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：

技術分析和緩解措施

2025 年 4 月 9 日

BADBAZAAR 和 MOONSHINE：技術分析和緩解措施

概要

在英國 網路聯盟 (Cyber League) 的支持下，英國國家網路安全中心 (NCSC UK) 和國際合作夥伴共同發布了此公告：

- **澳洲網路安全中心，隸屬於澳洲信號局**
- **加拿大網路安全中心，隸屬於加拿大通訊安全機構**
- **德國聯邦情報局**
- **德國聯邦憲法保衛局**
- **紐西蘭國家網路安全中心，隸屬於紐西蘭政府通訊安全局**
- **美國聯邦調查局**
- **美國國家安全局**

本公告提供了有關 BADBAZAAR 和 MOONSHINE 這兩種間諜軟件變種的最新和經整理的威脅情報，並為應用商店運營商、開發人員和社交媒體公司提供建議，以協助保障其用戶的安全。

此公告與另一**份針對這些惡意軟件受害人士的公告**同時發布。

本文件採用了 NCSC 詞彙表中對間諜軟件的定義：「一種未經用戶同意就安裝在裝置上，並收集資料然後將傳送給第三方的惡意軟件。」

個案研究（一）：**MOONSHINE**

MOONSHINE 是一款 Android 間諜軟件，由公民實驗室 (Citizen Lab) 於 2019 年報告，指其針對的是藏族群體。MOONSHINE 偽裝成合法的應用程式以引誘受害者安裝。這應用程式是透過 Telegram 頻道和 WhatsApp 發送的連結分享。

NCSC 對 MOONSHINE 的研究顯示：

- MOONSHINE 使用的管理介面自首次通報後已經有變化。
- 管理介面展示了廣泛的監控功能，包括從設備中外傳文件，以及錄取即時音訊和錄影屏幕畫面的能力。
- 亦發現了一組虛擬託管的 MOONSHINE 管理介面。這些介面的基礎設施與 UPSEC 相關的登入面板重疊，根據 情報在線 (Intelligence Online) 的說法，UPSEC 指的是「四川電科網路安全技術有限公司」。

管理介面

因 MOONSHINE 的管理介面和早前通報時已有所變化，這表明程式正在持續開發。

管理介面的第一個範例是來自公民實驗室 2019 年的報告。

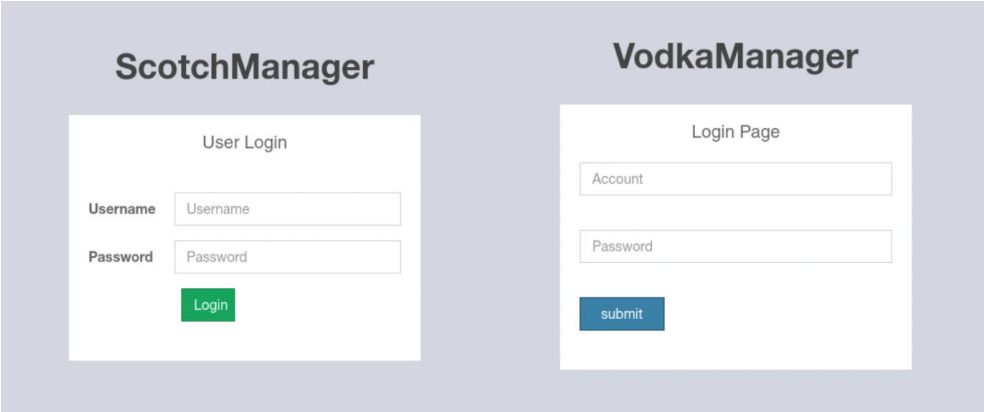


*圖 1:*公民實驗室 2019 年的報告《利用一鍵移動漏洞以入侵西藏群體》中所引用的 MOONSHINE 管理介面。

2022 年初，Lookout 通報了一個不同的管理介面，該介面經重新設計成如下（取代了圖 1 的舊介面）：

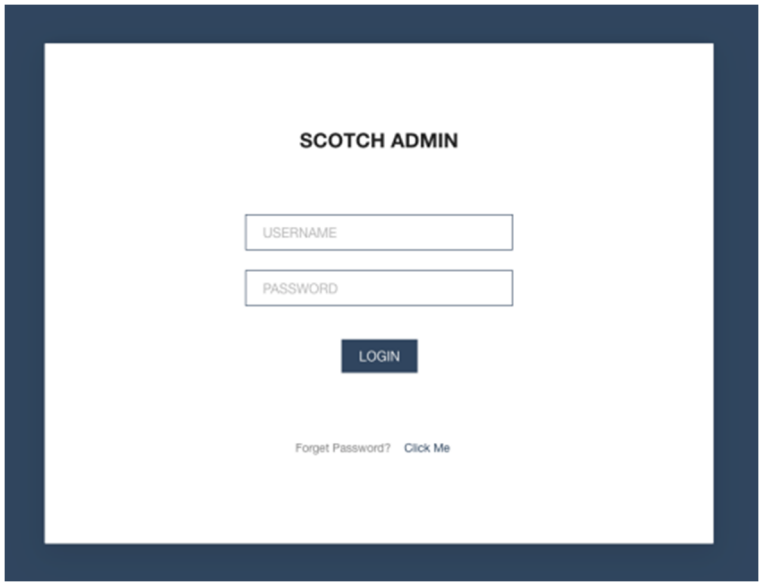


圖 2:Lookout 2022 年的 報告中所引用的 MOONSHINE 管理介面：中國的 APT POISON CARP 不斷改進 Android 監控軟件，以針對藏族和維吾爾族人。

在 2023 年 8 月，對 MOONSHINE 指令與控制 (C2) 的 掃描 發現了一個與 2022 年介面類似的介面，其中「**Forget Password (忘記密碼)**」的功能不再可用，如圖 2 所示：

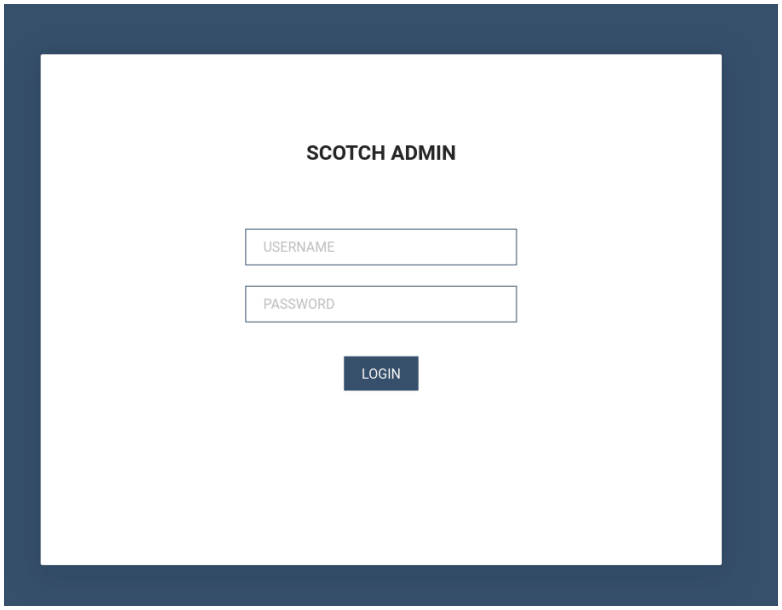


圖 3:MOONSHINE 管理介面於 2023 年 8 月被觀察到不再出現「忘記密碼」提示。

對管理介面的進一步調查顯示，面板內容揭示了受感染設備的詳細資訊將如何 儲存。

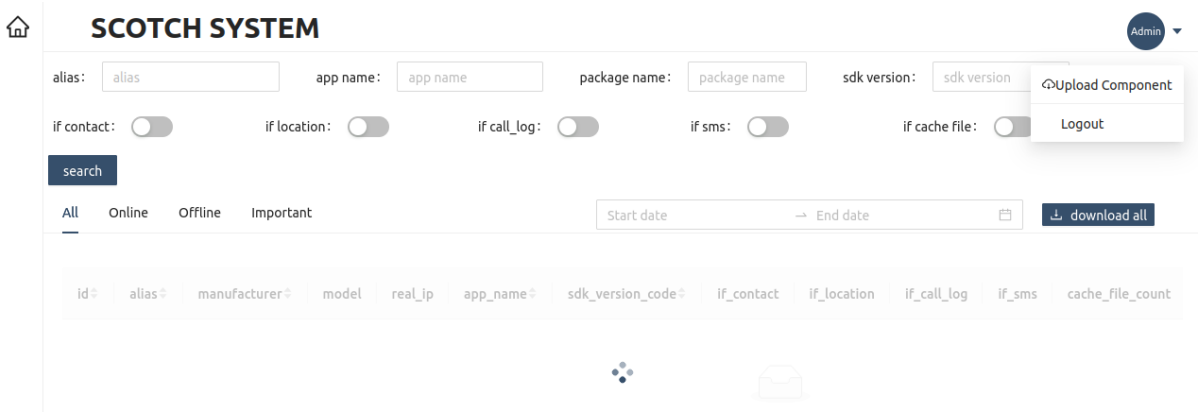


圖 4:於 MOONSHINE 管理介面頁面登入後的網頁。

Lookout 的研究顯示，受害者裝置會將「**分數**」傳遞到 MOONSHINE C2 伺服器。「分數」值取決於受害者裝置上惡意樣本的權限。

頁面中的「if_contact」、「if_location」、「if_call_log」和「if_sms」欄位顯示，並非所有 MOONSHINE 的樣本，都對受感染裝置有全權存取。透過了解這些欄位，以及從裝置傳遞到 C2 的「分數」，估計威脅行為者正在使用分數，將惡意軟件對受感染裝置的存取等級，傳達給存取管理介面的人士。

一般來說，防止應用程式從裝置收集資訊的最佳實務建議，是在下載之前檢查應用程式權限有否異常。然而，MOONSHINE 樣本尋求的權限是與應用程式功能相關，因此看起來並不可疑，但它們是利用這些權限從設備收集資訊。

MOONSHINE 還有應用程式介面 (API)，顯示其具有廣泛的功能。API 文件的早期版本是包含普通話拼音名稱。

虛擬主機

在搜尋 MOONSHINE 的面板時，亦發現了其虛擬託管。虛擬主機是指一個 IP 位址可以同時託管多個網站。這些虛擬主機的 IP 位址和網域並未觀察到有惡意軟件的樣本。

這些管理介面的實例有所不同，因為頁面的標題是「**LOGIN**」，而不是之前看到的「**SCOTCH ADMIN**」。

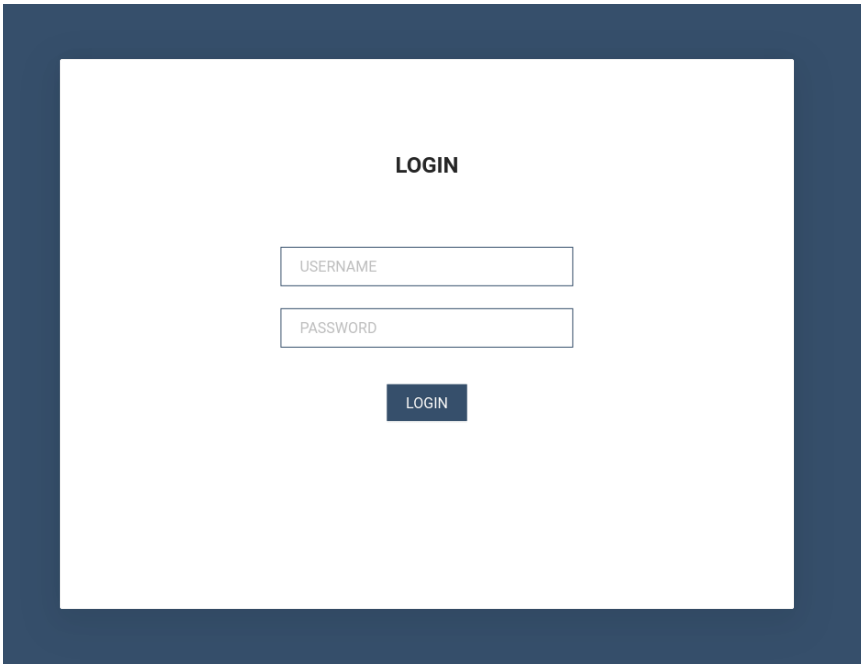


圖 5:MOONSHINE 管理介面使用 LOGIN 標題取代 SCOTCH ADMIN。

另外，面板上的內容也與圖 4 有所不同，如圖 6 所示：

*圖 6:*虛擬託管的 MOONSHINE 管理介面登入頁面後的網頁。

圖 6 的面板似乎是圖 4 面板的簡化版本。同樣出現的面板特徵是表格中的列名「id」、「製造商」和「型號」。

發現的虛擬託管的 MOONSHINE 場合包括：

網域	IP 位置
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

這些網域被 趨勢科技(Trend Micro) 列為 MOONSHINE 漏洞利用工具包，負責利用瀏覽器的漏洞，在移動裝置上安裝惡意軟件。趨勢科技將該惡意軟件命名為「Dark Nimbus」。

需要澄清的是，MOONSHINE 管理介面是 MOONSHINE 惡意軟件樣本進行通訊，並將受害者資料外洩至的介面。而趨勢科技通報的 MOONSHINE 入侵工具包，則具獨立能力，能利用瀏覽器漏洞在移動裝置上安裝名為 Dark Nimbus 的惡意軟件。而且，Dark Nimbus 和 MOONSHINE 是完全不同的惡意軟件。

MOONSHINE 管理介面和 MOONSHINE 入侵工具包都有程式碼重疊，因此圖 3 和圖 5 中的登入提示，以及圖 4 和圖 6 中的頁面內容有所相似。它們的原始程式碼中都包含字串「webpackJsonpreact-scotchui」。

威脅行為者會產生 URL 連結，連結至 MOONSHINE 的入侵工具包，然後重定向到和藏族和維吾爾族相關的影片，這與 MOONSHINE 的目標相同。

在許多託管 MOONSHINE 入侵工具包的地址上，都在連接埠 444 上有一個名為「VLiteUI」的登入頁面。這頁面並非常見，它存在於這些 IP 上，表明可能是與攻擊者的操作有所關聯。

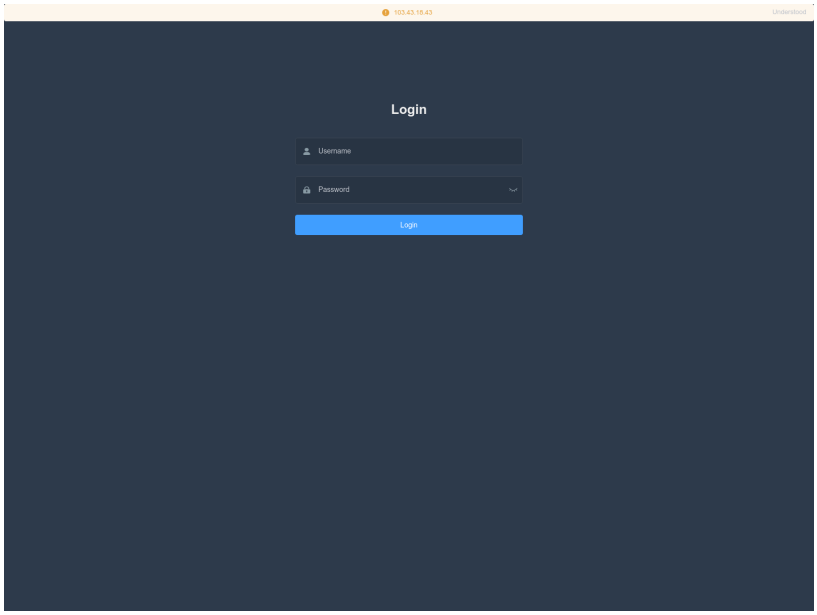


圖 7:在託管 MOONSHINE 入侵工具包的 IP 上觀察到帶有 HTML 標題「VLiteUI」的登入面板。

趨勢科技對 Dark Nimbus 的分析表明，該惡意軟件可以收集裝置上的詳盡資訊列表，並且利用 XMPP 協定與 C2 進行通訊。

趨勢科技也概述在 Dark Nimbus 的某些版本中，他們發現了字串「DKNS」經常存在。

也留意到在其他標題中帶有 DKNS 的網頁，其 IP 位址的 XMPP 服務中也留意到有「**ansec[.]com**」（ TrendMicro 列其為 Dark Nimbus C2）：

- 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)

XMPP 服務中另一組帶有「**ansec[.]com**」的 IP 位址，其網頁標題為：

- 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)

根據情報在線 (Intelligence Online)的報告，HTML 頁標題中出現的「UPSEC」指的是「四川電科網路安全技術有限公司」。

個案研究（二）：**BADBAZAAR**

BADBAZAAR 是一種具有 iOS 和 Android 版本的惡意移動應用軟件 ，以維吾爾族、藏族和台灣人為目標。本惡意軟件是透過社交媒體和官方應用程式商店傳播。Volexity 最近的報告顯示了 BADBAZAAR 的不同變種，分別稱為 BadSolar、BADBAZAAR 和 BadSignal。這三種變體因具備重疊功能而互相聯繫，用於收集裝置和操作員資訊。

NCSC 對 BADBAZAAR 的研究揭示了以下情況：

- 聚合的 C2 網域揭露了與以往威脅通報中的的其他網域存在進一步聯繫。
- C2 伺服器和惡意軟件樣本揭露了與攻擊者基礎設施相關的主機名稱。
- 威脅行為者會利用社會工程手段，將惡意軟件傳播至官方應用商店以外。

WHOIS 叢集/網域經紀人

'UJYJYUJ'

對 BADBAZAAR 網域「**signalplus[.]org**」的 WHOIS 記錄的分析（由 ESET 報告）顯示，「State」欄位中的值為「**UJYJYUJ**」。

以這個值作為條件，搜尋具有相同數值的其他網域後，得出下列值得留意的網域：

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

（見附件 A，圖 1）

域名 **signalplus[.]org**、**tubevideoplus[.]org** 和 **thetubeplus[.]com** 均被報告為 BADBAZAAR C2 域名，而 ESET 通報的子域名 **mail.pmumail[.]com** ，是 FlyGram 的代理伺服器。FlyGram 是一款由惡意網路行為者開發的 BADBAZAAR 應用程式（請參閱附錄中其他 BADBAZAAR 應用程式清單）。

鍵盤行走值

NCSC 也留意到在其他已註冊的 BADBAZAAR C2 網域中，發現了類似的鍵盤行走模式。

舉例，下列網域的「**State** 」欄位值含有「**REWR**」（如前所述）：

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

（見附件 A，圖 2）

網域的 State 欄位值具有「FSDF」

另一組 BADBAZAAR C2 網域的「**State**」值為「**FSDF**」：

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

（見附件 A，圖 3）

紀錄過往鍵盤步行值的報告

在 TA413 過往報導針對西藏人組織的攻擊中，也可以看到 BADBAZAAR 網域的 WHOIS 記錄內所含的鍵盤行走值。Recorded Future 留意到有攻擊者控制的網域名稱冒充西藏人組織，並使用「**asfasf**」在註冊組織值。

clublogs[.]com

Lookout 取得的 BADBAZAAR 樣本包含'xle.clublogs[.]com'作為 C2 網域。根網域「**clublogs[.]com**」存放託管在 IP 位址「**95.179.210[.]85**」上，並具有 SSL 證書，其主題和頒發者值為「**CN=WIN-50QO3EIRQVP**」。該值與 BADBAZAAR 樣本中的 SSL 憑證相匹配，該樣本是使用 SSL 固定來避免通訊被攔截。

IP 位址 **95.179.210[.]85** 的託管歷史記錄，有下列讓人留意的網域：

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

（見附件 A，圖 4）

www.voiceoftibet[.]net

網域「**www.voiceoftibet[.]net**」似乎是偽裝成「西藏之聲」廣播電台，手法類似於 TA413 所使用的 TTP。

網域「**rewrwer[.]com**」與先前在 BADBAZAAR 網域的 WHOIS 記錄中，所發現的「**State**」值「**REWR**」相似。

網域「**clublogs[.]com**」、「**rewrwer[.]com**」、「**voiceoftibet[.]net**」和「**myloughborough[.]com**」的註冊電子郵件地址都是「**tplutalova@list[.]ru**」。

actuallys[.]com

「**actuallys[.]com**」的 WHOIS 記錄顯示，技術人員和管理員的電子郵件地址為「**tplutalova@list[.]ru**」，但註冊者的電子郵件地址為「**ivan_s81@mail[.]ru**」。

網域「**actuallys[.]com**」的 WHOIS 資訊歷史紀錄列出，註冊郵箱在 2016 年 2 月 24 日是「**wangminghua6@gmail[.]com**」。在 2016 年 3 月 11 日，該電子郵件地址隨後更改為「**ivan_s81@mail.ru**」，但註冊商的註冊到期日保持不變。

wangminghua6@gmail[.]com

電郵地址「**wangminghua6@gmail[.]com**」在過往的威脅情報報告中曾被提及。在 2015 年，Palo Alto 發現該電郵地址用於為惡意軟件 Cmstar 的 C2 網域註冊。在 2014 年，Mandiant 發現該電郵用於註冊 APT3 發起的網路釣魚活動中的網域。2013 年，該電郵曾用於註冊 CrowdStrike 的一個惡意軟件植入程式的網域，而該惡意軟件的程式資料庫 (PDB) 路徑包含中文字符，顯示是在中文系統上進行編寫。

taoyujun@gmail[.]com

網域「**hcjbtt[.]com**」的註冊電郵地址為「**taoyujun@gmail[.]com**」，但管理員信箱的註冊是「**wangminghua6@gmail[.]com**」。

雖然未有顯示網域「**hcjbtt[.]com**」和任何惡意活動有所關連，但在過往的威脅情報報告中，曾提及電郵地址「**taoyujun@gmail[.]com**」。在 2014 年，Mandiant 發現該電郵用於註冊的網域，是被用於針對日本組織的「Cueisfry 木馬」。

該電子郵件地址還註冊了其他域名，如「**iaea-international[.]org**」似乎是為了偽裝成國際原子能機構，以及「**idc-ctbto[.]org**」似是為了偽裝成**全面禁止核試驗條約組織 (CTBTO)** 中的國際數據中心。

早期 Whois 記錄顯示，網域「**iaea-international[.]org**」的註冊者電郵地址是「**wangminghua6@gmail[.]com**」。

udtglobals[.]com

我們發現網域名稱「**udtglobals[.]com**」是使用「**wangminghua6@gmail[.]com**」作為管理員信箱，和「**ocean.nio@rediffmail[.]com**」作為註冊者信箱地址。其他 WHOIS 記錄顯示，該網域的註冊者電子郵件相同，但管理員電郵地址為「**taoyujun@gmail[.]com**」。

「**udtglobals[.]com**」似乎是為了偽裝成「**UDT Global**」一一項海底防禦和保安相關的全球性活動。電郵地址中的使用者名稱「**ocean.nio**」或是模仿多個國家的**國家海洋研究所（NIO）**。雖然使用「**Rediff**」電子郵件服務（總部位於印度）亦可是暗示模仿成**印度國家海洋研究所**。

Djibdiplomatie[.]com

網域「**djibdiplomatie[.]com**」似乎為了偽裝成吉布地的外交部門，其 WHOIS 記錄與「**utdglobals[.]com**」相類似。一項記錄顯示註冊者為「**ocean.nio@rediffmail[.]com**」，管理員為「**taoyujun@gmail[.]com**」，而其他記錄顯示管理員電郵件地址為「**wangminghua6@gmail[.]com**」，註冊者電郵地址為「**ocean.nio@rediffmail[.]com**」。

這兩個網域在 WHOIS 記錄中，也都有類似的鍵盤行走類型值。例如，「**udtglobals[.]com**」的註冊者城市值為「**ASDF**」，而「**djibdiplomatie[.]com**」的註冊者名稱值為「**DAF DAGF**」。這與在其他 BADBAZAAR 網域中所觀察到的值是相近類似。

雖然在 WHOIS 記錄中發現的電郵「**wangminghua6@gmail[.]com**」和「**taoyujun@gmail[.]com**」，是存在於偽裝成**全球海底防禦活動**、**吉布地外交服務**和**國際原子能機構**的網域，但這些電郵也存在於數個非惡意網域的 WHOIS 記錄中。

偽裝域名和非惡意域名的混合使用，或表明存在用於支援惡意網路行為者行動的基礎設施採購實體。

電子郵件地址「**ocean.nio@rediffmail[.]com**」僅出現在上述的偽裝網域中。而「**ivan_s81@mail[.]ru**」和「**tplutalova@list[.]ru**」分別註冊了極少數域名，其中一些域名託管在 BADBAZAAR 的基礎設施上。這三個電郵地址被認定為與惡意網路行為者的行動有密切聯繫。這是因為與電子郵件「**wangminghua6@gmail[.]com**」和「**taoyujun@gmail[.]com**」相比，它們的網域較多涉及惡意活動。

（見附件 A，圖 5）

與其他威脅行為者的聯繫

另一個共同特徵顯示是與 BADBAZAAR 相關，就是 網域「**actuallys[.]com**」、「**clublogs[.]com**」、「**myloughborough[.]com**」、「**rewrwer[.]com**」和「**voiceoftibet[.]net**」都是在 eNom 註冊的，並且停放在「**255.255.255[.]254**」。

根據 NCSC 早前的調查，其他有此特徵的網域也曾發現與 2019 年 **APT5** 及 2009 年至 2011 年 **APT14** 相關的活動。

APT5-關連的網域中的歷史 WHOIS 記錄顯示，「**taoyujun@gmail[.]com**」是註冊者的電子郵件地址。

APT14 連結的域名有三個字母的子域名，似乎代表惡意行為的預計目標。其中一個例子是「**bae.cisconline[.]net**」，表明其目標是 BAE 系統，這是在" **Poison Ivy**"的樣本中所發現。

在 BADBAZAAR 網域中也顯示類似的特徵，其子網域與木馬應用程式的名稱有所關聯：

應用程式標題	C2 URL
Muslim Pro	**mpp**.pmstwocqn[.]com
Video Player for Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
Radio Afghanistan	**afg**.collinformations[.]com
EN-UG Dictionary Free	**eud**.titeperformance[.]com
Disk Video Recovery	**dvr**.collinformations[.]com
TextNow	**ttn**.titeperformance[.]com

留意與 APT5 和 APT14 相關的活動都是過往紀錄，也有其他在 eNom 註冊，並解析為「**255.255.255.254**」的域名，這些域名不可能與惡意活動有所關聯。因此，無法確定這些活動背後的參與者是否相同或相關。

機器名稱

對 BADBAZAAR C2 和樣本的分析顯示，主機名稱是用作 SSL 憑證中的「Common Name (通用名稱)」值。NCSC 的調查發現 BADBAZAAR 的樣本和基礎設備顯示，這些主機名稱 使用在多個 IP 位址。在這些 IP 位址的託管網域就找到 BADBAZAAR 的樣本。在下面的部分有更多關於主機名稱，和託管 BADBAZAAR C2 域的主機名稱及其 IP 位址的詳細資訊。

在近乎所有情況，具有主機名稱值的憑證都與指定的惡意網域的 IP 地址的解析重疊，僅少數不存在這種情況。

WIN-EU0VLBL7TUJ

在主機名稱「**WIN-EU0VLBL7TUJ**」發現到下列值得留意的 IP 位址：

- 「**116.203.53[.]21**」 託管了 BADBAZAAR C2 的網域「**uyapkfinder[.]com**」 和「**thewestuniverse[.]com**」。
- 「**95.216.169[.]27**」 託管了 BADBAZAAR C2 的網域「**adysfunction[.]com**」和子網域名稱「**download.apkbazar[.]biz**」，在這些網域發現有 BADBAZAAR 樣本的下載連結。

（見附件 A，圖 6）

WIN-70E59JVOB9G

在主機名稱「**WIN-70E59JVOB9G**」發現到下列值得留意的 IP 位址：

- 「**23.88.28[.]220**」託管了 BADBAZAAR C2 子網域「**aua.rondwsign[.]com**」、「**nal.tokenmajorp[.]com**」、「**pep.rondwsign[.]com**」、「**doa.rondwsign[.]com**」、「**pls.rondwsign[.]com**」。從最後一次看到裝置的憑證，到第一次發現 IP 解析到惡意網域 ，中間隔了兩天。
- 「**23.88.28[.]221**」 託管和 BADBAZAAR 相關的子網域「-「**bt.bhvghg[.]com**」。
- 「**23.88.28[.]222**」 託管了 BADBAZAAR 的 C2 網域「**tubevideoplus[.]org**」和「**cde.mpoxcases[.]com**」。
- 「**65.21.92[.]67**」 託管 BADBAZAAR 的 C2 子網域「**bat.androidupdated[.]net**」。它亦託管子網域「**apps.androidupdated[.]net**」，一個 DoubleAgent 惡意軟件的 C2。

- 「 **65.21.92[.]77** 」 託 管 了 BADBAZAAR 的 C2 子 網 域 「 **wyo.titeperformance[.]com** 」、「 **big.collinformations[.]com** 」、「 **vpf.titeperformance[.]com** 」、「 **eud.titeperformance[.]com** 」 和 「**afg.collinformations[.]com**」。

- 「**65.108.192[.]134**」託管了 BADBAZAAR 的 C2 子網域「**upd.whoscaller.net**」和「**ggl.whoscaller[.]net**」。

- 「 **142.132.131[.]15** 」 託 管 了 BADBAZAAR 的 C2 子 網 域 「**bvn.lookincategory[.]com**」 和「**edr.lookincategory[.]com**」。從最後一次看到裝置名稱的憑證，到第一次發現 IP 解析到惡意網域，中間隔了十一天。

- 「 **142.132.131[.]20** 」託管了子網域「 **son.onlinegamersgroup[.]com** 」和「**system.onlinegamersgroup[.]com**」，這些子網域被認為是 BADBAZAAR 的 C2。因為它們是託管在同一 IP 上，亦觀察到與 BADBAZAAR 相關的 SSL 憑證。

- 「**142.132.131[.]28**」託管了 BADBAZAAR 的 C2 網域「**goldplusapp[.]net**」及其子網域「**who.goldplusapp[.]net**」和「**cgf.goldplusapp[.]net**」。

- 「 **162.55.103[.]211** 」 託 管 了 BADBAZAAR 的 C2 子 網 域 「 **oha.alpinemap[.]net** 」、「 **aru.alpinemap[.]net** 」、「 **aso.alpinemap[.]net** 」、「 **afr.alpinemap[.]net** 」 和 「**aar.alpinemap[.]net**」。

- 「**162.55.103[.]212**」託管 BADBAZAAR 的 C2 子網域「**pep.rondwsign[.]com**」、「 **ckp.jkiohreh[.]com** 」、「 **aar.tokenmajorp[.]com** 」、「 **nal.tokenmajorp[.]com** 」、「 **pls.rondwsign[.]com** 」 和 「**aua.rondwsign[.]com**」。

- 「**195.154.47[.]99**」託管了 BADBAZAAR 的 C2 子網域「**ggl.whoscaller[.]net**」和「**upd.whoscaller.net**」。從最初看到裝置名稱的憑證，到第一次發現 IP 解析到惡意網域，中間隔了三天。

- 「**195.154.60[.]3**」託管了 BADBAZAAR 的 C2 子網域「**upd.whoscaller[.]net**」。‘**ggl.whoscaller[.]net**’.

- 「**212.83.189[.]89**」託管了 BADBAZAAR 的 C2 子網域「**wyo.teleperformance[.]com**」、「**eud.teleperformance[.]com**」、「**vpf.teleperformance[.]com**」和「**afg.collinformations[.]com**」。

- 「**212.129.21[.]168**」託管了 BADBAZAAR 的 C2 網域「**fre.lookincategory[.]com**」、「**tgr.lookincategory[.]com**」、「**fgt.lookincategory[.]com**」、「**luj.lookincategory[.]com**」和「f**bvn.lookincategory[.]com**]。

（見附件 A，圖 7）

WIN-50QO3EIRQVP

主機名稱「**WIN-50QO3EIRQVP**」被發現在下列受關注的 IP 位置：

- 「**45.76.132[.]91**」託管網域名稱、「**yumoftion[.]com**」、「**androidupdated[.]net**」。這兩個網域都與 BADBAZAAR 有所關連，因為子網域「**fow.yumoftion[.]com**」和「**bat.androidupdated[.]net**」是 BADBAZAAR 的 C2 網域。此外，子網域「**apps.androidupdated[.]net**」是一個 DoubleAgent 的 C2 網域。它還託管網域「**pmstwocqn[.]com**」，透過 WHOIS 記錄顯示與 BADBAZAAR 有關連。

- 「**95.179.210[.]85**」託管了「**clublogs[.]com**」，其中「**xle.clublogs[.]com**」是 BADBAZAAR 的 C2 網域，也託管與 BADBAZAAR 有關連的網域，包括「**bre.myloughborough[.]com**」、「**img.rewrwer[.]com**」、「**'www.voiceoftibet[.]net**」和「**actuallys[.]com**'」。

- 「**199.247.21[.]34**」託管了「**titeperformance[.]com**」和「**collinformations[.]com**」，其子網域為 BADBAZAAR 的 C2 網域。

- 「**217.69.10[.]128**」託管了 BADBAZAAR 的 C2 網域「**uyghurdict[.]com**」。

（見附件 A，圖 8）

WMSvc-WIN-50QO3EIRQVP

主機名稱「**WMSvc-WIN-50QO3EIRQVP**」被發現在下列受關注的 IP 位置：

- 「**78.46.185[.]251**」託管了 BADBAZAAR 的 C2 網域「**groupgram[.]org**」，Volexity 的通報指該網域使用連接埠 4432 進行惡意連線。
- 「**65.21.92[.]69**」和「**163.172.205[.]207**」託管了域名「**widelygram[.]org**」，該域名被認為是 BADBAZAAR 的 C2 網域，因為在這兩個 IP 上的連接埠 4432 在託管時都是開放的。
- 「**163.172.198[.]206**」託管了網域「**maxgram[.]org**」，該網域被認為是 BADBAZAAR 的 C2 網域，因為網域託管的連接埠 4432 是開放的。

（見附件 A，圖 9）

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

主機名稱「**WMSvc-WIN-50QO3EIRQVP**」和「**WIN-7LSBB9R0F1L**」被發現同時在下列 IP 位址出現：

- 「**148.251.87[.]245**」託管了 BADBAZAAR 的 C2 網域「**flygram[.]org**」和「**groupgram[.]org**」。

（見附件 A，圖 10）

WIN-N8H8S9BG2P0

主機名稱「**WIN-N8H8S9BG2P0**」被發現在下列 IP 位址出現：

- 「**148.251.87[.]247**」託管了 BADBAZAAR 的 C2 網域「**omarwhatsapp[.]org**」和「**flygram[.]org**」。

（見附件 A，圖 11）

WIN-I6VBN8MR92A

主機名稱「**WIN-I6VBN8MR92A**」被發現在下列 IP 位址出現：

- 「**148.251.87[.]197**」託管了 BADBAZAAR 的 C2 網域「**tryhrwserf[.]com**」。

（見附件 A，圖 12）

根據現有的商業數據，這些機器名稱在網路上的流行程度各不相同。有些是在多個 IP 位址上同時觀察到的，這表明是由同一個模板創建的虛擬機器。留意有部份主機名稱所出現的 IP，並非全部都與惡意活動有所關連。這是指主機名稱的使用並非僅限威脅行為者獨有。

然而，這些機器名稱普遍存在於託管 BADBAZAAR C2 域的 IP 中，可能表明有使用基礎設施採購實體設定裝置，以支援惡意行為者的網路操作。

社交媒體存在

Volexity 早前的報告顯示，惡意網路行為者會製作 YouTube 影片來宣傳使用惡意應用程式。這些影片包括教導如何使用他們所開發的應用程式。

NCSC 還發現了另外兩個與威脅行為者有關的 YouTube 頻道。YouTube 頻道網址為「**@josephjoey3499**」是在推廣「**Maxgram**」，而另一個註冊網址為「**@uyghurapks3096**」的頻道則在推廣「**Uyghur APK Finder**」。

此外，YouTube 也有宣傳「**Flygram**」和「**Signal Plus**」的影片，顯示威脅行為者所使用的電話號碼。在「**Flygram**」的影片中，0:36 處顯示了電話號碼「**+1 (570) 378-7250**」；而在「**Signal Plus**」的影片中，則顯示了電話號碼「**+1 (267) 298 4259**」。

Volexity 通報了一個以西藏為主題的虛假新聞網站「**ignitetibet[.]net**」，他們在 Telegram 頻道中發現了這網站並相信由威脅行為者所運營的。並發現電郵地址「**choekyi.wangmo@ignitetibet[.]net**」在頁面「**tibetone.org**」上的貼文中留下了評論，該頁面已被 Lookout 公開報告為用於 BADBAZAAR iOS 版本的 C2 頁面。

相信該電子郵件地址是由威脅行為者所控制，以 **Choekyi Wangmo** 的身份活動。

評估

BADBAZAAR 和 MOONSHINE 使用多種社會工程方法，專門針對維吾爾族、藏族和台灣社群，如：

- 針對這些群體的興趣，為目標受害者度身訂製木馬應用程式（例如維吾爾語《古蘭經》應用程式）。
- 將這些木馬應用程式添加到官方應用程式商店，務求帶給人一種合法正當的感覺，而在聊天群組中分享，很可能是為了利用社群內的信任關係。

BADBAZAAR 和 MOONSHINE 所收集的數據，幾乎肯定是對中國政府有所價值。儘管根據觀察，BADBAZAAR 和 MOONSHINE 的目標是維吾爾族、藏族和台灣人，但也有其他惡意軟件的目標是中國境內的其他少數民族群體。來自封閉國家的人民，不論是在中國或國外，如果被認定為支持對政權穩定有威脅的議題，幾乎肯定會受到像 BADBAZAAR 和 MOONSHINE 之類的移動裝置惡意軟件所威脅。而具記錄位置、音訊和照片資料的能力，代表能顯示目標人物的活動和即時資訊，幾乎肯定會提供加強監視和進行騷擾行動的機會。

MITRE ATT&CK®

本報告是根據 MITRE ATT&CK® 框架編寫的，該框架是一個基於現實世界觀察、全球可用的對手戰術和技術知識庫。

戰術	身份	技術	步驟
偵察	T1593.001	搜尋公開的網站/網域：社交媒體	攻擊者找到與其目標受害者相符的網上群組和論壇，並分享惡意軟件
資源開發	T1583.001	取得基礎設備網域	攻擊者為其命令和控制伺服器註冊域名
資源開發	T1587.001	發展能力：惡意軟件	把惡意程式碼編寫插入於木馬應用程式
資源開發	T1608.001	部署能力：上載惡意軟件	將木馬應用程式上載到包括應用程式商店在內的網上平台
資源開發	T1585.001	建立帳戶：社交媒體帳戶	攻擊者在網站和社交媒體上建立帳戶來分享和宣傳惡意軟件
資源開發	T1585.002	建立帳戶：電郵帳戶	攻擊者利用私人或商業的電子郵件帳戶來託管和分享惡意軟件
初始入侵	T1189	路過式入侵	惡意的指令碼隱藏在合法的應用程式中，並上載到應用程式商店
初始入侵	T1566.003	網路釣魚：利用服務進行魚叉式網路釣魚	攻擊者透過 Telegram 等社交媒體向目標群體發送木馬應用程式
執行	T1204.002	使用者執行：惡意檔案	受害人必須安裝木馬應用程式才能執行負載內容
防禦迴避	T1027.009	混淆的檔案或資訊：嵌入式負載	惡意負載是隱藏於合法的應用程式中
防禦迴避	T1036.005	偽裝：和正當的名稱或位置相符	木馬的檔案是與正當的應用程式名稱、外觀和功能相符。
防禦迴避	T1656	冒充	攻擊者透過建立掩護網站，及使用與目標群體相關的使用者名稱來冒充可被信任的人
收集	T1123	錄音	木馬應用程式可能會要求不必要的權限，如麥克風的存取權限
收集	T1125	錄影	木馬應用程式可能會要求不必要的權限，如相機的存取權限
收集	T1005	本機系統的數據	木馬應用程式可能會要求不必要的權限，如取得本機檔案的存取權限
指揮與控制	T1071.001	應用層協定：網絡協定	惡意軟件使用 HTTPS 和 WebSocket 連線到 C2。
指揮與控制	T1509	非標準連接埠	使用非標準連接埠，例如 4432 和 2333
外傳	T1041	利用 C2 通道進行外傳	惡意軟件使用 HTTPS 和 WebSocket 連線進行外傳。
影響	T1565.002	資料操縱：操縱資料傳訊	透過啟用應用程式的網路流量，攻擊者可取得受害者的數據，而這些數據對於應用程式的功能來說並非必需

指標

MOONSHINE：

- 在 2025 年 4 月 1 日搜尋 VLiteUI 面板時，取得下列結果：

IP位址	連接埠	首次出現	最後出現
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

- 在 2025 年 4 月 1 日搜尋 SCOTCH ADMIN 面板時，取得下列結果：

IP位址	連接埠	首次出現	最後出現
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

- 在 2024 年 3 月 14 日搜尋 SCOTCH ADMIN 面板時，取得下列結果：

網域	IP 位址
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**的 **C2**上觀察到的 **SSL** 憑證。
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- 在 2025 年 4 月 1 日搜尋上述 BADBAZAAR 憑證時，取得下列結果：

IP 位址	連接埠	首次出現	最後出現
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

描述	在 **BADBAZAAR** 的 **C2** 上觀察到的 **SSL** 憑證。
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- 在 2025 年 4 月 1 日搜尋上述 BADBAZAAR 憑證時，取得下列結果：

IP位址	連接埠	首次出現	最後出現
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28
162.55.103[.]210	20121	2022-09-30	2023-02-23

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

- WHOIS 網域

下列表中所顯示的網域，其目前或過去 WHOIS 記錄中，有些值觀察到是與 BADBAZAAR C2 的網域相符。

WHOIS 值	網域
註冊者州份：**UJYJYUJ** 註冊者國家：玻利維亞 註冊商：**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
註冊者州份：**REWR** 註冊者國家：**CF** 註冊商：**eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

註冊者州份：**FSDF** 註冊者國家：**AL** 註冊商：**eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

電郵地址
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

下列連結是與 BADBAZAAR 和 MOONSHINE 相關的其他入侵指標（IoC）。NCSC 無法確認這些連結中所有資訊的有效性，建議讀者應獨立驗證其準確性和關聯性：

- ESET
- 趨勢科技
- Lookout
- Lookout
- Volexity
- 公民實驗室（Citizen Lab）

緩解措施

NCSC 鼓勵採用下列建議，以防禦研究個案中提及的威脅。

- **應用程式商店的營運商（包括第三方應用程式商店）和開發者應確保平台上的應用程式是安全的，並符合政府的行為準則。**請參閱指引：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

- **多語言支援：**應用程式開發人員應投放資源，將熱門應用程式本地化，給說少數民族語言（包括維吾爾語、藏語、台灣閩南語和粵語）的目標用戶使用。Apple 的應用程式本地化指引：https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app。Google 應用程式翻譯指引：https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **確保您在社交媒體平台的安全：**社交媒體公司可令惡意網路行為者更難在合法的網上社群中建立虛假帳戶，或在其平台上分享惡意檔案或連結。在可行情況下，公司應與更廣泛的行業分享惡意指標，以提升大家對威脅的理解，並協助採取保護措施。

- **給顧客的補救措施：**機構應制定程序，以通知因使用其服務而安裝了惡意應用程式的客戶。這些警報應該引人注目且資訊充足。在適當的情況下，機構應提供如何刪除該軟件的指導，並鼓勵受害者向其當局舉報，例如英國的 NCSC。
  請參閱 App Store 行為準則了解更多：https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **合作工作小組：**社交媒體公司可以組建工作小組，讓各自的安全團隊分享惡意指標、TTP 和觀察結果，使攻擊者更難利用平台進行不法惡意活動。

- **檢測已更改的應用程式：**在可行情況下，應用程式的開發人員應包括一個在使用者下載「非官方」版本時通知使用者的功能，以防止惡意版本的傳播。

附錄 A：BADBAZAAR 的 WHOIS 聚類 / 網域經紀人資訊

圖 1 – 'UKYJYUJ'

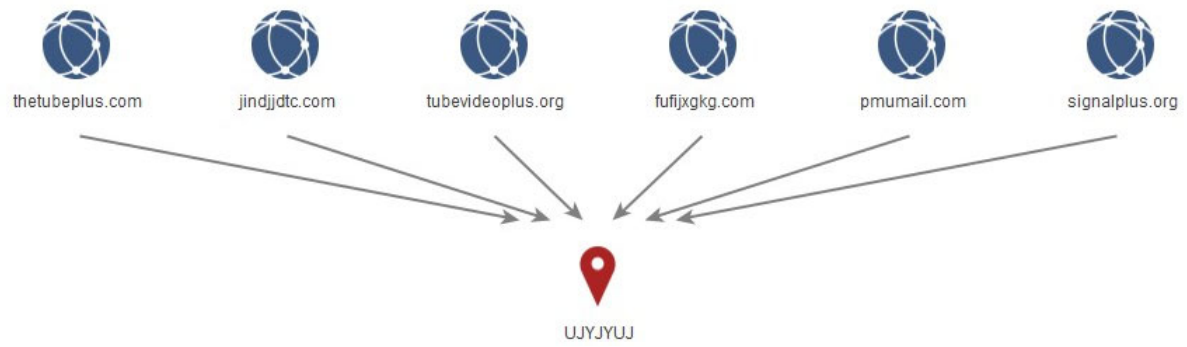


圖 2 – 鍵盤行走值

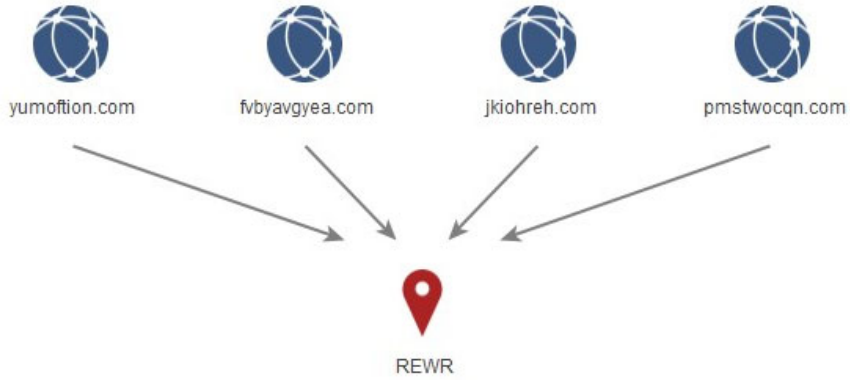


圖 3 – 具有「FSDF」狀態欄位值的附加網域

圖 4 – **95.179.210[.]85**

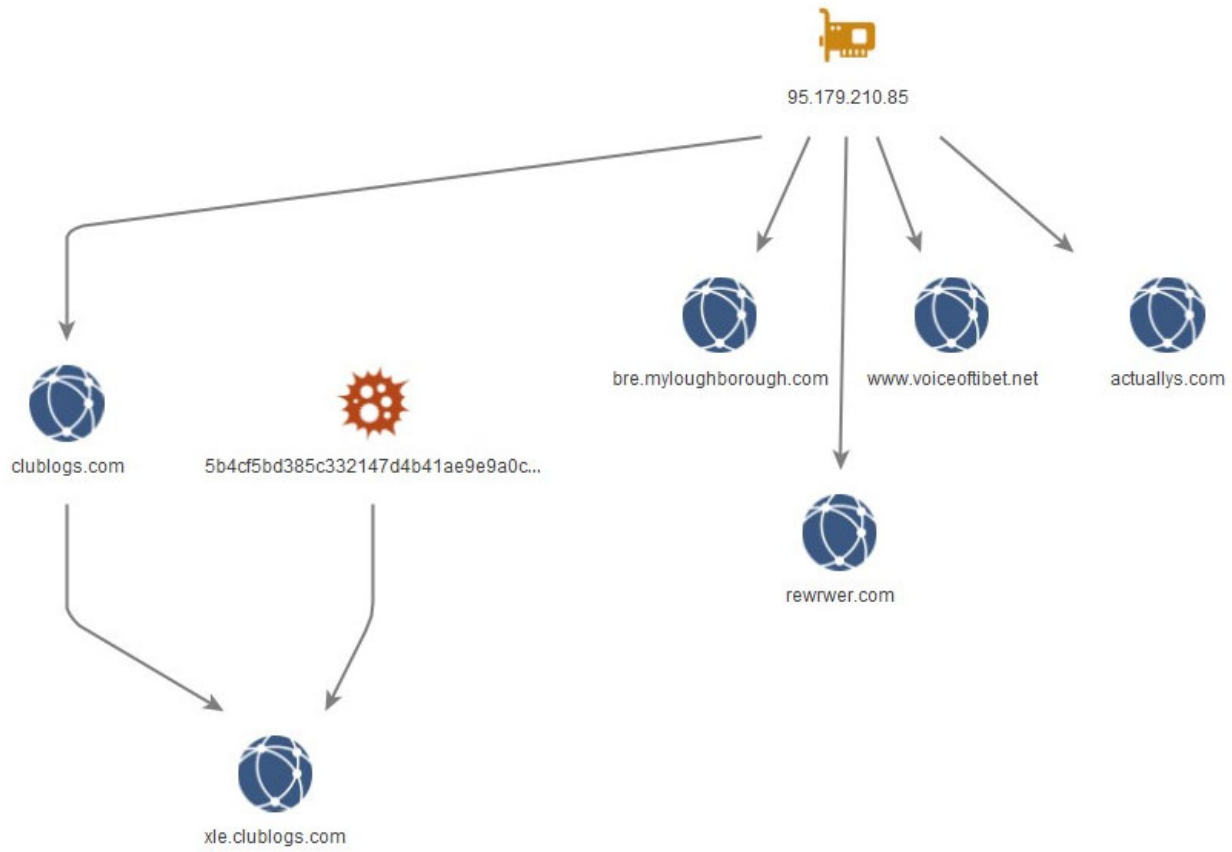


圖 5 – WHOIS 連結

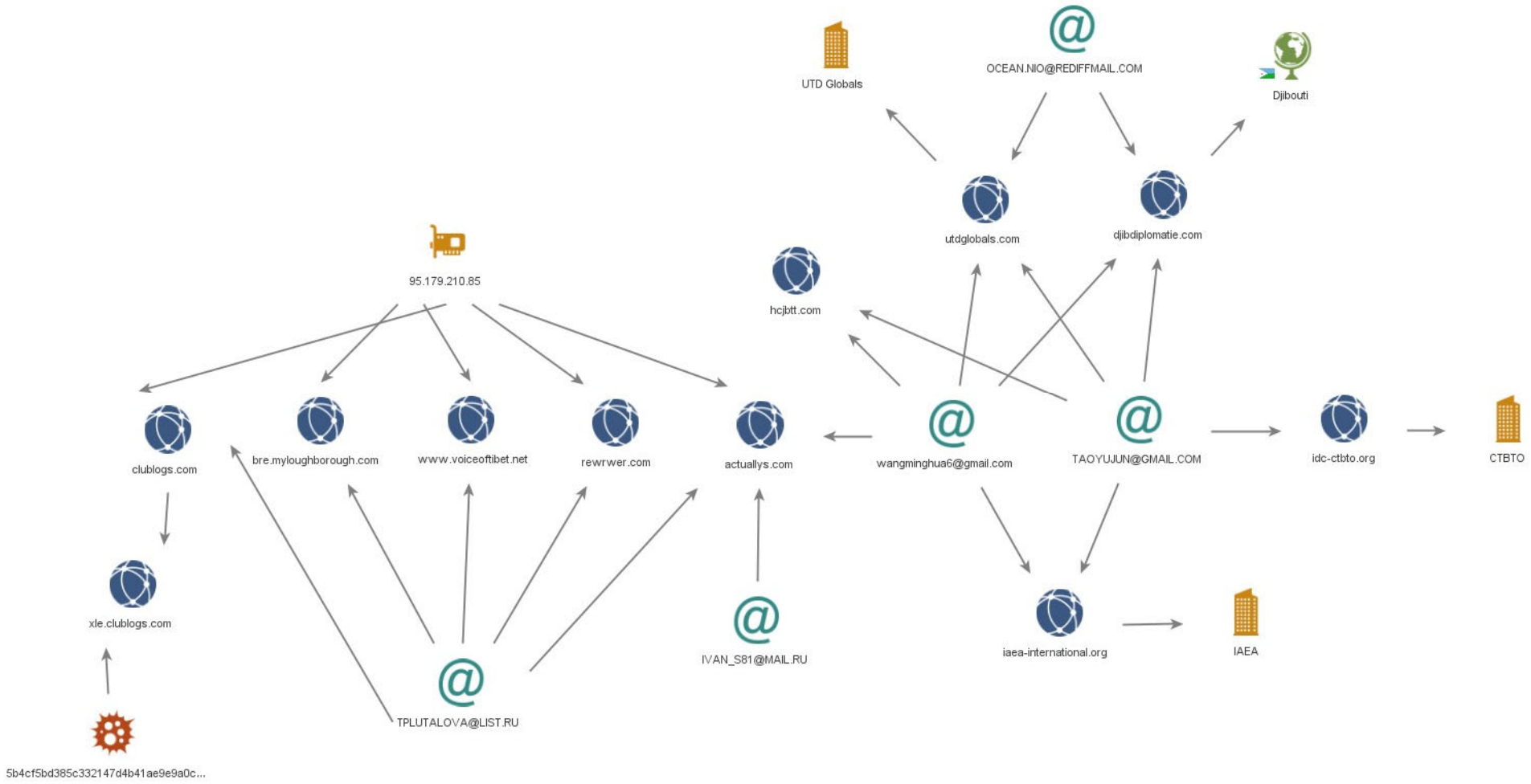

UTD Globals
OCEAN.NIO@REDIFFMAIL.COM
Djibouti
utdglobals.com
djibdiplomatie.com
95.179.210.85
hcjbtt.com
clublogs.com
bre.myloughborough.com
www.voiceoftibet.net
rewrwer.com
actuallys.com
wangminghua6@gmail.com
TAOYUJUN@GMAIL.COM
idc-ctbto.org
CTBTO
xle.clublogs.com
IVAN_S81@MAIL.RU
iaea-international.org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

圖 6 – **WIN-EU0VLBL7TUJ**

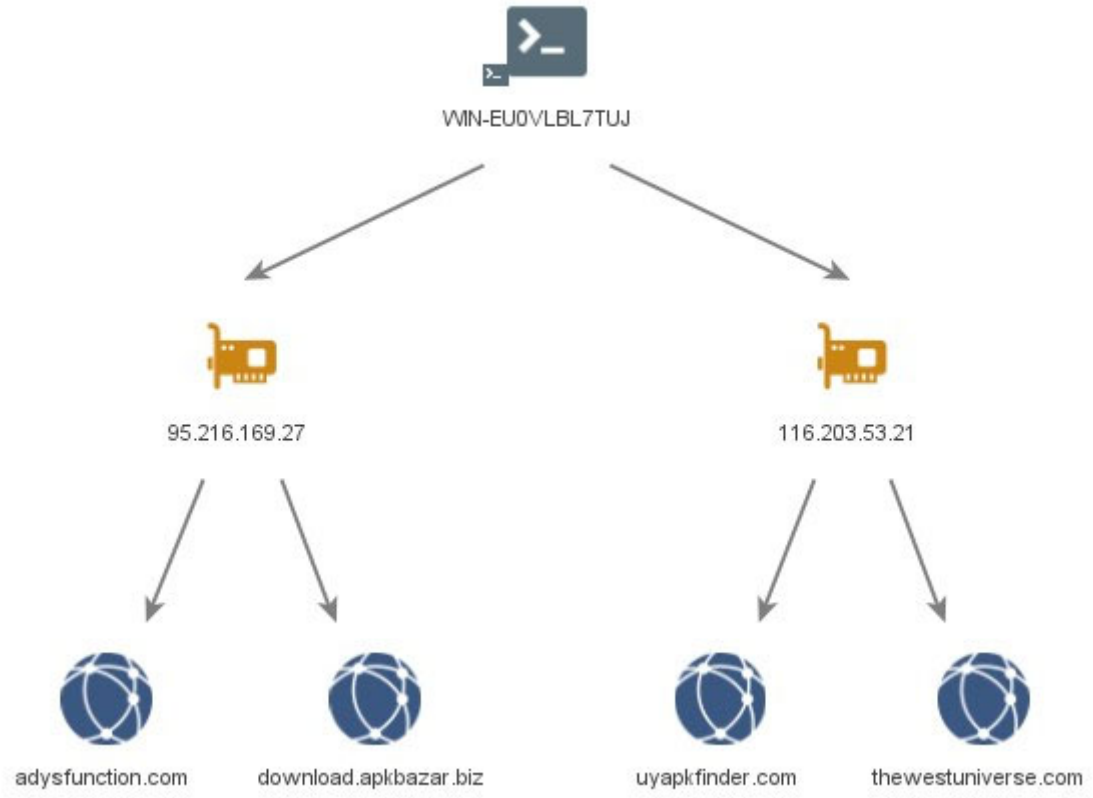


圖 7 – **WIN-70E59JVOB9G**

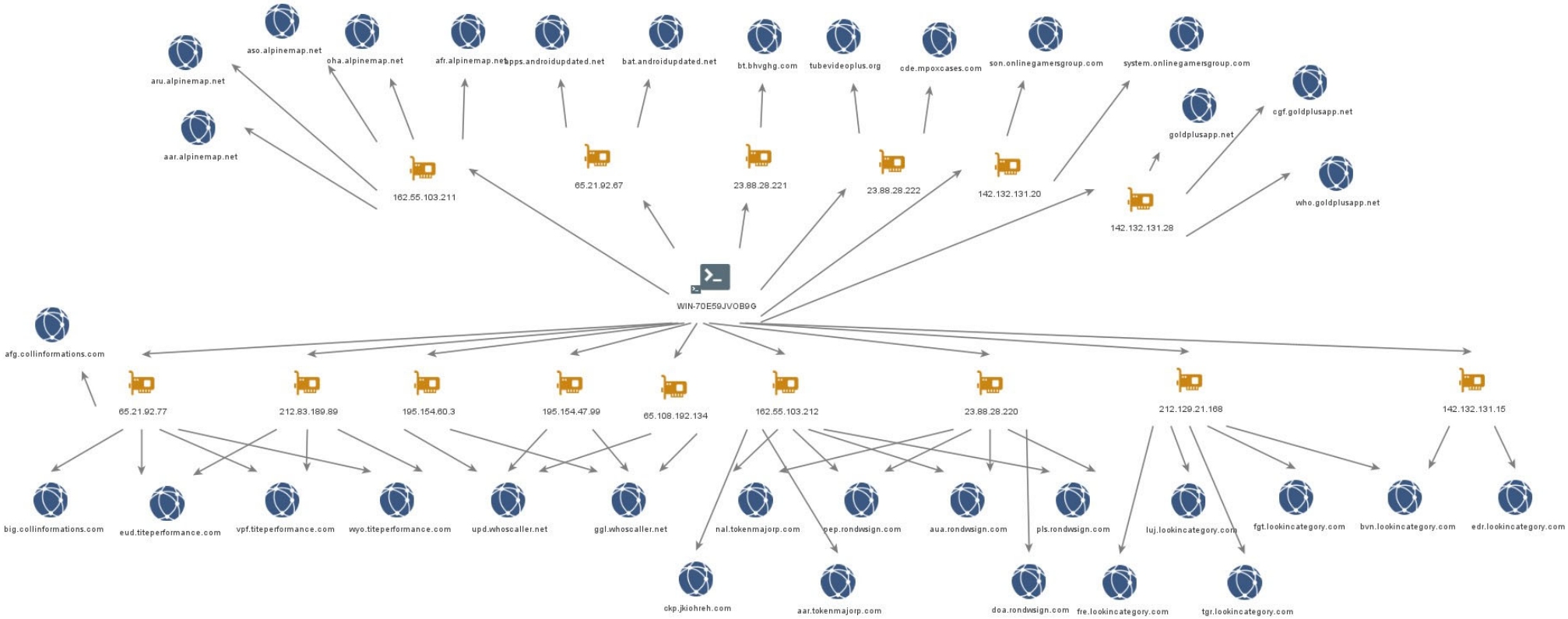


圖 8 - **WIN-50QO3EIRQVP**

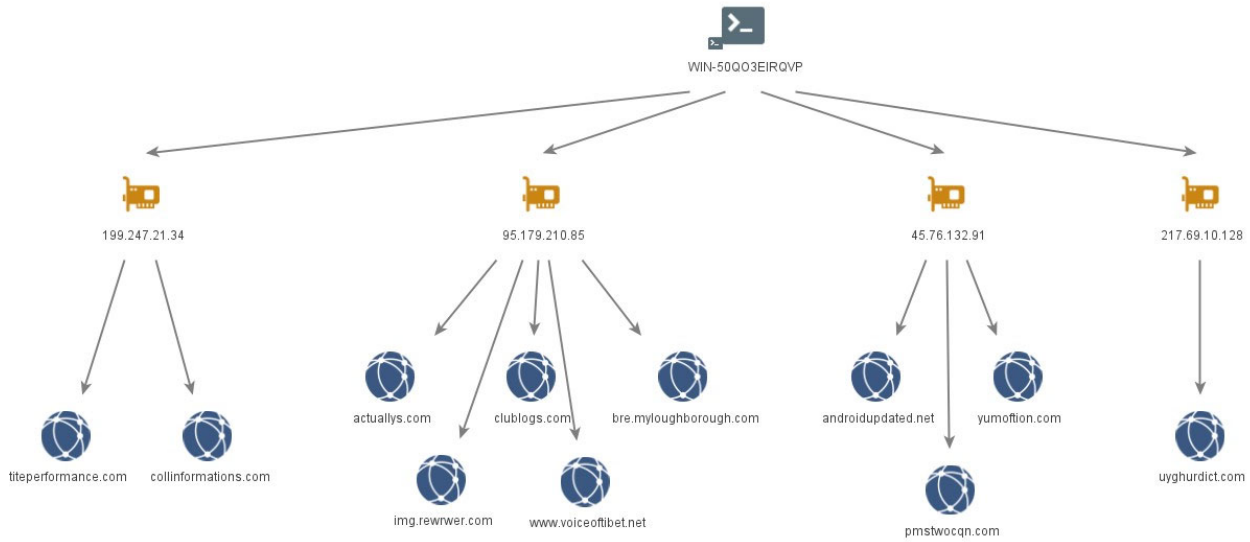


圖 9 - **VMSvc-WIN-50QO3EIRQVP**

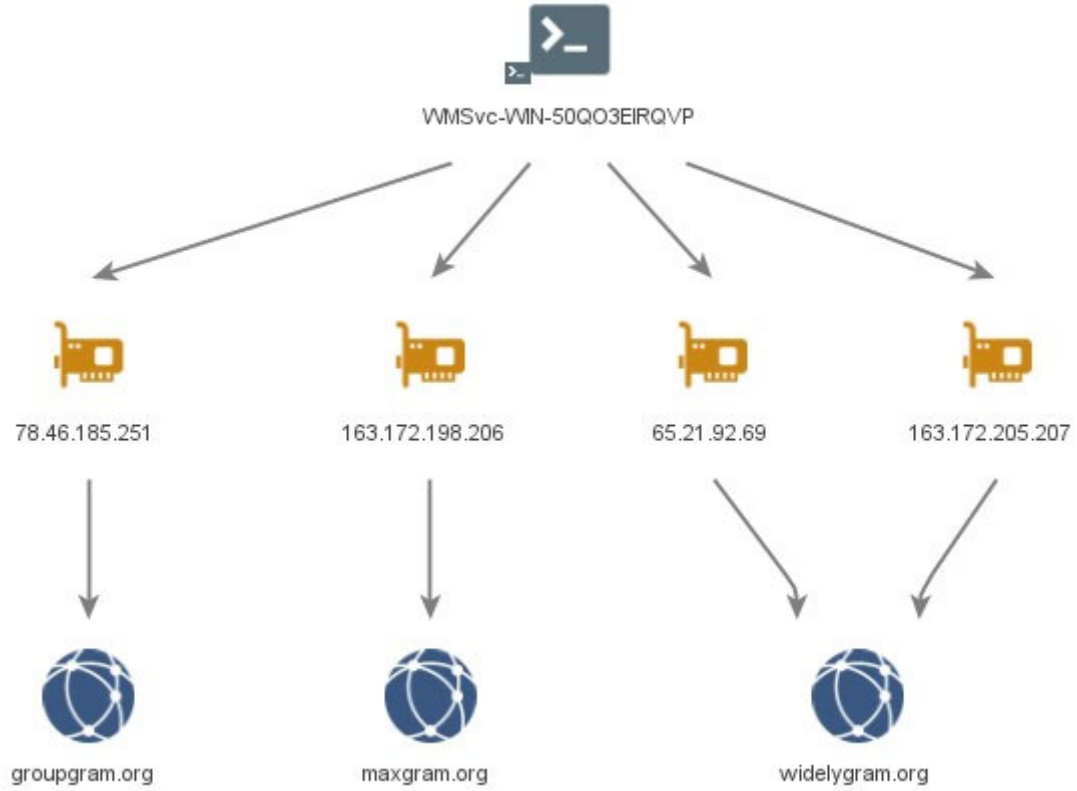


圖 10 – **VMSvc-WIN-50QO3EIRQVP** 和 **WIN-7LSBB9R0F1L**

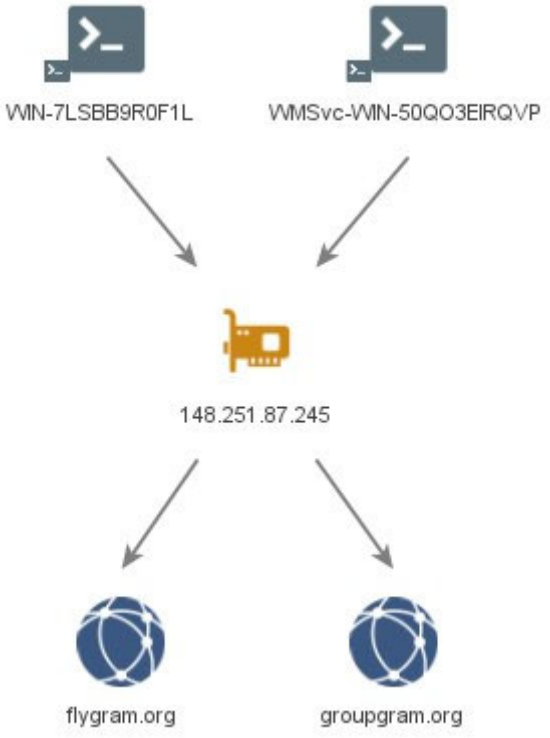


圖 11 - **WIN-N8H8S9BG2P0**

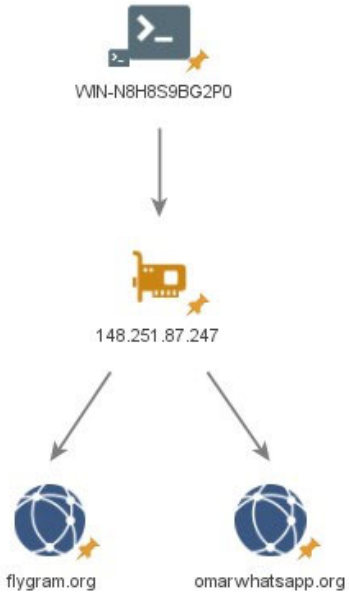


圖 12 – **WIN-I6VBN8MR92A**

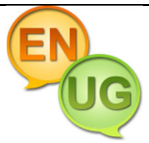
附錄 B：MOONSHINE 和 BADBAZAAR 的觀察樣本

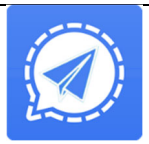
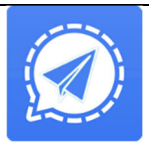
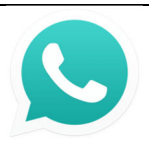
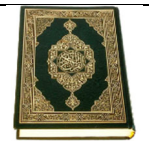
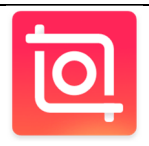
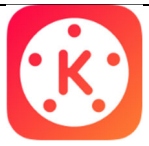
本表格列出了過去兩年 MOONSHINE 和 BADBAZAAR 活動時運用到的應用程式。

許多都與現有應用程式有明顯的相似，這很可能是攻擊者故意「模仿」知名品牌的伎倆。

請注意，應用程式的名稱、套件名稱和圖標都可以被模仿或設計成與真實的應用程式相同，因此不應只利於這些資訊以識別裝置有否被感染。

應用程式標題	套件名稱	應用程式圖標
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	

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

FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	

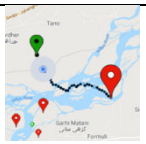
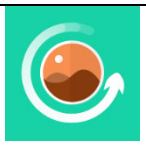
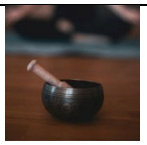
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur 输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	

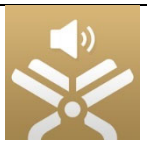
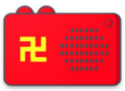
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	

Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO	net.rhombapp.mo	
Tibetan Prayer	com.chorig.tibetanprayer	
Translator AR-TR	free_translator.artr	

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

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

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

ئاۋازلىق قۇرئان	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى 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	
لۇغىتى ئاقاپ كۇ	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	

更多參考資料

澳洲網路安全中心的指引

- 報告網路犯罪、事件或漏洞
- 如何保護您的裝置
- 保護您的手機安全
- 網路釣魚
- 詐騙
- 保護您的社交媒體
- 社交媒體與通訊應用程式的安全建議

英國 NCSC 和 NPSA 的指引

- 捍衛民主
- 社交媒體：如何安全使用
- 適用於機構的裝置安全指引，包括手機
- 應用程式商店威脅報告。
- 高風險人士的人身安全與保障

美國國家安全局的指引

- 流動裝置最佳實務守則

免責聲明

請注意，本公告內容是在發布當時獲驗證的資訊。

報告借鑒了來自撰寫機構和業界提供的資訊。任何調查結果和建議均不是為了避免所有風險，遵循這些建議也不代表能消除所有此類風險。資訊風險的責任始終在於相關系統的所有者。

在英國，本資訊根據 2000 年《資訊自由法》（FOIA）獲得豁免，並可能根據其他英國的資訊法例獲得豁免。

如有任何 FOIA 查詢，請電郵至 ncscinfoleg@ncsc.gov.uk。