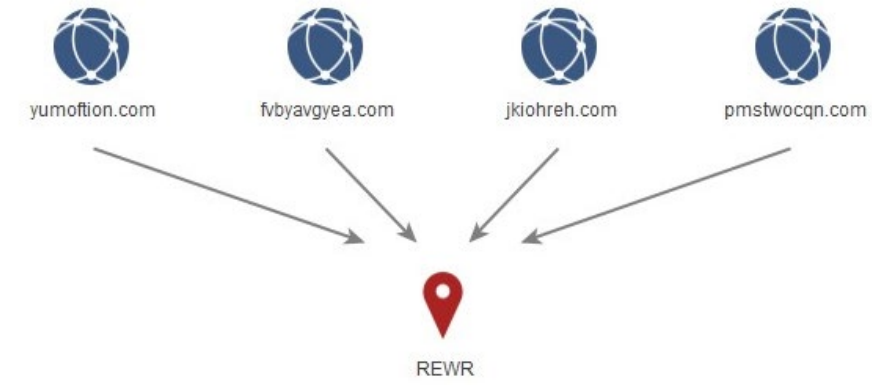
- **परिवर्तित ऐप्स की पहचान:** जहां संभव हो, ऐप डेवलपर्स को ऐसी फंक्शनैलिटी शामिल करनी चाहिए जो उपयोगकर्ता को सूचित करे कि क्या उन्होंने किसी ऐप का 'गैर-आधिकारिक' संस्करण डाउनलोड किया है, ताकि उन्हें दुर्भावनापूर्ण प्रतियों से सुरक्षा में सहायता मिल सके।

परिशिष्ट ए: BADBAZAAR की WHOIS क्लस्टरिंग / डोमेन ब्रोकर जानकारी के चित्र

चित्र 1 – 'UKYJYUJ'

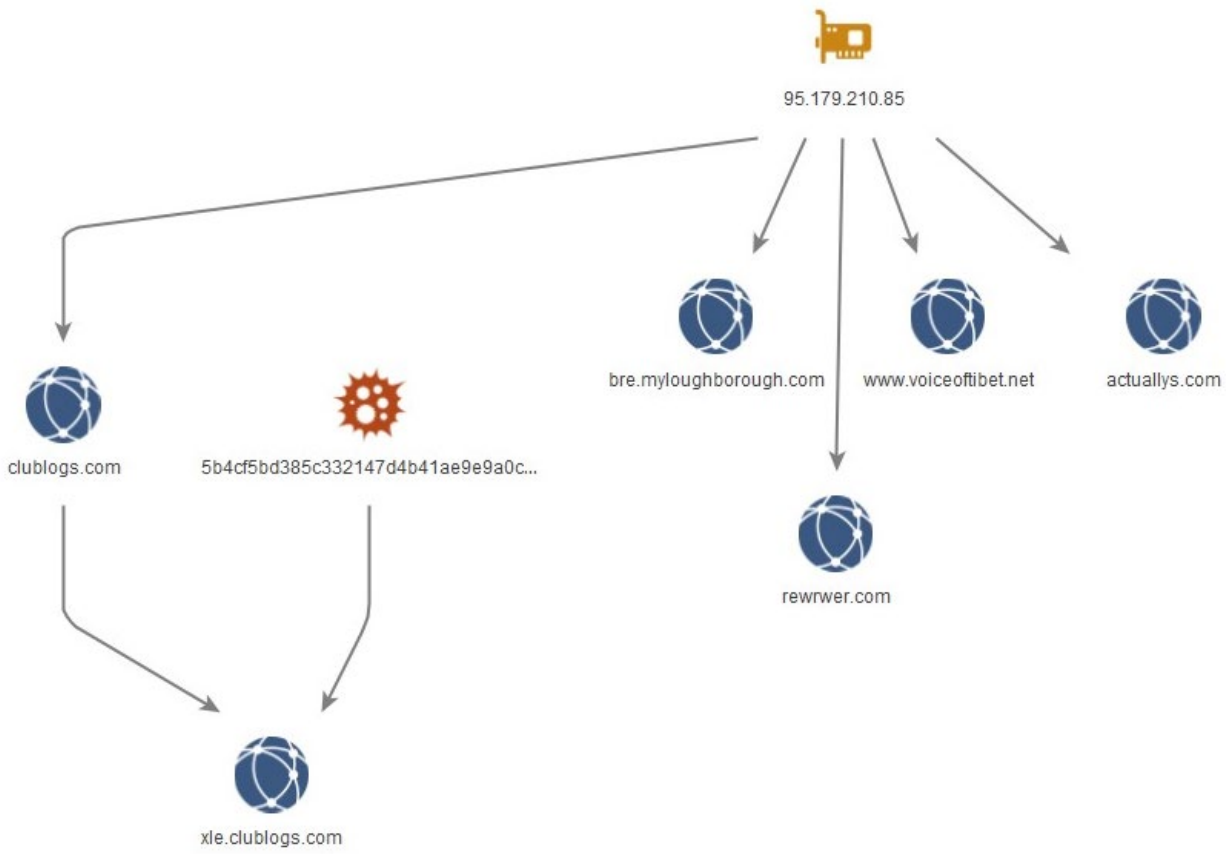


चित्र 2 – कीबोर्ड वॉकिंग वैल्यूज़

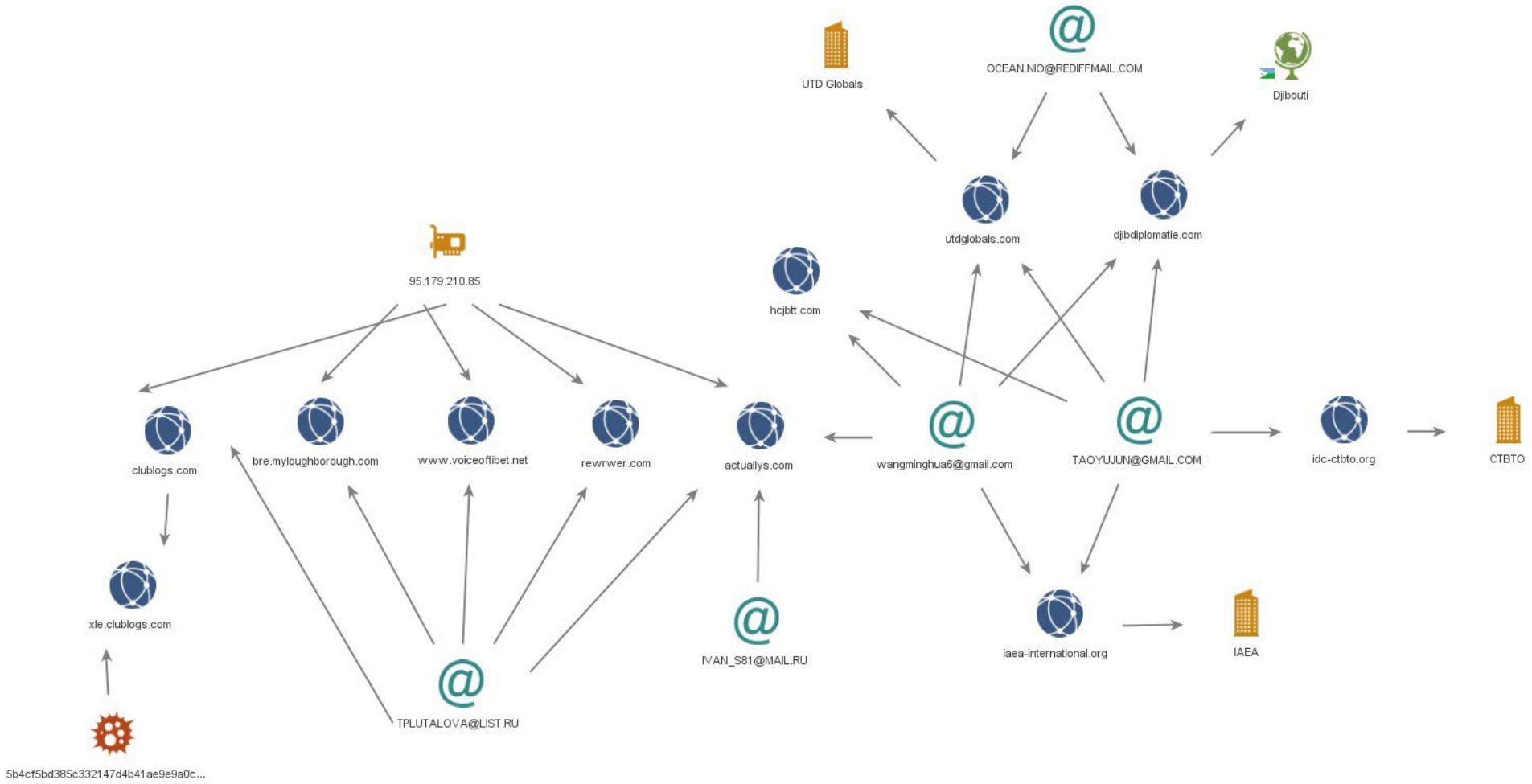


चित्र 3 – state फील्ड में 'FSDF' वैल्यू वाले अतिरिक्त डोमेन्स

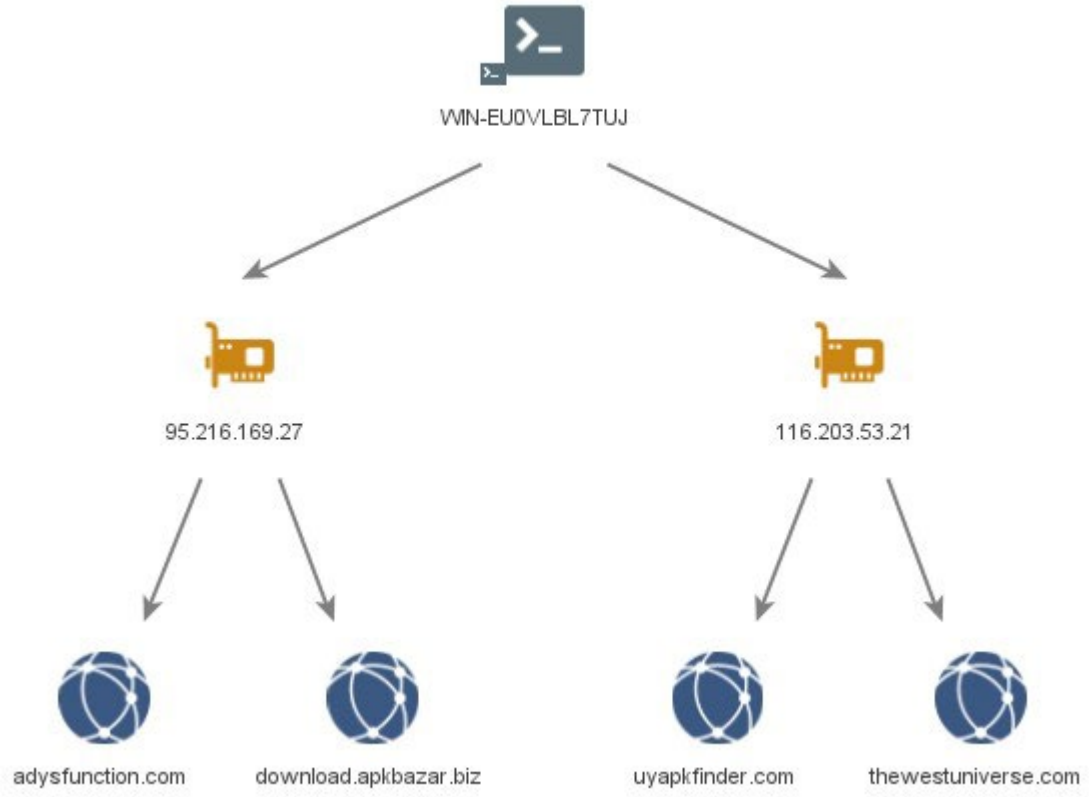
चित्र 4 – **95.179.210[.]85**



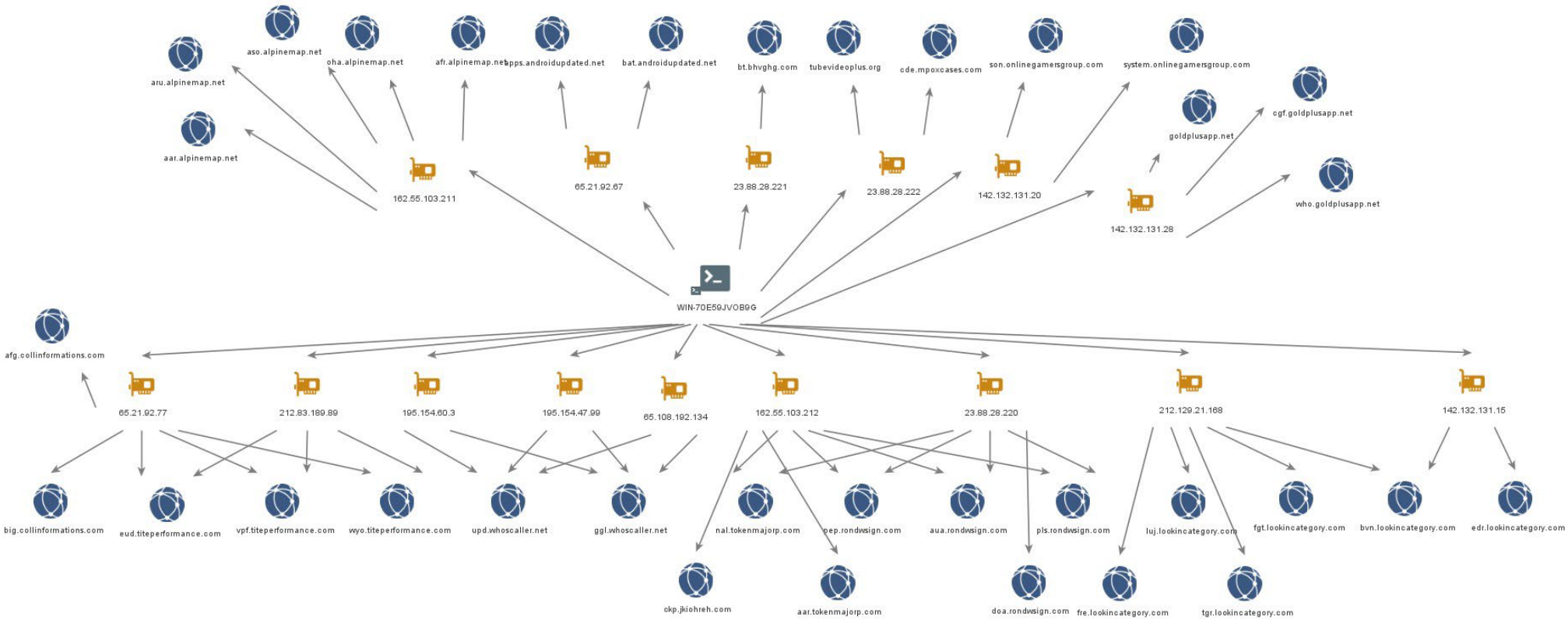
चित्र 5 – WHOIS लिंक्स



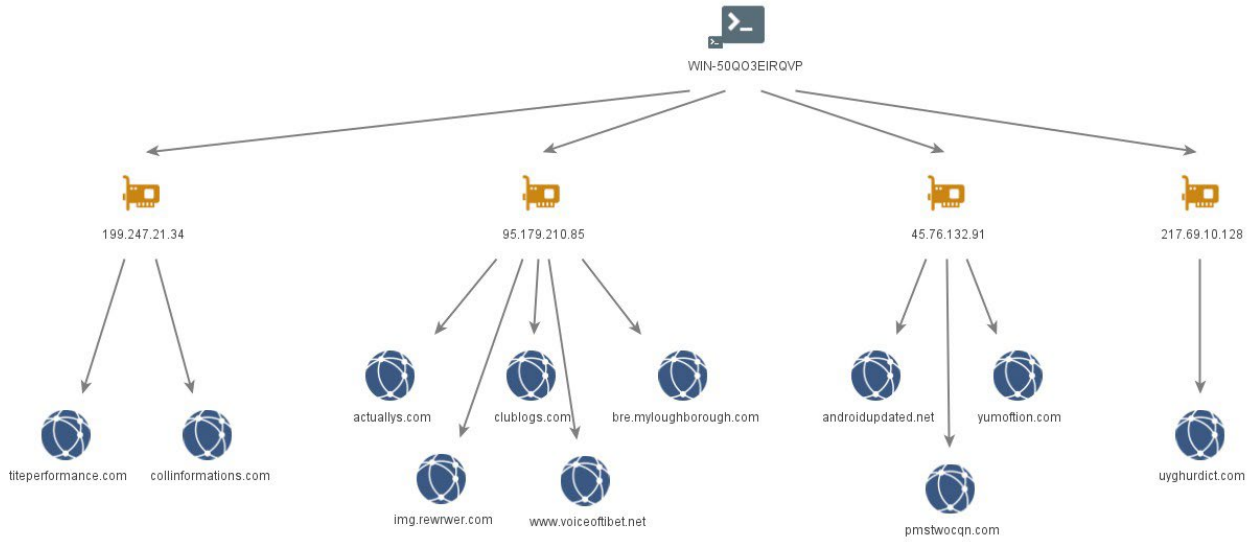
चित्र 6 – **WIN-EU0VLBL7TUJ**



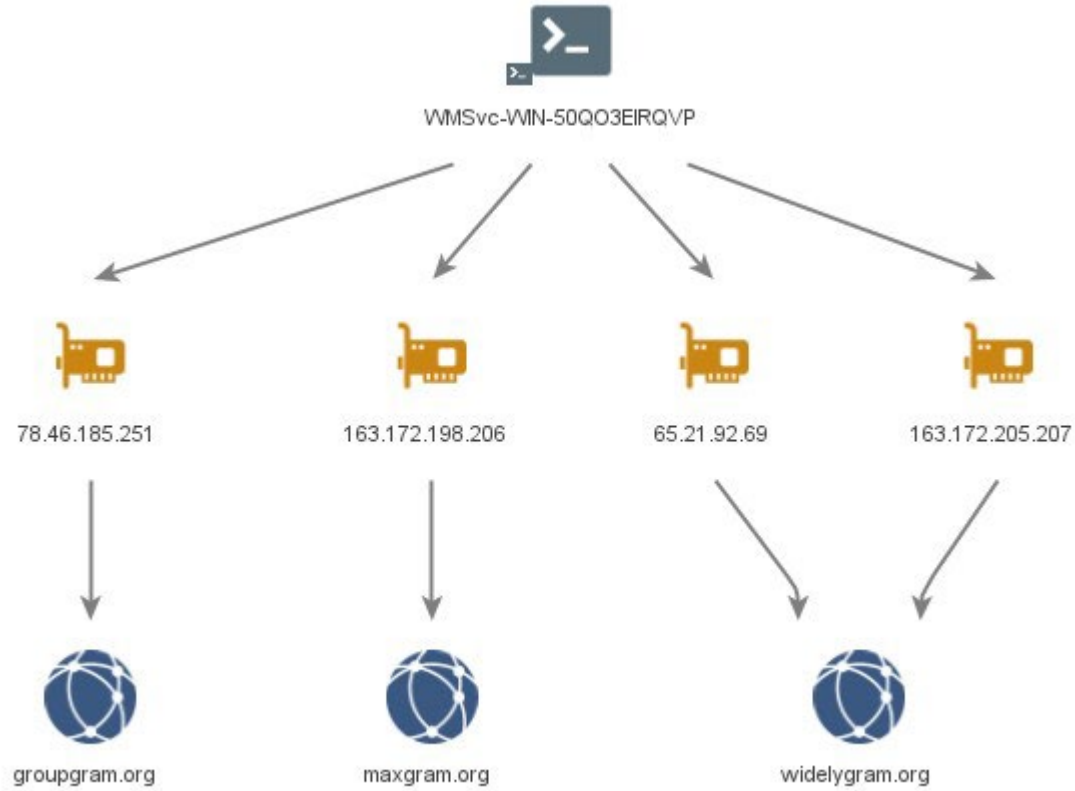
चित्र 7 – **WIN-70E59JVOB9G**



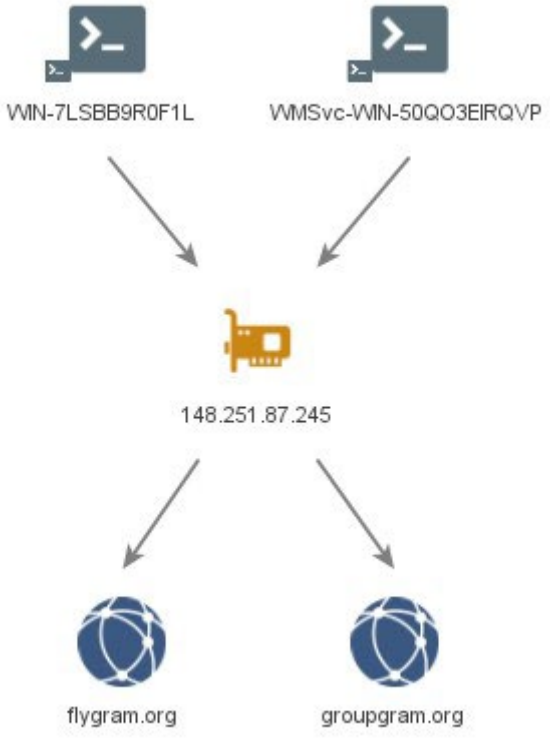
चित्र 8 - **WIN-50QO3EIRQVP**



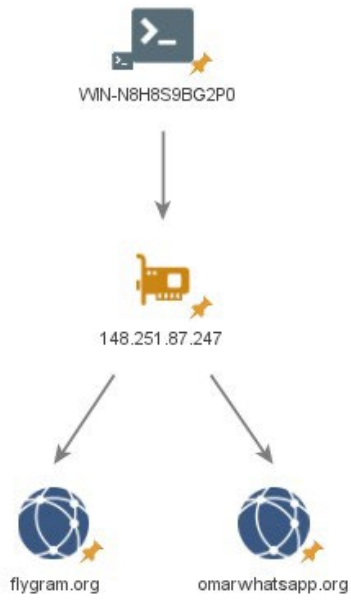
चित्र 9 - **VMSvc-WIN-50QO3EIRQVP**



चित्र 10 – **VMSvc-WIN-50QO3EIRQVP** and **WIN-7LSBB9R0F1L**



चित्र 11 - **WIN-N8H8S9BG2P0**



चित्र 12 – **WIN-I6VBN8MR92A**

परिशिष्ट बी: ध्यान में आए MOONSHINE व BADBAZAAR नमूने

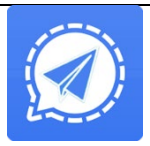
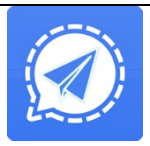
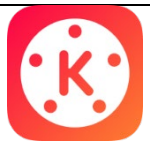
नीचे दी गई तालिका में पिछले दो वर्षों में MOONSHINE और BADBAZAAR अभियानों में उपयोग की गई ऐप्स की सूची दी गई है।

इनमें से कई ऐप्स भली-भांति स्थापित ऐप्स के साथ स्पष्ट रूप से समानता दिखाती हैं। इस बात की संभावना है कि यह प्रसिद्ध ब्रांडों को 'स्पूफ' करने के लिए हमलावर द्वारा जानबूझकर अपनाई गई तकनीक है।

यह नोट करना महत्वपूर्ण है कि ऐप का शीर्षक, पैकेज का नाम और ऐप का आइकन, ये सभी वास्तविक एप्लिकेशन की नकल या इससे मिलते-जुलते हो सकते हैं, और इसलिए केवल यह पहचान करने के लिए इसका उपयोग नहीं किया जाना चाहिए कि कोई डिवाइस संक्रमित है या नहीं।

ऐप का नाम	पैकेज का नाम	ऐप का आइकन
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	

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

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

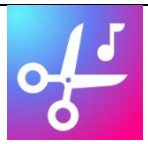
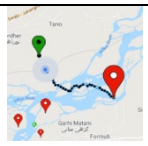
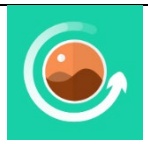
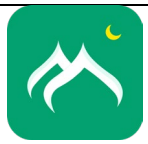
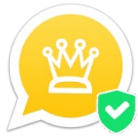
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra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

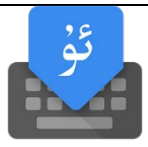
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video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

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

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

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

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

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

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

आगे पढ़ने के लिए सामग्री

ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र से मार्गदर्शन

- साइबर अपराध, घटना या कमजोरी के बारे में रिपोर्ट करें
- अपने डिवाइसेज़ को सुरक्षित कैसे करें
- अपना मोबाइल फोन सुरक्षित करें
- फिशिंग
- घोटाले
- अपने सोशल मीडिया को सुरक्षित करें
- सोशल मीडिया और मैसेजिंग ऐप्स की सुरक्षा के लिए सुझाव

यूके एनसीएससी और एनपीएसए की ओर से मार्गदर्शन

- लोकतंत्र की रक्षा
- सोशल मीडिया: इसका सुरक्षापूर्वक उपयोग कैसे करें
- संगठनों के लिए डिवाइस सुरक्षा मार्गदर्शन, जिसमें मोबाइल भी शामिल है
- एप्लिकेशन स्टोर्स में खतरों की रिपोर्ट।
- अधिक खतरे वाले व्यक्ति-विशेषों के लिए व्यक्तिगत सुरक्षा और संरक्षण

यूएस एनएसए की ओर से मार्गदर्शन

- मोबाइल डिवाइस के लिए सर्वोत्तम कार्यप्रथाएं

अस्वीकरण

कृपया ध्यान दें कि इस परामर्श-सूचना में प्रकाशन के समय प्रमाणित की गई जानकारी उपलब्ध कराई गई है।

यह रिपोर्ट संलेखन एजेंसी और उद्योग स्रोतों से प्राप्त जानकारी पर आधारित है। इसमें किसी भी निष्कर्ष और संस्तुति को सभी खतरों से बचाव के इरादे से प्रदर्शित नहीं किया गया है और संस्तुतियों का पालन करने से ऐसे सभी खतरे दूर नहीं होंगे। सिस्टम ओनर के लिए जानकारी के स्वामित्व से संबंधित खतरे हर समय मौजूद रहते हैं।

यूके में सूचना की स्वतंत्रता अधिनियम 2000 (एफओआईए) के तहत इस जानकारी के लिए अपवाद है और यूके के अन्य सूचना कानूनों के तहत भी इसके लिए अपवाद हो सकता है।

एफओआईए से संबंधित किसी भी पूछताछ को ncscinfoleg@ncsc.gov.uk पर भेजें।