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

Aviso

BADBAZAAR e MOONSHINE: Análise técnica e medidas de mitigação

9 de abril de 2025

BADBAZAAR e MOONSHINE: Análise técnica e medidas de mitigação

Resumo

Com o apoio do Reino Unido Cyber League, este aviso foi elaborado em conjunto pelo Centro Nacional de Segurança Cibernética (NCSC UK) e parceiros internacionais:

- **O Centro Australiano de Segurança Cibernética, parte da Direção Australiana de Sinais**
- **O Centro Canadiano para a Cibersegurança, parte do Estabelecimento de Segurança das Comunicações**
- **O Serviço Federal de Inteligência da Alemanha**
- **O Departamento Federal Alemão para a Proteção da Constituição**
- **O Centro Nacional de Segurança Cibernética da Nova Zelândia, parte do Gabinete de Segurança das Comunicações do Governo**
- **A Agência Federal de Investigação dos Estados Unidos**
- **A Agência de Segurança Nacional dos Estados Unidos**

Este aviso fornece informações atualizadas e compiladas sobre duas variantes de spyware conhecidas como BADBAZAAR e MOONSHINE, e inclui conselhos para operadores de lojas de aplicações, programadores e empresas de redes sociais para ajudar a manter os seus utilizadores seguros.

Este aviso está a ser publicado simultaneamente com um aviso para as vítimas deste malware.

Este documento utiliza a definição do glossário do NCSC para spyware: "Um tipo de malware que se instala num dispositivo sem o consentimento do utilizador, recolhendo dados e enviando-os a terceiros."

Estudo de caso um: MOONSHINE

MOONSHINE é um spyware para Android relatado em 2019 pelo Citizen Lab como almejando grupos tibetanos. O MOONSHINE se disfarça de uma aplicação legítima para induzir as vítimas a instalá-lo. Foi partilhado através de canais do Telegram e links enviados pelo WhatsApp.

A investigação do NCSC sobre o MOONSHINE indica o seguinte:

- O MOONSHINE usa uma interface que sofreu alterações desde que foi relatada pela primeira vez.
- A interface de gestão revela capacidades de vigilância extensas, incluindo a capacidade de extrair ficheiros de dispositivos, bem como capturar gravações áudio em tempo real e de ecrã.
- Um conjunto de interfaces de gestão MOONSHINE hospedadas virtualmente foi detectado. Essas interfaces têm infraestrutura sobreposta com painéis de login associados à UPSEC, que de acordo com Intelligence Online, refere-se à 'Sichuan Dianke Network Security Technology Co., Ltd.'.

Interface de gestão

Relatórios anteriores sobre as interfaces de gestão do MOONSHINE indicam que este passou por alterações, o que sugere um desenvolvimento contínuo.

O primeiro exemplo da interface de gestão consta no relatório do Citizen Lab de 2019.

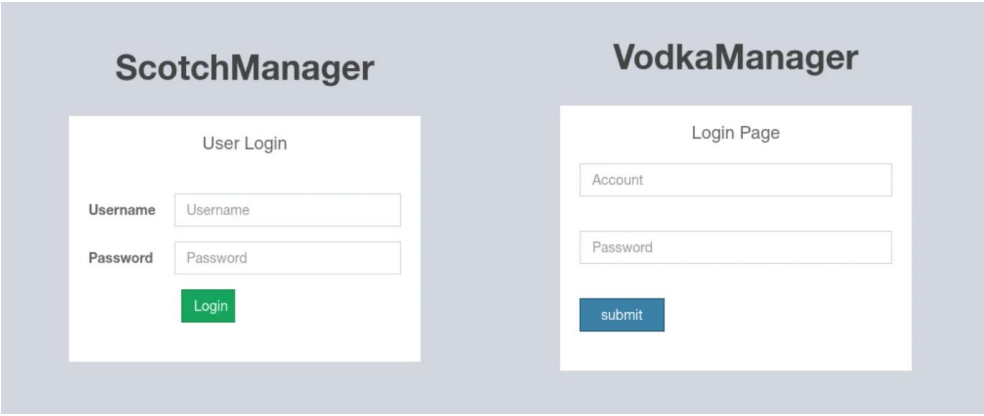


Figura 1: Interfaces de gestão MOONSHINE observadas no relatório do Citizen Lab de 2019 'Grupos Tibetanos Alvos de Explorações Móveis com um clique'.

No início de 2022, a Lookout divulgou uma interface de gestão diferente, a qual foi redesenhada para ter a aparência seguinte (substituindo as interfaces anteriores na figura 1):

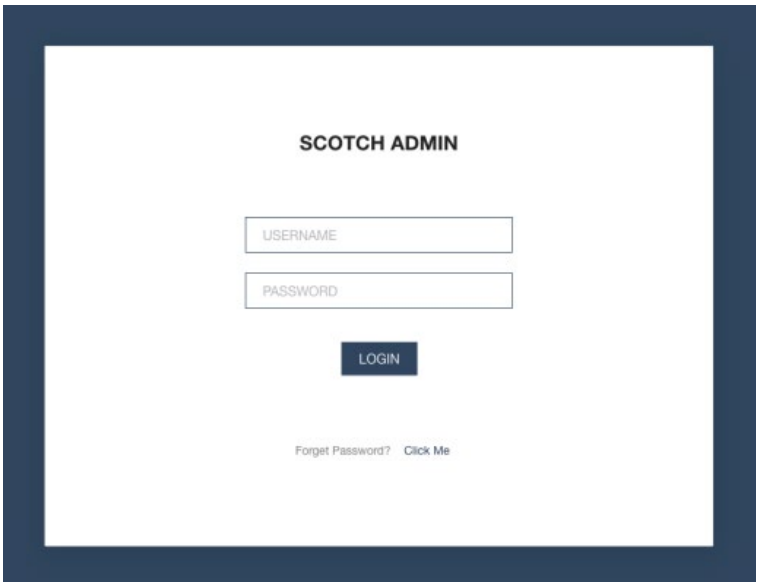


Figura 2: Interface de gestão do MOONSHINE vista no relatório 2022 da Lookout 'MOONSHINE: Evolução do Software de Vigilância Android da APT POISON CARP Chinesa para Almejar Tibetanos e Uigures'.

Em agosto de 2023, uma análise do comando e controlo (C2) do MOONSHINE revelou uma interface semelhante à de 2022, com a função **'Esqueci a palavra-passe'** já não disponível, como se pode ver na figura 2:

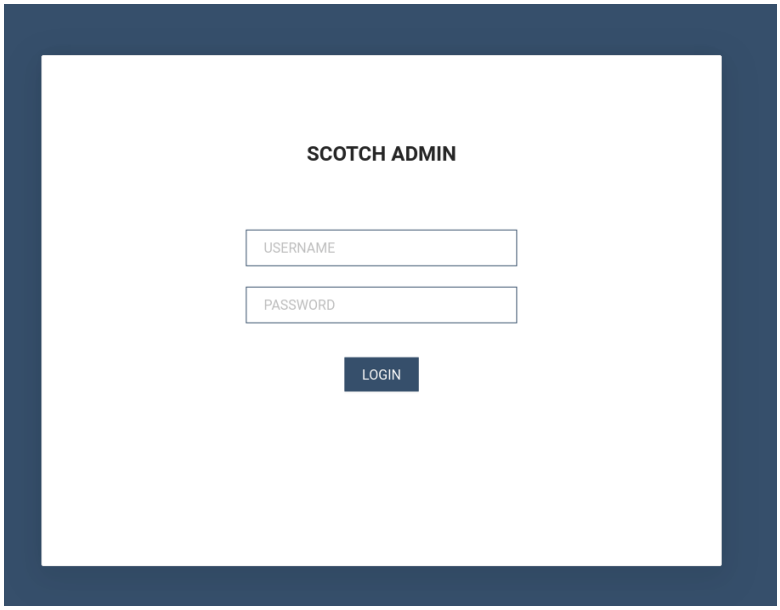


Figura 3: Interface de gestão do MOONSHINE observada em agosto de 2023, a qual já não apresenta a mensagem 'Esqueci a palavra-passe'.

Uma investigação mais aprofundada da interface de gestão mostrou conteúdo no painel que revelava como os detalhes dos dispositivos comprometidos seriam armazenados.

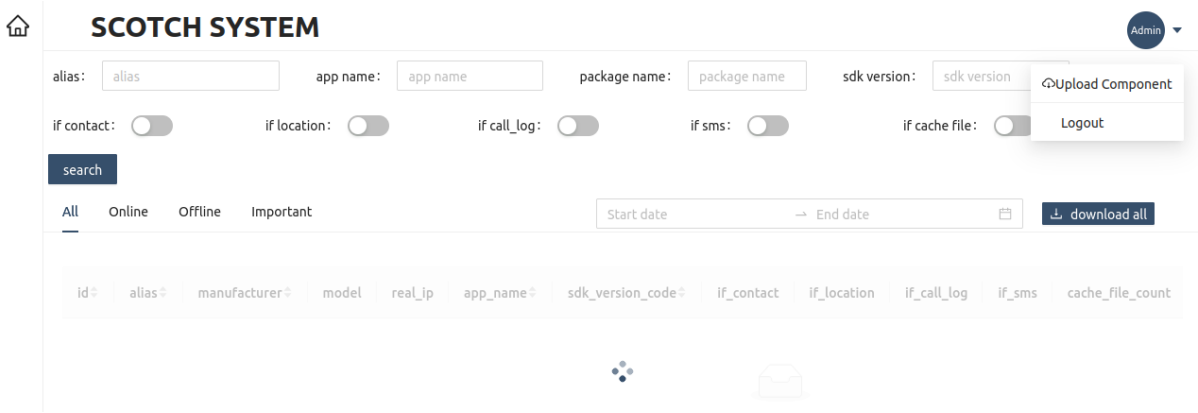


Figura 4: Página web por trás da página de login da interface de gestão do MOONSHINE.

A pesquisa da Lookout revelou a transmissão de uma **'pontuação'** do dispositivo da vítima para os servidores C2 do MOONSHINE. O valor da 'pontuação' baseia-se nas permissões da amostra maliciosa no dispositivo da vítima.

As colunas 'if_contact', 'if_location', 'if_call_log' e 'if_sms' na página sugerem que nem todas as amostras do MOONSHINE têm acesso total aos dispositivos comprometidos. O conhecimento dessas colunas e da 'pontuação' transmitida do dispositivo para o C2 sugere que os autores da ameaça estão a usar a pontuação para comunicar o nível de acesso que o malware tem ao dispositivo comprometido às pessoas que estão a aceder à interface de gestão.

Geralmente, a melhor prática para evitar que as aplicações recolham informações dos dispositivos é verificar as permissões da aplicação em busca de algo fora do comum antes de fazer o download. No entanto, as amostras do MOONSHINE solicitam permissões que são relevantes para a funcionalidade da aplicação, pelo que podem parecer inofensivas, mas também utilizam essas permissões para recolher informações dos dispositivos.

O MOONSHINE dispõe também de uma Interface de Programação de Aplicações (API) que revela a amplitude das suas capacidades. As versões anteriores da documentação da API continham nomes da API em mandarim.

Hóspedes virtuais

Em pesquisas por painéis do MOONSHINE, foram descobertas instâncias hospedadas virtualmente. Hospedagem virtual é quando um endereço IP pode hospedar vários sites ao mesmo tempo. Os endereços IP dessas instâncias hospedadas virtualmente e os domínios hospedados não foram observados em nenhuma amostra de malware conhecida.

Essas instâncias da interface de gestão eram diferentes, porque o título das páginas era **'LOGIN'** em vez do **'SCOTCH ADMIN'** como se viu anteriormente.

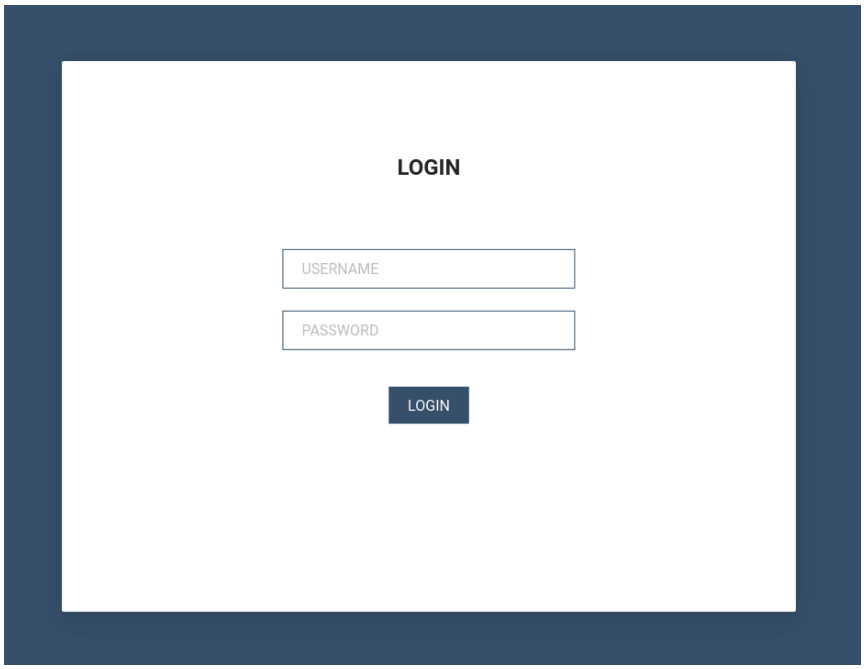


Figura 5: Interface de gestão do MOONSHINE utilizando o título LOGIN em vez de SCOTCH ADMIN.

Além disso, o conteúdo do painel também difere da figura 4, conforme se vê na figura 6:

Figura 6: Página web por trás da página de login da interface de gestão do MOONSHINE hospedada virtualmente.

O painel na figura 6 parece ser uma versão simplificada do painel na figura 4. As características sobrepostas dos painéis são os nomes das colunas 'id', 'fabricante' e 'modelo' na tabela.

As instâncias do MOONSHINE hospedadas virtualmente descobertas foram:

Domínio	Endereço IP
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

Esses domínios são listados pela Trend Micro como kits de exploração do MOONSHINE, responsáveis por explorar vulnerabilidades do navegador para instalar malware em dispositivos móveis. A Trend Micro designou este malware 'Dark Nimbus'.

Para esclarecer, as interfaces de gestão do MOONSHINE são aquelas com as quais as amostras de malware MOONSHINE comunicam e para as quais os dados das vítimas são exfiltrados. Os kits de exploração do MOONSHINE relatados pela Trend Micro são uma funcionalidade separada que explora vulnerabilidades do navegador para instalar um malware chamado Dark Nimbus em dispositivos móveis. Além disso, o Dark Nimbus e o MOONSHINE são malwares totalmente diferentes.

Tanto a interface de gestão do MOONSHINE como o kit de exploração do MOONSHINE têm código sobreposto, razão pela qual existem prompts de login semelhantes nas figuras 3 e 5, bem como o conteúdo da página nas figuras 4 e 6. Ambos também contêm a string 'webpackJsonpreact-scotchui' no código-fonte.

Os autores da ameaça criaram links de URL que se conectavam ao kit de exploração do MOONSHINE e, em seguida, redirecionavam para vídeos relevantes para tibetanos e uigures, o que coincide com o alvo do MOONSHINE.

Em muitos dos endereços IP que hospedam o domínio do kit de exploração do MOONSHINE, existe uma página de login intitulada 'VLiteUI' na porta 444. Esta página não é amplamente observada e a sua presença nestes IPs indica uma possível ligação às operações dos atores.

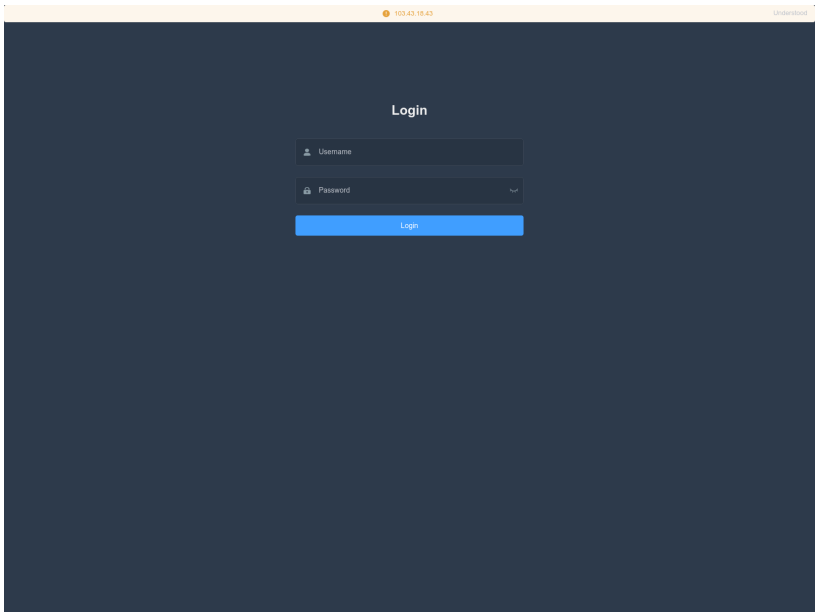


Figura 7: Painel de login com título HTML «VLiteUI» observado em IPs que também hospedam kits de exploração do MOONSHINE.

A análise do Dark Nimbus pela Trend Micro revelou que o malware pode recolher uma lista exaustiva de informações sobre o dispositivo e que comunica com o C2 utilizando o protocolo XMPP.

A Trend Micro também salienta que, em algumas versões do Dark Nimbus, identificou a prevalência da sequência 'DKNS'.

O **'ansec[.]com'** (listado como um Dark Nimbus C2 pela TrendMicro) também foi observado em serviços XMPP para outros endereços IP que servem páginas web com DKNS no título:

- DKNS Android远程取证系统 (Sistema Forense Remoto Android DKNS)
- DKNS云网侦控平台 (Plataforma de Investigação e Controlo de Redes Na Nuvem DKNS)
- DKNS 云网侦控平台 (Plataforma de Investigação e Controlo de Redes Na Nuvem DKNS)
- DKNS远程控制侦查系统 (Sistema de Investigação por Controlo Remoto DKNS)

Mais um conjunto de endereços de IP com '**ansec[.]com**' no serviço XMPP tinha páginas web com o título:

- UPSEC互联网控制指挥系统 (Sistema de Comando de Controlo da Internet UPSEC)
- UPSEC无线侦控系统 (Sistema de vigilância e controlo sem fios UPSEC)
- UPSEC重点人数据还原系统 (Sistema de restauração de dados de pessoa-chave UPSEC)

De acordo com Intelligence Online, 'UPSEC' observado nos títulos das páginas HTML referia-se à 'Sichuan Dianke Network Security Technology Co., Ltd'.

Estudo de caso dois: BADBAZAAR

O BADBAZAAR é um malware móvel com variantes para iOS e Android, cujo alvo são indivíduos uigures, tibetanos e taiwaneses. Este spyware é disseminado através de plataformas de redes sociais e lojas oficiais de aplicações. Relatórios recentes da Volexity mostram diferentes variantes do BADBAZAAR, designadas separadamente como BadSolar, BADBAZAAR e BadSignal. As três variantes estão interligadas por funções sobrepostas utilizadas para recolher informações sobre o dispositivo e o operador.

A investigação do NCSC sobre o BADBAZAAR revelou o seguinte:

- O agrupamento de domínios C2 revela mais ligações a domínios relatados em informações históricas sobre ameaças.
- Os servidores C2 e as amostras de malware revelam nomes de hóspedes associados à infraestrutura do ator.
- Outros perfis que os atores de ameaças utilizam para engenharia social, com o objetivo de espalhar o seu malware para além das lojas oficiais de aplicações.

Agrupamento WHOIS / corretor de domínios

'UJYJYUJ'

A análise dos registos WHOIS para o domínio BADBAZAAR **'signalplus[.]org'** (relatado por ESET) mostra o valor **'UJYJYUJ'** no campo **'Estado'**.

Uma pesquisa por outros domínios com o mesmo valor revela os seguintes domínios de interesse:

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

(Ver Anexo A, imagem 1)

Os domínios **signalplus[.]org**, **tubevideoplus[.]org** e **thetubeplus[.]com** são reportados como domínios C2 do BADBAZAAR, enquanto ESET reporta o subdomínio **mail.pmumail[.]com** como um servidor proxy FlyGram. O FlyGram é uma aplicação BADBAZAAR desenvolvida por cibercriminosos maliciosos (consulte o apêndice para obter uma lista de outras aplicações BADBAZAAR).

Valores de deslocamento do teclado

O NCSC também observou padrões semelhantes de teclas digitadas em outros domínios C2 registados do BADBAZAAR.

Por exemplo, todos os domínios a seguir têm o valor **'REWR'** observado no campo **'Estado'** (conforme usado anteriormente):

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

(Ver Anexo A, imagem 2)

Domínios com valores de campo de estado 'FSDF'

Outro conjunto de domínios BADBAZAAR C2 tem o valor **'State' 'FSDF'**:

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

(Ver Anexo A, imagem 3)

Relatórios históricos com valores de deslocamento do teclado

O uso de valores de navegação por teclado nos registos WHOIS dos domínios BADBAZAAR também pode ser observado em casos historicamente relatados de ataques a organizações tibetanas por TA413. Recorded Future observou domínios controlados por atores que falsificam organizações tibetanas e o uso do valor **'asfasf'** como organização registante.

clublogs[.]com

As amostras do BADBAZAAR obtidas pela Lookout continham '**xle.clublogs[.]com'** como domínio C2 O domínio raiz '**clublogs[.]com**' estava alojado no endereço IP '**95.179.210[.]85**' e tinha um certificado SSL com o assunto e o valor do emissor '**CN=WIN-50QO3EIRQVP**'. Este valor corresponde aos certificados SSL encontrados nas amostras do BADBAZAAR, que utilizavam o SSL pinning para evitar a intercepção das comunicações.

A história de alojamento do endereço IP **95.179.210[.]85** retorna os seguintes domínios de interesse:

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

(Ver Anexo A, imagem 4)

www.voiceoftibet[.]net

O domínio **'www.voiceoftibet[.]net'** parece estar a mascarar-se como a estação de rádio 'Voice of Tibet', semelhante ao TTP utilizado pelo TA413.

O domínio **'rewrwer[.]com'** é semelhante ao valor '**Estado**' anteriormente identificado como '**REWR'** nos registos WHOIS dos domínios BADBAZAAR.

Os domínios '**clublogs[.]com**', '**rewrwer[.]com**', '**voiceoftibet[.]net**' e '**myloughborough[.]com**' estavam todos registados com endereço eletrónico '**tplutalova@list[.]ru**'.

actuallys[.]com

Os registos WHOIS para '**actuallys[.]com**' mostraram um caso em que os endereços de e-mail técnico e administrativo eram '**actuallys[.]com**', mas o e-mail do registante era '**ivan_s81@mail[.]ru**'.

As informações históricas do WHOIS para o domínio '**actuallys[.]com**' revelaram o e-mail de registo '**wangminghua6@gmail[.]com**' listado a 24 de fevereiro de 2016. Em 11 de março de 2016, o e-mail foi subsequentemente alterado para '**ivan_s81@mail.ru**', embora a data de expiração do registo do registador permanecesse a mesma.

wangminghua6@gmail[.]com

O endereço de e-mail '**wangminghua6@gmail[.]com**' foi utilizado para registar domínios encontrados em relatórios históricos de inteligência sobre ameaças. Em 2015, a Palo Alto identificou o e-mail usado para registar domínios C2 do malware, Cmstar. Em 2014, também foi usado para registar domínios identificados pela

Mandiant em campanhas de phishing conduzidas por APT3. Em 2013, foi usado para registar domínios encontrados pela CrowdStrike num dropper de malware com um caminho do banco de dados de programas (PDB) que contém caracteres chineses. Isso sugere uma compilação num sistema chinês.

taoyujun@gmail[.]com

O domínio '**hcjbtt[.]com**' está registado com o endereço de e-mail '**taoyujun@gmail[.]com**', mas o e-mail do seu administrador está registado com '**wangminghua6@gmail[.]com**'.

Não há nenhuma atividade maliciosa associada ao domínio '**hcjbtt[.]com**', no entanto o endereço de e-mail '**taoyujun@gmail[.]com**' foi encontrado em relatórios históricos de inteligência sobre ameaças. Em 2014, foi usado para registar um domínio encontrado pela Mandiant em amostras do '**Cueisfry Trojan**' utilizadas para almejar organizações japonesas.

O endereço de e-mail também registou domínios como '**iaea-international[.]org**', que parecia mascarar-se como a **International Atomic Energy Agency**, e '**idc-ctbto[.]org**', mascarando-se como o **International Data Centre** da **Organização do Tratado de Proibição Total de Testes Nucleares (CTBTO).**

Um registo Whois anterior para o domínio '**iaea-international[.]org**' mostrava o e-mail do registante como '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Observou-se que o domínio '**udtglobals[.]com**' utilizava '**wangminghua6@gmail[.]com**' como e-mail do administrador e '**ocean.nio@rediffmail[.]com**' como endereço de e-mail do registante. Outros registos WHOIS para este domínio mostravam o mesmo e-mail do registante, mas com o endereço de e-mail do administrador '**taoyujun@gmail[.]com**'.

'**udtglobals[.]com**' parecia estar a mascarar-se como '**UDT Global**', que é um evento global para empresas de defesa e segurança submarina. O nome de utilizador '**ocean.nio'** no endereço de e-mail pode estar a imitar o **Instituto Nacional de Oceanografia (NIO)**, que existe em vários países. Embora o uso do serviço de e-mail **'Rediff'** (com sede na Índia) possa sugerir uma imitação do **Instituto Nacional de Oceanografia da Índia**.

Djibdiplomatie[.]com

O domínio '**djibdiplomatie[.]com**' parecia mascarar os serviços diplomáticos do Djibuti, apresentando um registo WHOIS semelhante ao '**utdglobals[.]com'.** Um registo parecia indicar o registante **'ocean.nio@rediffmail[.]com'** e o administrador **'taoyujun@gmail[.]com'**, enquanto outros registos indicavam '**wangminghua6@gmail[.]com**' como endereço de e-mail do administrador e '**ocean.nio@rediffmail[.]com**' como endereço de e-mail do registante.

Ambos os domínios também apresentavamvalores do tipo keyboard walking nos registos WHOIS. Por exemplo, '**udtglobals[.]com**' tem o valor **'ASDF'** como cidade do seu registante e '**djibdiplomatie[.]com**' tem '**DAF DAGF**' como valor do nome do registante. Isso é comparável aos valores observados em outros domínios BADBAZAAR.

Embora os endereços de e-mail '**wangminghua6@gmail[.]com**' e '**taoyujun@gmail[.]com**' sejam encontrados nos registos WHOIS de domínios mascarados como um **evento global de defesa submarina, serviços diplomáticos do Djibuti** e a **Agência Internacional de Energia Atómica**, eles estão também nos registos WHOIS de vários domínios não maliciosos.

A mistura de domínios mascarados e domínios não maliciosos pode sugerir a existência de uma entidade de aquisição de infraestrutura usada para apoiar as operações dos cibercriminosos.

O endereço de e-mail **'ocean.nio@rediffmail[.]com'** só é encontrado nos domínios mascarados descritos acima. '**ivan_s81@mail[.]ru**' e '**tplutalova@list[.]ru**' registaram um número muito pequeno de domínios, respetivamente, e alguns desses domínios foram hospedados na infraestrutura BADBAZAAR. Pensa-se que estes três endereços de e-mail estejam mais intimamente ligados às operações dos cibercriminosos. Isso é porque um número maior de domínios com os quais estão associados está ligado a atividades maliciosas, em comparação com os e-mails '**wangminghua6@gmail[.]com**' e '**taoyujun@gmail[.]com**'.

(Ver Anexo A, imagem 5)

Ligações com outros atores de ameaças

Outra característica comum dos domínios ligados ao BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', e '**voiceoftibet[.]net**' é que todos eles foram registados na eNom e tinham sido 'estacionados' em '**255.255.255[.]254**'

Na sequência de investigações anteriores do NCSC, outros domínios com estas características revelaram atividade ligada ao **APT5** em 2019 e ao **APT14** entre 2009 e 2011

Os domínios ligados ao APT5 tinham registos WHOIS históricos que indicavam **'taoyujun@gmail[.]com'** como endereço de e-mail do registante.

Os domínios ligados ao APT14 tinham subdomínios de três letras que pareciam representar o alvo pretendido das suas operações maliciosas. Um exemplo disso é **'bae.cisconline[.]net'**, que sugeria um ataque destinado à BAE Systems e foi encontrado numa amostra '**Poison Ivy**'.

Uma característica semelhante é observada nos domínios do BADBAZAAR, onde os subdomínios estão relacionados com o nome da aplicação trojanizada:

Título da aplicação	URL de C2
Muslim Pro	**mpp**.pmstwocqn[.]com
Reprodutor de vídeo para Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Rádio Afeganistão	**afg**.collinformations[.]com
Dicionário IN-UG gratuito	**eud**.titeperformance[.]com
Recuperação de vídeo em disco	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

É importante notar que as atividades relacionadas com o APT5 e o APT14 são históricas e que existiam também outros domínios registados na eNom e resolvidos para **'255.255.255.254'** que não podem ser associados a atividades maliciosas. Portanto, não é certo que os atores por trás dessas campanhas sejam os mesmos ou estejam relacionados.

Nomes das máquinas

A análise dos C2s e das amostras do BADBAZAAR revelou nomes de host usados como valor de 'Nome comum' nos certificados SSL. As investigações do NCSC sobre os nomes de hosts observados nas amostras e na infraestrutura do BADBAZAAR revelaram que esses nomes de hosts são usados em vários endereços IP. Esses endereços IP estão a hospedar domínios encontrados em amostras do BADBAZAAR. Existem mais detalhes na secção seguinte sobre os nomes de hosts e endereços IP com o nome de host que hospeda os domínios C2 do BADBAZAAR.

Em quase todos os casos, a presença de certificados com o valor do nome do host sobrepõe-se às resoluções IP para os nomes de domínio maliciosos especificados, os poucos casos em que isso não ocorreu foram delineados.

WIN-EU0VLBL7TUJ

O nome de host '**WIN-EU0VLBL7TUJ**' foi observado nos seguintes endereços IP de interesse:

- '**116.203.53[.]21**' hospedou domínios do BADBAZAAR C2 '**uyapkfinder[.]com**' e '**thewestuniverse[.]com**'.
- **'95.216.169[.]27**' hospedou domínios do BADBAZAAR C2 '**adysfunction[.]com'** e sub-domínio '**download.apkbazar[.]biz**' observado como um link de download para uma amostra do BADBAZAAR.

(Ver Anexo A, imagem 6)

WIN-70E59JVOB9G

O nome de host **'WIN-70E59JVOB9G'** foi observado nos seguintes endereços IP de interesse:

- '**23.88.28[.]220**' hospedou os subdomínios C2 do BADBAZAAR, **'aua.rondwsign[.]com',** **'nal.tokenmajorp[.]com',**

‘pep.rondwsign[.]com’ ‘**doa.rondwsign[.]com**’, e **‘pls.rondwsign[.]com’.** Houve um período de dois dias entre a última vez que o certificado associado à máquina foi visto e a primeira vez que os domínios maliciosos foram vistos a resolver para o IP.

- ‘**23.88.28[.]221**’ hospedou o subdomínio vinculado ao BADBAZAAR ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222**’ hospedou domínios C2 do BADBAZAAR ‘**tubevideoplus[.]org**’ e ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67**’ hospedou o subdomínio C2 do BADBAZAAR ‘**bat.androidupdated[.]net**’. Também hospedou o subdomínio ‘**apps.androidupdated[.]net**’ que é um DoubleAgent malware C2.

- ‘**65.21.92[.]77**’ hospedou os subdomínios C2 do BADBAZAAR ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ e ‘**afg.collinformations[.]com**’

- ‘**65.108.192[.]134**’ hospedou os subdomínios C2 do BADBAZAAR ‘**upd.whoscaller.net**’. e ‘**ggl.whoscaller[.]net**’.

- ‘**142.132.131[.]15**’ hospedou os subdomínios C2 do BADBAZAAR ‘**bvn.lookincategory[.]com’** e ‘**edr.lookincategory[.]com’.** Houve um período de onze dias entre a última vez que o certificado com o nome da máquina foi visto e a primeira vez que os domínios maliciosos foram vistos a resolver para o IP.

- **‘142.132.131[.]20’** hospedou os subdomínios ‘**son.onlinegamersgroup[.]com’** e ‘**system.onlinegamersgroup[.]com’,** que se julga serem C2s do BADBAZAAR porque foram hospedados enquanto certificados SSL associados ao BADBAZAAR foram observados no IP.

- ‘**142.132.131[.]28’** hospedou o domínio C2 do BADBAZAAR ‘**goldplusapp[.]net**’ e sub-domínios ‘**who.goldplusapp[.]net**’ e ‘**cgf.goldplusapp[.]net**’.

- ‘**162.55.103[.]211**’ hospedou os subdomínios Cdo BADBAZAAR ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, e ‘**aar.alpinemap[.]net**’.

- ‘**162.55.103[.]212**’ hospedou os subdomínios C2 do BADBAZAAR **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** e **‘aua.rondwsign[.]com’.**

- ‘**195.154.47[.]99**’ hospedou os subdomínios C2 do BADBAZAAR ‘**ggl.whoscaller[.]net**’ e ‘**upd.whoscaller.net**’. Houve um período de três dias entre o momento em que o certificado com o nome da máquina foi visto pela primeira vez e o momento em que os domínios maliciosos foram vistos pela última vez a resolver para o IP.

- ‘**195.154.60[.]3**’ hospedou os subdomínios C2 do BADBAZAAR ‘**upd.whoscaller[.]net**’
‘**ggl.whoscaller[.]net**’.

- ‘**212.83.189[.]89**’ hospedou os subdomínios C2 do BADBAZAAR ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ e ‘**afg.collinformations[.]com**’.

- ‘**212.129.21[.]168**’ hospedou os domínios C2 do BADBAZAAR, ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ ed ‘**bvn.lookincategory[.]com**’.

(Ver Anexo A, imagem 7)

WIN-50QO3EIRQVP

O nome de host '**WIN-50QO3EIRQVP**' foi observado nos seguintes endereços IP de interesse:

- '**45.76.132[.]91**' hospedou domínios, '**yumoftion[.]com**', '**androidupdated[.]net**'. Ambos os domínios estão ligados ao BADBAZAAR como subdomínios '**fow.yumoftion[.]com**' e '**bat.androidupdated[.]net**' são domínios C2 do BADBAZAAR. Além disso, o subdomínio '**apps.androidupdated[.]net**' é um domínio C2 do DoubleAgent. Também hospeda o domínio '**pmstwocqn[.]com**' ligado ao BADBAZAAR por meio de registos WHOIS.

- '**95.179.210[.]85**' hospedou '**clublogs[.]com**', do qual '**xle.clublogs[.]com**' é um domínio C2 do BADBAZAAR e também hospedou domínios ligados ao BADBAZAAR '**bre.myloughborough[.]com**', '**img.rewrwer[.]com**', '**www.voiceoftibet[.]net**' e '**actuallys[.]com**'.

- '**199.247.21[.]34**' hospedou '**titeperformance[.]com**', e '**collinformations[.]com'** cujos subdomínios são domínios C2 do BADBAZAAR.

- '**217.69.10[.]128**' hospedou o domínio C2 do BADBAZAAR '**uyghurdict[.]com**'.

(Ver Anexo A, imagem 8)

WMSvc-WIN-50QO3EIRQVP

O nome de host '**WMSvc-WIN-50QO3EIRQVP**' foi observado nos seguintes endereços IP de interesse:

- **'78.46.185[.]251'** hospedou o domínio C2 do BADBAZAAR **'groupgram[.]org'**, relatado pela Volexity como utilizando a porta 4432 para conexões maliciosas.

- **‘65.21.92[.]69’** e **‘163.172.205[.]207’** hospedaram o domínio **‘widelygram[.]org’** que se julga ser um domínio C2 do BADBAZAAR, porque, quando foi hospedado em ambos os IPs, a porta 4432 estava aberta.

- **‘163.172.198[.]206’** hospedou o domímio **‘maxgram[.]org’** que se julga ser um domínio C2 do BADBAZAAR, porque, quando estava a ser hospedado a porta 4432 estava aberta.

(Ver Anexo A, imagem 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Os nomes de host ‘**WMSvc-WIN-50QO3EIRQVP**’ e ‘**WIN-7LSBB9R0F1L**’ foram observados simultaneamente nos seguintes endereços de IP:

- ‘**148.251.87[.]245**’ hospedou os domínios C2 do BADDBAZAAR ‘**flygram[.]org**’ e ‘**groupgram[.]org**’.

(Ver Anexo A, imagem 10)

WIN-N8H8S9BG2P0

O nome de host ‘**WIN-N8H8S9BG2P0**’ foi observado nos seguintes endereços IP de interesse:

- ‘**148.251.87[.]247**’ hospedou os domínios C2 do BADDBAZAAR ‘**omarwhatsapp[.]org**’ e ‘**flygram[.]org**’.

(Ver Anexo A, imagem 11)

WIN-I6VBN8MR92A

O nome de host ‘**WIN-I6VBN8MR92A**’ foi observado nos seguintes endereços IP de interesse:

- **148.251.87[.]197**’ hospedou o domínio C2 do BADBAZAAR ‘**tryhrwserf[.]com**’.

(Ver Anexo A, imagem 12)

A prevalência desses nomes de máquinas na Internet varia com base nos dados comerciais disponíveis. Algumas delas são observadas simultaneamente em vários endereços IP o que indica que as VMs estão a ser criadas a partir do mesmo modelo. É importante notar que, para alguns dos nomes de host, nem todos os IPs nos quais eles foram observados podem ser associados a atividades maliciosas. Isso pode significar que o uso dos nomes de host não é exclusivo desses atores de ameaças.

Porém, a prevalência de alguns desses nomes de máquinas em IPs que hospedaram domínios C2 do BADBAZAAR pode sugerir que uma entidade de aquisição de infraestrutura está a ser usada para configurar máquinas com o objetivo de apoiar as operações cibernéticas dos atores maliciosos.

Presença nas redes sociais

Relatórios anteriores da Volexity mostraram que os vídeos do YouTube (que promovem o uso de aplicações maliciosas) foram criados por cibercriminosos. Esses vídeos incluíam tutoriais sobre como usar as aplicações desenvolvidas.

O NCSC descobriu dois canais adicionais no YouTube associados às operações dos atores da ameaça. O YouTube canal com o identificador de URL '**@josephjoey3499**' parecia estar a promover a utilização do '**Maxgram**' e um adicional canal registado com '**@uyghurapks3096**' promove o '**Uyghur APK Finder**'.

Além disso, vídeos do YouTube que promovem o '**Flygram**' e '**Signal Plus**', mostraram os autores das ameaças usando números de telefone visíveis. No '**Flygram**' video, aos 0:36, o número de telefone '**+1 (570) 378-7250**' é visível e no '**Signal Plus**' video, o número de telefone '**+1 (267) 298 4259**' é revelado.

A Volexity denunciou um site de notícias falso com temática tibetana, chamado '**ignitetibet[.]net**', que eles descobriram em canais do Telegram que se julga serem operados pelos autores da ameaça. O endereço eletrónico '**choekyi.wangmo@ignitetibet[.]net**' foi observado a deixar comentários em publicações na página '**tibetone.org**' que foi publicamente denunciada pela Lookout como uma página C2 utilizada para a variante iOS do BADBAZAAR.

Acredita-se que este endereço eletrónico seja controlado pelos atores, usando a persona de '**Choekyi Wangmo**'.

Avaliação

O BADBAZAAR e o MOONSHINE utilizam vários métodos de engenharia social para visar especificamente as comunidades uigur, tibetana e taiwanesa, nomeadamente:

- a trojanização de aplicações de interesse para essas comunidades, como uma aplicação do Alcorão em língua uigur, é quase certamente adaptada à base de vítimas-alvo.
- a adição destas aplicações trojanizadas às lojas oficiais de aplicações muito provavelmente confere uma sensação de legitimidade, e a partilha em conversas em grupo tem provavelmente como objetivo explorar as relações de confiança dentro dessas comunidades .

O BADBAZAAR e o MOONSHINE recolhem dados que certamente seriam valiosos para o Estado chinês. Embora o BADBAZAAR e o MOONSHINE tenham sido observados a atacar indivíduos uigures, tibetanos e taiwaneses, existem outros malwares que atacam outros grupos minoritários na China. Os cidadãos das nações co-guardiões, na China e no exterior, que são considerados apoiantes de causas que ameaçam a estabilidade do regime, estão quase certamente sob ameaça de malware móvel, como o BADBAZAAR e o MOONSHINE. A capacidade de capturar dados de localização, áudio e fotos certamente oferece a oportunidade de informar futuras operações de vigilância e assédio, fornecendo informações em tempo real sobre a atividade do alvo.

MITRE ATT&CK®

Este relatório foi compilado com base na estrutura MITRE ATT&CK®, uma base de conhecimento globalmente acessível sobre táticas e técnicas adversárias com base em observações do mundo real.

Tática	ID	Técnica	Procedimento
Reconhecimento	T1593.001	Pesquisar Sites/Domínios Abertos: Redes Sociais	Os atores encontram grupos e fóruns online que correspondem às suas vítimas pretendidas para partilhar o malware.
Desenvolvimento de Recursos	T1583.001	Adquirir Infraestrutura: Domínios	Os atores registam domínios para os seus servidores de comando e controlo
Desenvolvimento de Recursos	T1587.001	Desenvolver capacidades: Malware	Código malicioso é escrito para ser inserido em aplicações trojanizadas.
Desenvolvimento de Recursos	T1608.001	Capacidades da cena: Carregar Malware	Aplicações trojanizadas são carregadas em plataformas online, incluindo lojas de aplicações.
Desenvolvimento de Recursos	T1585.001	Criar Contas: Contas de Redes Sociais	Os atores criam contas em sites e redes sociais para partilhar e divulgar o malware.
Desenvolvimento de Recursos	T1585.002	Criar Contas: Contas de e-mail	Os atores utilizam contas de e-mail privadas e comerciais para hospedar e partilhar malware.
Acesso Inicial	T1189	Ataque drive-by	Scripts maliciosos são ocultados em aplicações aparentemente legítimas e enviados para lojas de aplicações.
Acesso Inicial	T1566.003	Phishing: Spearphishing através do Serviço	Os atores enviam aplicações trojanizadas para grupos específicos através das redes sociais, incluindo o Telegram.
Execução	T1204.002	Execução do utilizador: Ficheiro Malicioso	As vítimas têm de instalar as aplicações trojanizadas para executar a carga útil.

Evasão da defesa	T1027.009	Ficheiros ou informações ofuscados: Cargas Incorporadas	A carga maliciosa está escondida em aplicações que, de outra forma, seriam legítimas.
Evasão da defesa	T1036.005	Disfarce: Corresponder ao nome ou localização legítimos	Os ficheiros trojanizados correspondem ao nome, aparência e função de aplicações legítimas.
Evasão da defesa	T1656	Identidade falsificada	Os atores fazem-se passar por pessoas de confiança criando sites falsos e usando nomes de utilizador associados aos grupos-alvo.
Recolha	T1123	Captura de áudio	As aplicações trojanizadas podem pedir permissões desnecessárias, incluindo acesso ao microfone.
Recolha	T1125	Captura de vídeo	As aplicações trojanizadas podem pedir permissões desnecessárias, incluindo acesso às câmeras.
Recolha	T1005	Dados do sistema local	As aplicações trojanizadas podem pedir permissões desnecessárias, incluindo ficheiros locais.
Comando e Controlo	T1071.001	Protocolo da camada de aplicação: Protocolos da Web	O malware liga-se ao C2 utilizando HTTPS e WebSockets.
Comando e Controlo	T1509	Porta não padrão	São usadas portas não-padrão como porta 4432 e 2333
Exfiltração	T1041	Exfiltração através do canal C2	O malware exfiltra dados utilizando ligações HTTPS e WebSocket.
Impacto	T1565.002	Manipulação de dados: Manipulação de dados transmitidos	Os atores obtêm dados das vítimas ativando o tráfego da web do aplicativo que não é necessário para o funcionamento do aplicativo.

Indicadores:

MOONSHINE:

- Em 1 de abril de 2025, uma pesquisa por painéis VLiteUI retornou o seguinte:

Endereço IP	Porta	Visto pela primeira vez	Visto pela última vez
103.254.108[.]87	888	2024-10-17	2025-02-14
43.159.192[.]7	444	2024-11-21	2025-02-13
103.27.109[.]109	444	2024-07-11	2025-02-07
45.119.99[.]83	444	2024-12-26	2025-01-24
103.254.108[.]76	444	2024-09-12	2024-12-05
194.71.107[.]160	444	2023-12-10	2024-11-01
103.254.108[.]108	444	2023-11-12	2024-09-25
103.56.17[.]194	444	2024-04-03	2024-08-23
103.254.108[.]87	444	2023-11-14	2024-08-15
62.72.58[.]168	444	2024-01-29	2024-08-07
103.43.18[.]43	444	2024-02-12	2024-07-19
77.91.123[.]208	444	2024-02-04	2024-04-09
46.246.98[.]229	444	2024-03-07	2024-03-26
2.58.15[.]101	444	2024-02-23	2024-02-27
46.246.98[.]209	444	2024-01-08	2024-02-14
103.254.108[.]87	8000	2023-10-17	2023-10-17
103.254.108[.]87	8080	2023-04-15	2023-10-16
103.254.108[.]108	9090	2023-04-13	2023-10-16
103.45.66[.]123	9090	2023-03-02	2023-04-08
103.45.66[.]32	8080	2022-07-29	2023-04-06
27.124.20[.]23	9090	2022-05-28	2023-03-24
27.124.20[.]22	9090	2022-05-28	2023-03-23
27.124.20[.]24	9090	2022-05-27	2023-03-17
69.176.94[.]148	9090	2023-03-04	2023-03-10
69.176.94[.]228	9090	2022-12-24	2023-02-25
103.253.40[.]137	8000	2022-06-24	2022-09-02
27.124.4[.]80	8080	2022-02-25	2022-06-23
27.124.4[.]81	8080	2022-02-25	2022-06-23
47.242.46[.]79	8080	2021-05-03	2022-06-17
27.124.4[.]82	8080	2022-02-24	2022-06-15
27.124.4[.]165	9090	2022-05-14	2022-05-28

27.124.4[.]184	9090	2022-05-14	2022-05-27
27.124.4[.]178	9090	2022-05-13	2022-05-26
103.15.28[.]165	8080	2022-03-05	2022-05-25
69.176.94[.]226	8080	2022-03-05	2022-04-22
27.124.4[.]3	8080	2022-03-11	2022-04-02
103.140.238[.]235	8080	2022-03-04	2022-04-01
27.124.4[.]2	8080	2022-03-12	2022-04-01
165.84.180[.]107	8000	2022-02-25	2022-03-19
69.176.94[.]156	8000	2022-02-25	2022-03-05
141.98.212[.]70	9090	2021-10-05	2022-03-04
5.188.33[.]50	8000	2022-02-15	2022-03-04
5.188.70[.]193	8000	2022-02-15	2022-03-04
69.176.94[.]140	8080	2022-02-24	2022-02-24
27.124.20[.]83	8000	2022-02-14	2022-02-18
208.87.200[.]106	8000	2022-01-02	2022-01-02
121.127.241[.]37	8000	2021-12-08	2021-12-08
156.255.2[.]211	443	2021-10-05	2021-10-05
156.255.2[.]211	8000	2021-10-04	2021-10-04
156.255.2[.]203	8000	2021-10-03	2021-10-03
47.243.43[.]248	8000	2021-07-05	2021-07-05
45.115.236[.]6	8080	2021-05-03	2021-06-01
43.251.118[.]97	8000	2021-01-03	2021-03-01
185.243.43[.]138	8000	2021-01-04	2021-02-02
47.245.59[.]33	8000	2021-01-05	2021-01-05

- Em 1 de abril de 2025, uma pesquisa por painéis SCOTCH ADMIN retornou o seguinte:

Endereço IP	Porta	Visto pela primeira vez	Visto pela última vez
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

- Em 14 de março de 2024, uma pesquisa por painéis virtuais SCOTCH ADMIN retornou o seguinte:

Domínio	Endereço IP
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

BADBAZAAR:

Descrição	Certificado SSL observado nos C2s do BADBAZAAR.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Em 1 de abril de 2025, uma pesquisa pelo certificado BADBAZAAR acima retornou o seguinte:

Endereço IP	Porta	Visto pela primeira vez	Visto pela última vez
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

Descrição	Certificado SSL observado nos C2s do BADBAZAAR.
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Em 1 de abril de 2025, uma pesquisa pelo certificado BADBAZAAR acima retornou o seguinte:

Endereço IP	Porta	Visto pela primeira vez	Visto pela última vez
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

- Domínios de WHOIS

Segue uma tabela de domínios que atualmente ou historicamente têm registos WHOIS com valores que correspondem aos observados nos domínios C2 do BADBAZAAR.

Valor de WHOIS	Domínios
Estado Registante: UJYJYUJ **País Registante: Bolívia** **Registador: 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
Estado Registante: REWR **País Registante: CF** **Registador: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com

	• suguestions[.]com • searching2[.]com
Estado Registante: FSDF **País Registante: AL** **Registador: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

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

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

Seguem os links para outros indicadores de comprometimento (IoCs) associados ao BADBAZAAR e ao MOONSHINE. O NCSC não pode confirmar a validade de toda a informação contida nestes links e os leitores são aconselhados a verificar independentemente a sua exatidão e relevância:

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

Mitigação

O NCSC encoraja a adoção das recomendações a seguir para se defender contra as ameaças descritas nos estudos de caso.

- **Os operadores de lojas de aplicações, incluindo lojas de aplicações de terceiros, e os desenvolvedores devem assegurar que as aplicações nas suas plataformas são seguras e que cumprem o Código de Conduta governamental.** Ver orientação: 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

- **Apoio multilingue**: Os desenvolvedores de aplicações devem investir em esforços emlocalizar aplicações populares para os utilizadores que falam línguas minoritárias entre os grupos-alvo, incluindo uigur, tibetano, hokkien taiwanês e cantonês. Orientação da Apple para a localização em aplicações: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Orientação do Google sobre a tradução de aplicações: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Manter segura a sua plataforma de redes sociais:** As empresas de redes sociais podem tornar mais difícil para os cibercriminosos criarem contas falsas e partilharem ficheiros ou links maliciosos nas suas plataformas em comunidades online que, de outra forma, seriam legítimas. Sempre que possível, as empresas devem partilhar indicadores maliciosos com o setor em geral, a fim de melhorar a compreensão coletiva da ameaça e ajudar nas medidas de proteção.

- **Plano de remediação para clientes:** As organizações devem ter procedimentos em vigor para notificar os clientes que instalaram aplicações maliciosas por meio dos seus serviços. Esses alertas devem ser apelativos e informativos. Quando apropriado, as organizações devem

fornecer orientações sobre como remover o software e incentivar as vítimas a denunciarem o caso às autoridades, como o NCSC no Reino Unido.
Ver o Código de Conduta da App Store para mais informação: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Grupos de trabalho para colaboração:** As empresas de redes sociais podem formar grupos de trabalho, permitindo que as suas respetivas equipas de segurança partilhem indicadores maliciosos, TTPs e observações, o que torna mais difícil para os atores utilizarem as suas plataformas para apoiar campanhas maliciosas.

- **Detecção de aplicações alteradas:** Sempre que possível, os desenvolvedores de aplicações devem incluir uma funcionalidade que informe o utilizador se ele baixou uma versão 'não oficial' de uma aplicação, para ajudar a proteger contra cópias maliciosas.

Apêndice A: Gráficos de agrupamento WHOIS da BADBAZAAR / informações do corretor de domínios

Imagem 1 - 'UKYJYUJ'

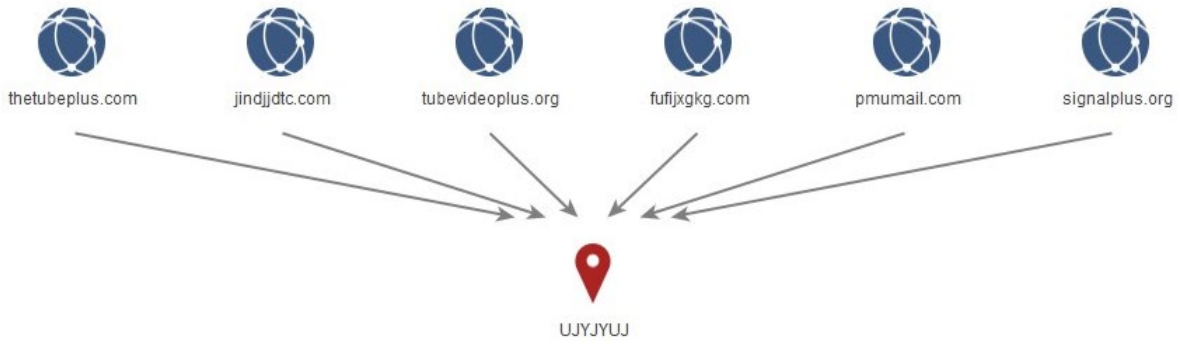


Imagem 2 – Valores de deslocamento do teclado

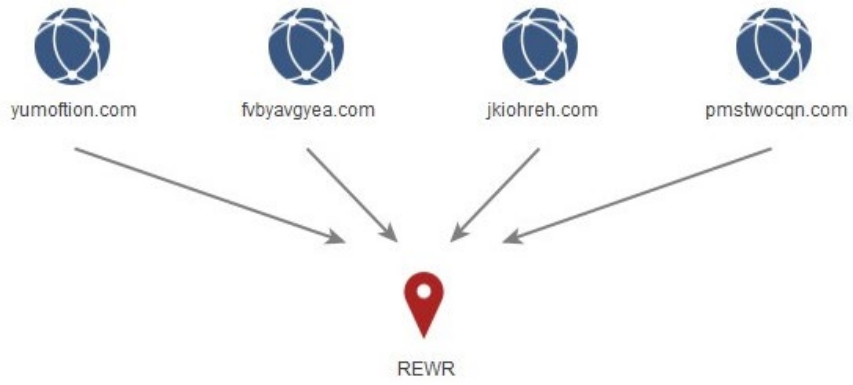


Imagem 3 – Domínios adicionais com valores do campo de estado 'FSDF'

Imagem 4 – **95.179.210[.]85**

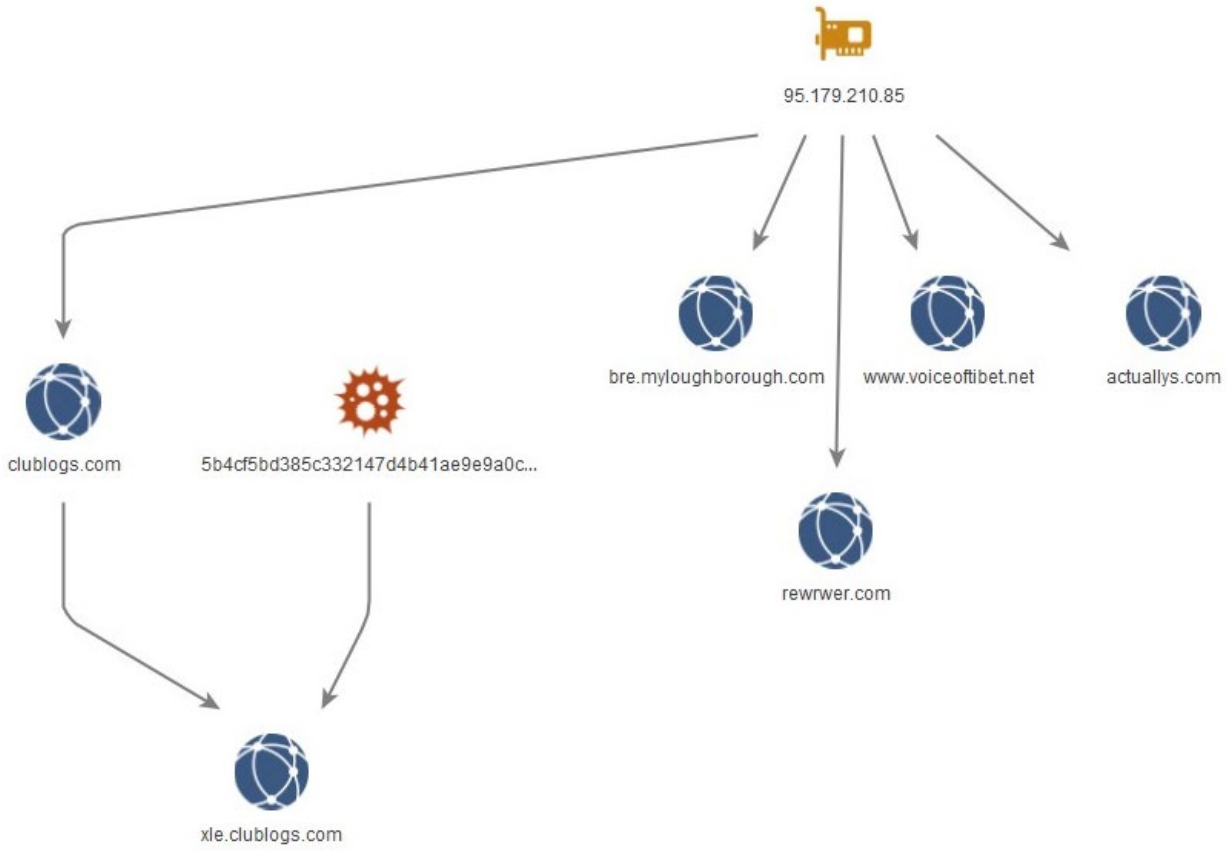


Imagem 5 – Links de WHOIS

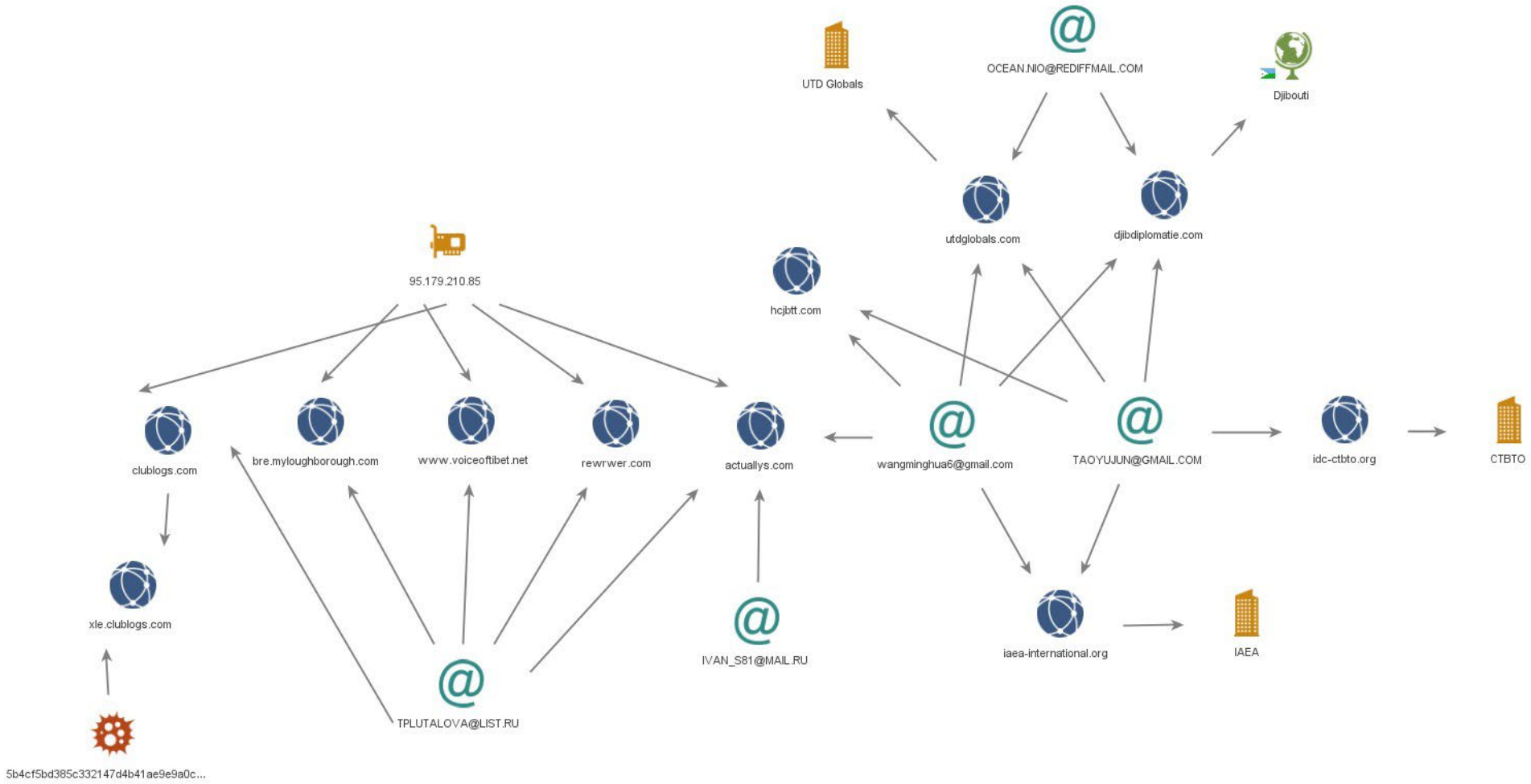


Imagem 6 – **WIN-EU0VLBL7TUJ**

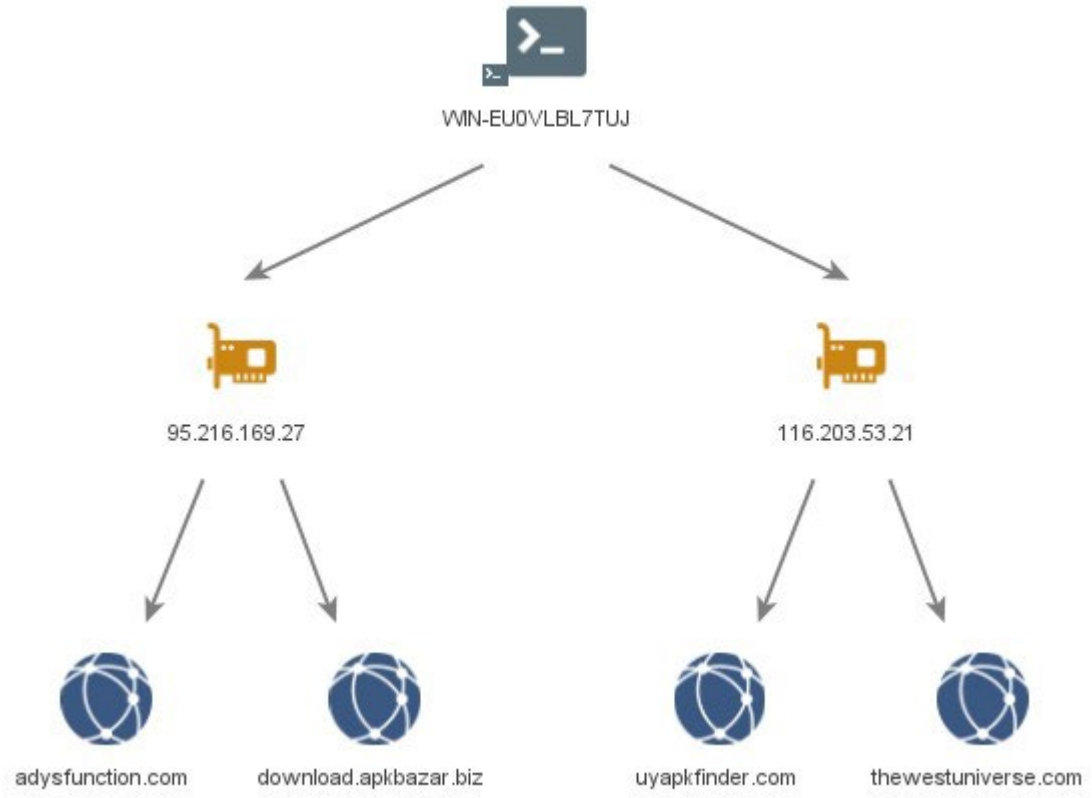


Imagem 7 – **WIN-70E59JVOB9G**

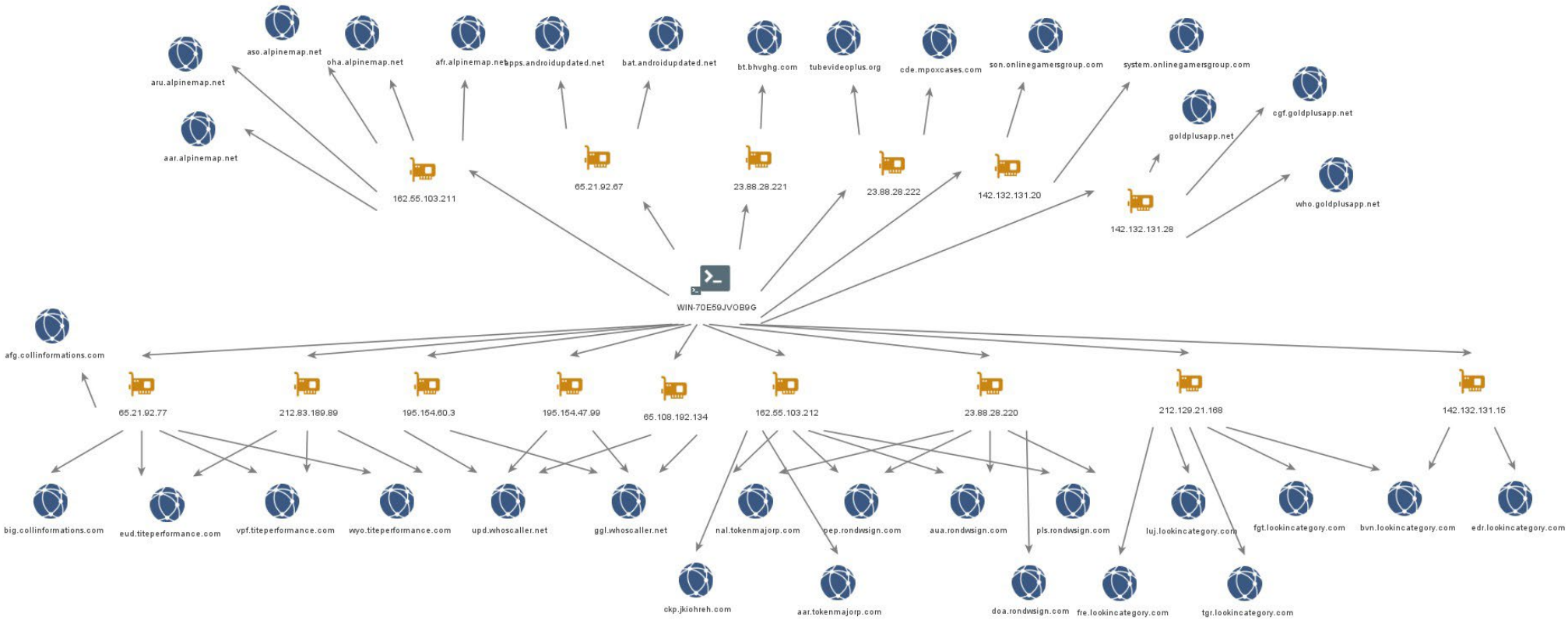


Imagem 8 - **WIN-50QO3EIRQVP**

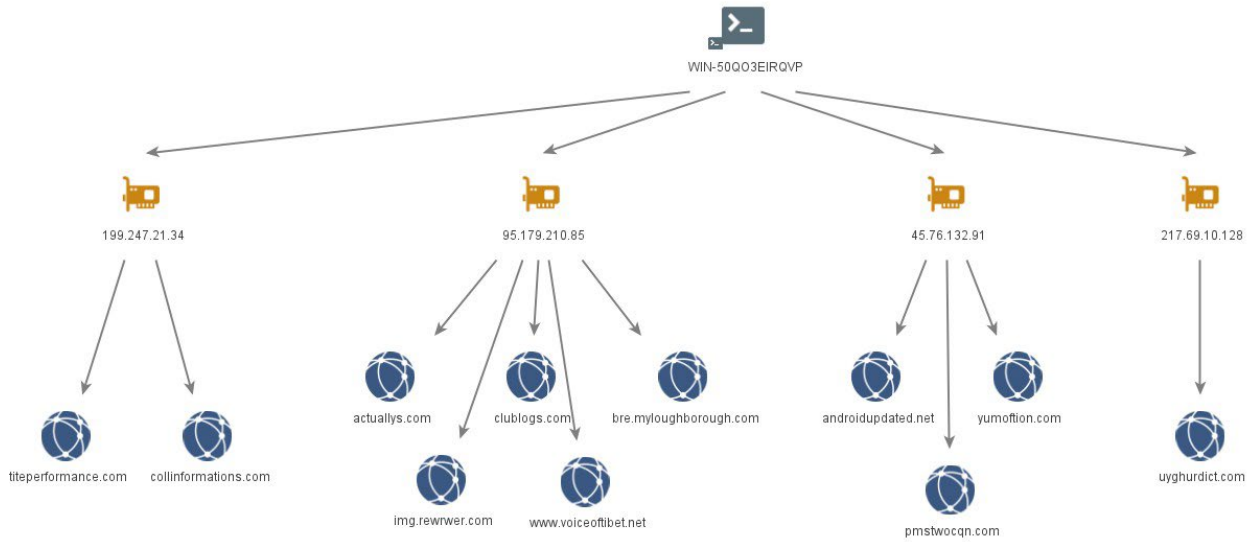


Imagem 9 - **VMSvc-WIN-50QO3EIRQVP**

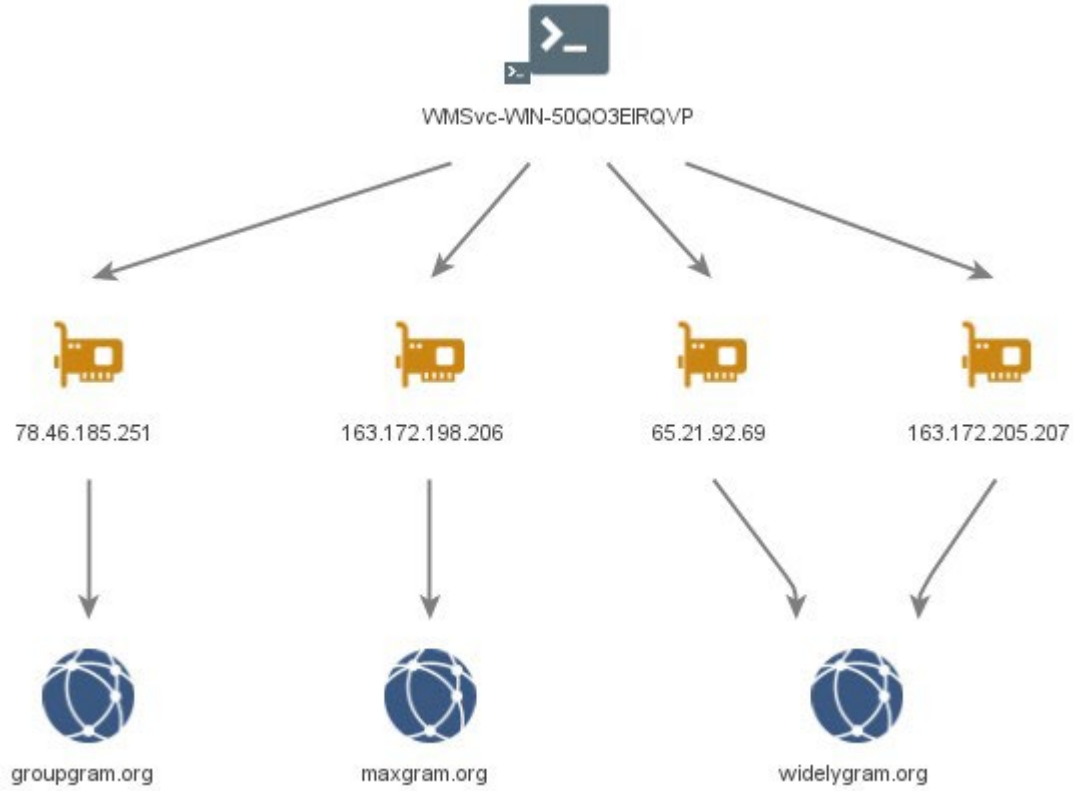


Imagem 10 – **VMSvc-WIN-50QO3EIRQVP** e **WIN-7LSBB9R0F1L**

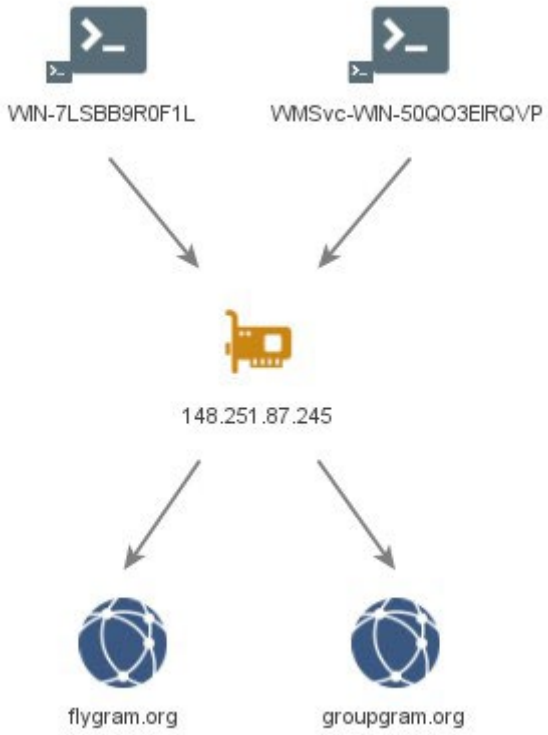


Imagem 11 - **WIN-N8H8S9BG2P0**

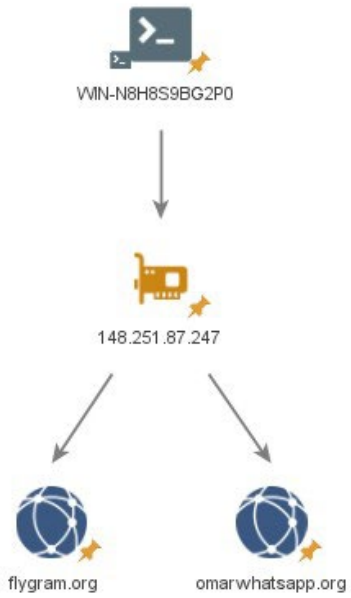


Imagem 12 – **WIN-I6VBN8MR92A**

Apêndice B: Amostras MOONSHINE & BADBAZAAR observadas

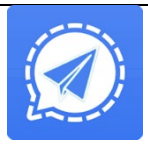
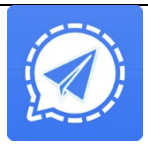
A tabela seguinte lista as aplicações utilizadas nas campanhas MOONSHINE e BADBAZAAR nos últimos dois anos.

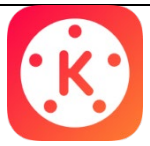
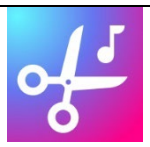
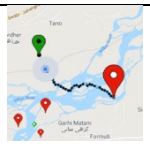
Muitas destas aplicações mostram uma semelhança clara com aplicações já estabelecidas. Provavelmente, é uma técnica deliberada do autor para 'falsificar' marcas conhecidas.

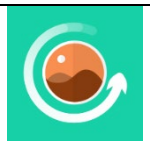
É importante observar que o título da aplicação, o nome do pacote e o ícone da aplicação podem imitar ou corresponder à aplicação real e, portanto, não devem ser usados exclusivamente para identificar se um dispositivo está infectado.

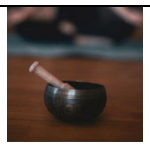
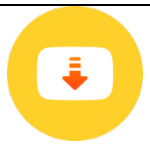
Título da aplicação	Nome do pacote	Ícone da aplicação
99 Nomes de ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Teclado Árabe	com.arabic.keyboard.arabic.language.keyboard.app	
Cortador de áudio e vídeo	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Canções budistas (1)	com.bigkidsapps.buddhistsongs1	
Calculadora	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

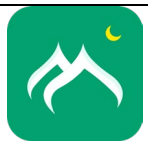
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
Gestor de Ficheiros +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Calendário Hijri	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	

KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
Cortador de MP3 e criador de toques	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Calculadora de distâncias em mapas	com.routemap.mapdownload.gpsroute planner	
Recuperação de redes sociais	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	
Leitor de PDF	pdf.pdfreader.pdfviewer.pdfeditor	

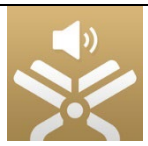
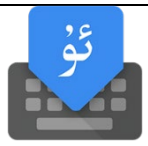
Leitor de PDF	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Editor de fotos	com.iudesk.android.photo.editor	
Recuperação de fotos	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Livro de Orações	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restaurar fotos apagadas	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	
Conversor de vídeo	com.inverseai.video_converter	
Cortador de vídeo	com.naing.cutter	
Descarregador de vídeos	downloader.video.download.free	

Criador de vídeos	com.bstech.slideshow.videomaker	
Reprodutor de vídeo para Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Gravador de voz	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Previsão do tempo	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	

WhatsApp	com.WhatsApp3Plus	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
YouTube Downloader	dentex.youtube.downloader	
Zom	im.zom.messenger	

iQuran Lite	com.guidedways.iQuran	
ئاۋازلىق ئەسەرلەر	com.ewlat.eserler	
ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
ئۇيغۇرچە قۇرئان	com.c9.uyghurquran	
القرآن الكريم	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
قۇرئان كەرىم	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
نۇر كىرگۈزگۈچ	com.nur.ime	

《心灵法门》念佛机	com.guanyincitta.chant	
汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	

Leitura adicional

Orientação do Centro Australiano de Segurança Cibernética

- Denuncie um crime cibernético, incidente ou vulnerabilidade
- Como proteger os seus dispositivos
- Proteja o seu telemóvel
- Phishing
- Scams
- Proteja as suas redes sociais
- Dicas de segurança para redes sociais e aplicações de mensagens

Orientação do NCSC e da NPSA do Reino Unido

- Defendendo a Democracia
- Redes sociais: como utilizá-las com segurança
- Orientação sobre segurança de dispositivos para organizações, incluindo dispositivos móveis
- Relatório de ameaças em lojas de aplicações.
- Segurança pessoal e proteção para indivíduos de alto risco

Orientação da NSA dos EUA

- Melhores práticas para dispositivos móveis

Isenção de responsabilidade

Observe que este aviso fornece informação que se encontra validada na altura da publicação.

Este relatório baseia-se em informações obtidas junto de agências autorizadas e fontes do setor. Quaisquer conclusões e recomendações apresentadas não foram fornecidas com a intenção de evitar todos os riscos e seguir as recomendações não eliminará todos esses riscos. A responsabilidade pelos riscos relacionados com a informação recai sempre sobre o proprietário do sistema relevante.

No Reino Unido, esta informação está isenta ao abrigo da Lei da Liberdade de Informação de 2000 (FOIA) e pode estar isenta ao abrigo de outra legislação britânica na área de informação.

Envie quaisquer consultas relacionadas à FOIA para ncscinfoleg@ncsc.gov.uk.