Unknown Title

⋮ 9/30/2024

Research

Datzbro: RAT Hiding Behind Senior Travel Scams

30 September 2025

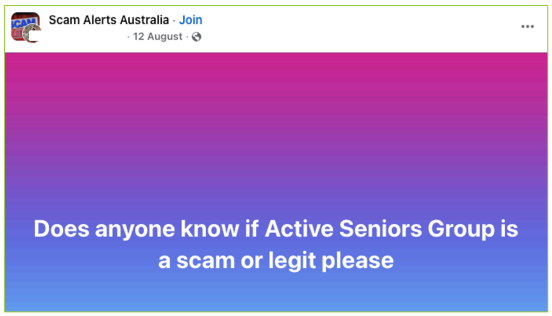
In August 2025, multiple scam alerts were issued in Australia. Users reported scammers managing Facebook groups promoting “active senior trips.” ThreatFabric researchers analyzed the campaign and identified several groups, managed by fraudsters, targeting various regions and using multiple disguises. Moreover, a new Device-Takeover Android Trojan, which we named **“Datzbro”,** was discovered as part of the campaign**.** This report uncovers the capabilities of this Trojan. While most of its features are typically seen in spyware, our research shows how Datzbro is actively used in financial fraud, leveraging its remote access capabilities.

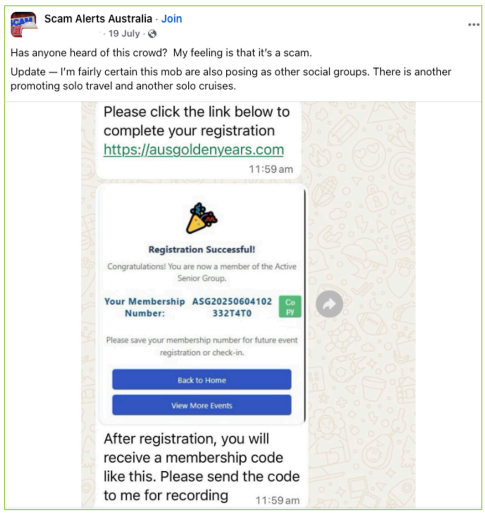
Mobile Threat Intelligence service also identified a leaked Command-and-Control application and builder of Datzbro, making this threat freely available to the threat actors all over the world, turning Datzbro into a global threat.

Targeting Seniors

The campaigns that led to the discovery of Datzbro had a very specific audience: seniors looking for social activities, trips, in-person meetings, and similar events. Multiple users posted online about suspicious Facebook groups promoting “active senior trips,” dance events, and related gatherings.

User's reports online

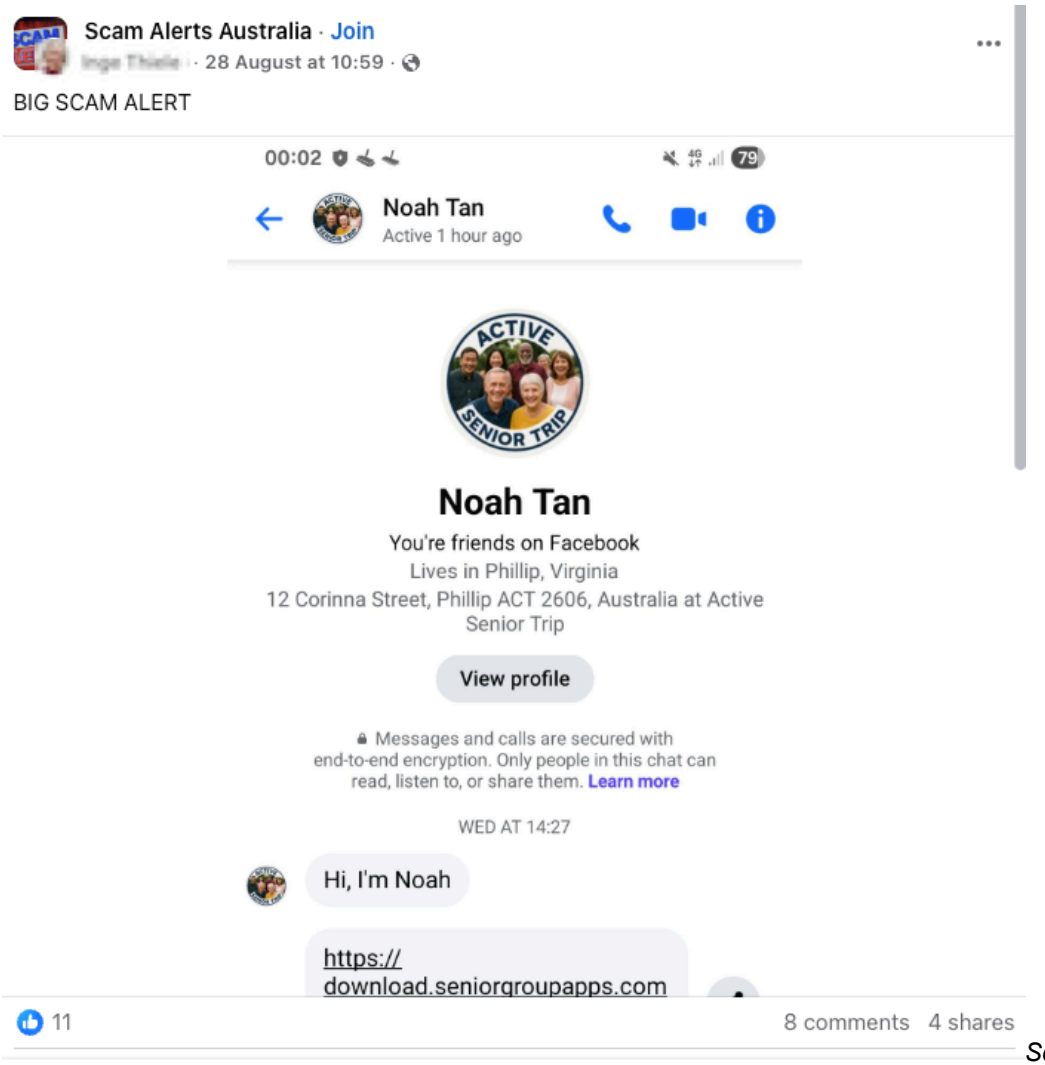




Our research revealed numerous Facebook groups filled with AI-generated content, pretending to organize activities for seniors. We found that not only Australia was targeted, but also users in Singapore, Malaysia, Canada, South Africa, and the UK. The content across these groups looked similar, suggesting they came from the same threat actor. The pictures below show screenshots of groups targeting Australia, Malaysia, and Canada.

Fake Facebook senior's groups

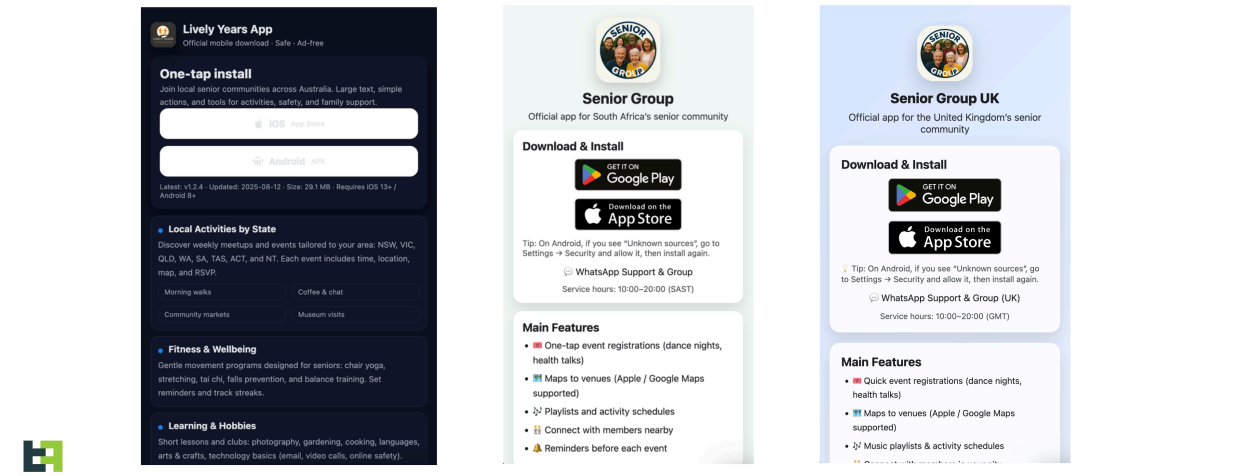
Despite being AI-generated, content in these groups was appealing to the target audience and received multiple responses from people willing to participate. Based on reports from affected users, fraudsters then contacted victims via Messenger or WhatsApp and shared links to download an application to register for the activities. In some cases, victims were also asked to pay a sign-up fee on the same website, leading to phishing and card detail theft.



Scam alert on Facebook sharing messages from fraudster's account

The fake websites prompted visitors to install a so-called community application, claiming it would allow them to register for events, connect with members, and track scheduled activities. These websites usually included a button to download an “iOS application.” At the time of writing, these were only placeholders that did not download anything. However, criminals could later update them to display phishing pages or distribute WebClip/TestFlight apps for iOS, tricking victims into sharing credentials or payment details.

Clicking the “Google Play” button, however, triggered the download of a malicious APK. During our research, we observed cases where Datzbro was directly installed on devices, as well as cases where a dropper bypassing Android 13+ restrictions - namely **Zombinder** - was used.



Clicking the “Google Play” button, however, triggered the download of a malicious APK. During our research, we observed cases where Datzbro was directly installed on devices, as well as cases where a dropper bypassing Android 13+ restrictions - namely Zombinder - was used.

Meet Datzbro

ThreatFabric’s Mobile Threat Intelligence team named this newly discovered Trojan **“Datzbro,”** referencing one of the strings found inside the malware. The analysis revealed a broad set of capabilities with a focus on spyware activity, such as audio recording, camera capture, and access to files and photos. However, its feature set is sufficient to conduct financial fraud through remote control, “black overlay” attacks, and keylogging - making it a significant threat to users worldwide.

Moreover, we discovered Accessibility Logging capabilities with a specific focus on banking and crypto-related applications.

Taking over infected device with remote control

Datzbro is equipped with remote access features that allow it to perform actions on a victim’s behalf, manage files and photos, and capture audio and video.

Like other Android Trojans, it relies on Accessibility Services to perform these remote actions. Each action corresponds to a single gesture or global function (such as simulating Home or Back button clicks). Operators can:

- Start / stop remote screen sharing
- Start / stop remote control (interaction with the interface)
- Enable / disable black overlay with custom text
- Start / stop “schematic” remote control mode
- Lock / unlock screen

"Schematic" remote control mode is a basic representation of the screen layout based on the data from Accessibility events. Sending information about all the elements displayed on the screen, its position and content, Datzbro allows criminals to re-create the layout on their side and effectively control the device if the quality of the screen streaming

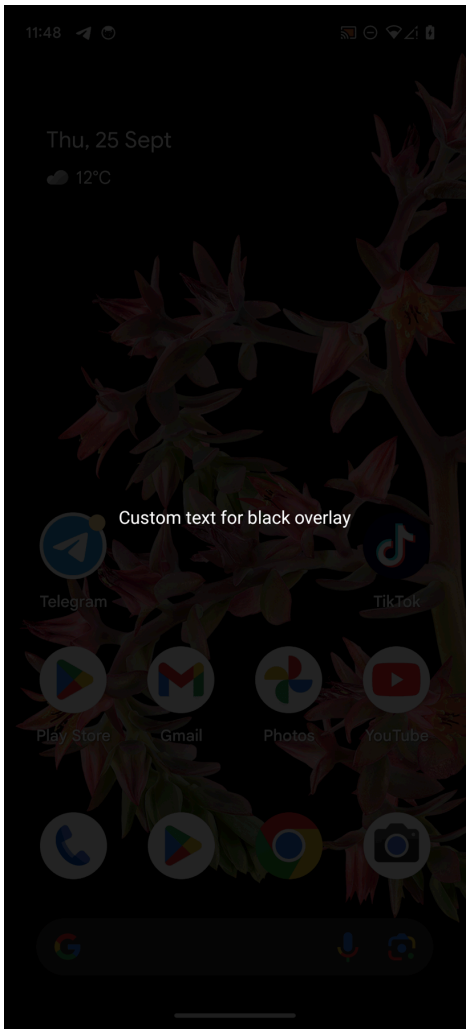
video is not sufficient or "black overlay" is enabled. The operator can interact with the elements, sending the actions to be performed by the malware.

Screenshot of "schematic" remote control mode in Datzbro as seen by operator

Full list of the commands supported by Datzbro is available in Appendix

Hiding fraudulent activity

Black overlay is a current trend amongst the modern malware families; it is also a significant part of the remote-control features provided by Datzbro. This overlay helps operator to hide their activity from a victim.



Semi-transparent overlay with custom text (in actual attack victim sees nothing below the overlay)

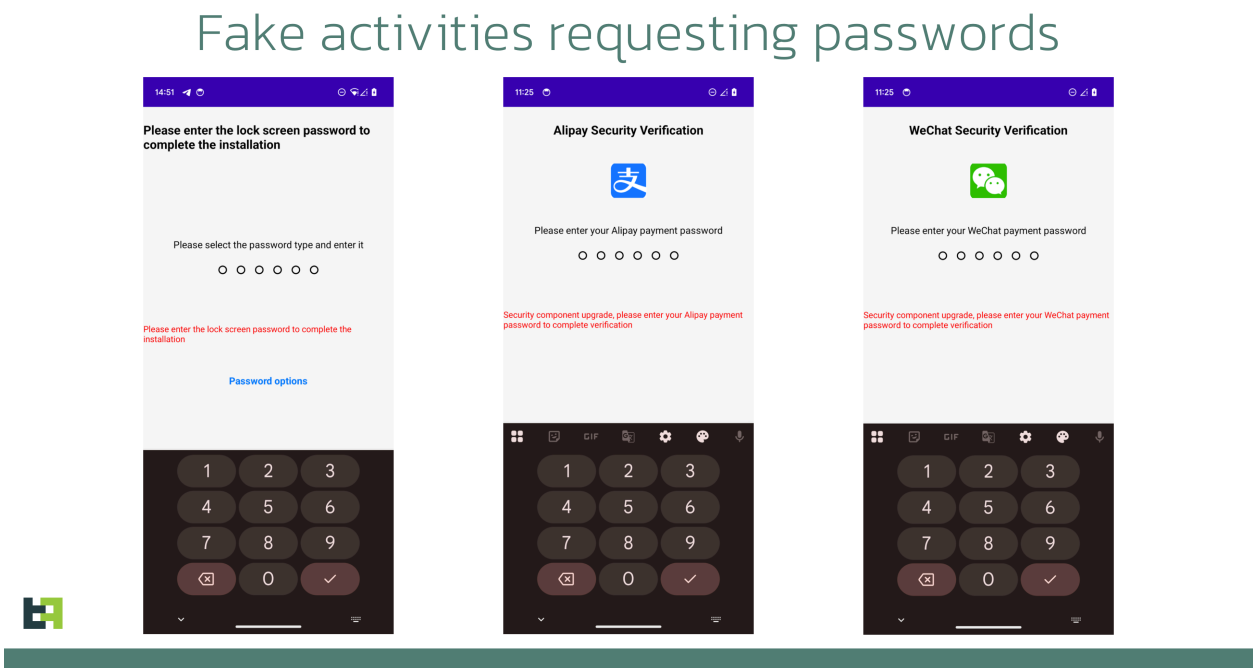
Operators can customize the text displayed in overlay (can be empty string to mimic device being idle) and the level of its transparency for user. However, the overlay remains semi-transparent for operator and allows convenient control of the device. “Schematic” mode is also there to help with device control if the quality of the screen streaming video is not sufficient. Meanwhile, unsuspecting user do not see any signs of fraudulent interaction on the screen.

Targeting banking and payment apps

While Datzbro lacks the full overlay arsenal of classic banking Trojans, it still poses a financial threat. Datzbro steals passwords with the help of special activities, that will be displayed to the victim and request password from a specific service. At the moment of writing the report, hardcoded list of targets include:

- Alipay (com.eg.android.AlipayGphone)
- WeChat (com.tencent.mm)
- Device PIN / pattern / password

When triggered, the activities will request user to enter their PIN codes used to login to the services.



One feature stands apart as it clearly shows the intent of the actors to develop Datzbro as a threat targeting financials of victims, thus making it a Banking Trojan: hardcoded filter for banking- and crypto-related Accessibility events logs. The filter will check if:

- Package name from accessibility event contains any of:
  - "bank"
  - "pay"
  - "alipay"
  - "wechat"
  - "wallet"
  - "finance"
- Text from accessibility event contains any of:
  - "password"
  - "密码验证" ("password" from Chinese)
  - "pin"
  - "验证码" ("verification code" from Chinese)
  - "code"
  - "验证" ("verify" from Chinese)

Such a filter clearly shows the focus of the developers behind Datzbro, not only using its Spyware capabilities, but also turning it into a financial threat. With the help of keylogging capabilities Datzbro can successfully capture login credentials for mobile banking applications entered by unsuspecting victims.

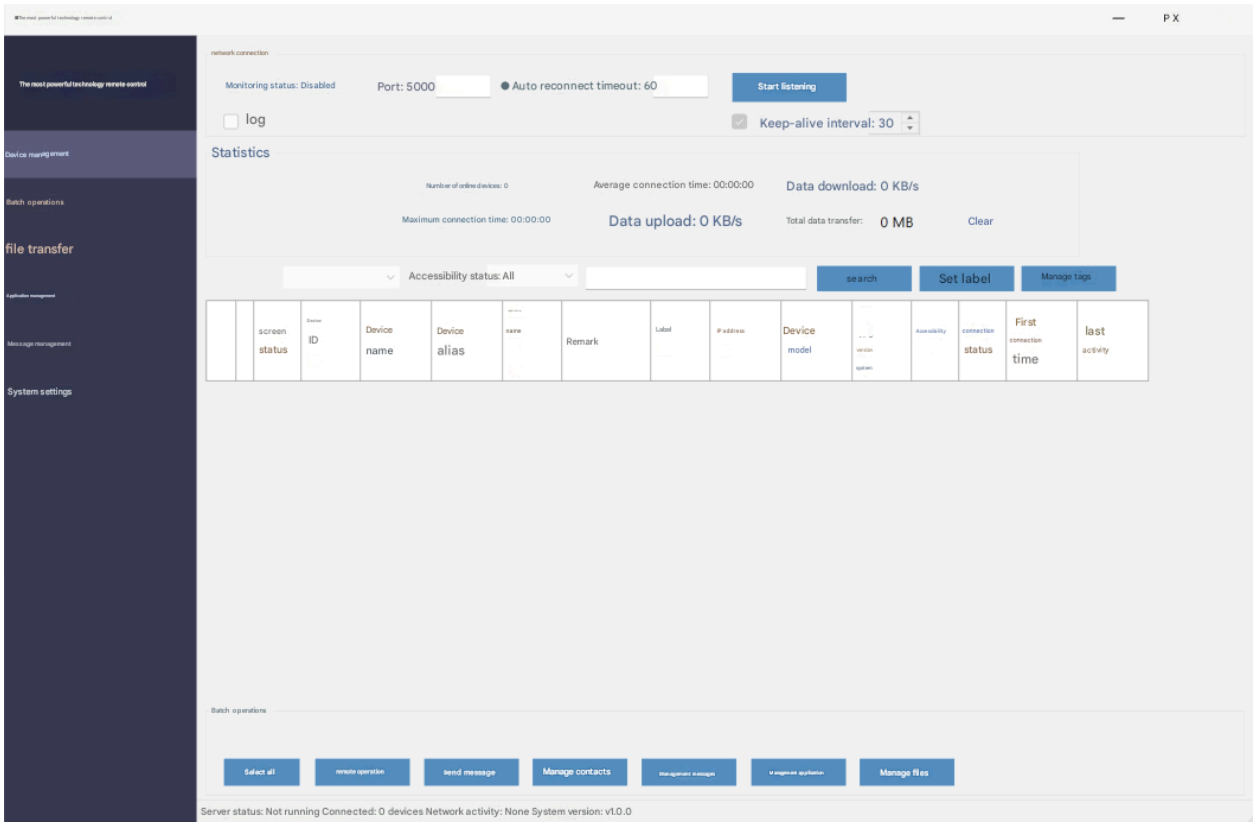
A look behind the curtains

The analysis of the malware source code reveals a lot of debug/logging strings written in Chinese, which reflect the language spoken by the developers of the threat. Mobile Threat Intelligence service also observed samples of Datzbro named "最强远控.apk" which can be translated to "The most powerful remote control" from Chinese, likely a name given by the threat actors to the malware.

Investigation of the backend infrastructure of Datzbro reveals another difference from most of the modern banking Trojans: Datzbro command and control panel is a desktop application, unlike many web-based command and control panels we observe in other malware families.

Further threat hunting allowed our researchers to obtain a compiled version of the C2 app leaked to public virus share. This leads us to a hypothesis that malware was leaked and is distributed freely amongst cybercriminals.

The interface of the C2 application is in Chinese, further supporting the hypothesis of the developers' origin. The following screenshot contains machine-translated version of the Datzbro's C2 application interface:



Monitoring of Datzbro's activity, Mobile Threat Intelligence service also identified other campaigns, run by different threat actor groups,. targeting Chinese-speaking users, showing the background of the threat before it was available to the global actors.

Icon / App name / Package name	Malware family	Malware variant
作 业 帮 (io.mobile.ltool) 26a2044c857777ad5bb0976f6f00dec5d1fe7e1cb779853d2a8976a2682fb7b3	Datzbro	Datzbro.A
麻豆传媒 (fsxhibqhbh.hlyzqkd.aois) 1928ce9c26589a9a8ab5a443319f43b9e99702c37735cae9a6c8b4234c1ae834	Datzbro	Datzbro.A
麻豆传媒 (mobi.audio.aassistant) a1350f977597964ace24e25230604279a05f2f0152e2279224791d7548ca6d96	Datzbro	Datzbro.A
谷歌 浏览器 (tvmhnrvsp.zltlxkpp.mdok) 2016edd6ac78a342c24a2a1fac3c17f667d6a61a08e836744d24d3d8c133cd35	Datzbro	Datzbro.A
MT 管理器 (varuhphk.vadneozj.tltldo) bde3546047014efd5e499ff61dcacfed52fd62a51a098afc0ea03e45eda652e0	Datzbro	Datzbro.A
MT 管理器 (spvojpr.bkkhxobj.twfwf) ab0ba7cb9d5cf091c93a73eebaf09f7b3eba397aa092974d838e6d1c0364c54c	Datzbro	Datzbro.A
大 麦 (mnamrdrefa.edldylo.zish) 800feca44e1136c85fa8af48603bf695a2cf546a8c29fb1f4d0a89e30b942c52	Datzbro	Datzbro.A
MT 管理器 (io.red.studio.tracker) 9a04df247b22ec27e8ff779c127e7493ce525ab629e4c9292b2db6e49d12040e	Datzbro	Datzbro.A

Datzbro samples on Mobile Threat Intelligence portal

Conclusion

The discovery of Datzbro highlights the evolution of mobile threats targeting unsuspecting users through social engineering campaigns. By focusing on seniors, fraudsters exploit trust and community-oriented activities to lure victims into installing malware. What begins as seemingly harmless event promotion on Facebook can escalate into device takeover, credential theft, and financial fraud.

With its spyware functionality, remote access tools, and growing focus on banking apps, Datzbro represents a significant step in the blending of spyware and banking Trojan capabilities. The use of AI-generated content, social platforms, and advanced technical tricks like schematic remote control and black overlays demonstrates the sophistication of today's mobile fraud campaigns.

As criminals continue to refine these tactics, raising awareness among vulnerable communities—especially seniors—remains crucial. Organizations, financial institutions, and individuals must stay vigilant against such schemes, as the boundary between social scams and advanced mobile malware grows increasingly blurred.

Appendix

Bot commands

Commands	Description
1	Enable / disable screen streaming
2	Enable / disable "schematic" mode
3	Perform Accessibility action (gesture, click)
4	Wake up device, unlock it
5	Enable / disable black overlay, set custom text
6	SMS management (list, send, delete SMS, query SMS messages by filter)
7	Applications management (list applications, launch application, uninstall application)
8	Contact list management (add, update, delete contact)
9	File management (read, write, delete, rename files)
10	Get device state / device information
11	Trigger password stealer (fake activities requesting password)
12	Enable / disable Accessibility event processing
13	Start / stop camera capture, switch from front to back camera
14	Start / stop audio recording
15	Update C2 server details
16	Get crash logs
17	Accessibility Logs processing: search, delete records about Accessibility Events
18	Photo Stealer (list albums, upload photos, delete photos)

Indicators of Compromise

SHA-256	Package name	Applica name

a57d70b2873d9a3672eda76733c5b2fb96dca502958064fab742cfc074bf0feb	twzlibwr.rlrkvsdw.bcfwgozi	Senior Group
453b0a62e414e9b40185c63842546fc96e8e1ab3f77d3230b02988dd8834c555	orgLivelyYears.browses646	Lively Ye
ed2313bfebe03ff29a7c802ddd471583cc8da76bf5cb9f418ae7d999d6a0b9fb	com.forest481.security	ActiveSe
fac119c569ba7dd19df9154f22f928cf3f0b0165bbe7d6b11a77215bdfc2a11a	inedpnok.kfxuvnie.mggfqzhl	DanceW