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

Khuyến cáo

BADBAZAAR và MOONSHINE:

Phân tích kỹ thuật và các biện pháp giảm thiểu

Ngày 9 tháng 4 năm 2025

BADBAZAAR và MOONSHINE: Phân tích kỹ thuật và các biện pháp giảm thiểu

Tóm tắt

Với sự hỗ trợ từ Cyber League(Liên Minh Mạng) Vương quốc Anh, khuyến cáo này được Trung tâm An ninh Mạng Quốc gia Vương quốc Anh (National Cyber Security Centre - NCSC UK) và các đối tác quốc tế phối hợp soạn thảo:

- **Trung tâm An ninh Mạng Úc, trực thuộc Tổng Cục Tín hiệu Úc**
- **Trung tâm An ninh Mạng Gia Nã Đại, trực thuộc Cơ quan An ninh Truyền thông Gia Nã Đại**
- **Cơ quan Tình báo Liên bang Đức**
- **Văn phòng Liên bang Đức về Bảo vệ Hiến pháp**
- **Trung tâm An ninh Mạng Quốc gia Tân Tây Lan, trực thuộc Cục An ninh Truyền thông Chính phủ**
- **Cục Điều tra Liên bang Hoa Kỳ**
- **Cơ quan An ninh Quốc gia Hoa Kỳ**

Khuyến cáo này cung cấp thông tin tình báo về mối đe dọa mới và đã được tổng hợp liên quan đến hai biến thể phần mềm gián điệp mang tên BADBAZAAR và MOONSHINE, đồng thời đưa ra các khuyến nghị dành cho các nhà điều hành cửa hàng ứng dụng, nhà phát triển và các công ty mạng xã hội nhằm giúp bảo vệ người sử dụng.

Khuyến cáo này được đăng tải song song với một khuyến cáo dành cho nạn nhân của các phần mềm độc hại này.

Tài liệu này sử dụng định nghĩa có trong bảng thuật ngữ của NCSC về phần mềm gián điệp :"Một loại phần mềm độc hại *(malware)* được cài đặt trên thiết bị mà không có sự đồng ý của người sử dụng, thu thập dữ liệu và sau đó gởi đến bên thứ ba."

Nghiên cứu trường hợp điển hình 1: MOONSHINE

MOONSHINE là một phần mềm gián điệp trên hệ điều hành Android được trình báo vào năm 2019 bởi Citizen Lab, với mục đích nhắm đến các nhóm người Tây Tạng. MOONSHINE nguỵ trang thành một ứng dụng hợp pháp để dụ dỗ nạn nhân cài đặt nó. MOONSHINE đã được chia sẻ qua các kênh Telegram và qua các đường dẫn được gởi qua WhatsApp.

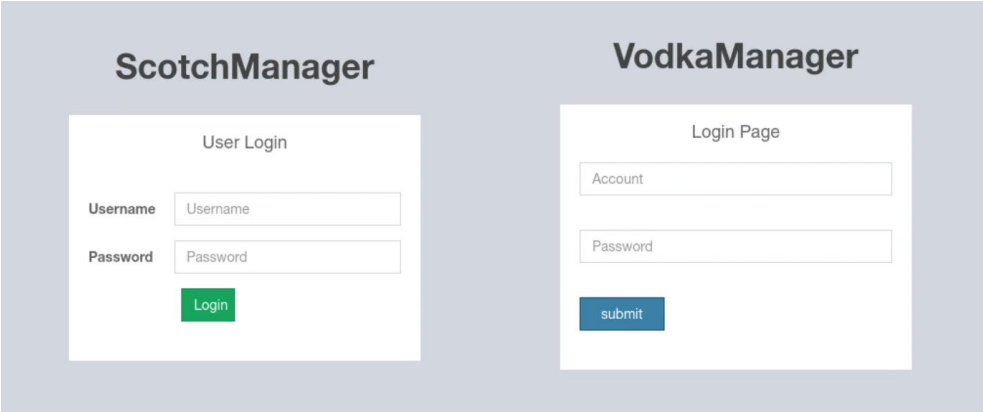
Nghiên cứu của NCSC về MOONSHINE cho thấy những điểm sau đây:

- MOONSHINE sử dụng một giao diện quản lý đã có nhiều thay đổi kể từ khi nó được trình báo lần đầu tiên.
- Giao diện quản lý tiết lộ các khả năng giám sát sâu rộng, bao gồm khả năng di chuyển các tập hồ sơ từ thiết bị cũng như ghi âm trực tiếp và quay màn hình.
- Một loạt giao diện quản lý MOONSHINE được lưu trữ ảo đã được phát hiện. Các giao diện này có sự trùng khớp về hạ tầng cơ sở với các bảng đăng nhập liên quan đến UPSEC, mà theo Intelligence Online *(Thông tin Tình báo Mạng)* ám chỉ đến 'Công ty TNHH Công nghệ An ninh Mạng Điện Khoa Tứ Xuyên'.

Quản lý giao diện

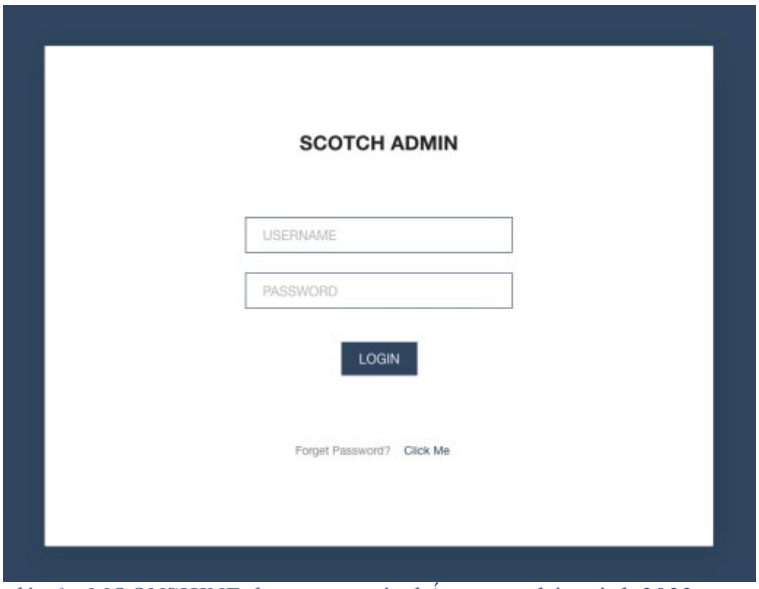
Các phúc trình trước đây về giao diện quản lý của MOONSHINE cho thấy nó đã trải qua nhiều thay đổi, có nghĩa là phần mềm này vẫn đang được liên tục phát triển.

Ví dụ đầu tiên về giao diện quản lý này được ghi nhận trong phúc trình của Citizen Lab vào năm 2019.



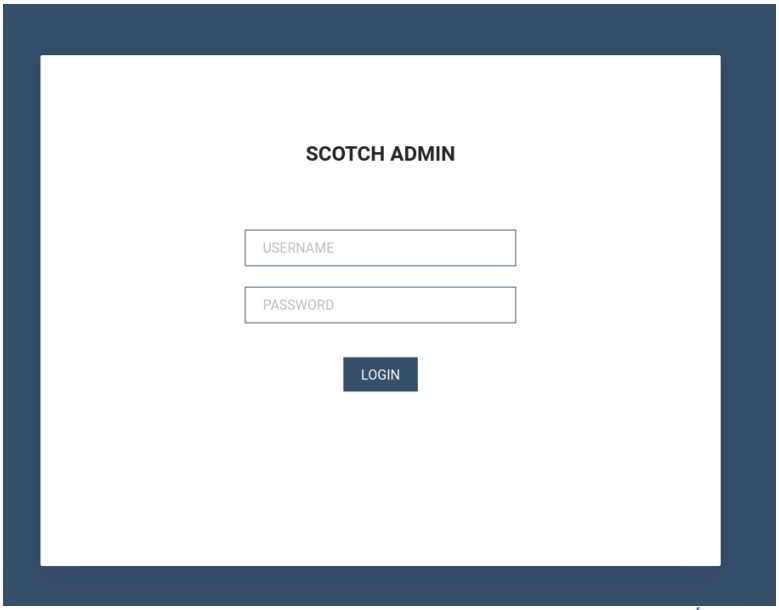
Hình 1: Các giao diện quản lý MOONSHINE được đề cập trong phúc trình vào năm 2019 của Citizen Lab 'Một thứ cần thiết Nhóm Tây Tạng bị nhắm Mục tiêu bằng Lỗ hổng Di động chỉ bằng 1 Cú Nhấp chuột'.

Vào đầu năm 2022, Lookout đã trình báo một giao diện quản lý khác, được thiết kế lại như trong hình bên dưới (thay thế cho các giao diện trước đó trong hình 1):



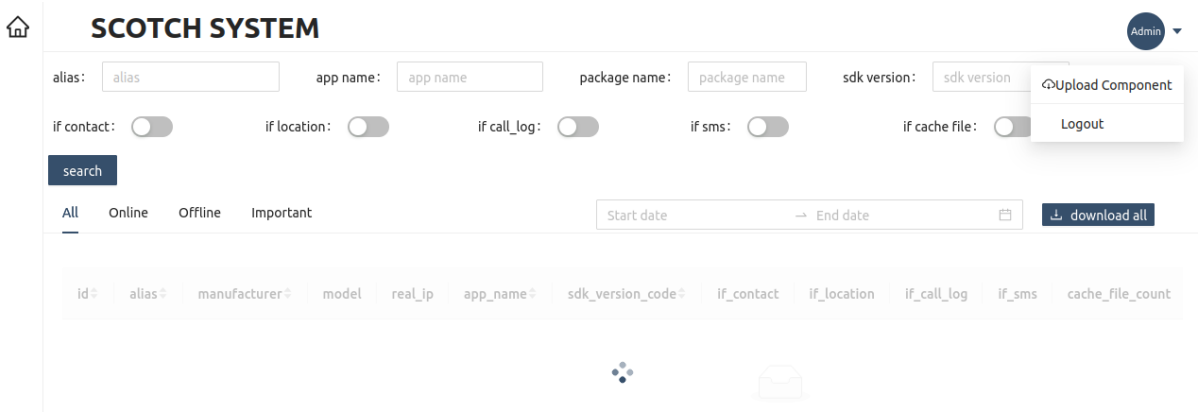
Hình 2: Giao diện quản lý của MOONSHINE được quan sát thấy trong phúc trình 2022 report 'MOONSHINE: Phần Mềm Giám sát Android tiên tiến APT POISON CARP của Trung Quốc nhắm vào người Tây Tạng và người Duy Ngô Nhĩ'.

Vào tháng 8 năm 2023, một đợt quét của máy chủ điều khiển và chỉ huy (C2) của MOONSHINE đã phát hiện một giao diện tương tự như giao diện năm 2022, tuy nhiên chức năng **"Quên Mật mã"** không còn như trong hình 2:



Hình 3: Giao diện quản lý MOONSHINE được ghi nhận vào tháng 8 năm 2023 cho thấy không còn hiển thị tùy chọn 'Quên Mật mã'.

Việc điều tra thêm về giao diện quản lý đã phát hiện nội dung trong bảng điều khiển cho thấy cách thức lưu trữ thông tin của các thiết bị bị xâm phạm.



Hình 4: Trang mạng phía sau trang đăng nhập của giao diện quản lý MOONSHINE.

Nghiên cứu của Lookout cho thấy một "**điểm số**" được truyền đi từ thiết bị của nạn nhân tới các máy chủ điều khiển và chỉ huy (C2) của MOONSHINE. Giá trị của "điểm số" này dựa trên các quyền hạn mà mẫu phần mềm độc hại có trên thiết bị của nạn nhân.

Các cột 'if_contact', 'if_location', 'if_call_log' và 'if_sms' trong trang cho thấy không phải tất cả các mẫu MOONSHINE đều có quyền truy cập đầy đủ vào các thiết bị bị xâm phạm. Việc hiểu biết về các cột này cùng với "điểm số" được truyền từ thiết bị tới máy chủ C2 cho thấy các tác nhân đe dọa đang sử dụng điểm số để truyền đạt mức độ truy cập mà phần mềm độc hại có trên thiết bị bị xâm phạm tới những người truy cập giao diện quản lý.

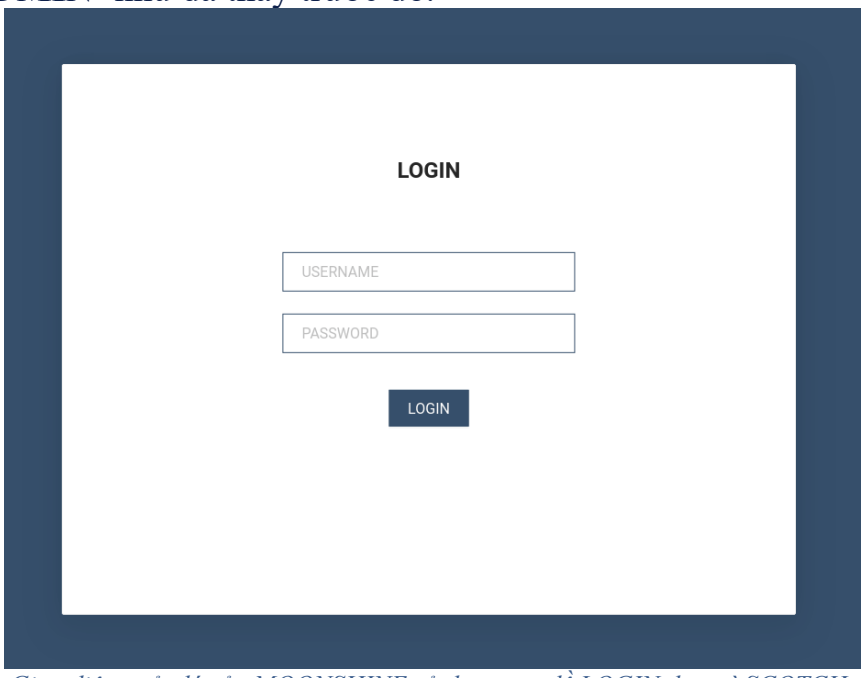
Thông thường, lời khuyên về cách thực hành tốt nhất để ngăn chặn ứng dụng thu thập thông tin từ thiết bị là nên kiểm tra các quyền hạn của ứng dụng đó xem có gì bất thường không trước khi tải về. Tuy nhiên, các mẫu MOONSHINE chỉ xin được cấp các quyền hạn phù hợp với chức năng của ứng dụng, do đó có thể không gây nghi ngờ, nhưng chúng cũng sử dụng những quyền hạn này để thu thập thông tin từ thiết bị.

MOONSHINE cũng có một Giao diện Lập trình Ứng dụng *(Application Programming Interface - API)* thể hiện phạm vi khả năng của nó. Các phiên bản đầu tiên của tài liệu API có chứa tên các API bằng tiếng Phổ thông.

Máy chủ Ảo

Trong quá trình tìm kiếm các bảng điều khiển của MOONSHINE, một số phiên bản được lưu trữ ảo đã được phát hiện. Lưu trữ ảo là khi một địa chỉ IP có thể lưu trữ nhiều trang mạng cùng một lúc. Các địa chỉ IP của những phiên bản được lưu trữ ảo này và các tên miền được lưu trữ không xuất hiện trong bất kỳ mẫu phần mềm độc hại nào đã biết.

Các phiên bản giao diện quản lý này có sự khác biệt vì tựa đề trang là **'LOGIN'** thay vì **'SCOTCH ADMIN'** như đã thấy trước đó.



Hình 5: Giao diện quản lý của MOONSHINE sử dụng tựa đề LOGIN thay vì SCOTCH ADMIN.

Ngoài ra, nội dung trong bảng điều khiển cũng khác so với hình 4, như được thấy trong hình 6.

Hình 6: Trang mạng phía sau trang đăng nhập của giao diện quản lý của MOONSHINE được lưu trữ ảo.

Bảng điều khiển trong hình 6 có vẻ là phiên bản 'rút gọn' của bảng trong hình 4. Các đặc điểm trùng khớp giữa hai bảng điều khiển là tên các cột 'id (mã định danh)', 'manufacturer (nhà sản xuất)' và 'model (mẫu)' trong bảng dữ liệu.

Các phiên bản MOONSHINE được lưu trữ ảo được phát hiện gồm:

Tên miền	Địa chỉ 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

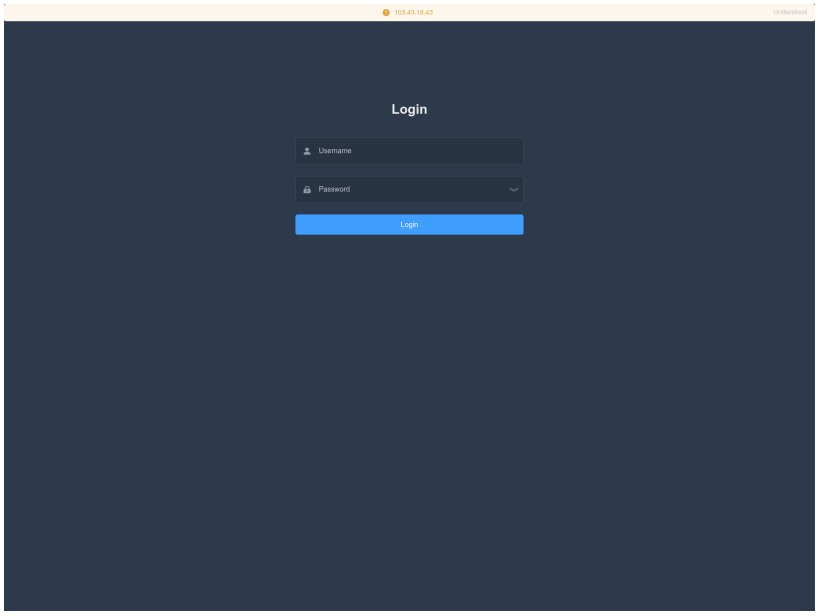
Các tên miền này được Trend Micro liệt kê là bộ công cụ khai thác của MOONSHINE, chịu trách nhiệm về việc khai thác các lỗ hổng trình duyệt để cài đặt phần mềm độc hại lên thiết bị di động. Trend Micro đặt tên cho phần mềm độc hại này là 'Dark Nimbus'.

Để làm cho rõ: giao diện quản lý của MOONSHINE là nơi các mẫu phần mềm độc hại của MOONSHINE kết nối, và gởi dữ liệu của nạn nhân về. Bộ công cụ khai thác của MOONSHINE được Trend Micro trình báo là một năng lực riêng biệt, dùng để khai thác lỗ hổng trình duyệt nhằm cài đặt một phần mềm độc hại có tên là Dark Nimbus lên các thiết bị di động. Hơn nữa, Dark Nimbus và MOONSHINE là hai loại phần mềm độc hại hoàn toàn khác nhau.

Cả giao diện quản lý của MOONSHINE và bộ công cụ khai thác của MOONSHINE đều có sự trùng khớp mã nguồn, vì vậy mới có sự tương đồng trong giao diện đăng nhập ở hình 3 và hình 5, cũng như nội dung của trang trong hình 4 và hình 6. Cả hai cũng đều chứa chuỗi ký tự ‘webpackJsonpreact-scotchui’ trong mã nguồn.

Các tác nhân đã tạo ra các đường dẫn URL dẫn tới bộ công cụ khai thác MOONSHINE, sau đó chuyển hướng đến các video có nội dung liên quan đến người Tây Tạng và Duy Ngô Nhĩ, trùng khớp với mục tiêu tấn công của MOONSHINE.

Trên nhiều địa chỉ IP lưu trữ tên miền của bộ công cụ khai thác của MOONSHINE, có một trang đăng nhập mạng tựa đề ‘VLiteUI’ được phát hiện trên cổng 444. Trang này không được để ý tới nhiều, và sự hiện diện của nó trên các địa chỉ IP này cho thấy một mối liên hệ có thể có với các hoạt động của tác nhân đe dọa.



Hình 7: Bảng đăng nhập mang tựa đề HTML 'VLiteUI' được phát hiện thấy trên các địa chỉ IP cũng lưu trữ bộ công cụ khai thác của MOONSHINE.

Phân tích của Trend Micro về Dark Nimbus cho thấy phần mềm độc hại này có thể thu thập một danh sách thông tin toàn diện từ thiết bị, và giao tiếp với máy chủ điều khiển (C2) thông qua giao thức XMPP.

Trend Micro cũng phân tích rằng trong một số phiên bản của Dark Nimbus, họ đã nhận ra rằng chuỗi ký tự 'DKNS' xuất hiện nhiều lần.

Tên miền **'ansec[.]com'** *(được Trend Micro liệt kê là máy chủ điều khiển C2 của Dark Nimbus)* cũng đã được phát hiện trong các dịch vụ XMPP trên các địa chỉ IP khác, những địa chỉ này phục vụ các trang mạng có tựa đề chứa chuỗi ký tự 'DKNS'.

- DKNS Android远程取证系统 *(Hệ thống Giám định Phân tích có Hệ thống từ Xa DKNS dành cho Android)*
- DKNS云网侦控平台 *(Nền tảng Điều tra và Kiểm soát Mạng trên Nền tảng Đám mây của DKNS)*
- DKNS云网侦控平台 *(Nền tảng Điều tra và Kiểm soát Mạng trên Nền tảng Đám mây của DKNS)*
- DKNS远程控制侦查系统 *(Hệ thống Điều tra Điều khiển từ Xa của DKNS)*

Một nhóm địa chỉ IP khác có **'ansec[.]com'** trong dịch vụ XMPP đã phục vụ các trang mạng với tựa đề:

- UPSEC互联网控制指挥系统 *(Hệ thống Chỉ huy Kiểm soát Internet của UPSEC)*
- UPSEC无线侦控系统 *(Hệ thống Giám sát và Kiểm soát Không Dây của UPSEC)*
- UPSEC重点人数据还原系统 *(Hệ thống Khôi phục Dữ liệu Cá nhân Quan trọng của UPSEC)*

Theo Intelligence Online, cụm từ 'UPSEC' xuất hiện trong tựa đề các trang HTML được cho là liên quan đến Công ty TNHH Công nghệ An ninh Mạng Điện Khoa Tứ Xuyên

Nghiên cứu trường hợp điển hình 2: BADBAZAAR

BADBAZAAR là một phần mềm độc hại di động với các biến thể trên iOS và Android, đã nhắm vào các cá nhân người Duy Ngô Nhĩ, người Tây Tạng và người Đài Loan. Phần mềm gián điệp này được phát tán qua các nền tảng mạng xã hội và các cửa hàng ứng dụng chính thức. Trình báo gần đây từ Volexity cho thấy các biến thể khác nhau của BADBAZAAR, được phân loại thành BadSolar, BADBAZAAR và BadSignal. Cả ba biến thể đều được liên kết với nhau bằng các chức năng trùng khớp được sử dụng để thu thập thông tin về thiết bị và người vận hành.

Nghiên cứu của NCSC về BADBAZAAR đã phát hiện những điểm sau đây:

- Phân nhóm các tên miền C2 cho thấy thêm nhiều sự liên kết đến các tên miền được trình báo trong thông tin tình báo về mối đe dọa trước đây.
- Các máy chủ C2 và mẫu phần mềm độc hại tiết lộ các tên máy chủ liên quan đến hạ tầng cơ sở của tác nhân đe dọa.
- Các hồ sơ bổ sung mà các tác nhân đe dọa sử dụng để áp dụng kỹ thuật xã hội nhằm phát tán phần mềm độc hại vượt ra ngoài các cửa hàng ứng dụng chính thức.

Phân nhóm WHOIS / nhà môi giới tên miền

'UJYJYUJ'

Phân tích hồ sơ WHOIS để tìm tên miền BADBAZAAR '**signalplus[.]org**' (được trình báo bởi ESET) cho thấy giá trị '**UJYJYUJ**' trong cột '**State**'.

Việc tìm kiếm các tên miền khác có cùng giá trị này đã phát hiện ra các tên miền quan trọng sau đây:

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

(Xem Phụ lục A, hình ảnh 1)

Các tên miền **signalplus[.]org, tubevideoplus[.]org và thetubeplus[.]com** được trình báo là các tên miền máy chủ điều khiển (C2) của BADBAZAAR, trong khi ESET trình báo rằng tên miền phụ **mail.pmumail[.]com** được sử dụng như một máy chủ trung gian *(proxy)* của FlyGram. FlyGram là một ứng dụng BADBAZAAR do các tác nhân mạng độc hại thiết kế (xem Phụ lục để biết danh sách các ứng dụng BADBAZAAR khác).

Giá trị gõ bàn phím *(Keyboard walking values)*

NCSC cũng đã ghi nhận các mẫu gõ bàn phím tương tự trong các tên miền máy chủ điều khiển (C2) BADBAZAAR khác đã đăng ký.

Ví dụ, các tên miền sau đây đều có giá trị '**REWR**' được phát hiện trong cột '**State**' (như đã được sử dụng trước đó):

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

(Xem Phụ lục A, hình ảnh 2)

Các tên miền có giá trị cột 'State' là 'FSDF'

Một nhóm tên miền máy chủ điều khiển (C2) BADBAZAAR khác có '**State**' giá trị '**FSDF**':

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

(Xem Phụ lục A, hình ảnh 3)

Trình báo với các giá trị gõ bàn phím trước đây

Việc sử dụng các giá trị gõ bàn phím trong hồ sơ WHOIS của các tên miền BADBAZAAR cũng đã được ghi nhận trong các phúc trình trước đây bởi TA413 về việc nhắm vào các tổ chức Tây Tạng. Recorded Future *(là một công ty tình báo nổi tiếng về mối đe dọa mạng)* đã quan sát thấy các tên miền do nhóm tác nhân kiểm soát giả mạo các tổ chức Tây Tạng và sử dụng giá trị tổ chức đăng ký là "**asfasf**".

clublogs[.]com

Các mẫu của BADBAZAAR do Lookout thu thập được có chứa tên miền '**xle.clublogs[.]com**' làm máy chủ điều khiển (C2). Tên miền gốc **'clublogs[.]com'** được lưu trữ trên địa chỉ IP '**95.179.210[.]85**' và có chứng chỉ SSL với giá trị chủ thể và đơn vị cấp là '**CN=WIN-50QO3EIRQVP**'. Giá trị này trùng khớp với các chứng chỉ SSL được tìm thấy trong các mẫu của BADBAZAAR, vốn sử dụng kỹ thuật SSL pinning nhằm tránh bị chặn và can thiệp vào quá trình truyền thông tin.

Tiểu sử lưu trữ của địa chỉ IP **95.179.210[.]85** cho thấy các tên miền đáng quan tâm như sau đây:

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

(Xem Phụ lục A, hình ảnh 4)

www.voiceoftibet[.]net

Tên miền **'www.voiceoftibet[.]net'** có vẻ đang giả mạo đài phát thanh 'Voice of Tibet', tương tự như chiến thuật, kỹ thuật và phương sách (TTP) được nhóm TA413 sử dụng.

Tên miền **'rewrwer[.]com'** có sự tương đồng với giá trị **'State'** là **'REWR'** đã được xác định trước đó trong hồ sơ WHOIS của các tên miền BADBAZAAR.

Các tên miền **'clublogs[.]com'**, **'rewrwer[.]com'**, **'voiceoftibet[.]net'** và **'myloughborough[.]com'** đều được đăng ký sử dụng địa chỉ email **'tplutalova@list[.]ru'**.

actuallys[.]com

Hồ sơ WHOIS của tên miền **'actuallys[.]com'** cho thấy trường hợp địa chỉ email kỹ thuật và quản trị viên là **'tplutalova@list[.]ru'**, nhưng địa chỉ email người đăng ký lại là **'ivan_s81@mail[.]ru'**.

Thông tin WHOIS tiểu sử cho tên miền **'actuallys[.]com'** cho thấy địa chỉ email đăng ký **'wangminghua6@gmail[.]com'** được liệt kê vào ngày 24 tháng 2 năm 2016. Vào ngày 11 tháng 3 năm 2016, địa chỉ email đã được thay đổi thành **'ivan_s81@mail.ru'** mặc dù ngày hết hạn đăng ký với nhà đăng ký, vẫn giữ nguyên.

wangminghua6@gmail[.]com

Địa chỉ email '**wangminghua6@gmail[.]com'** đã được sử dụng để đăng ký các tên miền được tìm thấy trong các phúc trình tình báo mối đe dọa trước đây. Năm 2015, Palo Alto đã xác định địa chỉ email này được dùng để đăng ký các tên miền máy chủ điều khiển (C2) cho phần mềm độc hại Cmstar. Năm 2014, email này cũng được dùng để đăng ký các tên miền được Mandiant xác định trong các chiến dịch lừa đảo do nhóm APT3 tiến hành. Năm 2013, địa chỉ email này đã được sử dụng để đăng ký các tên miền được CrowdStrike phát hiện trong một phần mềm thả mã độc có đường dẫn Program

Database (PDB) chứa các ký tự tiếng Hoa. Điều này cho thấy phần mềm được biên soạn trên một hệ thống sử dụng tiếng Hoa.

taoyujun@gmail[.]com

Tên miền **'hcjbtt[.]com'** được đăng ký với địa chỉ email **'taoyujun@gmail[.]com'**, tuy nhiên địa chỉ email quản trị viên lại được đăng ký là **'wangminghua6@gmail[.]com'**.

Không có hoạt động độc hại nào liên quan đến tên miền **'hcjbtt[.]com'**, tuy nhiên địa chỉ email **'taoyujun@gmail[.]com'** đã được phát hiện trong các phúc trình tình báo mối đe dọa trước đây. Năm 2014, địa chỉ email này đã được sử dụng để đăng ký một tên miền được Mandiant phát hiện trong các mẫu phần mềm độc hại '**Cueisfry Trojan**' được dùng để tấn công các tổ chức của Nhật Bản.

Địa chỉ email cũng đăng ký các tên miền như **'iaea-international[.]org'**, có vẻ nhằm giả mạo **Cơ quan Năng lượng Nguyên tử Quốc tế** , và **'idc-ctbto[.]org'**, giả mạo là **Trung tâm Dữ liệu Quốc tế** thuộc **Tổ chức Hiệp ước Cấm Thử Hạt nhân Toàn diện (CTBTO)**

Một hồ sơ WHOIS trước đây của tên miền '**iaea-international[.]org**' cho thấy địa chỉ email người đăng ký là '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

Tên miền '**udtglobals[.]com**' được phát hiện sử dụng '**wangminghua6@gmail[.]com**' làm email của quản trị viên và '**ocean.nio@rediffmail[.]com**' làm địa chỉ email của người đăng ký. Các hồ sơ WHOIS khác của tên miền này cho thấy cùng địa chỉ email người đăng ký nhưng sử dụng email của quản trị viên là '**taoyujun@gmail[.]com**'.

Tên miền '**udtglobals[.]com**' dường như đang giả mạo '**UDT Global**' một sự kiện toàn cầu dành cho các công ty trong lĩnh vực quốc phòng và an ninh dưới biển. Tên người sử dụng '**ocean.nio**' trong địa chỉ email có thể đang cố ý bắt chước **Viện Hải dương học Quốc gia (National Institute of Oceanography - NIO)**, tổ chức có mặt ở nhiều quốc gia. Mặc dù việc sử dụng dịch vụ email **Rediff** (có trụ sở tại Ấn Độ) có thể cố tình giả mạo **Viện Hải dương học Quốc gia Ấn Độ.**

Djibdiplomatie[.]com

Tên miền '**djibdiplomatie[.]com**' dường như giả mạo dịch vụ ngoại giao của Djibouti, và có hồ sơ WHOIS tương tự như tên miền '**utdglobals[.]com'.** Một hồ sơ cho thấy người đăng ký là '**ocean.nio@rediffmail[.]com**' và quản trị '**taoyujun@gmail[.]com**' trong khi các hồ sơ khác cho thấy '**wangminghua6@gmail[.]com**' là email của quản trị viên và '**ocean.nio@rediffmail[.]com**' là email của người đăng ký.

Cả hai tên miền này đều có các giá trị kiểu gõ bàn phím (keyboard walking) trong hồ sơ WHOIS. Ví dụ: '**udtglobals[.]com**' có giá trị '**ASDF**' là thành phố đăng ký và

‘**djibdiplomatie[.]com’** có giá trị ‘**DAF DAGF**’ là giá trị tên người đăng ký. Những giá trị này tương tự với các giá trị đã được phát hiện trong các tên miền BADBAZAAR khác.

Mặc dù các địa chỉ email **‘wangminghua6@gmail[.]com’** và **‘taoyujun@gmail[.]com’** được tìm thấy trong hồ sơ WHOIS của các tên miền giả mạo **sự kiện quốc tế về quốc phòng dưới biển**, **dịch vụ ngoại giao Djibouti** và **Cơ quan Năng lượng Nguyên tử Quốc tế**, nhưng chúng cũng xuất hiện trong hồ sơ WHOIS của nhiều tên miền không liên quan đến hoạt động độc hại.

Sự kết hợp giữa các tên miền giả mạo và các tên miền không độc hại có thể cho thấy sự tồn tại của một thực thể đang mua sắm hạ tầng cơ sở, được sử dụng để hỗ trợ hoạt động của các tác nhân mạng độc hại.

Địa chỉ email ‘**ocean.nio@rediffmail[.]com**’ chỉ được tìm thấy trong các tên miền giả mạo như đã được mô tả bên trên. Hai địa chỉ email **‘ivan_s81@mail[.]ru’** và **‘tplutalova@list[.]ru’** đã đăng ký một số ít tên miền, và một số trong số đó từng được lưu trữ trên hạ tầng cơ sở của BADBAZAAR. Ba địa chỉ email này được cho là có liên hệ chặt chẽ hơn với các hoạt động của các tác nhân mạng độc hại. Điều này là do số lượng tên miền cao hơn mà chúng liên kết có liên quan đến hoạt động độc hại so với email ‘**wangminghua6@gmail[.]com**’ và ‘**taoyujun@gmail[.]com**’.

(Xem Phụ lục A, hình ảnh 5)

Liên kết đến các tác nhân đe dọa khác

Một đặc điểm chung khác của các tên miền liên quan đến BADBAZAAR như ‘**actuallys[.]com**’, ‘**clublogs[.]com**’, ‘**myloughborough[.]com**’, ‘**rewrwer[.]com**’, và ‘**voiceoftibet[.]net**’ là tất cả đều được đăng ký qua nhà cung cấp eNom và được “để không” *(parked)* tại **‘255.255.255[.]254’**.

Theo các cuộc điều tra trước đây của NCSC, các tên miền khác có đặc điểm tương tự đã tiết lộ hoạt động liên quan đến nhóm **APT5** vào năm 2019, và **APT14** trong giai đoạn từ năm 2009 đến năm 2011.

Các tên miền được liên kết với APT5- có hồ sơ WHOIS trước đây liệt kê ‘**taoyujun@gmail[.]com**’ là địa chỉ email của người đăng ký.

Các tên miền liên kết với APT14 có tên miền phụ gồm ‘ba chữ cái’ dường như đại diện cho mục tiêu dự kiến của các hoạt động độc hại của chúng. Một ví dụ là tên miền ‘**bae.cisconline[.]net**’, cho thấy mục tiêu nhắm tới có thể là công ty BAE Systems, và được phát hiện trong một ‘**Poison Ivy**’ mẫu phần mềm độc hại.

Một đặc điểm tương tự cũng được phát hiện trong các tên miền BADBAZAAR, nơi các tên miền phụ liên quan đến tên ứng dụng bị nhiễm Trojan:

Tên của Ứng dụng	C2 URL
Ủng hộ người Hồi giáo	**mpp**.pmstwocqn[.]com
Lập trình phát video cho Android	**vpf**.titeperformance[.]com
Batter Master (Cao thủ đánh bóng)	**bat**.androidupdated[.]net
Radio Afghanistan	**afg**.collinformations[.]com
Từ điển EN-UG Miễn phí	**eud**.titeperformance[.]com
Khôi phục Đĩa Video	**dvr**.collinformations[.]com
TextNow (Ứng dụng nhắn tin)	**ttn**.titeperformance[.]com

Cần lưu ý rằng các hoạt động liên quan đến APT5 và APT14 là trong quá khứ, và cũng có những tên miền khác được đăng ký qua eNom và và được phân giải thành địa chỉ **'255.255.255.254'** không thể liên kết với hoạt động độc hại. Do đó, không chắc chắn rằng các tác nhân đứng sau những chiến dịch này là cùng một nhóm hoặc có liên quan đến nhau.

Tên Máy

Phân tích các máy chủ điều khiển (C2) và mẫu của BADBAZAAR đã tiết lộ các tên máy được sử dụng làm giá trị 'Common Name *(Tên thường thấy)*' trong chứng chỉ SSL. Các cuộc điều tra của NCSC về tên máy chủ được phát hiện trong các mẫu và hạ tầng cơ sở của BADBAZAAR cho thấy rằng các tên máy chủ này được sử dụng trên nhiều địa chỉ IP khác nhau. Các địa chỉ IP này đang lưu trữ các tên miền được tìm thấy trong các mẫu của BADBAZAAR. Phần bên dưới sẽ cung cấp thêm chi tiết về các tên máy chủ, và địa chỉ IP có chứa các tên máy chủ này, đồng thời lưu trữ các tên miền C2 độc hại của BADBAZAAR.

Trong hầu hết các trường hợp, sự hiện diện của chứng chỉ có giá trị tên máy chủ trùng khớp với các giải pháp IP cho tên miền độc hại được chỉ định, một số ít trường hợp không xảy ra tình trạng này và đã được nêu lên.

WIN-EU0VLBL7TUJ

Tên máy chủ **‘WIN-EU0VLBL7TUJ’** đã được quan sát thấy xuất hiện trên các địa chỉ IP sau:

- ‘**116.203.53[.]21**’ lưu trữ các tên miền máy chủ điều khiển (C2) của BADBAZAAR ‘**uyapkfinder[.]com**’ và ‘**thewestuniverse[.]com**’.

- **‘95.216.169[.]27’** lưu trữ các tên miền máy chủ điều khiển (C2) của BADBAZAAR **‘adysfunction[.]com’** và tên miền phụ **‘download.apkbazar[.]biz’** được phát hiện là đường dẫn tải xuống mẫu BADBAZAAR.

(Xem Phụ lục A, hình ảnh 6)

WIN-70E59JVOB9G

Tên máy chủ ‘**WIN-70E59JVOB9G’** đã được phát hiện trên các địa chỉ IP sau đây:

- **‘23.88.28[.]220’**: lưu trữ các tên miền phụ thuộc BADBAZAAR C2 bao gồm: **‘aua.rondwsign[.]com’, ‘nal.tokenmajorp[.]com’, ‘pep.rondwsign[.]com’** ‘**doa.rondwsign[.]com**’, và **‘pls.rondwsign[.]com’.** Có khoảng thời gian hai ngày giữa thời điểm chứng chỉ với máy được nhìn thấy lần cuối, và thời điểm các tên miền độc hại được nhìn thấy lần đầu tiên phân giải thành IP đó.

- **‘23.88.28[.]221’** được lưu trữ trên BADBAZAAR liên kết đến tên miền phụ **‘bt.bhvghg[.]com’**.

- **‘23.88.28[.]222’** lưu trữ các tên miền C2 của BADBAZAAR **‘tubevideoplus[.]org’** và **‘cde.mpoxcases[.]com’**.

- **‘65.21.92[.]67’** lưu trữ tên miền phụ C2 của BADBAZAAR **‘bat.androidupdated[.]net’**, Nó cũng lưu trữ tên miền phụ ‘**apps.androidupdated[.]net’** là phần mềm độc hại DoubleAgent C2.

- **‘65.21.92[.]77’** lưu trữ các tên miền phụ C2 của BADBAZAAR ‘**wyo.titeperformance[.]com**’, ‘**big.collinformations[.]com**’ ‘**vpf.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’ và ‘**afg.collinformations[.]com**’

- **‘65.108.192[.]134’** lưu trữ các tên miền phụ C2 của BADBAZAAR **‘upd.whoscaller[.]net’** và **‘ggl.whoscaller[.]net’.**

- **‘142.132.131[.]15’** lưu trữ các tên miền phụ C2 của BADBAZAAR **‘bvn.lookincategory[.]com’** và **‘edr.lookincategory[.]com’.** Có khoảng thời gian mười một ngày giữa thời điểm chứng chỉ có tên máy được nhìn thấy lần cuối, và thời điểm các tên miền độc hại được nhìn thấy lần đầu tiên phân giải thành IP đó.

- Địa chỉ **‘142.132.131[.]20’** đã lưu trữ các tên miền phụ **‘son.onlinegamersgroup[.]com’** và **‘system.onlinegamersgroup[.]com’** được cho là máy chủ điều khiển (C2) của BADBAZAAR, vì các tên miền này được lưu trữ trong cùng thời điểm mà các chứng chỉ SSL liên quan với BADBAZAAR được quan sát thấy trên IP này.

- **‘142.132.131[.]28’** lưu trữ tên miền C2 của BADBAZAAR **‘goldplusapp[.]net’** cùng với các tên miền phụ: **‘who.goldplusapp[.]net’** và **‘cgf.goldplusapp[.]net’.**

- **‘162.55.103[.]211’** lưu trữ các tên miền phụ C2 của BADBAZAAR dưới miền ‘**oha.alpinemap[.]net**’, ‘**aru.alpinemap[.]net’**, ‘**aso.alpinemap[.]net**’, ‘**afr.alpinemap[.]net**’, và ‘**aar.alpinemap[.]net**’.

- **‘162.55.103[.]212’** lưu trữ các tên miền phụ C2 của BADBAZAAR **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** và **‘aua.rondwsign[.]com’.**

- **‘195.154.47[.]99’** lưu trữ các tên miền phụ C2 của BADBAZAAR **‘ggl.whoscaller[.]net’** và **‘upd.whoscaller[.]net’.** Có khoảng thời gian ba ngày giữa thời điểm chứng chỉ có tên máy được nhìn thấy lần đầu tiên, và thời điểm tên miền độc hại được nhìn thấy lần cuối cùng phân giải thành IP đó.

- **‘195.154.60[.]3’** lưu trữ các tên miền phụ C2 của BADBAZAAR **‘upd.whoscaller[.]net’**.
‘**ggl.whoscaller[.]net**’.

- **‘212.83.189[.]89’** lưu trữ các tên miền phụ C2 của BADBAZAAR ‘**wyo.titeperformance[.]com**’, ‘**eud.titeperformance[.]com**’, ‘**vpf.titeperformance[.]com**’ và ‘**afg.collinformations[.]com**’.

- **‘212.129.21[.]168’** lưu trữ các tên miền C2 của BADBAZAAR: ‘**fre.lookincategory[.]com**’, ‘**tgr.lookincategory[.]com**’, ‘**fgt.lookincategory[.]com**’ ‘**luj.lookincategory[.]com**’ và ‘**bvn.lookincategory[.]com**’.

(Xem Phụ lục A, hình ảnh 7)

WIN-50QO3EIRQVP

Tên máy **‘WIN-50QO3EIRQVP’** đã được quan sát thấy trên các địa chỉ IP sau đây:

- **‘45.76.132[.]91’** lưu trữ các tên miền‘**yumoftion[.]com**’, ‘**androidupdated[.]net**’. Cả hai tên miền này đều liên quan đến BADBAZAAR, vì với các tên miền phụ ‘**fow.yumoftion[.]com**’ và ‘**bat.androidupdated[.]net**’ là các tên miền C2 của BADBAZAAR. Ngoài ra, tên miền phụ **‘apps.androidupdated[.]net’** là máy chủ điều khiển (C2) của phần mềm độc hại DoubleAgent. Nó cũng lưu trữ tên miền ‘**pmstwocqn[.]com’**, được liên quan với BADBAZAAR thông qua hồ sơ WHOIS.

- **‘95.179.210\[.]85’** lưu trữ tên miền **‘clublogs[.]com’**, trong đó **‘xle.clublogs[.]com’** là một tên miền C2 của BADBAZAAR. Địa chỉ này cũng lưu trữ các tên miền liên quan đến BADBAZAAR khác gồm: ‘**bre.myloughborough[.]com**’, ‘**img.rewrwer[.]com**’, **'www.voiceoftibet[.]net'** và ‘**actuallys[.]com**’.

- **‘199.247.21[.]34’** lưu trữ các tên miền **‘titeperformance[.]com’** và **‘collinformations[.]com’** trong đó các tên miền phụ đều là tên miền C2 của BADBAZAAR.

- **‘217.69.10[.]128’** lưu trữ tên miền C2 của BADBAZAAR: **‘uyghurdict[.]com’**.

(Xem Phụ lục A, hình ảnh 8)

WMSvc-WIN-50QO3EIRQVP

Tên máy **‘WMSvc-WIN-50QO3EIRQVP’** đã được phát hiện trên các địa chỉ IP sau đây:

- **‘78.46.185[.]251’** lưu trữ tên miền C2 của BADBAZAAR **‘groupgram[.]org’**, được Volexity trình báo sử dụng cổng 4432 cho các kết nối độc hại.
- **‘65.21.92[.]69’** và **‘163.172.205[.]207’** lưu trữ tên miền **‘widelygram[.]org’** được cho là tên miền C2 của BADBAZAAR, vì trong thời gian lưu trữ trên cả hai IP này, cổng 4432 đều được mở.
- **‘163.172.198[.]206’** lưu trữ tên miền **‘maxgram[.]org’**, cũng được cho là tên miền C2 của BADBAZAAR khi cổng 4432 mở trong suốt thời gian lưu trữ.

(Xem Phụ lục A, hình ảnh 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

Tên máy **‘WMSvc-WIN-50QO3EIRQVP’** và **‘WIN-7LSBB9R0F1L’** được phát hiện trên địa chỉ IP sau đây cùng một lúc:

- ‘**148.251.87[.]245**’ lưu trữ các tên miền C2 của BADBAZAAR: **‘flygram[.]org’** và **‘groupgram\[.]org’**

(Xem Phụ lục A, hình ảnh 10)

WIN-N8H8S9BG2P0

Tên máy **‘WIN-N8H8S9BG2P0’** đã được phát hiện trên địa chỉ IP sau đây:

- **‘148.251.87[.]247’** lưu trữ các tên miền C2 của BADBAZAAR **‘omarwhatsapp[.]org’** và **‘flygram[.]org’.**

(Xem Phụ lục A, hình ảnh 11)

WIN-I6VBN8MR92A

Tên máy **‘WIN-I6VBN8MR92A’** đã được phát hiện trên địa chỉ IP sau đây:

- **‘148.251.87[.]197’**, nơi lưu trữ tên miền C2 của BADBAZAAR: **‘tryhrwserf[.]com’**.

(Xem Phụ lục A, hình ảnh 12)

Dựa trên dữ liệu thương mại hiện có, mức độ xuất hiện của các tên máy này trên internet khá đa dạng. Một số được phát hiện cùng một lúc trên nhiều địa chỉ IP khác nhau, điều này cho thấy các VM được tạo từ cùng một mẫu. Điều quan trọng cần lưu ý là đối với một số tên máy chủ, không phải tất cả các IP bị theo dõi đều có thể liên quan đến hoạt động độc hại. Điều này có nghĩa là việc sử dụng tên máy chủ không chỉ giới hạn ở những kẻ đe dọa.

Tuy nhiên, sự phổ biến của một số tên máy này trên các IP từng lưu trữ các tên miền C2 của BADBAZAAR, có thể cho thấy có một thực thể mua sắm hạ tầng cơ sở đang được sử dụng để cấu hình các máy chủ nhằm hỗ trợ các hoạt động mạng độc hại của các tác nhân này.

Sự hiện diện trên mạng xã hội

Các phúc trình trước đây từ Volexity cho thấy các tác nhân mạng độc hại đã tạo ra các video trên YouTube (nhằm quảng bá việc sử dụng các ứng dụng độc hại này). Những video này bao gồm các hướng dẫn chi tiết về cách sử dụng các ứng dụng mà họ đã thiết kế.

NCSC đã phát hiện thêm hai kênh YouTube liên quan đến hoạt động của các tác nhân đe dọa. Kênh YouTube có tên URL là '**@josephjoey3499'** dường như đang quảng bá việc sử dụng '**Maxgram**' và một kênh khác được đăng ký với tên '**@uyghurapks3096'** đang quảng bá '**Uyghur APK Finder'**.

Ngoài ra, các video trên YouTube quảng bá cho '**Flygram**' và '**Signal Plus**' đã cho thấy các tác nhân đe dọa sử dụng các số điện thoại hiển thị rõ ràng. Trong '**Flygram**' video, ở phút 0:36, số điện thoại **'+1 (570) 378-7250'** được hiển thị và trong '**Signal Plus'** video, số điện thoại **'+1 (267) 298 4259'** được tiết lộ.

Volexity đã phúc trình một trang tin giả chủ đề Tây Tạng có tên **'ignitetibet[.]net'**, được phát hiện trong các phương tiện Telegram được cho là do các tác nhân đe dọa vận hành. Địa chỉ email **'choekyi.wangmo@ignitetibet[.]net'** được quan sát thấy để lại bình luận trên các bài đăng của trang **'tibetone.org'**, trang này đã được Lookout công khai phúc trìnhlà trang C2 được sử dụng cho iOS biến thể của BADBAZAAR.

Địa chỉ email này được cho là do các tác nhân đe dọa kiểm soát, sử dụng nhân vật giả danh '**Choekyi Wangmo**'.

Đánh giá

BADBAZAAR và MOONSHINE sử dụng nhiều phương pháp kỹ thuật xã hội để tấn công nhằm nhắm mục tiêu cụ thể vào cộng đồng người Duy Ngô Nhĩ, Tây Tạng và Đài Loan, bao gồm:

- việc cấy mã độc vào các ứng dụng được cộng đồng này quan tâm, chẳng hạn như ứng dụng Kinh Koran bằng tiếng Duy Ngô Nhĩ, gần như chắc chắn được thiết kế riêng để phù hợp với nhóm nạn nhân được nhắm đến
- việc đưa các ứng dụng đã được cài mã độc vào các cửa hàng ứng dụng chính thức rất có thể nhằm tạo cảm giác hợp pháp, và việc chia sẻ chúng trong các nhóm trò chuyện cũng rất có thể được dùng để lợi dụng các mối quan hệ tin cậy trong các cộng đồng này

BADBAZAAR và MOONSHINE thu thập dữ liệu mà gần như chắc chắn rất có giá trị đối với nhà nước Trung Quốc. Mặc dù BADBAZAAR và MOONSHINE đã được quan sát thấy nhắm vào các cá nhân người Duy Ngô Nhĩ, Tây Tạng và Đài Loan, vẫn có các phần mềm độc hại khác nhắm tới các nhóm thiểu số khác ở Trung Quốc. Công dân từ các quốc gia cùng ký kết, kể cả ở Trung Quốc và nước ngoài, những người được cho là ủng hộ các phong trào gây nguy hại đến sự ổn định của chế độ, gần như chắc chắn đang bị đe dọa bởi các phần mềm độc hại như BADBAZAAR và MOONSHINE trên thiết bị di động. Khả năng thu thập dữ liệu vị trí, âm thanh và hình ảnh gần như chắc chắn tạo cơ hội để hỗ trợ các hoạt động giám sát và quấy rối trong tương lai, bằng cách cung cấp thông tin theo thời gian thực về hoạt động của mục tiêu.

MITRE ATT&CK®

Phúc trình này được biên soạn dựa trên khung làm việc của MITRE ATT&CK®, một cơ sở tri thức toàn cầu về các chiến thuật và kỹ thuật của tác nhân dựa trên các quan sát thực tế ngoài đời.

Chiến thuật	ID	Kỹ thuật	Phương sách
Dò thám	T1593.001	Tìm kiếm Trang mạng/Tên Miền mở Rộng: Mạng Xã hội	Tác nhân tìm kiếm các nhóm và diễn đàn trực tuyến phù hợp với các nạn nhân mà chúng nhắm đến để chia sẻ phần mềm độc hại
Phát triển Nguồn lực	T1583.001	Mua sắm Hạ tầng Cơ sở: Tên miền	Tác nhân đăng ký tên miền cho các máy chủ điều khiển và kiểm soát
Phát triển Nguồn lực	T1587.001	Phát triển Năng lực: Phần mềm độc hại	Mã độc hại được viết để chèn vào các ứng dụng đã bị nguỵ trang hoá
Phát triển Nguồn lực	T1608.001	Biểu diễn Năng lực: Tải Phần mềm Độc hại Lên	Các ứng dụng đã bị nhiễm trojan được tải lên các nền tảng trực tuyến, bao gồm cả các cửa hàng ứng dụng
Phát triển Nguồn lực	T1585.001	Tạo Tài khoản: Tài khoản Mạng Xã hội	Tác nhân tạo tài khoản trên các trang mạng và mạng xã hội để chia sẻ và quảng cáo phần mềm độc hại
Phát triển Nguồn lực	T1585.002	Tạo Tài khoản: Tài khoản Email	Tác nhân sử dụng tài khoản email thương mại và được lưu trữ riêng tư để lưu trữ và chia sẻ phần mềm độc hại
Quyền Truy cập Ban đầu	T1189	Xâm nhập bằng Drive-by	Các tập lệnh độc hại nằm ẩn trong các ứng dụng hợp pháp và được tải lên các cửa hàng ứng dụng
Quyền Truy cập Ban đầu	T1566.003	Lừa đảo: Lừa đảo qua Dịch vụ	Tác nhân gởi các ứng dụng đã bị nhiễm trojan đến các nhóm được nhắm vào, qua phương tiện truyền thông xã hội bao gồm Telegram
Thi hành	T1204.002	Thực thi bởi Người Sử dụng: Tập Hồ sơ Độc hại	Nạn nhân phải cài đặt các ứng dụng đã bị nguỵ trang hóa để khởi động mã độc
Né tránh Phòng thủ	T1027.009	Tập Hồ sơ hoặc Thông tin bị Làm rối: Mã độc được Chèn vào	Mã độc hại nằm ẩn bên trong các ứng dụng trông có vẻ hợp pháp để tránh bị phát hiện
Né tránh Phòng thủ	T1036.005	Nguỵ trang: Giả mạo Tên hoặc Địa điểm Hợp pháp	Các các tập hồ sơ được nguỵ trang trùng khớp với tên, giao diện và chức năng của các ứng dụng hợp lệ.
Né tránh Phòng thủ	T1656	Mạo danh	Tác nhân mạo danh những cá nhân đáng tin cậy bằng cách tạo ra các trang mạng được nguỵ trang

			và sử dụng tên người dùng liên quan đến các nhóm bị nhắm đến
Thu thập	T1123	Ghi âm	Các ứng dụng bị nhiễm trojan có thể yêu cầu các quyền hạn không cần thiết bao gồm quyền truy cập micrô
Thu thập	T1125	Quay Video	Các ứng dụng bị nhiễm trojan có thể yêu cầu các quyền hạn không cần thiết bao gồm quyền truy cập máy ảnh
Thu thập	T1005	Dữ liệu từ Hệ thống Cục bộ	Các ứng dụng bị nhiễm trojan có thể yêu cầu các quyền không cần thiết bao gồm cả các tập hồ sơ cục bộ.
Chỉ huy và Kiểm soát	T1071.001	Giao thức Lớp Ứng dụng: Giao thức Mạng	Phần mềm độc hại kết nối với C2 bằng HTTPS và WebSocket.
Chỉ huy và Kiểm soát	T1509	Cổng Không Chuẩn	Cổng không chuẩn được sử dụng như cổng 4432 và 2333
Di chuyển Dữ liệu	T1041	Di chuyển Dữ liệu Qua Kênh C2	Phần mềm độc hại di chuyển dữ liệu bằng kết nối HTTPS và WebSocket.
Tác động	T1565.002	Thao túng Dữ liệu: Thao túng Dữ liệu được Truyền đi	Tác nhân lấy dữ liệu từ nạn nhân bằng cách khởi động lưu lượng truy cập mạng ứng dụng không cần thiết cho chức năng ứng dụng

Dấu chỉ

MOONSHINE:

- Vào ngày 1 tháng 4 năm 2025, một đợt tìm kiếm các bảng điều khiển VLiteUI cho ra kết quả sau đây:

Địa chỉ IP	Cổng	Lần đầu Phát hiện	Lần cuối Phát hiện
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

- Vào ngày 1 tháng 4 năm 2025, một đợt tìm kiếm các bảng điều khiển SCOTCH ADMIN cho ra kết quả sau đây:

Địa chỉ IP	Cổng	Lần đầu Phát hiện	Lần cuối Phát hiện
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

- Vào ngày 14 tháng 3 năm 2024, một đợt tìm kiếm các bảng điều khiển SCOTCH ADMIN cho ra kết quả sau đây:

Tên miền	Địa chỉ 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:

Mô tả	Chứng chỉ SSL được phát hiện trên các máy chủ điều khiển (C2) của BADBAZAAR.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- Vào ngày 1 tháng 4 năm 2025, một đợt tìm kiếm chứng chỉ BADBAZAAR nêu trên đã cho ra các kết quả sau đây:

Địa chỉ IP	Cổng	Lần đầu Phát hiện	Lần cuối Phát hiện
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

Mô tả	Chứng chỉ SSL được phát hiện trên các máy chủ điều khiển và kiểm soát (C2) của BADBAZAAR
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- Vào ngày 1 tháng 4 năm 2025, một đợt tìm kiếm chứng chỉ BADBAZAAR nêu trên cho ra các thông tin sau đây:

Địa chỉ IP	Cổng	Lần đầu Phát hiện	Lần cuối Phát hiện
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

- Tên miền của WHOIS

Bên dưới là bảng liệt kê các tên miền hiện tại hoặc trong quá khứ mà có thông tin WHOIS trùng khớp với các giá trị được quan sát thấy trong các tên miền C2 của BADBAZAAR.

Giá trị WHOIS	Tên miền
Tiểu bang của Người Đăng ký: UJYJYUJ **Quốc gia của Người Đăng ký: Bolivia** **Người Đăng ký: 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
Tiểu bang của Người Đăng ký: REWR **Quốc gia của Người Đăng ký: CF** **Người Đăng ký: eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com

	• ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com
Tiểu bang của người Đăng ký: FSDF **Quốc gia của người Đăng ký: AL** **Người Đăng ký: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

Địa chỉ Email
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

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

Dưới đây là các đường dẫn tới các dấu chỉ xâm nhập (indicators of compromise - IoCs) liên quan đến BADBAZAAR và MOONSHINE. NCSC không thể xác nhận tính chính xác của toàn bộ thông tin trong các đường dẫn này, vì vậy độc giả nên tự kiểm tra và đánh giá tính xác thực cũng như tính thích hợp của các thông tin đó:

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

Các biện pháp giảm thiểu

NCSC khuyến khích việc áp dụng các khuyến nghị dưới đây nhằm phòng thủ trước các mối đe dọa được mô tả trong các tình huống được nghiên cứu.

- **Các nhà điều hành cửa hàng ứng dụng, bao gồm cả các cửa hàng ứng dụng bên thứ ba, và các nhà phát triển nên bảo đảm rằng các ứng dụng trên nền tảng của họ được bảo mật và tuân thủ Bộ Quy tắc Thực hành của chính phủ.** Xin xem Hướng dẫn: 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

- **Hỗ trợ đa ngôn ngữ**: Các nhà phát triển ứng dụng nên đầu tư vào việc điều chỉnh các ứng dụng phổ biến cho phù hợp với người dùng nói các ngôn ngữ thiểu số trong các nhóm bị nhắm đến, bao gồm tiếng Duy Ngô Nhĩ, tiếng Tây Tạng, tiếng Phúc Kiến Đài Loan và tiếng Quảng Đông. Hướng dẫn của Apple về việc điều chỉnh các ứng dụng cho phù hợp: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. Hướng dẫn của Google về ứng dụng dịch thuật: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **Giữ cho nền tảng mạng xã hội của bạn an toàn:** Các công ty mạng xã hội có thể làm cho các tác nhân mạng độc hại khó tạo tài khoản giả mạo và chia sẻ các tập hồ sơ hoặc đường dẫn độc hại trên nền tảng của họ trong các cộng đồng trực tuyến hợp pháp. Khi có thể, các công ty nên chia sẻ các chỉ số tấn công độc hại với toàn ngành để nâng cao nhận thức tập thể về mối đe dọa và hỗ trợ các biện pháp bảo vệ.

- **Kế hoạch khắc phục cho khách hàng:** Các tổ chức nên có các cách thức thông qua dịch vụ của mình để thông báo cho khách hàng đã cài đặt ứng dụng độc hại. Những cảnh báo này cần thu hút sự chú ý và cung cấp đầy đủ thông tin. Khi thích hợp, các tổ chức nên cung cấp hướng dẫn về cách xóa bỏ phần mềm và khuyến khích nạn nhân trình báo với cơ quan chức năng, chẳng hạn như NCSC ở Vương quốc Anh.

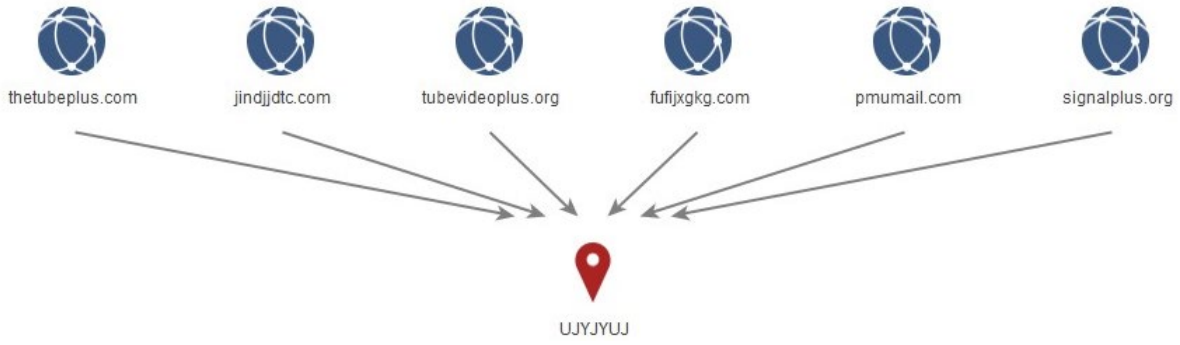
Xem Bộ Quy tắc Thực hành của App Store để biết thêm thông tin: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **Các nhóm làm việc nhằm mục đích hợp tác:** Các công ty truyền thông xã hội có thể thành lập các nhóm làm việc, cho phép các nhóm bảo mật của họ chia sẻ các dấu chỉ độc hại (IoC), chiến thuật, kỹ thuật và phương sách (TTPs) cũng như các quan sát thực tế. Điều này sẽ giúp hạn chế các tác nhân lợi dụng nền tảng của họ để thực hiện các chiến dịch độc hại.

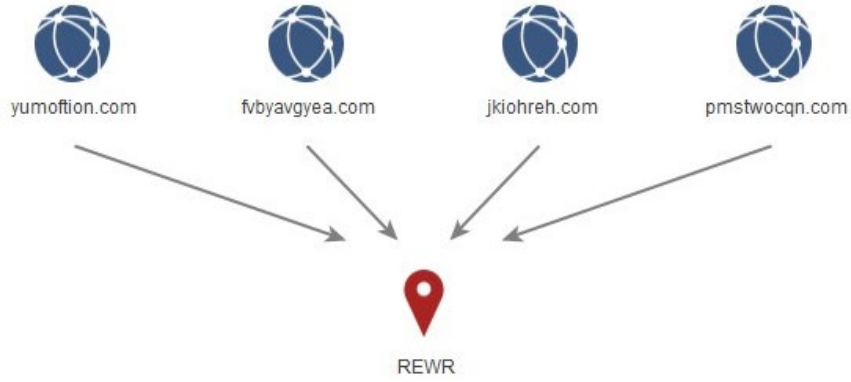
- **Phát hiện các ứng dụng bị chỉnh sửa:** Khi có thể, các nhà phát triển ứng dụng nên bao gồm chức năng thông báo cho người dùng nếu họ đã tải xuống phiên bản 'không chính thức' của ứng dụng. Điều này giúp bảo vệ người dùng khỏi các bản sao chứa mã độc.

Phụ lục A: Biểu đồ phân cụm WHOIS của BADBAZAAR / thông tin nhà môi giới tên miền

Hình ảnh 1 – 'UKYJYUJ'

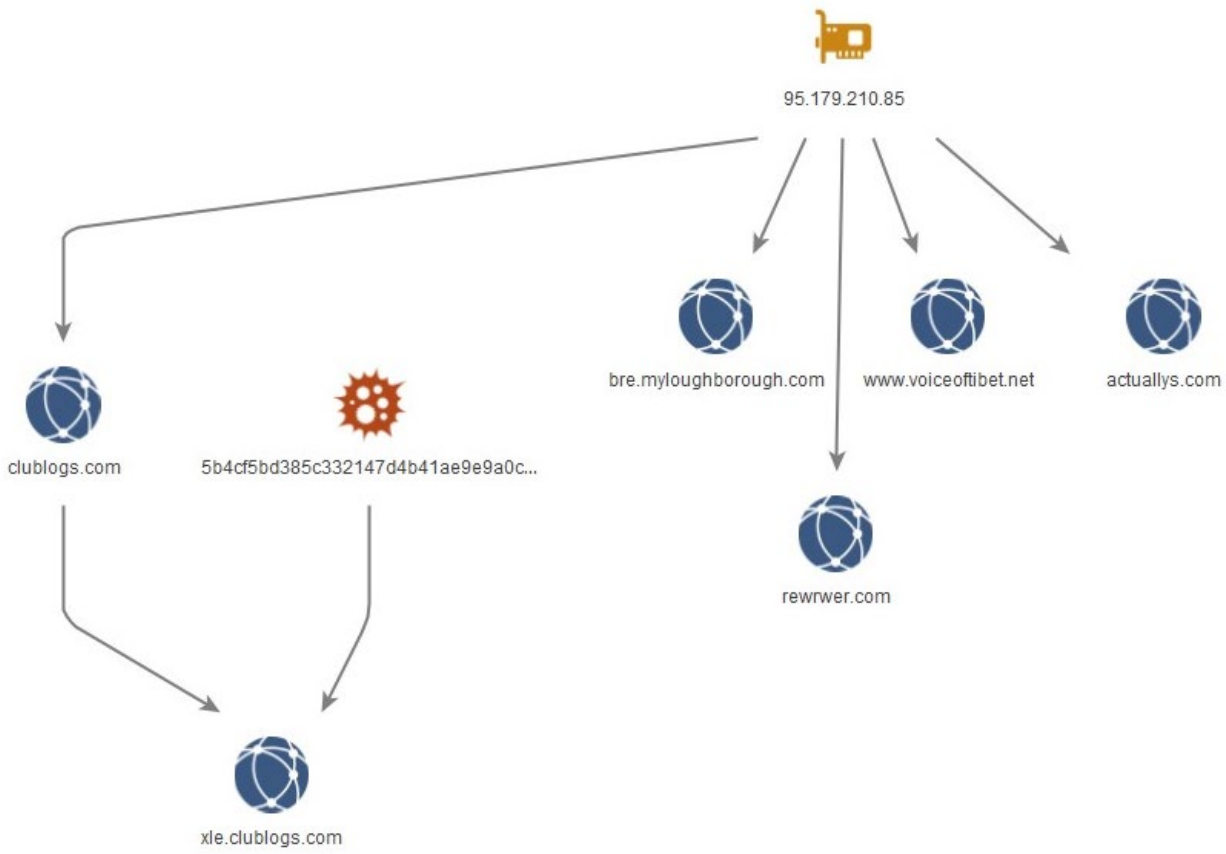


Hình ảnh 2 – Giá trị gõ bàn phím

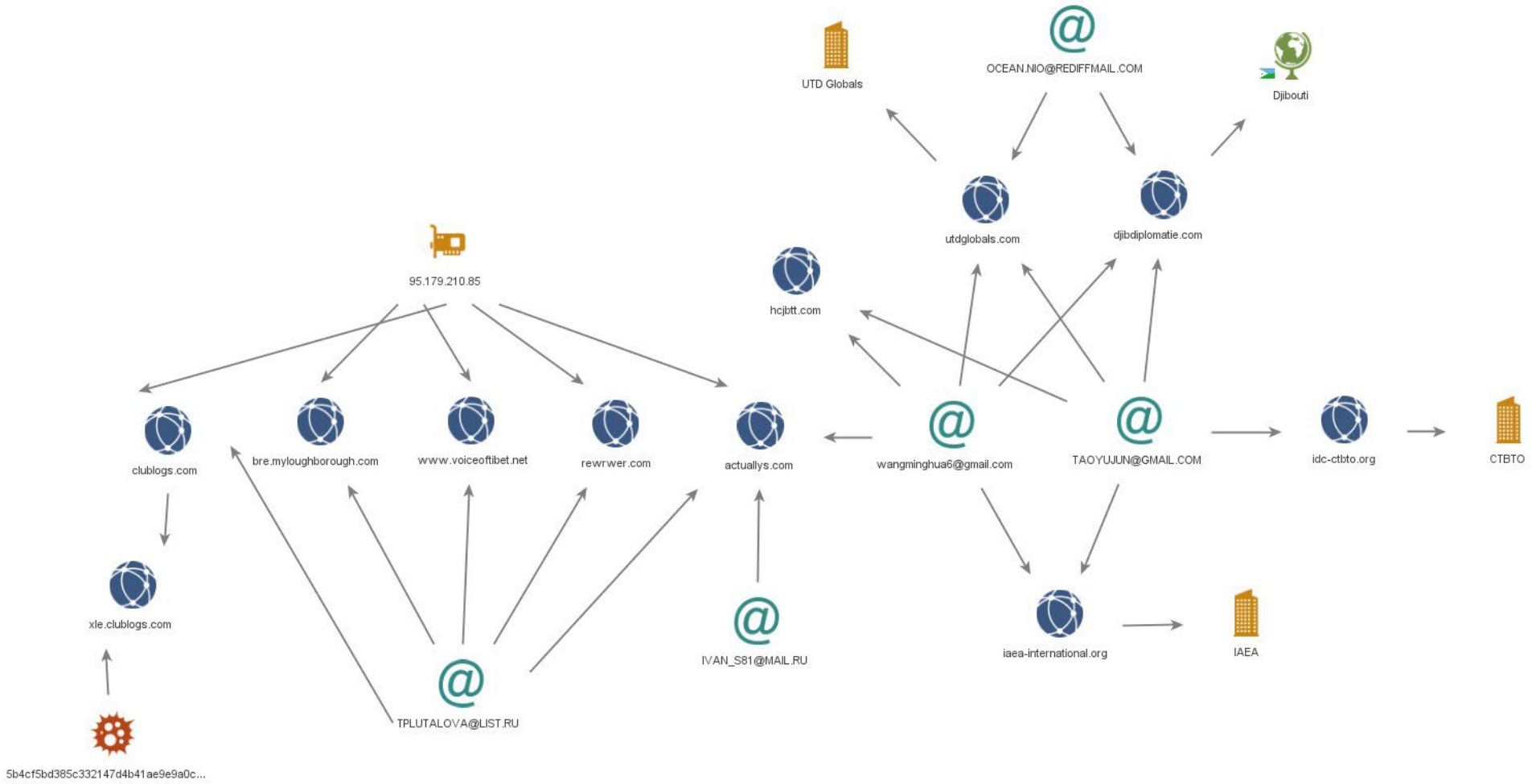


Hình ảnh 3 – Các miền bổ sung với 'FSDF' giá trị của cột trường tiểu bang

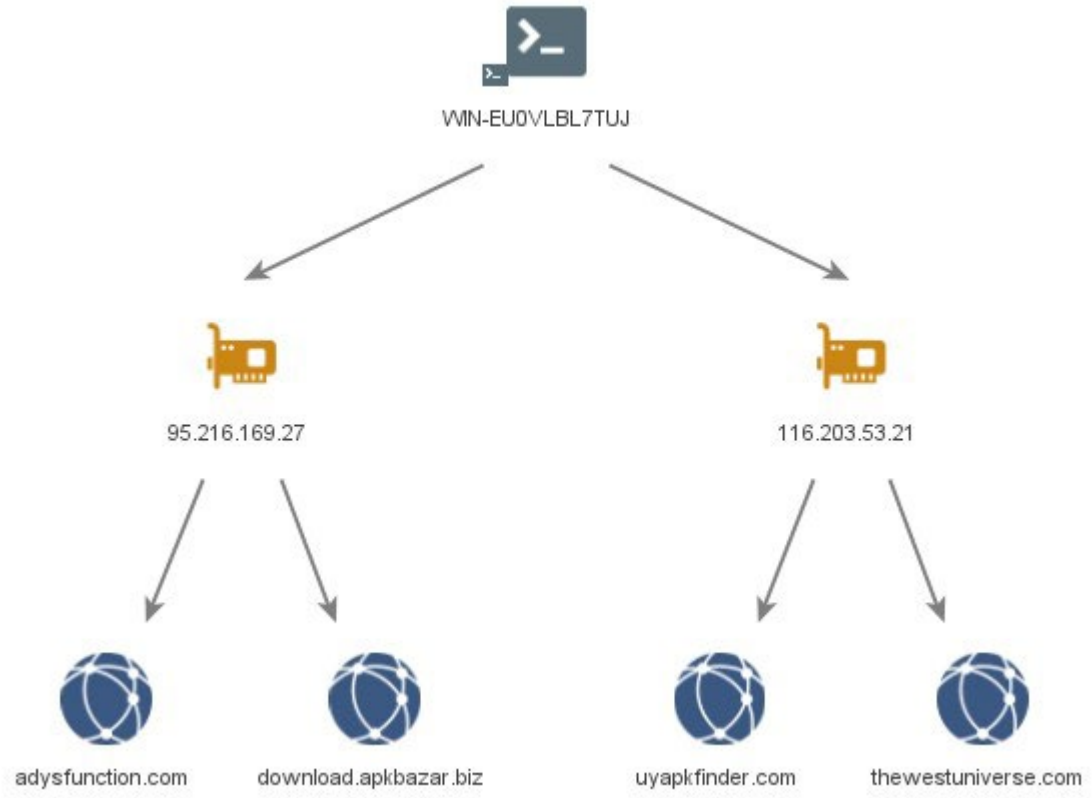
Hình ảnh 4 – **95.179.210[.]85**



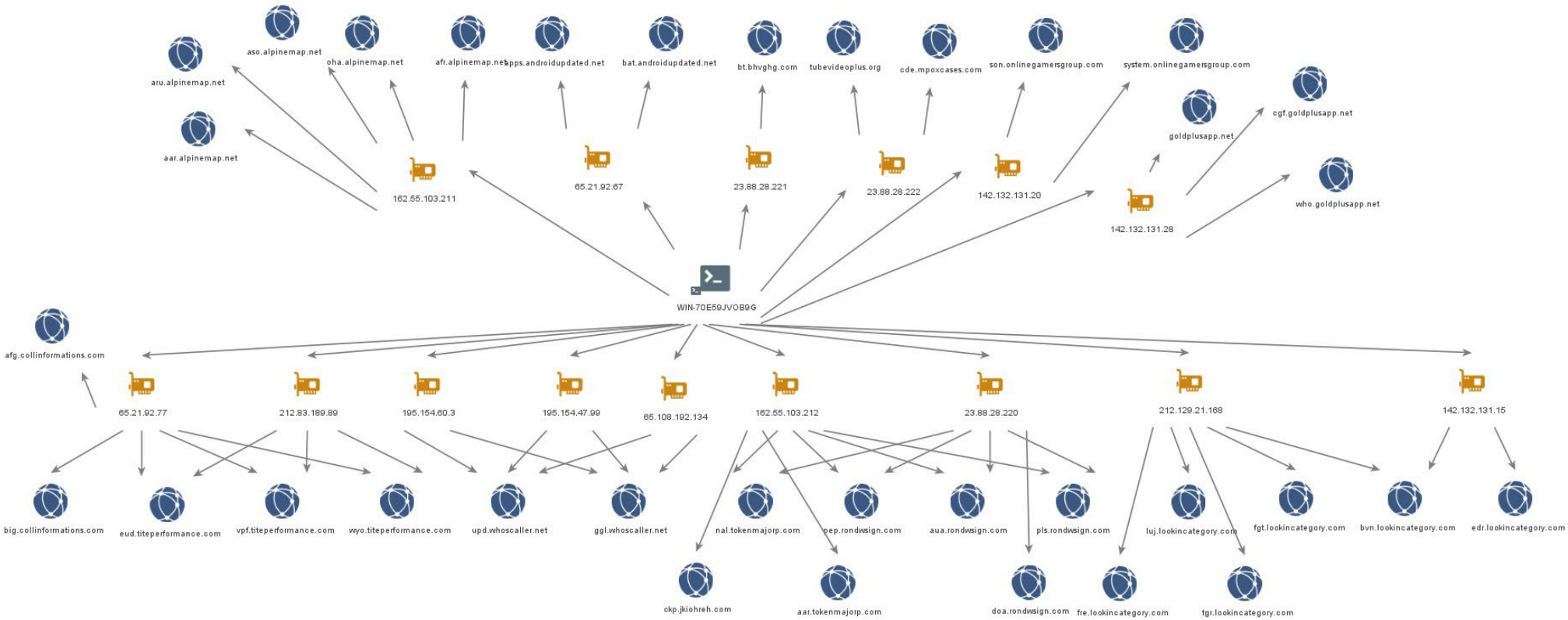
Hình ảnh 5 – WHOIS links



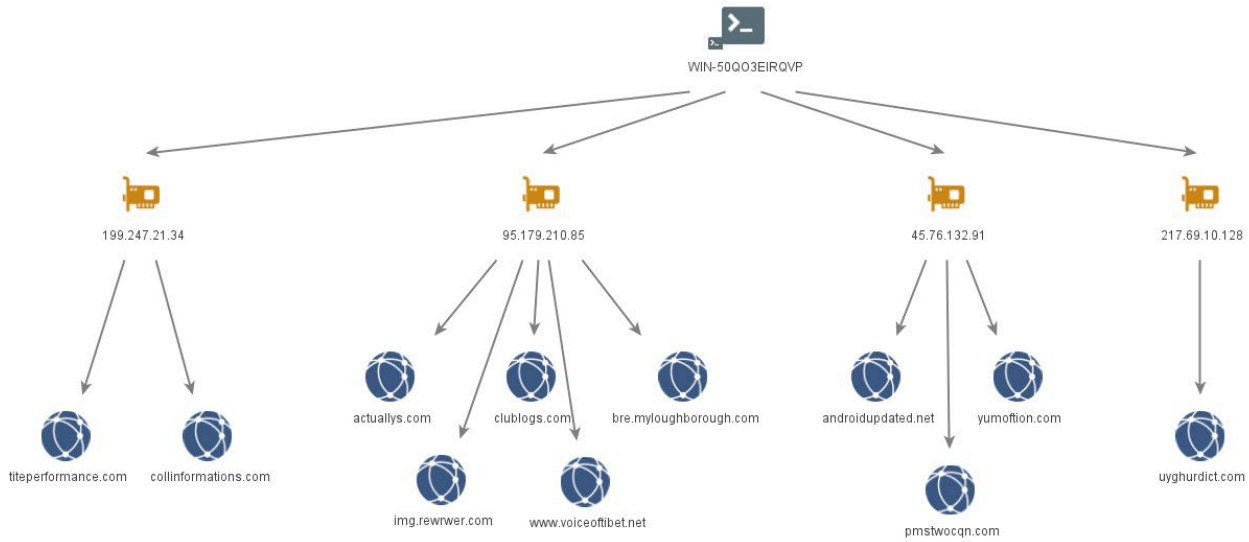
Hình ảnh 6 – **WIN-EU0VLBL7TUJ**



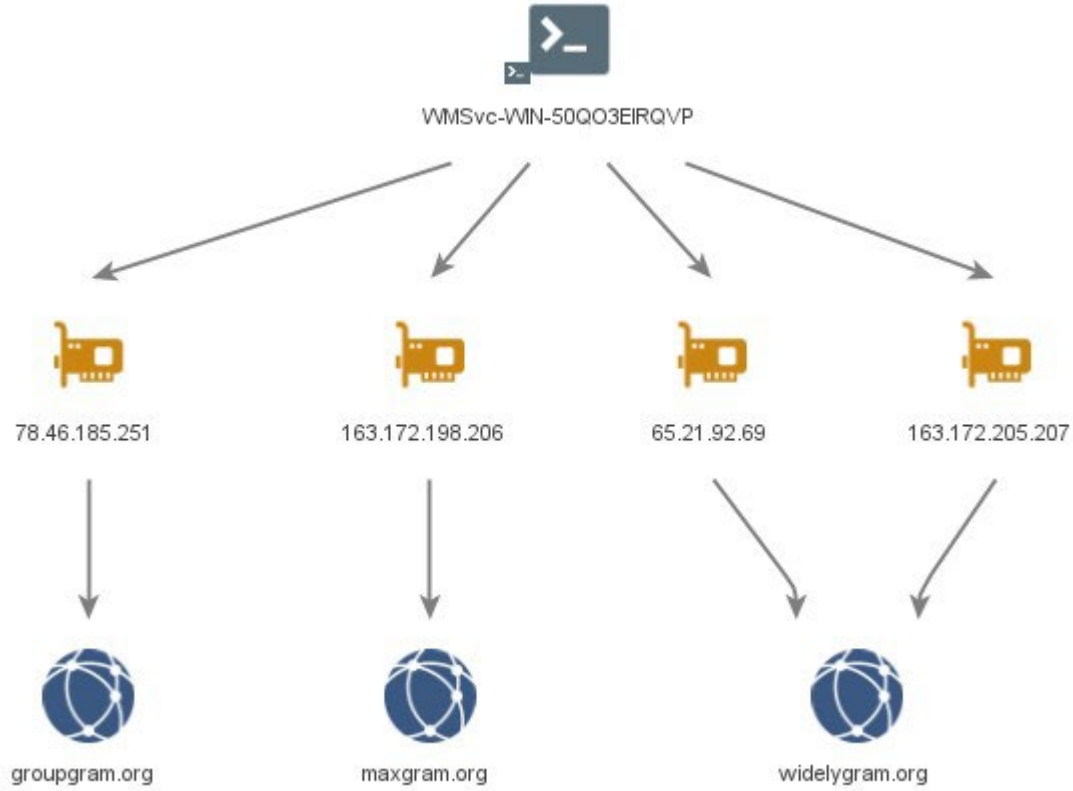
Hình ảnh 7 – **WIN-70E59JVOB9G**



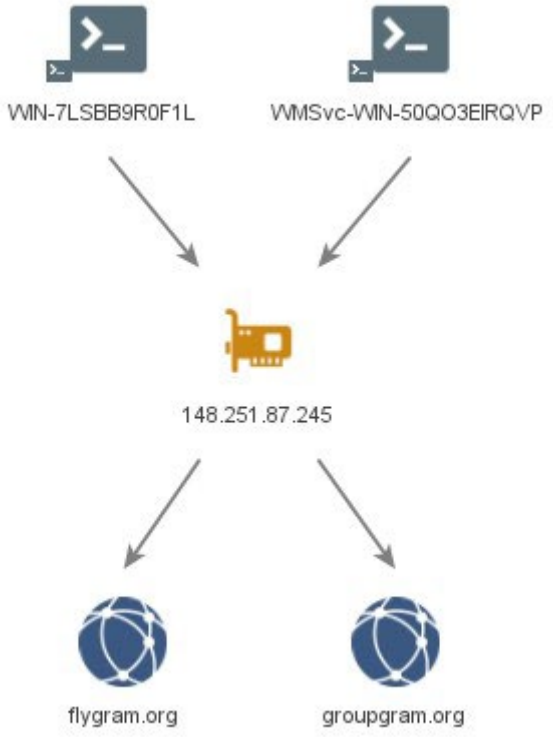
Hình ảnh 8 - **WIN-50QO3EIRQVP**



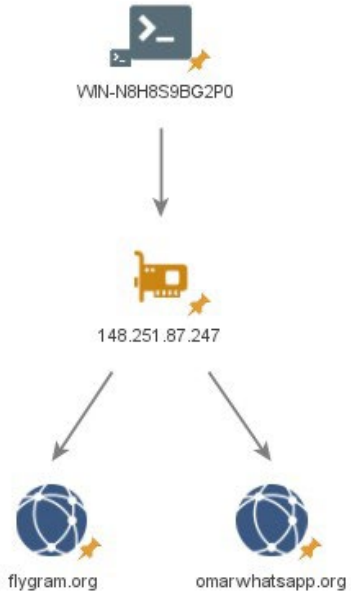
Hình ảnh 9 - **VMSvc-WIN-50QO3EIRQVP**



Hình ảnh 10 – **VMSvc-WIN-50QO3EIRQVP** và **WIN-7LSBB9R0F1L**



Hình ảnh 11 - **WIN-N8H8S9BG2P0**



Hình ảnh 12 – **WIN-I6VBN8MR92A**

Phụ lục B: Các mẫu MOONSHINE & BADBAZAAR đã được quan sát thấy

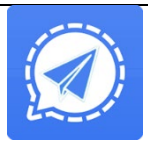
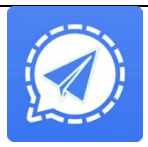
Bảng dưới đây liệt kê các ứng dụng đã được sử dụng trong các chiến dịch MOONSHINE và BADBAZAAR trong hai năm qua.

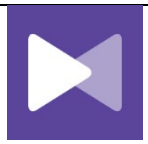
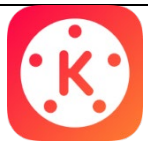
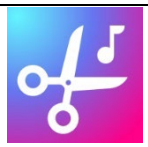
Nhiều ứng dụng trong số này thể hiện sự tương đồng rõ rệt với các ứng dụng nổi tiếng đã có. Đây rất có thể là một kỹ thuật cố ý của các tác nhân tấn công nhằm 'giả mạo' các thương hiệu nổi tiếng.

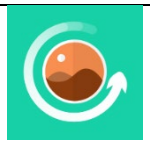
Điều quan trọng cần lưu ý là tên ứng dụng, tên của gói, và biểu tượng có thể đều bắt chước hoặc trùng khớp với ứng dụng thật, vì vậy, không nên chỉ đơn thuần dựa vào các yếu tố này để xác định xem thiết bị có bị nhiễm phần mềm độc hại hay không.

Tên ứng dụng	Tên của gói	Biểu tượng ứng dụng
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 (Khám phá địa hình)	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (Khám phá địa hình)	psyberia.alpinequest.full	

AlpineQuest Off- Road Explorer (Khám phá địa hình) (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard (Bàn phím tiếng Ả Rập)	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter (Cắt video & âm thanh)	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1) (Bài Hát Phật Giáo)	com.bigkidsapps.buddhistsongs1	
Calculator (Máy tính)	com.android2.calculator3	
Compass (La bàn) 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

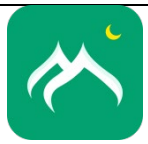
FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager + (Quản lý tập hồ sơ)	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	

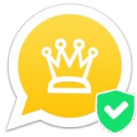
KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker (Máy cắt MP3 & Tạo nhạc chuông)	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator (Máy tính khoảng cách trên bản đồ)	com.routemap.mapdownload.gpsroute planner	
Media Recovery (Phục hồi phương tiện)	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 (Lập trình đọc PDF)	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader (Lập trình đọc PDF)	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor (Lập trình chỉnh sửa hình ảnh)	com.iudesk.android.photo.editor	
Photo Recovery (Phục hồi hình ảnh)	recover.restore.undelete.photo.video.file	
Không gian Chụp Hình ảnh (Photo Studio)	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Sách Kinh (Prayer Book)	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran (Kinh Koran)	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics (Khôi phục hình ảnh đã xóa)	com.restore.deleted.pictures.video	

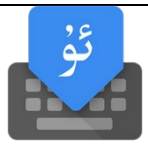
Signal (Tín hiệu)	org.thoughtcrime.securesms	
Signal (Tín hiệu) Plus	org.thoughtcrime.securesmsplus	
SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
Bàn phím SwiftKey	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 (Lời nguyện tiếng Tây Tạng)	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 (Lập trình chuyển đổi video)	com.inverseai.video_converter	
Video Cutter (Lập trình cắt video)	com.naing.cutter	

Video Downloader (Lập trình tải video)	downloader.video.download.free	
Video Maker (Lập trình tạo video)	com.bstech.slideshow.videomaker	
Video Player for Android (Lập trình phát video cho 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 (Dự báo thời tiết)	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 (Lập trình tải xuống YouTube)	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	

Tham khảo thêm

Hướng dẫn của Trung tâm An ninh Mạng Úc

- Report a cybercrime, incident or vulnerability(Trình báo tội phạm mạng, các vấn đề hoặc lỗ hổng bảo mật)
- How to secure your devices (Bảo vệ thiết bị của quý vị)
- Secure your mobile phone (Bảo mật điện thoại di động của quý
- Phishing(Lừa đảo qua mạng, email hoặc tin nhắn)
- Scams (Các hình thức lừa đảo)
- Secure your social media(Bảo mật mạng xã hội của quý vị)
- Security tips for social media and messaging apps(Mẹo bảo mật cho mạng xã hội và ứng dụng nhắn tin)

Hướng dẫn của Trung tâm An ninh Mạng Quốc gia (NCSC) và Cơ quan An ninh Hạ tầng Quốc gia (NPSA) Vương quốc Anh

- Defending Democracy (Bảo vệ nền dân chủ)
- Social Media: how to use it safely (Mạng xã hội: cách sử dụng an toàn)
- Device Security Guidance for organisations including mobile (Hướng dẫn bảo mật thiết bị cho các tổ chức, bao gồm cả thiết bị di động)
- Threat report on application stores. (Trình báo mối đe dọa liên quan đến các cửa hàng ứng dụng)
- Personal safety and security for high-risk individuals (An toàn và bảo mật cá nhân cho những người có nguy cơ cao)

Hướng dẫn của Cơ quan An ninh Quốc gia Hoa Kỳ (NSA)

- Mobile Device Best Practices (Thực hành Tốt Nhất cho Thiết bị Di động)

Tuyên bố miễn trừ trách nhiệm

Xin lưu ý rằng bản khuyến cáo này cung cấp thông tin đã được xác thực tại thời điểm đăng tải.

Phúc trình này dựa trên thông tin thu thập từ các cơ quan soạn thảo và các nguồn trong ngành. Tất cả những phát hiện và khuyến nghị đưa ra không nhằm mục đích loại bỏ hoàn toàn mọi rủi ro, và việc tuân theo các khuyến nghị này cũng không bảo đảm sẽ loại bỏ được tất cả các rủi ro đó. Việc chịu trách nhiệm về các rủi ro thông tin, vào mọi lúc, luôn thuộc về chủ sở hữu hệ thống có liên quan.

Tại Vương quốc Anh, thông tin này được miễn trừ theo Đạo luật Tự do Thông tin năm Năm 2000 (Freedom of Information Act - FOIA) và có thể được miễn trừ theo các quy định pháp luật về thông tin khác của Vương quốc Anh.

Vui lòng gởi mọi thắc mắc về FOIA, tới: ncscinfoleg@ncsc.gov.uk.