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

公告

BADBAZAAR 和 MOONSHINE：技术分析和缓解措施

2025 年 4 月 9 日

BADBAZAAR 和 MOONSHINE：技术分析和缓解措施

概要

在英国网络联盟（Cyber League）的支持下，此公告由英国国家网络安全中心（National Cyber Security Centre，简称 NCSC UK）和以下国际合作伙伴联合发布：

- **澳大利亚网络安全中心，隶属于澳大利亚信号局**
- **加拿大网络安全中心，隶属于通信安全机构**
- **德国联邦情报局**
- **德国联邦宪法保卫局**
- **新西兰国家网络安全中心，隶属于政府通信安全局**
- **美国联邦调查局**
- **美国国家安全局**

此公告汇总并发布了有关名为 BADBAZAAR 和 MOONSHINE 的两种间谍软件变种的最新威胁情报，并向应用商店运营商、开发商和社交媒体公司提供建议，以帮助保护其用户的安全。

此公告与一份专门面向这些恶意软件受害者的公告同步发布。

本文档使用了 NCSC 术语表对“间谍软件”的定义，即：“一种未经用户同意安装在其设备上、收集数据然后将数据发送给第三方的恶意软件”。

案例研究一：MOONSHINE

MOONSHINE 是一款针对藏人团体的 Android 间谍软件，由"公民实验室"于 2019 年披露。MOONSHINE 伪装成合法应用程序，诱导受害者进行安装。该程序通过 Telegram 频道和 WhatsApp 链接传播。

NCSC 对 MOONSHINE 的研究表明：

- MOONSHINE 使用的管理界面自首次被披露以来已经有所改变。
- 该管理界面具有广泛的监控能力，包括从设备中提取文件以及录制实时音频和屏幕画面的能力。
- 发现了一组虚拟托管的 MOONSHINE 管理界面。这些界面的基础设施与 UPSEC 相关的登录面板存在重叠，根据《情报在线》的信息，UPSEC 指的是"四川电科网安科技有限公司"（Sichuan Dianke Network Security Technology Co., Ltd）。

管理界面

此前关于 MOONSHINE 管理界面的报告表明，该界面已经发生改变，这说明该软件在持续开发中。

管理界面的最早示例可见于"公民实验室"2019 年发布的报告中。

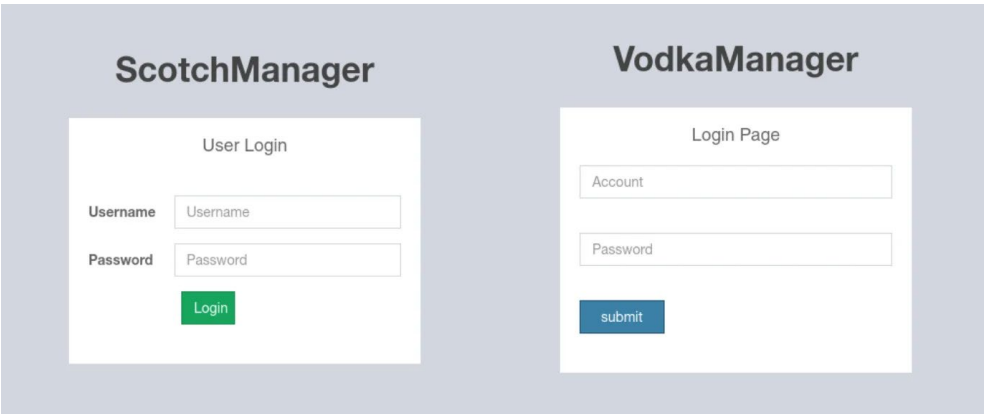


图 1："公民实验室"在其 2019 年发布的报告《缺失的链接：藏人团体遭"一键式"移动攻击》（Missing Link Tibetan Groups Targeted with 1-Click Mobile Exploits）中披露了 MOONSHINE 管理界面。

在 2022 年初，Lookout 报告了一个不同的管理界面，该界面经过重新设计，如下所示（取代了图 1 所示的旧版界面）：

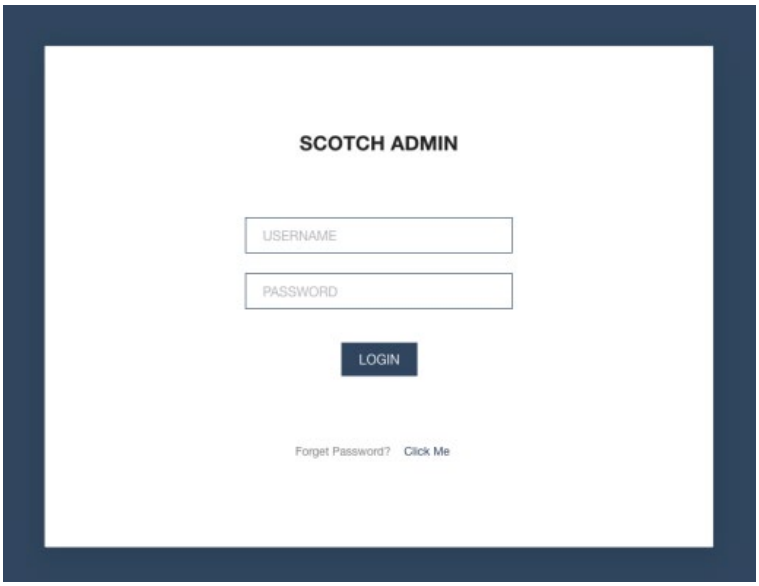


图 2：Lookout 于 2022 年发布的报告中披露了 MOONSHINE 管理界面，报告名为《MOONSHINE：中国 APT 组织 POISON CARP 演化的 Android 间谍软件，用于针对藏人和维吾尔人》（MOONSHINE: Evolving Android Surveillanceware by Chinese APT POISON CARP To Target Tibetans and Uyghurs）。

2023 年 8 月，对 MOONSHINE 的命令和控制(C2)服务器进行的一次扫描发现了一个与 2022 年版本相似的界面，如图 2 所示，但其**"忘记密码"（Forget Password）**功能已被移除：

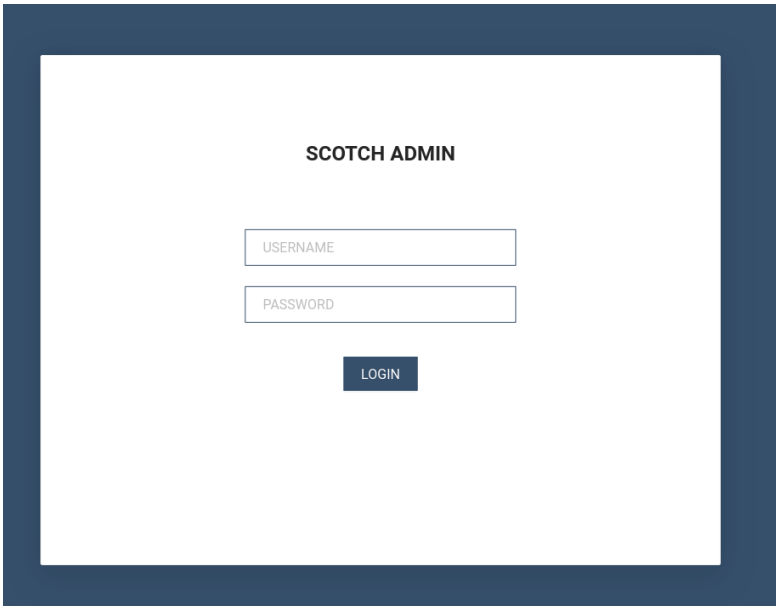


图 3：2023 年 8 月观察到的 MOONSHINE 管理界面已移除"忘记密码"提示。

对管理界面的进一步调查显示，面板内的内容揭示了存储受感染设备详细信息的方式。

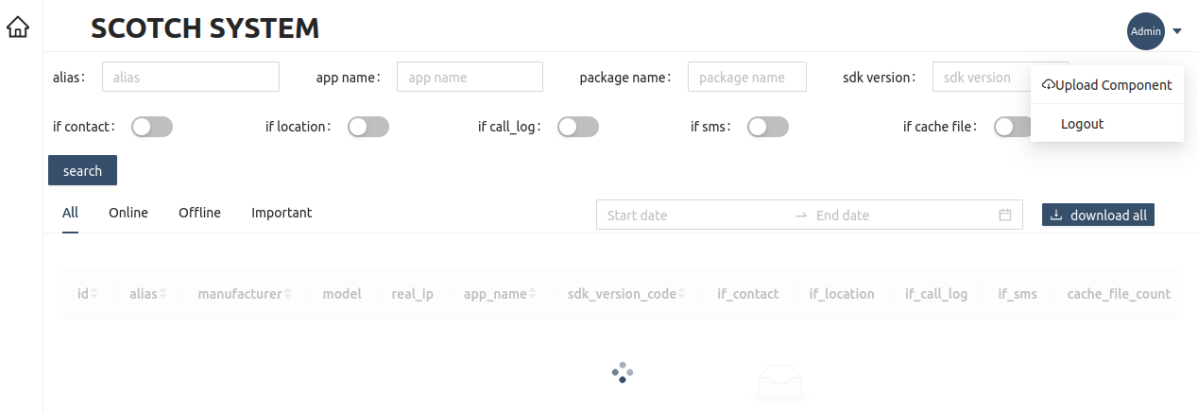


图 4：MOONSHINE 管理界面登录页面背后的网页内容。

Lookout 的研究显示，受害者设备会向 MOONSHINE C2 服务器传递一个名为**“分数”**的参数。“分数”的值是根据该恶意样本在受害者设备上所拥有的权限计算得出的。

页面中的“if_contact”、“if_location”、“if_call_log”和“if_sms”等字段表明，并非所有 MOONSHINE 样本都拥有对受感染设备所有数据的访问权。这些字段以及从设备传递到 C2“分数”的存在表明，威胁行为者利用该评分机制，将恶意软件对受感染设备的访问权限级别传达给访问管理界面的人。

一般来说，为防止应用程序收集设备信息的最佳做法是，在下载之前检查应用程序权限是否存在任何异常。然而，MOONSHINE 样本往往请求与应用程序功能相关的权限，因此可能看起来并不可疑，但它们也利用这些权限收集设备信息。

MOONSHINE 还具有应用程序编程接口(Application Programming Interface，简称 API)，表明其具有广泛的能力。API 文档的早期版本含有简体中文的 API 名称。

虚拟主机

在搜索 MOONSHINE 面板时发现了若干虚拟托管的实例。虚拟主机是指一个 IP 地址可以同时承载多个网站的技术。在已知的恶意软件样本中均未观察到这些虚拟主机实例所使用的 IP 地址和所托管的域名。

这些实例中的管理界面与早期版本有所不同，页面的标题是**“LOGIN”**，而非此前所看到的**“SCOTCH ADMIN”**。

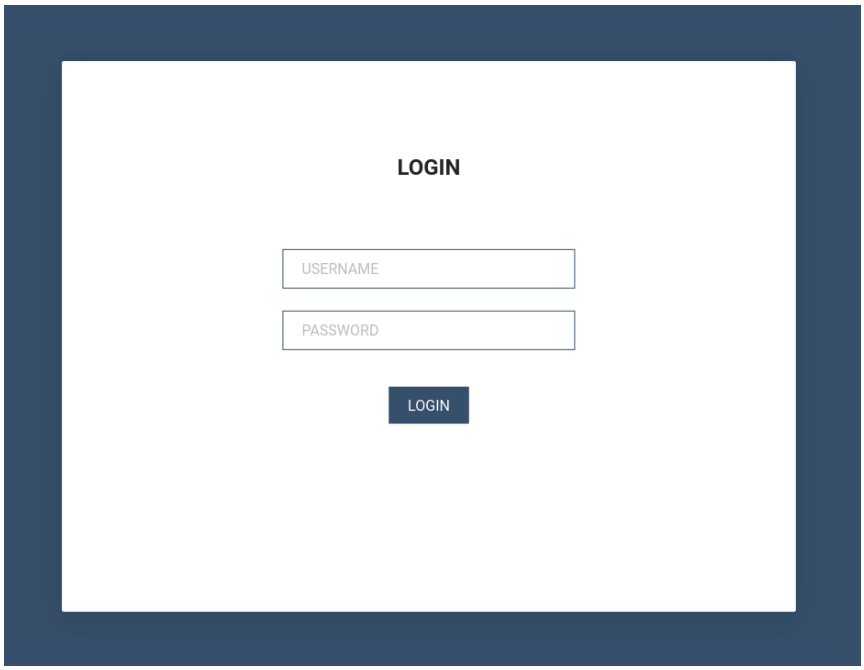


图 5：MOONSHINE 管理界面标题从“SCOTCH ADMIN”更改为“LOGIN”。

另外，如图 6 所示，面板上的内容也与图 4 不同：

图 6：虚拟托管的 MOONSHINE 管理界面中，登录页面背后的网页内容。

图 6 中的面板似乎是图 4 中面板的简化版本。这些面板的共同特征是表中的列名有“id”（设备编号）、“manufacturer"（制造商）和“model"（型号）这几项。

所发现的虚拟托管 MOONSHINE 实例包括：

域名	IP 地址
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

这些域名被趋势科技（Trend Micro）列为 MOONSHINE 漏洞利用工具包，负责利用浏览器的漏洞将恶意软件安装在移动设备上。趋势科技将这个恶意软件命名为“Dark Nimbus”。

需要澄清的是，MOONSHINE 管理界面是 MOONSHINE 恶意软件样本与之通信的平台，受害者的数据会被传送至该界面。趋势科技报告中的 MOONSHINE 漏洞利用工具包是一种单独的功能，该工具包利用浏览器漏洞将一个名为 Dark Nimbus 的恶意软件安装在移动设备上。此外，Dark Nimbus 和 MOONSHINE 是全然不同的恶意软件。

MOONSHINE 管理界面和 MOONSHINE 漏洞利用工具包之间存在代码重叠，因此图 3 和图 5 中的登录提示类似，而且图 4 和图 6 中的页面内容也类似。它们的源代码中都包含字符串“webpackJsonpreact-scotchui”。

威胁实施者会生成 URL 链接，连接至 MOONSHINE 漏洞利用工具包，然后重定向至与藏人和维吾尔人相关的视频内容，这与 MOONSHINE 的目标群体重合。

在托管 MOONSHINE 漏洞利用工具包域名的许多 IP 地址中，于端口 444 上有一个名为“VLiteUI”的登录页面。该页面在其他环境中很少见，其出现在这些 IP 上表明可能与威胁实施者的操作行为有关联。

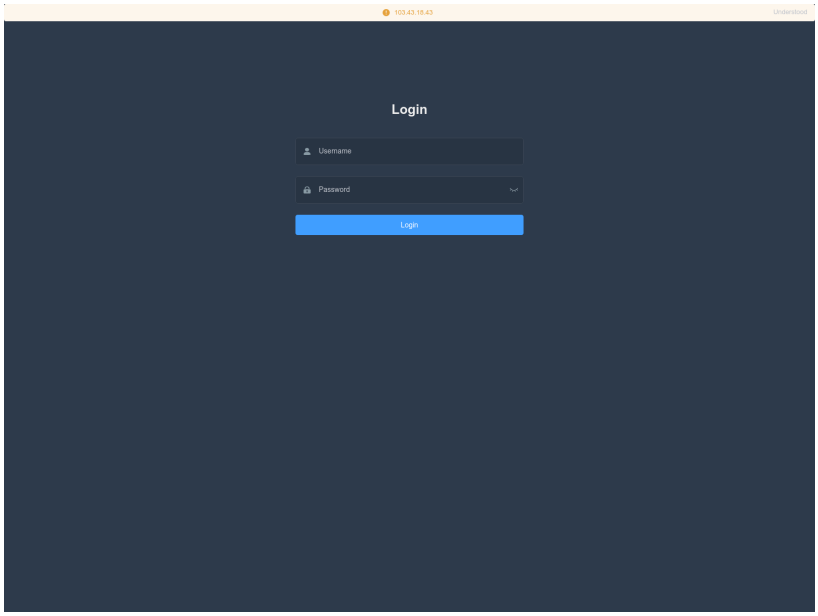


图 7：在托管 MOONSHINE 漏洞利用工具包的 IP 上，观察到 HTML 标题为“VLiteUI”的登录面板。

趋势科技对 Dark Nimbus 的分析发现，该恶意软件能够收集设备上的详尽信息列表，并使用 XMPP 协议与 C2 进行通信。

趋势科技还概述，他们在 Dark Nimbus 的一些版本中发现了其普遍使用字符串“DKNS”。

在其他 IP 地址使用的 XMPP 服务中还观察到“**ansec[.]com**”（被趋势科技列为 Dark Nimbus C2），这些地址服务的网页标题中带有“DKNS”：

- 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)

另一组在 XMPP 服务中带有“**ansec[.]com**”的 IP 地址，其网页标题为：

- 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)

据《情报在线》称，在 HTML 页面标题中所观察到的“UPSEC”指的是“四川电科网安科技有限公司”。

案例研究二：**BADBAZAAR**

BADBAZAAR 是一款主要针对维吾尔人、藏人和台湾人群体的移动恶意软件，它有 iOS 和 Android 两个版本。这种间谍软件是通过社交媒体平台和官方应用商店传播的。Volexity 最近的报告显示 BADBAZAAR 有不同的变体，分别为 BadSolar、BADBAZAAR 和 BadSignal。这三个变体都具有收集设备和操作者信息的功能，且通过这些重叠的功能相互关联。

NCSC 对 BADBAZAAR 的研究揭示出以下情况：

- C2 域名聚类分析揭示了其与历史威胁情报中报告的域名之间存在进一步关联。
- C2 服务器和恶意软件样本显示出与威胁实施者基础设施相关联的主机名。
- 威胁实施者利用社交工程手段创建虚假账号，以在官方应用商店之外传播恶意软件。

WHOIS 聚类/域名经纪人

"UJYJYUJ"

对 BADBAZAAR 域名**"signalplus[.]org"**的 WHOIS 记录所做的分析（由 ESET 报告）表明，**"State"**字段中包含值**"UJYJYUJ"**。

搜索具有相同值的其他域名，发现以下关键域名：

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

（见附件 A，图 1）

域名 **signalplus[.]org**、**tubevideoplus[.]org** 和 **thetubeplus[.]com** 被报告为 BADBAZAAR 的 C2 域名，而 ESET 报告指出子域名 **mail.pmumail[.]com** 是 FlyGram 的代理服务器。FlyGram 是一款由恶意网络行为者开发的 BADBAZAAR 应用程序（见附录中其他 BADBAZAAR 应用程序的列表）。

键盘行走密码

NCSC 在其他已注册的 BADBAZAAR C2 域名中，也观察到了类似的键盘行走模式。

例如，以下域名中**"State"**字段的密码均为**"REWR"**（与先前使用的密码一致）：

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

（见附件 A，图 2）

具有"FSDF"状态字段密码的域名

另一组 BADBAZAAR C2 域名中，**"State"**字段密码为**"FSDF"**：

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

（见附件 A，图 3）

历史报告中的键盘行走密码

在 TA413 过往报告的针对西藏组织的攻击中，亦可看到在 BADBAZAAR 域名的 WHOIS 记录中使用键盘行走密码的情况。Recorded Future 情报公司观察到有威胁实施者控制的域名伪装成藏人组织，并使用**"asfasf"**作为注册人组织字段密码。

clublogs[.]com

Lookout 获取的 BADBAZAAR 样本中包含 C2 域名**"xle.clublogs[.]com"**。其根域名**"clublogs[.]com"**托管在 IP 地址**"95.179.210[.]85"**上，并具有 SSL 证书，该证书的主题和签发者字段密码为**"CN=WIN-50QO3EIRQVP"**。该密码与 BADBAZAAR 样本中发现的 SSL 证书相匹配，这些样本使用 SSL 锁定机制来防止通信遭到拦截。

IP 地址 **95.179.210[.]85** 的托管历史记录显示以下关键域名：

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

（见附件 A，图 4）

www.voiceoftibet[.]net

域名“**www.voiceoftibet[.]net**”似乎伪装成《西藏之声》（Voice of Tibet）广播电台，与 TA413 使用的战术技术程序（TTP）类似。

域名“**rewrwer[.]com**”与先前在 BADBAZAAR 域名的 WHOIS 记录中发现的“**State**”字段密码“**REWR**”类似。

域名“**clublogs[.]com**”、“**rewrwer[.]com**”、“**voiceoftibet[.]net**”和“**myloughborough[.]com**”全部是使用电子邮件地址“**tplutalova@list[.]ru**”注册的。

actuallys[.]com

“actuallys[.]com”的 WHOIS 记录显示，技术人员和管理员的电子邮件地址为“**tplutalova@list[.]ru**”，而注册人的电子邮件地址则为“**ivan_s81@mail[.]ru**”。

域名“**actuallys[.]com**”的历史 WHOIS 信息表明，在 2016 年 2 月 24 日，注册人电子邮件地址为“**wangminghua6@gmail[.]com**”。该电子邮件地址随后在 2016 年 3 月 11 日更改为“**ivan_s81@mail.ru**”，但注册人的注册到期日期保持不变。

wangminghua6@gmail[.]com

电子邮件地址“**wangminghua6@gmail[.]com**”曾被用于注册历史威胁情报报告中所发现的域名。在 2015 年，Palo Alto 发现该电子邮箱用于注册恶意软件 Cmstar 的 C2 域名。在 2014 年，Mandiant 报告显示，该邮箱还被用于注册 APT3 发起的钓鱼攻击活动中使用的域名。在 2013 年，CrowdStrike 发现该邮箱被用于注册一个

恶意软件投放器中所使用的域名，该投放器的程序数据库(PDB)路径中包含中文字符。这表明它是在中文系统上编译的。

taoyujun@gmail[.]com

域名“**hcjbtt[.]com**”是使用电子邮件地址“**taoyujun@gmail[.]com**”注册的，但其管理员电子邮件是使用“**wangminghua6@gmail[.]com**”注册的。

虽然目前尚未发现与域名“**hcjbtt[.]com”**相关的恶意行为，但电子邮件地址“**taoyujun@gmail[.]com”**曾在历史威胁情报报告中出现。在 2014 年，Mandiant 报告指出，该邮箱曾用于**“Cueisfry 木马程序”**样本中所使用的域名，这些木马程序被用于针对日本组织的攻击活动。

该电子邮件地址还注册了“**iaea-international[.]org**”和“**idc-ctbto[.]org”**之类的域名，前者疑似伪装成国际原子能机构（**International Atomic Energy Agency**），后者则疑似伪装成**全面禁止核试验条约组织(简称 CTBTO)**下的国际数据中心（**International Data Centre**）。

域名“**iaea-international[.]org**”的早期 Whois 记录显示，其注册人的电子邮件地址为“**wangminghua6@gmail[.]com**”。

udtglobals[.]com

据观察，域名“**udtglobals[.]com”**使用**“wangminghua6@gmail[.]com**”作为管理员电子邮件地址，并使用“**ocean.nio@rediffmail[.]com**”作为注册人电子邮件地址。该域名的其他 WHOIS 记录显示使用了相同的注册人电子邮箱，但管理员电子邮件地址则为“**taoyujun@gmail[.]com**”。

域名“**udtglobals[.]com**”似乎在伪装成一个面向海底防御和安全技术公司的全球性活动——“**UDT Global**”。电子邮件地址中的用户名“**ocean.nio”**可能是在模仿多个国家所存在的**国家海洋研究所（简称 NIO）**。但该邮箱使用“**Rediff**”电子邮件服务（总部设在印度），这可能表明其在模仿**印度国家海洋研究所（Indian National Institute of Oceanography**）。

Djibdiplomatie[.]com

域名“**djibdiplomatie[.]com**”似乎在伪装成吉布提外交服务网站，其 WHOIS 记录与 “**utdglobals[.]com**” 相似。其中一份记录似乎显示注册人为

“**ocean.nio@rediffmail[.]com**”，管理员为“**taoyujun@gmail[.]com”**，而其他记录显示管理员电子邮件地址为“**wangminghua6@gmail[.]com”**，注册人电子邮件地址为**“ocean.nio@rediffmail[.]com**”。

这两个域名在 WHOIS 记录中都包含了键盘行走式的密码。例如，“**udtglobals[.]com”**的注册城市为“**ASDF”**，“**djibdiplomatie[.]com”**的注册人名称为“**DAF DAGF”**。这与在其他 BADBAZAAR 域名中观察到的模式一致。

虽然在伪装成**全球海底防御活动**、**吉布提外交服务**和**国际原子能机构的**域名的 WHOIS 记录中发现了电子邮件地址“**wangminghua6@gmail[.]com**”和“**taoyujun@gmail[.]com”**，但这些电子邮件地址也出现在多个非恶意域名的 WHOIS 记录中。

这种伪装域名和非恶意域名混合存在的情况，可能表明存在一个专门为恶意网络行为者采购基础设施的实体。

电子邮件地址“**ocean.nio@rediffmail[.]com**”仅在上述伪装域中发现。而分别以“**ivan_s81@mail[.]ru**”和“**tplutalova@list[.]ru**”注册的域名数量很少，但其中的一些域名托管在 BADBAZAAR 基础设施上。这三个电子邮件地址据信与恶意网络行为者的操作关联更为密切。这是因为与电子邮箱“**wangminghua6@gmail[.]com**”和“**taoyujun@gmail[.]com**”相比，与这三个电子邮件地址相关联的域名中关涉恶意行为的数量更多。

（见附件 A，图 5）

与其他威胁实施者的关联

与 BADBAZAAR 相关的域名“**actuallys[.]com**”、“**clublogs[.]com**”、“**myloughborough[.]com**”、“**rewrwer[.]com**”和“**voiceoftibet[.]net”**还有一个共同的特征，即它们都是在 eNom 注册的，并且“停放”在“**255.255.255[.]254**”。

根据 NCSC 之前的调查，具有这些特征的其他域名在 2019 年出现了与 **APT5** 相关的活动，并在 2009 年至 2011 年期间出现了与 **APT14** 相关的活动。

与 APT5-关联的域名的历史 WHOIS 记录将“taoyujun@gmail[.]com”列为了注册人的电子邮件地址。

与 APT14 关联的域名具有三个字母的子域名，这些子域名似乎代表了其恶意行动的目标。其中一个例子是“**bae.cisconline[.]net**”，暗示其攻击目标是贝宜系统（BAE Systems），并且是在“**Poison Ivy**”恶意软件样本中被发现的。

据观察，在 BADBAZAAR 域名中也有类似的特征，其子域名与被植入恶意代码的应用程序的名称相关：

应用程序标题	C2 URL
穆斯林专业版	**mpp**.pmstwocqn[.]com
Android 视频播放器	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
阿富汗电台	**afg**.collinformations[.]com
英语-维吾尔语词典免费版	**eud**.titeperformance[.]com
光盘视频恢复	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

务必要注意，与 APT5 和 APT14 相关的活动都属于历史事件，而且在 eNom 注册并解析至 IP 地址“**255.255.255.254**”的还存在其他域名，但这些域名并未与恶意行为存在联系。因此，无法确定这些攻击活动背后的行为者是否相同或存在关联。

机器名称

对 BADBAZAAR C2 及其样本的分析发现，主机名被用作了 SSL 证书中的“通用名称”（Common Name）密码。NCSC 对 BADBAZAAR 样本及其基础设施中观察到的主机名进行了调查，发现这些主机名被用于多个 IP 地址。这些 IP 地址托管着在 BADBAZAAR 样本中发现的域名。以下章节将详细说明这些主机名，以及托管 BADBAZAAR C2 域名的主机名的 IP 地址。

在几乎所有案例中，证书中使用的主机名都与所述恶意域名的 IP 解析结果存在重叠，而少数例外情况也已在报告中列出。

WIN-EU0VLBL7TUJ

主机名“**WIN-EU0VLBL7TUJ**”出现了在以下关键 IP 地址上：

- “**116.203.53[.]21**”托管了 BADBAZAAR C2 域名“**uyapkfinder[.]com”**和“**thewestuniverse[.]com”**。

- **“95.216.169[.]27”**托管了 BADBAZAAR C2 域名“**adysfunction[.]com”**和子域名“**download.apkbazar[.]biz**”，后者据观察是 BADBAZAAR 样本的下载链接。

（见附件 A，图 6）

WIN-70E59JVOB9G

主机名“**WIN-70E59JVOB9G**”出现在以下关键 IP 地址上：

- “**23.88.28[.]220”**托管了 BADBAZAAR C2 子域名**“aua.rondwsign[.]com”**、**“nal.tokenmajorp[.]com”** 、 **“pep.rondwsign[.]com”** 、“**doa.rondwsign[.]com”**和**“pls.rondwsign[.]com”**。证书中该主机名最后一次出现与这些恶意域名首次解析到该 IP 之间相隔两天。

- “**23.88.28[.]221**”托管了与 BADBAZAAR 关联的子域名“**bt.bhvghg[.]com**”。

- **“23.88.28[.]222”**托管了 BADBAZAAR C2 域名“**tubevideoplus[.]org**”和“**cde.mpoxcases[.]com**”。

- “**65.21.92[.]67**” 托管了 BADBAZAAR C2 子域名“**bat.androidupdated[.]net**” 。它还托管了子域名“**apps.androidupdated[.]net**”，这是 DoubleAgent 恶意软件的 C2 子域名。

- **“65.21.92[.]77”** 托管了 BADBAZAAR C2 子域名：**“wyo.titeperformance[.]com”**、**“big.collinformations[.]com”**、**“vpf.titeperformance[.]com”**、**“eud.titeperformance[.]com”** 和 **“afg.collinformations[.]com”**

- **“65.108.192[.]134”**托管了 ADBAZAAR C2 子域名**“upd.whoscaller.net”**和**“ggl.whoscaller[.]net”**。

- **“142.132.131[.]15”** 托管了 BADBAZAAR C2 子域名 **“bvn.lookincategory[.]com”**和**“edr.lookincategory[.]com”。**证书中该主机名最后一次出现与这些恶意域名首次解析到该 IP 之间相隔 11 天。

- **“142.132.131[.]20”** 托管了子域名 **“son.onlinegamersgroup[.]com”** 和 **“system.onlinegamersgroup[.]com”**，这些子域名被认为是 BADBAZAAR C2 子域名，因为它们在 BADBAZAAR 相关 SSL 证书出现期间被托管。

- “**142.132.131[.]28”**托管了 BADBAZAAR C2 域名“**goldplusapp[.]net**”及其子域名“**who.goldplusapp[.]net**”和“**cgf.goldplusapp[.]net**”。

- “**162.55.103[.]211**”托管了 BADBAZAAR C2 子域名“**oha.alpinemap[.]net**”、“**aru.alpinemap[.]net**”、“**aso.alpinemap[.]net**”、“**afr.alpinemap[.]net**”和“**aar.alpinemap[.]net**”。

- “**162.55.103[.]212**”托管了 BADBAZAAR C2 子域名“**pep.rondwsign[.]com**”、**“ckp.jkiohreh[.]com”**、“**aar.tokenmajorp[.]com**”、“**nal.tokenmajorp[.]com**”、**“pls.rondwsign[.]com”** 和 **“aua.rondwsign[.]com”。**

- “**195.154.47[.]99**”托管了 BADBAZAAR C2 子域名“**ggl.whoscaller[.]net**”和“**upd.whoscaller.net**”。证书中该主机名最后一次出现与这些恶意域名首次解析到该 IP 之间相隔三天。

- “**195.154.60[.]3**”托管了 BADBAZAAR C2 子域名“**upd.whoscaller[.]net**”“**ggl.whocaller[.]net**”。

- “**212.83.189[.]89**” 托管了 BADBAZAAR C2 子域名“**wyo.titeperformance[.]com**” 、 “**eud.titeperformance[.]com**” 、“**vpf.titeperformance[.]com**”和“**afg.collinformations[.]com**”。

- “**212.129.21[.]168**” 托管了 BADBAZAAR C2 域名、“**fre.lookincategory[.]com**” 、 “**tgr.lookincategory[.]com**” 、“**fgt.lookincategory[.]com**” 、 “**luj.lookincategory[.]com**” 和“**bvn.lookincategory[.]com**”。

（见附件 A，图 7）

WIN-50QO3EIRQVP

主机名“**WIN-50QO3EIRQVP**”出现了在以下关键 IP 地址上：

- “**45.76.132[.]91**” 所托管的域名“**yumoftion[.]com**” 和“**androidupdated[.]net**”。这两个域名都与 BADBAZAAR 相关联，因为其子域名“**fow.yumoftion[.]com**” 和 “**bat.androidupdated[.]net**” 是 BADBAZAAR 的 C2 域名。此外，子域名“**apps.androidupdated[.]net**”是 DoubleAgent 的 C2 域名。它还托管了域名“**pmstwocqn[.]com**”，通过 WHOIS 记录与 BADBAZAAR 相关联。

- “**95.179.210[.]85**” 托管了“**clublogs[.]com**” ， 其子域名“**xle.clublogs[.]com**”是 BADBAZAAR 的 C2 域名，并且还托管了“**bre.myloughborough[.]com**” 、 “**img.rewrwer[.]com**” 、“**www.voiceoftibet[.]net**”和“**actuallys[.]com**”这几个与 BADBAZAAR 有关联的域名。

- “**199.247.21[.]34**” 托管了 “**titeperformance[.]com**” 和 “**collinformations[.]com**”，其子域名是 BADBAZAAR 的 C2 域名。

- “**217.69.10[.]128**”托管了 BADBAZAAR 的 C2 域名“**uyghurdict[.]com**”。

（见附件 A，图 8）

WMSvc-WIN-50QO3EIRQVP

主机名“**WMSvc-WIN-50QO3EIRQVP**”出现了在以下关键 IP 地址上：

- **“78.46.185[.]251”**托管了 BADBAZAAR 的 C2 域名**“groupgram[.]org”**，据 Volexity 报告，该域名使用端口 4432 进行恶意通信。

- **“65.21.92[.]69”**和**“163.172.205[.]207”**托管了域名**“widelygram[.]org”**，据信该域名是 BADBAZAAR 的 C2 域名，因为在托管于这两个 IP 上的期间，端口 4432 处于开放状态。

- **“163.172.198[.]206”** 托管了域名 **“maxgram[.]org”**，据信该域名是 BADBAZAAR 的 C2 域名，因为其在被托管期间，端口 4432 处于开放状态。

（见附件 A，图 9）

WMSvc-WIN-50QO3EIRQVP 和 WIN-7LSBB9R0F1L

主机名“**WMSvc-WIN-50QO3EIRQVP”**和“**WIN-7LSBB9R0F1L**”被观察到同时出现在以下 IP 地址上：

- “**148.251.87[.]245**”托管了 BADBAZAAR 的 C2 域名“**flygram[.]org**”和“**groupgram[.]org**”。

（见附件 A，图 10）

WIN-N8H8S9BG2P0

主机名“**WIN-N8H8S9BG2P0**”被观察到出现在以下 IP 地址上：

- “**148.251.87[.]247**”托管了 BADBAZAAR 的 C2 域名“**omarwhatsapp[.]org**”和“**flygram[.]org**”。

（见附件 A，图 11）

WIN-I6VBN8MR92A

主机名“**WIN-I6VBN8MR92A**”被观察到出现在以下 IP 地址上：

- “**148.251.87[.]197**”托管了 BADBAZAAR 的 C2 域名“**tryhrwserf[.]com**”。

（见附件 A，图 12）

根据现有的商业数据，这些机器名称在互联网上出现的频率各不相同。其中一些主机名同时出现在多个 IP 地址上，表明这些虚拟机是通过同一个模板创建的。务必要注意，并非所有观察到这些主机名的 IP 地址都与恶意行为相关联。这可能意味着这些主机名的使用并非专属于这群威胁实施者。

然而，其中一些机器名称频繁出现在托管 BADBAZAAR C2 域名的 IP 地址上，这可能表明存在一个专门为恶意网络行为者配置机器的基础设施采购实体，用于支持其网络攻击行为。

社交媒体活动

Volexity 早前的报告显示，恶意网络行为者制作了（用于推广恶意应用程序的）YouTube 视频。这些视频包含了其所开发的应用程序使用教程。

NCSC 还发现了另外两个与威胁实施者行为有关的 YouTube 频道。URL 标识符为“**@josephjoey3499**”的 YouTube 频道似乎在推广名为“**Maxgram**”的应用，而另一个 URL 标识符为“**@uyghurapks3096**”的频道则在推广“**Uyghur APK Finder**”应用。

此外，推广“**Flygram**”和“**Signal Plus**”的 YouTube 视频中，威胁实施者公开了其使用的电话号码。在“**Flygram**”视频的 0:36 处可见电话号码“**+1 (570) 378-7250**”，而在“**Signal Plus**”视频中，则显示了电话号码“**+1 (267) 298 4259**”。

Volexity 报告了一个伪装成西藏主题新闻网站的域名“**ignitetibet[.]net**”，该网站出现在被认为由威胁实施者运营的 Telegram 频道中。据观察，电子邮件地址“**choekyi.wangmo@ignitetibet[.]net**”在页站“**tibetone.org**”上的帖子中发表留言，Lookout 公开报告称，该网站是 BADBAZAAR 在 iOS 版本中使用的 C2 页面。

该电子邮件地址据信是由威胁实施者控制的，使用了名为“**Choekyi Wangmo**”的虚假身份。

评估

评估 BADBAZAAR 和 MOONSHINE 使用多种社交工程手段来专门针对维吾尔人、藏人和台湾人社区，具体包括：

- 对这些社区感兴趣的应用程序进行木马化，例如维吾尔语应用程序《古兰经》，几乎可以确定是针对目标受害者群体量身定制的
- 将这些木马化的应用程序上传到官方应用商店，很可能赋予其一定的合法性，并且在群聊中进行分享，极有可能是为了利用这些社区内部的信赖关系进行传播

BADBAZAAR 和 MOONSHINE 收集的数据几乎可以肯定对中国政府具有价值。尽管据目前观察，BADBAZAAR 和 MOONSHINE 一直针对维吾尔人、藏人和台湾人，但还有其他恶意软件针对中国其他少数民族群体。来自共同签章国家的公民（无论是在中国境内还是海外），若被视为威胁政权稳定事业的支持者，几乎可以肯定会面临来自 BADBAZAAR 和 MOONSHINE 等移动装置恶意软件的威胁。这些恶意软件具备获取位置、音频和照片数据的能力，几乎可以肯定会通过提供目标者的实时活动信息，来为未来的监视和骚扰行动提供情报支持的机会。

MITRE ATT&CK®

本报告是对照 MITRE ATT&CK®框架编撰的，该框架是一个全球可以访问的知识库，基于现实世界中的观察，系统整理了对手的战术和技术手段。

战术	ID	技术	程序
侦察	T1593.001	搜索开放网站/域名：社交媒体	攻击者搜索与其目标受害者相匹配的在线群组和论坛，以便传播恶意软件
资源开发	T1583.001	获取基础设施：域名	威胁实施者为其命令和控制服务器注册域名
资源开发	T1587.001	开发能力：恶意软件	编写恶意代码，以插入木马化应用程序
资源开发	T1608.001	阶段能力：上传恶意软件	将木马化应用程序上传到包括应用商店在内的在线平台
资源开发	T1585.001	建立帐户：社交媒体账户	恶意行为者在网站和社交媒体上创建账户，用于分享和宣传恶意软件
资源开发	T1585.002	建立帐户：电子邮件帐户	恶意行为者使用自建和商业电子邮件账户来托管和传播恶意软件
初始访问	T1189	偷渡式泄露攻击	攻击者将恶意脚本隐藏在看似合法的应用程序中，并将其上传到应用商店
初始访问	T1566.003	网络钓鱼：通过服务进行鱼叉式网络钓鱼	恶意行为者通过 Telegram 等社交媒体向目标群体发送木马化的应用程序
执行	T1204.002	用户执行：恶意文件	受害者必须安装木马化应用程序，攻击者才能执行恶意载荷
防御逃避	T1027.009	混淆文件或信息：嵌入式有效载荷	将恶意载荷隐藏在看似合法的应用程序中
防御逃避	T1036.005	伪装：匹配合法名称或位置	将木马化的文件与合法应用程序的名称、外观和功能相匹配。
防御逃避	T1656	冒充	恶意行为者通过创建伪装网站并使用与目标群体相关的用户名，来冒充受信任的个人
收集	T1123	音频捕获	木马化的应用程序可能会请求不必要的权限，例如麦克风访问权限
收集	T1125	视频捕获	木马化的应用程序可能会请求不必要的权限，例如摄像头访问权限
收集	T1005	从本地系统获取数据	木马化的应用程序可能会请求不必要的权限，例如访问本地文件。
指挥与控制	T1071.001	应用层协议：Web 协议	恶意软件使用 HTTPS 和 WebSocket 协议与 C2 服务器建立通信。
指挥与控制	T1509	非标准端口	使用非标准端口，如端口 4432 和 2333

外传	T1041	通过 C2 通道外传	恶意软件使用 HTTPS 和 WebSocket 连接将数据外传。
影响	T1565.002	数据操控：传输数据篡改	恶意行为者通过启用应用程序中非必要的网络流量功能，来获取受害者的数据

指标

MOONSHINE:

- 2025 年 4 月 1 日对 VLiteUI 面板进行的搜索获得了以下结果：

IP 地址	端口	第一次看到的日期	最后一次看到的日期
103.254.108[.]87	888	2024 年 10 月 17 日	2025 年 2 月 14 日
43.159.192[.]7	444	2024 年 11 月 21 日	2025 年 2 月 13 日
103.27.109[.]109	444	2024 年 7 月 11 日	2025 年 2 月 7 日
45.119.99[.]83	444	2024 年 12 月 26 日	2025 年 1 月 24 日
103.254.108[.]76	444	2024 年 9 月 12 日	2024 年 12 月 5 日
194.71.107[.]160	444	2023 年 12 月 10 日	2024 年 11 月 1 日
103.254.108[.]108	444	2023 年 11 月 12 日	2024 年 9 月 25 日
103.56.17[.]194	444	2024 年 4 月 3 日	2024 年 8 月 23 日
103.254.108[.]87	444	2023 年 11 月 14 日	2024 年 8 月 15 日
62.72.58[.]168	444	2024 年 1 月 29 日	2024 年 8 月 7 日
103.43.18[.]43	444	2024 年 2 月 12 日	2024 年 7 月 19 日
77.91.123[.]208	444	2024 年 2 月 4 日	2024 年 4 月 9 日
46.246.98[.]229	444	2024 年 3 月 7 日	2024 年 3 月 26 日
2.58.15[.]101	444	2024 年 2 月 23 日	2024 年 2 月 27 日
46.246.98[.]209	444	2024 年 1 月 8 日	2024 年 2 月 14 日
103.254.108[.]87	8000	2023 年 10 月 17 日	2023 年 10 月 17 日
103.254.108[.]87	8080	2023 年 4 月 15 日	2023 年 10 月 16 日
103.254.108[.]108	9090	2023 年 4 月 13 日	2023 年 10 月 16 日
103.45.66[.]123	9090	2023 年 3 月 2 日	2023 年 4 月 8 日
103.45.66[.]32	8080	2022 年 7 月 29 日	2023 年 4 月 6 日
27.124.20[.]23	9090	2022 年 5 月 28 日	2023 年 3 月 24 日
27.124.20[.]22	9090	2022 年 5 月 28 日	2023 年 3 月 23 日
27.124.20[.]24	9090	2022 年 5 月 27 日	2023 年 3 月 17 日
69.176.94[.]148	9090	2023 年 3 月 4 日	2023 年 3 月 10 日
69.176.94[.]228	9090	2022 年 12 月 24 日	2023 年 2 月 25 日
103.253.40[.]137	8000	2022 年 6 月 24 日	2022 年 9 月 2 日
27.124.4[.]80	8080	2022 年 2 月 25 日	2022 年 6 月 23 日
27.124.4[.]81	8080	2022 年 2 月 25 日	2022 年 6 月 23 日
47.242.46[.]79	8080	2021 年 5 月 3 日	2022 年 6 月 17 日
27.124.4[.]82	8080	2022 年 2 月 24 日	2022 年 6 月 15 日
27.124.4[.]165	9090	2022 年 5 月 14 日	2022 年 5 月 28 日

27.124.4[.]184	9090	2022 年 5 月 14 日	2022 年 5 月 27 日
27.124.4[.]178	9090	2022 年 5 月 13 日	2022 年 5 月 26 日
103.15.28[.]165	8080	2022 年 3 月 5 日	2022 年 5 月 25 日
69.176.94[.]226	8080	2022 年 3 月 5 日	2022 年 4 月 22 日
27.124.4[.]3	8080	2022 年 3 月 11 日	2022 年 4 月 2 日
103.140.238[.]235	8080	2022 年 3 月 4 日	2022 年 4 月 1 日
27.124.4[.]2	8080	2022 年 3 月 12 日	2022 年 4 月 1 日
165.84.180[.]107	8000	2022 年 2 月 25 日	2022 年 3 月 19 日
69.176.94[.]156	8000	2022 年 2 月 25 日	2022 年 3 月 5 日
141.98.212[.]70	9090	2021 年 10 月 5 日	2022 年 3 月 4 日
5.188.33[.]50	8000	2022 年 2 月 15 日	2022 年 3 月 4 日
5.188.70[.]193	8000	2022 年 2 月 15 日	2022 年 3 月 4 日
69.176.94[.]140	8080	2022 年 2 月 24 日	2022 年 2 月 24 日
27.124.20[.]83	8000	2022 年 2 月 14 日	2022 年 2 月 18 日
208.87.200[.]106	8000	2022 年 1 月 2 日	2022 年 1 月 2 日
121.127.241[.]37	8000	2021 年 12 月 8 日	2021 年 12 月 8 日
156.255.2[.]211	443	2021 年 10 月 5 日	2021 年 10 月 5 日
156.255.2[.]211	8000	2021 年 10 月 4 日	2021 年 10 月 4 日
156.255.2[.]203	8000	2021 年 10 月 3 日	2021 年 10 月 3 日
47.243.43[.]248	8000	2021 年 7 月 5 日	2021 年 7 月 5 日
45.115.236[.]6	8080	2021 年 5 月 3 日	2021 年 6 月 1 日
43.251.118[.]97	8000	2021 年 1 月 3 日	2021 年 3 月 1 日
185.243.43[.]138	8000	2021 年 1 月 4 日	2021 年 2 月 2 日
47.245.59[.]33	8000	2021 年 1 月 5 日	2021 年 1 月 5 日

- 2025 年 4 月 1 日对 SCOTCH ADMIN 面板进行的搜索获得了以下结果：

IP 地址	端口	第一次看到的日期	最后一次看到的日期
104.194.152[.]24	2333	2025 年 2 月 6 日	2025 年 2 月 27 日
172.86.80[.]126	2333	2025 年 2 月 7 日	2025 年 2 月 27 日
154.90.59[.]62	2333	2024 年 6 月 20 日	2024 年 9 月 20 日
154.90.59[.]88	2333	2024 年 6 月 21 日	2024 年 9 月 20 日
154.90.58[.]210	2333	2024 年 5 月 16 日	2024 年 6 月 14 日
154.90.59[.]225	2333	2024 年 5 月 17 日	2024 年 6 月 13 日
38.60.199[.]208	2333	2023 年 11 月 26 日	2024 年 1 月 9 日
38.60.199[.]254	2333	2023 年 11 月 28 日	2024 年 1 月 9 日
38.60.199[.]99	2333	2023 年 8 月 26 日	2023 年 11 月 21 日

38.60.199[.]44	2333	2023 年 7 月 20 日	2023 年 9 月 11 日
194.163.34[.]23	443	2022 年 9 月 30 日	2023 年 4 月 14 日
45.32.125[.]112	10443	2022 年 10 月 1 日	2023 年 3 月 17 日

- 2024 年 3 月 14 日对虚拟 SCOTCH ADMIN 面板进行的搜索获得了以下结果：

域名	IP 地址
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：

描述	在 **BADBAZAAR C2s** 上观察到的 **SSL** 证书。
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- 2025 年 4 月 1 日对上述 BADBAZAAR 证书进行的搜索返回了以下结果：

IP 地址	端口	第一次看到的日期	最后一次看到的日期
65.108.192[.]173	31237	2025 年 3 月 14 日	2025 年 3 月 28 日
65.108.192[.]173	31236	2025 年 3 月 14 日	2025 年 3 月 28 日
65.108.192[.]173	31235	2025 年 3 月 14 日	2025 年 3 月 28 日
157.90.129[.]73	31236	2025 年 3 月 27 日	2025 年 3 月 27 日
142.132.131[.]15	31236	2024 年 7 月 24 日	2025 年 3 月 27 日

142.132.131[.]15	31235	2024 年 7 月 26 日	2025 年 3 月 27 日
142.132.131[.]20	31237	2023 年 8 月 11 日	2025 年 3 月 27 日
142.132.131[.]15	31237	2024 年 7 月 24 日	2025 年 3 月 27 日
142.132.131[.]20	31236	2023 年 9 月 27 日	2025 年 3 月 26 日
142.132.131[.]20	31235	2023 年 10 月 18 日	2025 年 3 月 26 日
65.108.192[.]155	31236	2024 年 12 月 5 日	2025 年 2 月 20 日
65.108.192[.]155	31237	2024 年 12 月 5 日	2025 年 2 月 20 日
65.108.192[.]155	31235	2024 年 12 月 5 日	2025 年 2 月 19 日
23.88.28[.]222	31237	2024 年 4 月 25 日	2024 年 11 月 29 日
23.88.28[.]222	31235	2024 年 5 月 2 日	2024 年 11 月 28 日
23.88.28[.]222	31236	2024 年 5 月 1 日	2024 年 11 月 28 日
212.129.21[.]168	31235	2023 年 10 月 16 日	2024 年 3 月 17 日
212.129.21[.]168	31237	2023 年 8 月 24 日	2024 年 3 月 17 日
212.129.21[.]168	31236	2023 年 9 月 26 日	2024 年 3 月 14 日

描述	在 **BADBAZAAR C2s** 上观察到的 **SSL** 证书
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- 2025 年 4 月 1 日对上述 BADBAZAAR 证书进行的搜索获得了以下结果：

IP 地址	端口	第一次看到的日期	最后一次看到的日期
162.55.103[.]211	20122	2023 年 1 月 12 日	2025 年 3 月 28 日
162.55.103[.]212	20121	2022 年 6 月 30 日	2025 年 3 月 28 日
162.55.103[.]212	20122	2023 年 7 月 14 日	2025 年 3 月 28 日
162.55.103[.]211	20121	2022 年 6 月 3 日	2025 年 3 月 28 日
162.55.103[.]211	20123	2023 年 7 月 22 日	2025 年 3 月 27 日
162.55.103[.]212	20123	2023 年 7 月 22 日	2025 年 3 月 27 日
212.83.162[.]152	9090	2022 年 10 月 13 日	2025 年 3 月 27 日
23.88.28[.]221	20422	2023 年 7 月 28 日	2023 年 9 月 30 日
23.88.28[.]221	20421	2023 年 5 月 18 日	2023 年 9 月 28 日

23.88.28[.]221	20423	2023 年 7 月 28 日	2023 年 9 月 28 日
162.55.103[.]210	20121	2022 年 9 月 30 日	2023 年 2 月 23 日
65.21.92[.]67	20121	2021 年 11 月 2 日	2022 年 10 月 13 日
65.21.92[.]67	20122	2022 年 8 月 10 日	2022 年 10 月 13 日
23.88.28[.]220	20121	2021 年 12 月 8 日	2022 年 5 月 13 日
94.130.92[.]230	20121	2021 年 1 月 4 日	2021 年 10 月 5 日
88.99.150[.]246	20121	2021 年 4 月 6 日	2021 年 9 月 8 日
45.76.132[.]91	20121	2021 年 2 月 2 日	2021 年 3 月 1 日

WHOIS 域名

以下是一个域名表格，下列域名目前或历史上在 WHOIS 记录中的字段值与 BADBAZAAR C2 域名中观察到的值相匹配。

WHOIS 值	域名
注册人所在州：**UJYJYUJ** 注册人所在国家：玻利维亚 注册商：**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
注册人所在州：**REWR** 注册人所在国家：**CF** 注册商：**eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

注册人所在州：**FSDF** 注册人所在国家：**AL** 注册商：**eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

电子邮件地址
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

以下是与 BADBAZAAR 和 MOONSHINE 相关的其他攻击指标（IoC）的链接。NCSC 无法确认这些链接中所有信息的有效性，建议读者独立验证其准确性和相关性：

- ESET
- 趋势科技（Trend Micro）
- Lookout
- Lookout
- Volexity
- 公民实验室(Citizen Lab)

缓解措施

NCSC 鼓励采纳以下建议来防范案例研究中所述的威胁。

- **应用商店运营商（包括第三方应用商店）和开发者应确保其平台上的应用安全，并遵守政府的行为准则。**请参阅指南：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

- **多语言支持：**应用程序开发商应投入精力将热门应用程序本地化，以针对目标群体中讲少数民族语言的用户，包括使用维吾尔语、藏语、台湾闽南语和粤语的用户。Apple 关于在应用程序中进行本地化的指南：https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app。Google 关于翻译应用程序的指南：https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **确保您的社交媒体平台安全：**社交媒体公司可以通过各种措施，使恶意网络行为者更难在其平台上本是合法的在线社区中创建虚假账户及分享恶意文件或链接。在可能的情况下，公司应与更广泛的行业共享恶意指标，提高对威胁的集体了解，并帮助采取保护措施。

- **客户补救计划：**组织应配备程序来通知使用其服务并安装了恶意应用程序的客户。这些警报应引人注意且信息详实。在适当的情况下，组织应提供有关如何删除软件的指南，并鼓励受害者向管理部门（如英国的 NCSC）举报。
  有关更多信息，请参阅《App Store 行为准则》（App Store Code of Practice）：https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **组建工作组开展协作：**社交媒体公司可以组建工作组，允许各自的安全团队共享恶意指标、TTPs 和观察结果，使威胁实施者更难利用其平台支持恶意行为。

- **检测被修改的应用程序：**在可能的情况下，应用程序开发人员应加入提示功能，即在用户下载"非官方"版本程序时提示用户，从而帮助防范恶意仿冒应用。

附录 A：BADBAZAAR WHOIS 聚类/域名经纪人信息图表

图 1 – “UKYJYUJ”

图 2 – 键盘行走密码

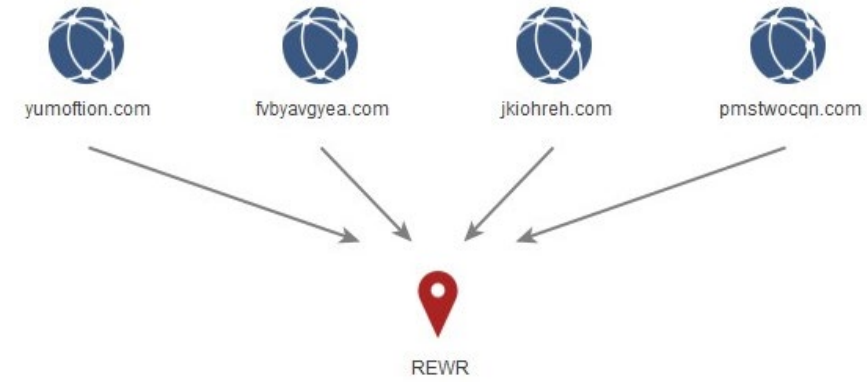


图 3 – 具有“FSDF”状态字段密码的其他域名

图 4 – **95.179.210[.]85**

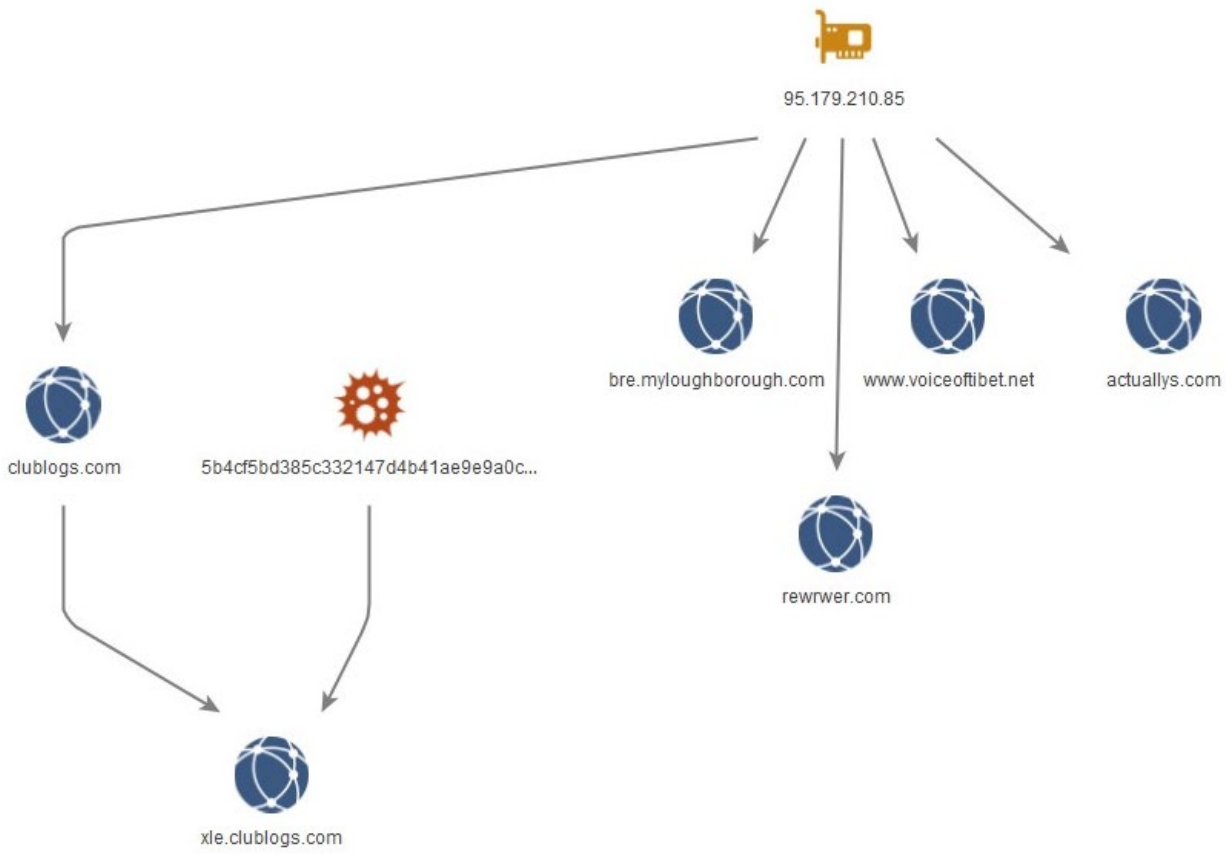


图 5 – WHOIS 连接

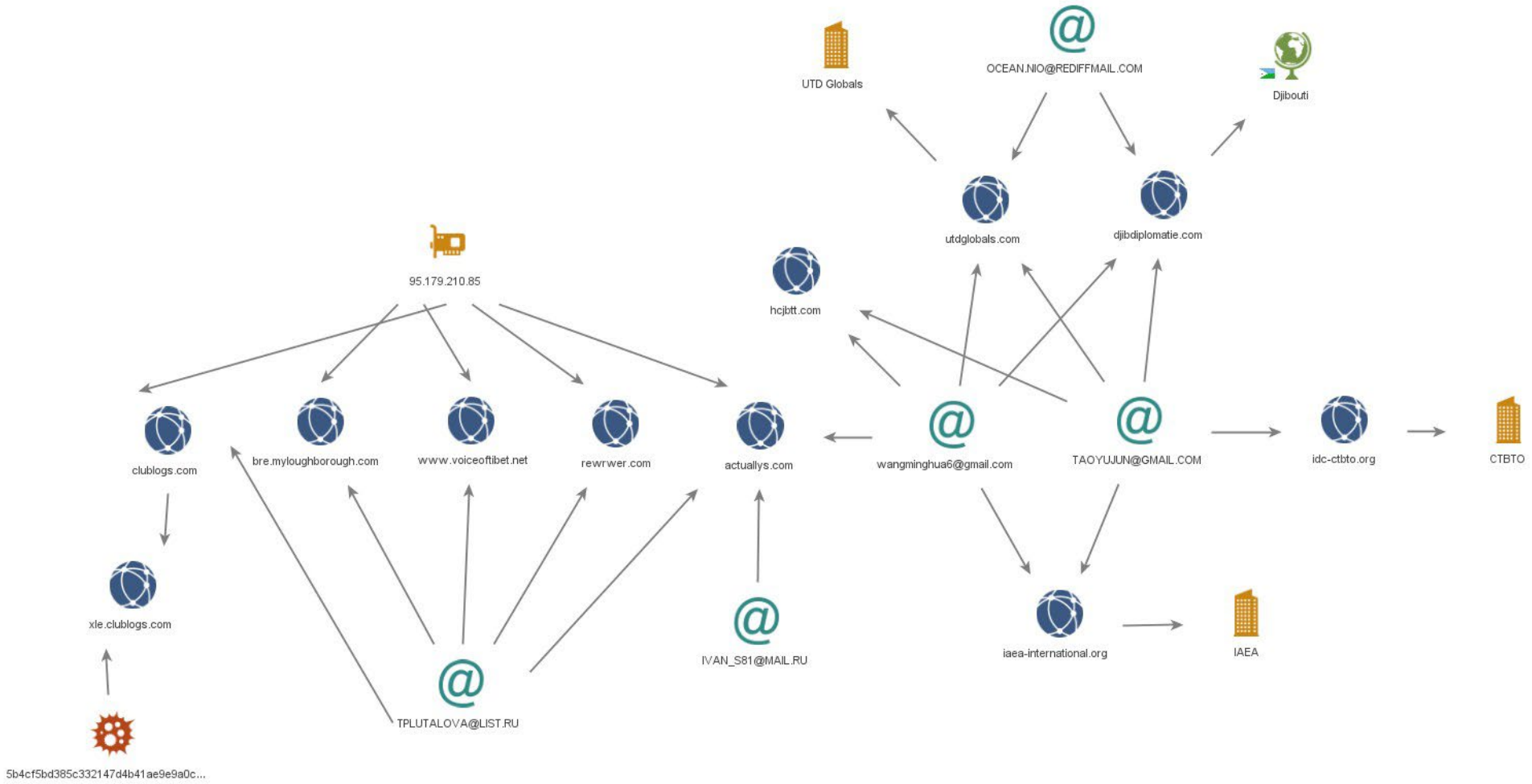

UTD Globals
OCEAN.NIO@REDIFFMAIL.COM
Djibouti
utdglobals.com
djibdiplomatie.com
95.179.210.85
hcjbtt.com
clublogs.com
bre.myloughborough.com
www.voiceoftibet.net
rewrwer.com
actuallys.com
wangminghua6@gmail.com
TAOYUJUN@GMAIL.COM
idc-ctbto.org
CTBTO
xle.clublogs.com
IVAN_S81@MAIL.RU
iaea-international.org
IAEA
TPLUTALOVA@LIST.RU
5b4cf5bd385c332147d4b41ae9e9a0c...

图 6 – **WIN-EU0VLBL7TUJ**

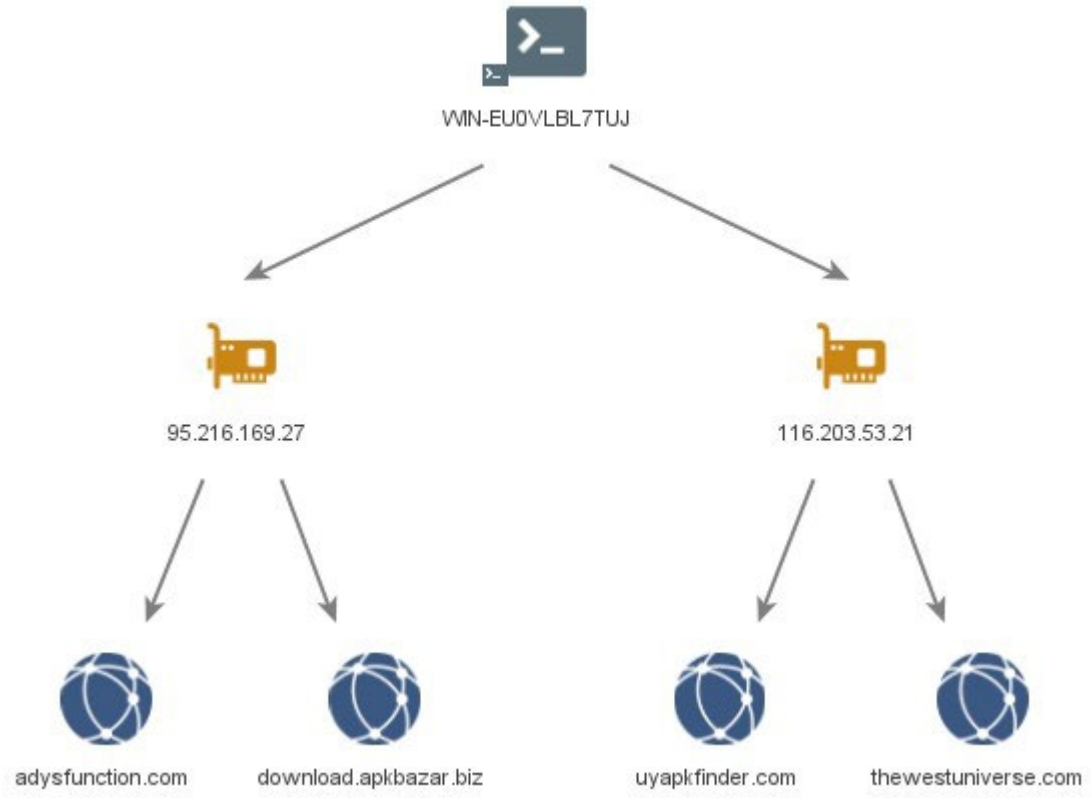


图 7 – **WIN-70E59JVOB9G**

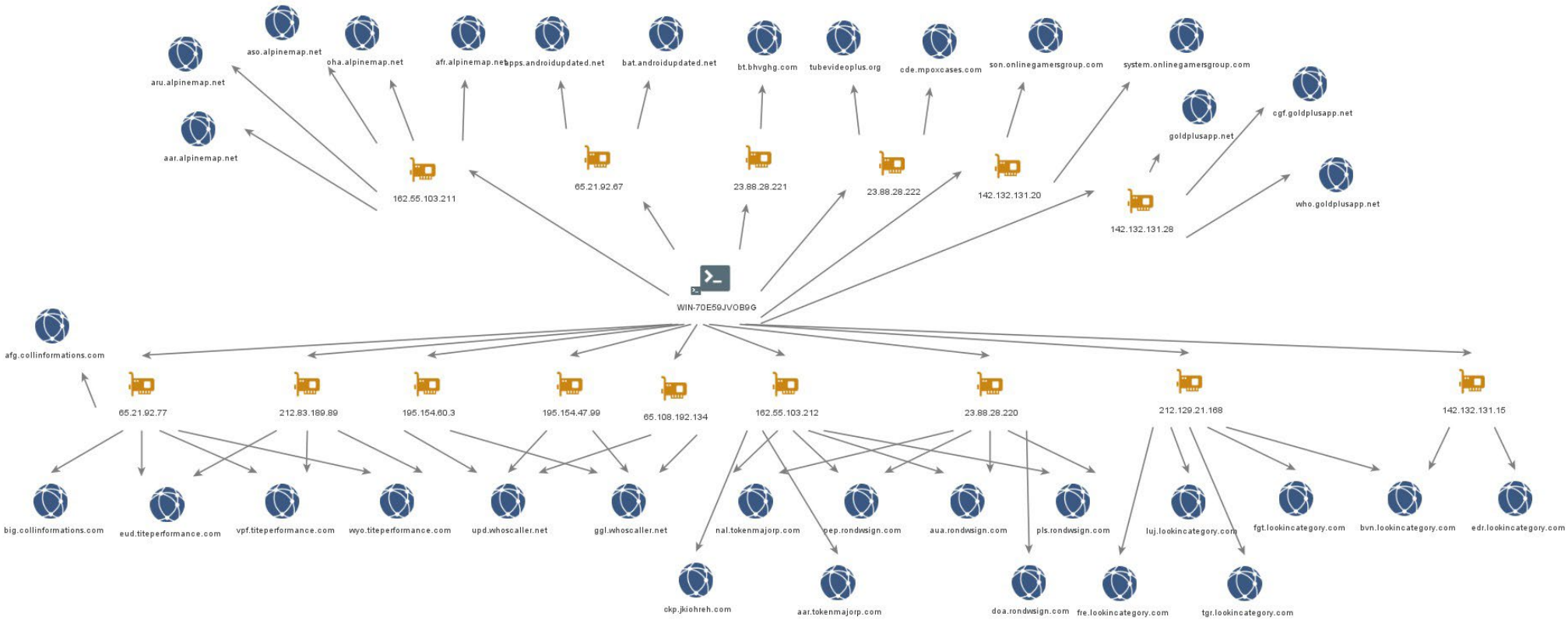


图 8 – **WIN-50QO3EIRQVP**

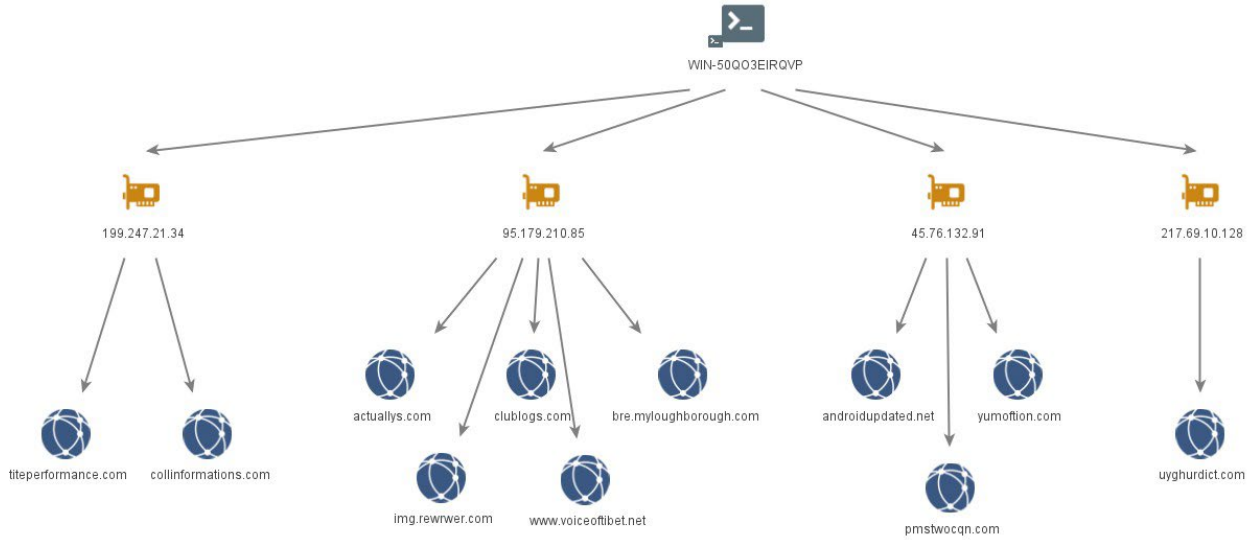


图 9 – **VMSvc-WIN-50QO3EIRQVP**

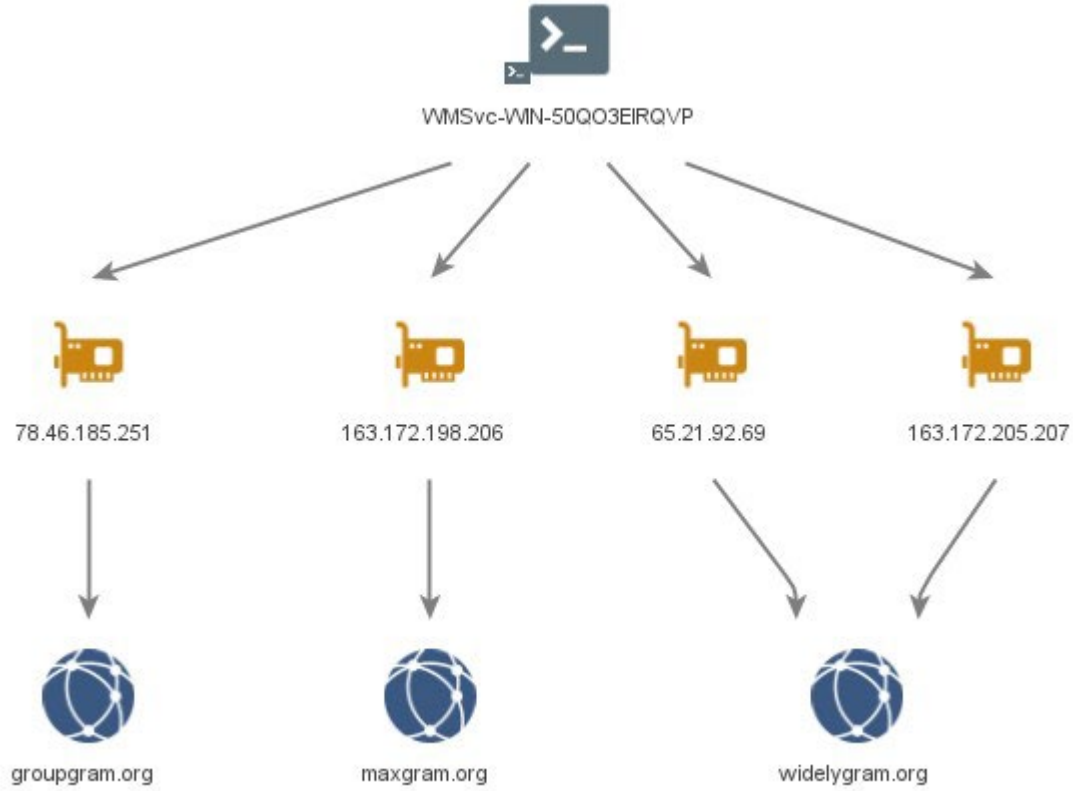


图 10 – **VMSvc-WIN-50QO3EIRQVP** 和 **WIN-7LSBB9R0F1L**

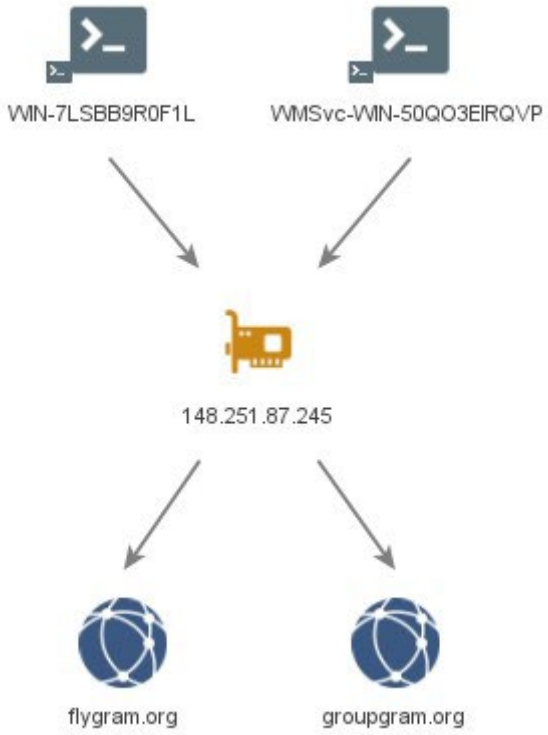


图 11 – **WIN-N8H8S9BG2P0**

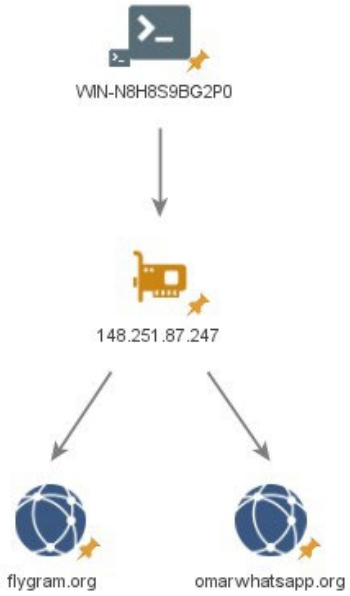


图 12 – **WIN-I6VBN8MR92A**

附录 B：已观察到的 MOONSHINE 和 BADBAZAAR 样本

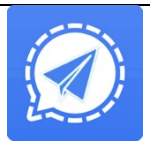
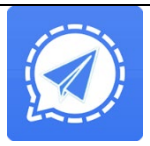
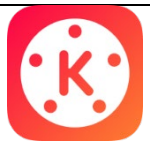
下表列出了过去两年在 MOONSHINE 和 BADBAZAAR 行动中使用的应用程序。

其中许多应用程序与现有应用程序有明显的相似性。这很可能是恶意行为者故意“仿冒”知名品牌的手段。

务必要注意，应用程序的名称、软件包名称和图标都可能模仿或完全复制真实的应用程序，因此不能仅凭这些特征来判断设备是否被感染。

应用程序名称	软件包名称	应用程序图标
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	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	

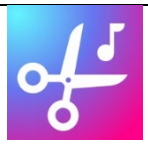
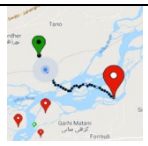
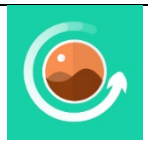
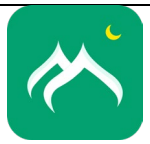
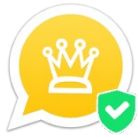
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur 输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra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

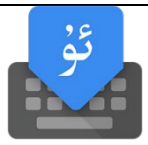
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video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

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

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

延伸阅读

以下是澳大利亚网络安全中心的指南

- 报告网络犯罪、事件或漏洞
- 如何保护您的设备安全
- 保护您的手机安全
- 钓鱼攻击
- 诈骗
- 保护您的社交媒体账户安全
- 社交媒体和通讯应用的安全建议

以下是英国 NCSC 和 NPSA 的指南

- 捍卫民主
- 社交媒体：如何安全使用
- 包括移动设备在内的组织设备安全指南
- 关于应用商店的威胁报告。
- 高风险个体的个人安全和安保

以下是美国国家安全局（NSA）的指南

- 移动设备最佳操作规范

免责声明

请注意，本公告提供的信息在发布时已经过验证。

本报告借鉴了来自编制机构和行业渠道的信息。其中的任何调查结果及建议并非旨在完全规避所有风险，并且遵循这些建议无法完全消除相关风险。信息风险的责任始终由相关系统的所有者承担。

在英国，此类信息根据《2000 年信息自由法》（简称 FOIA）被豁免公开，亦可能受其他英国信息立法的豁免条款保护。

如有任何 FOIA 相关查询，请发送电邮至 ncscinfoleg@ncsc.gov.uk。