UBINODES

GUIDE:

SID MESSENGER APP

Review: SID Messenger App

Updated 05 January 2024.

SID, a messenger claiming End-to-End encryption, was examined. Results revealed user traffic routed directly to Sid servers in Madrid, disregarding the countries where our consultants conducted tests.

Disclaimer: We have no affiliation with these companies. The information presented in this article is solely based on our independent findings. The provided links are solely for your convenience, and no affiliate marketing is involved.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing criteria:

• Real-time usage on genuine projects.

• Evaluation by diverse team members across various countries.

• Testing on different devices and operating systems.

• Minimum testing duration of two weeks, typically spanning four weeks.

• Peer review by team members precedes the final review sent to the app's publisher.

Contents of this article.

Ever wondered if your encrypted app truly safeguards your data? Recent revelations of tech giants exploiting our data stress the critical need to prioritize our privacy and security, whether for personal or business use.

How can we validate claims of an app's security and authenticity? How do we prevent falling prey to deceptive apps created by malicious actors? We dedicated time to research encrypted apps, rigorously testing them across diverse devices. One such app under scrutiny is SID. Our findings were startling. But before delving into specifics, let's briefly examine the app.

1. What is SID?

SID, a messenger that uses End-to-End encryption, streamlines team communication for simplicity, efficiency, and enhanced security. It offers options for group or individual chats and secure file sharing among team members, prioritizing data protection. Contacts are seamlessly exchanged when new members join the team. Users can create customizable channels for streamlined team communication, adjusting them as needed.

SID's key focus is on security and privacy. The platform is purportedly structured to prioritize these aspects. Their core philosophy emphasizes user-exclusive access to private messages, striving to prevent interception by state-sponsored entities.

Website: http://sid.co/

2. Pros:

• SID is freely accessible.

• Stream encryption in SID is constantly active and cannot be disabled.

• It offers rapid file transfer for large files, particularly beneficial on local networks (Refer to Testing Criteria: peer-to-peer transfer).

• No user's personal information is required within SID (Refer to Testing Criteria: Zero knowledge).

• Suitable for individuals and businesses valuing data security and privacy.

• Compatible with major platforms: iOS, Android, Linux, and desktop (Refer to Testing Criteria: Multiplatform).

• Users can create, customize, and manage multiple chatrooms and groups on SID.

• Exit option available for leaving groups when desired.

• Flexibility to add multiple members to group chats.

• SID uses the bittorrent protocol alongside a central server for offline chat, minimizing risk of a central failure point.

• On installing SID on a new device, users input their ID, then confirm the new device via notification from an active device. No login/password is necessary. Note: Previous conversations won't appear on the new device, but all chat rooms are accessible albeit empty (Refer to Testing Criteria: Sid address).

3. Cons:

• Voice/video chat unavailable.

Documents lack peer-to-peer synchronization and updates. Only you possess access to files sent to you, without the harmonization and synchronization found in tools like Resilio and SyncThing. This drawback is particularly significant for teams, companies, and organizations aiming to securely collaborate on files.

• Absence of an in-app support panel.

• SID's code remains unpublished, rendering it not open source at the time of writing (Refer to Testing Criteria: Open source).

• Specific image sizes required for chat room thumbnails; smaller images won't upload.

• Message syncing across devices isn't immediate; reading a message on one device doesn't instantly reflect on others until the app is reopened.

• No read receipts available to confirm message viewing by recipients.

• Lack of message quoting, hindering coherent conversation tracking.

• Servers based in Madrid, part of the 9 eyes alliance (Refer to Testing Criteria: Resistance to state-sponsored criminals).

• For offline use, encrypted messages stored on servers could potentially be intercepted by state-sponsored entities (Refer to Testing Criteria: Resistance to state-sponsored criminals).

• Deleting messages during chats removes them only from the sender's end, not the receiver's.

• Absence of ephemeral (self-destructing) messages.

• All files sent/received on SID can be accessed from the installation folder, compromising app security if the hard drive isn't encrypted, potentially accessible by state-sponsored entities.

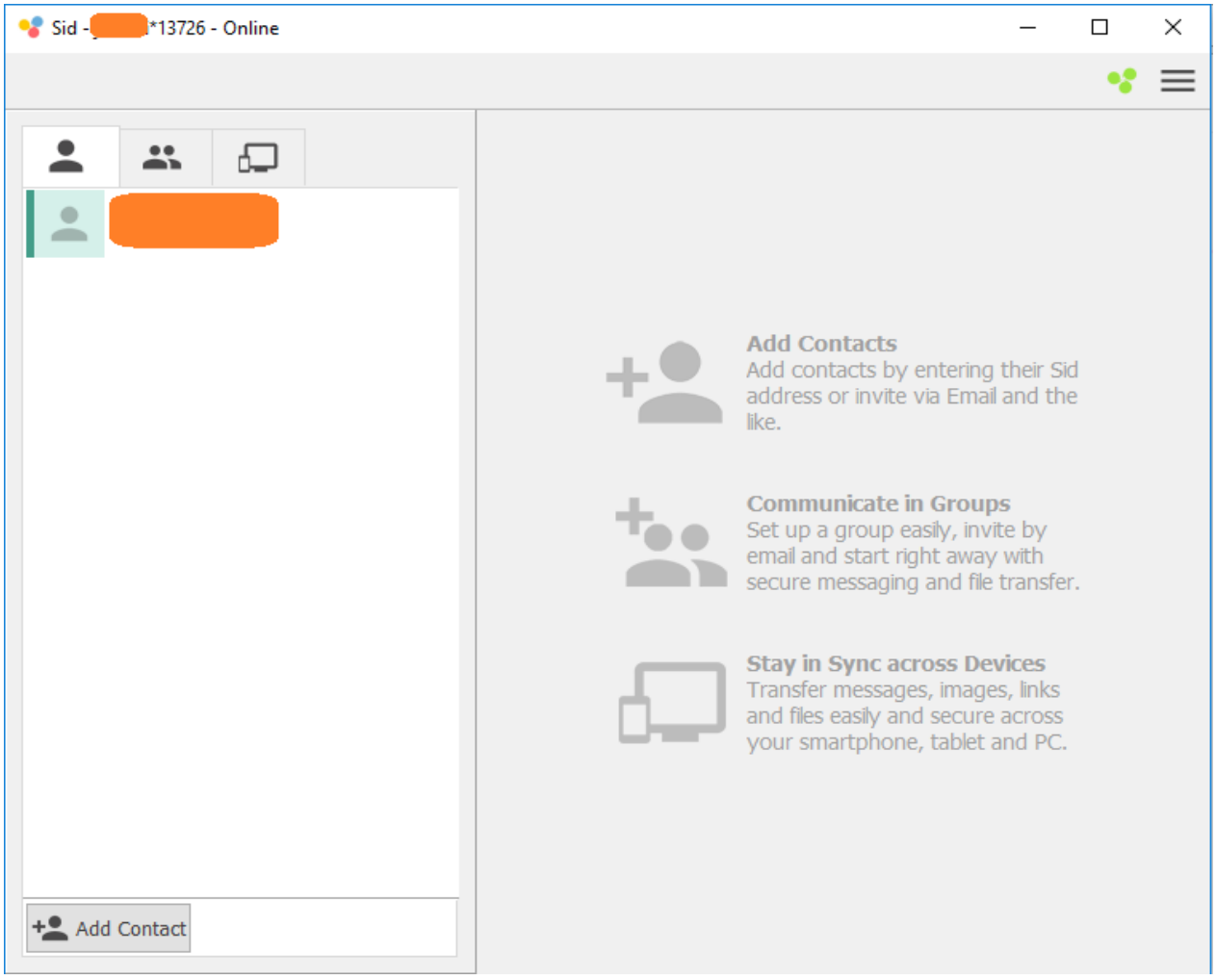
Note: For comprehensive details, refer to the elaborated explanations in the Criteria used for testing section below.

4. Conclusions.

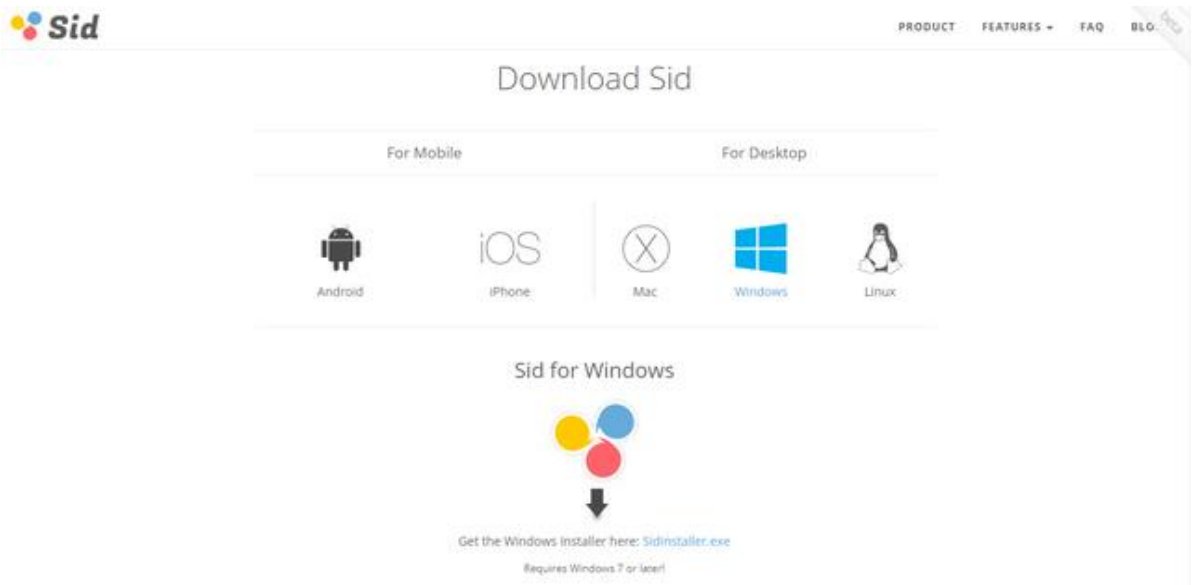
Following comprehensive testing of the Sid app by diverse consultants across various countries using different devices and operating systems, including Wireshark analysis for peer-to-peer encryption verification, our investigation revealed a concerning finding. All user traffic funneled directly to Madrid, where Sid's servers are based, rather than maintaining localized communication among our testing consultants across different countries. This highlights Sid's utilization of a central server, contradicting their claim of not storing user data.

Furthermore, the app's closed-source nature prevents independent verification of their proclaimed end-to-end encryption and zero-knowledge policies. The pivotal issue of Sid's server location in Madrid, a member of the 9 eyes alliance, raises significant privacy concerns. An optimal choice for server location would have been a neutral country with no affiliation to the US or EU. Despite forwarding our article to Sid support for review, as of the publication time, we are yet to receive their feedback.

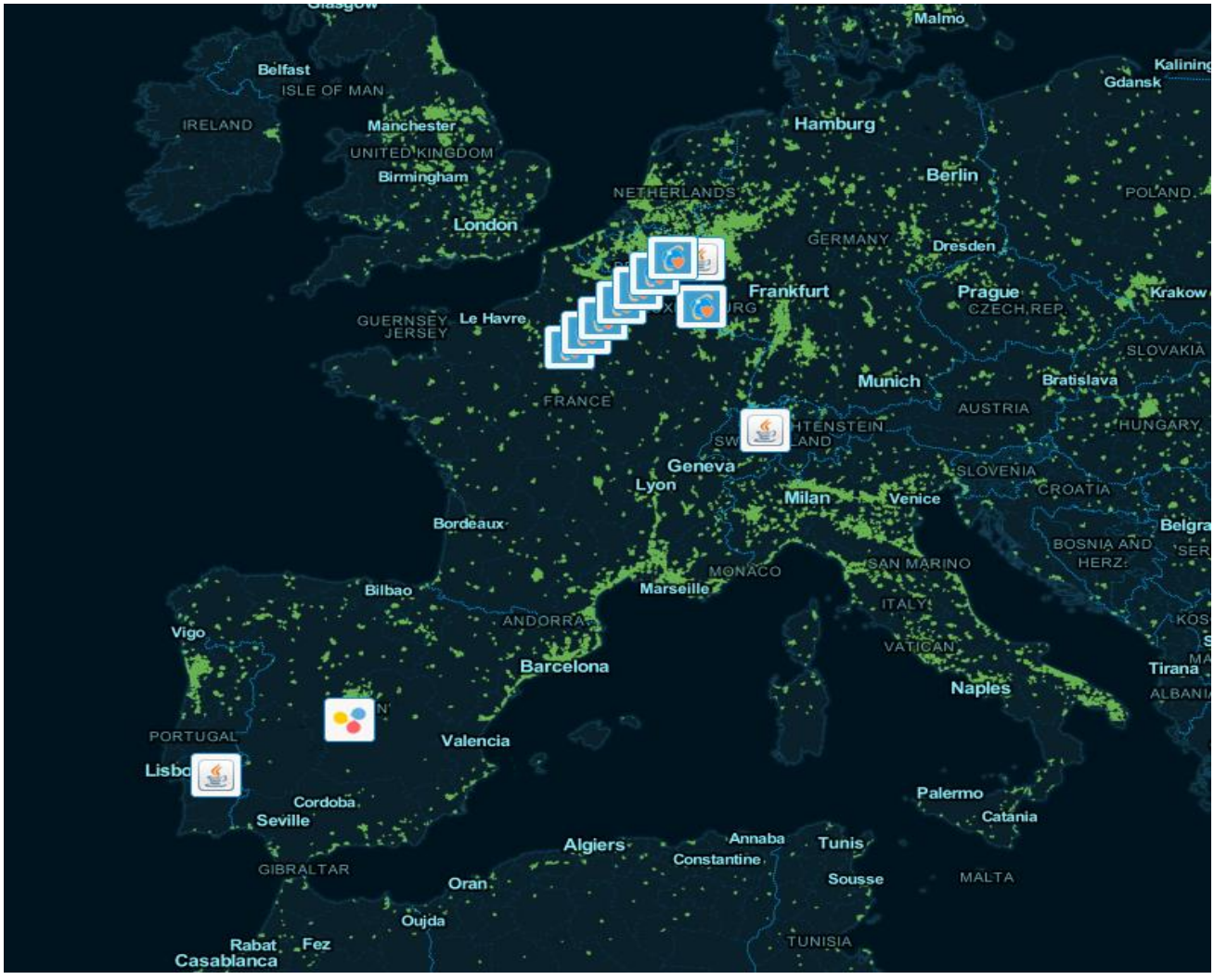
5. Screenshots:



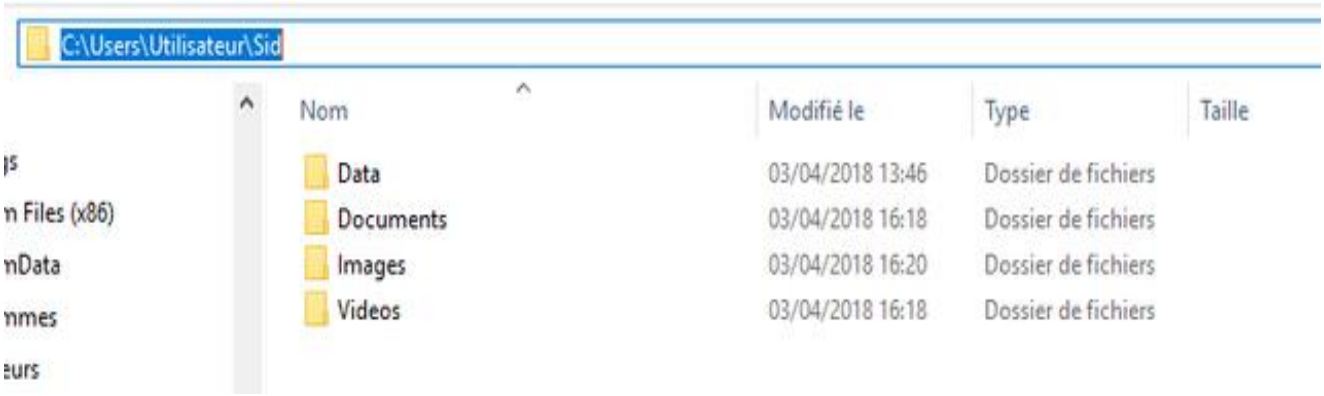
SID app interface



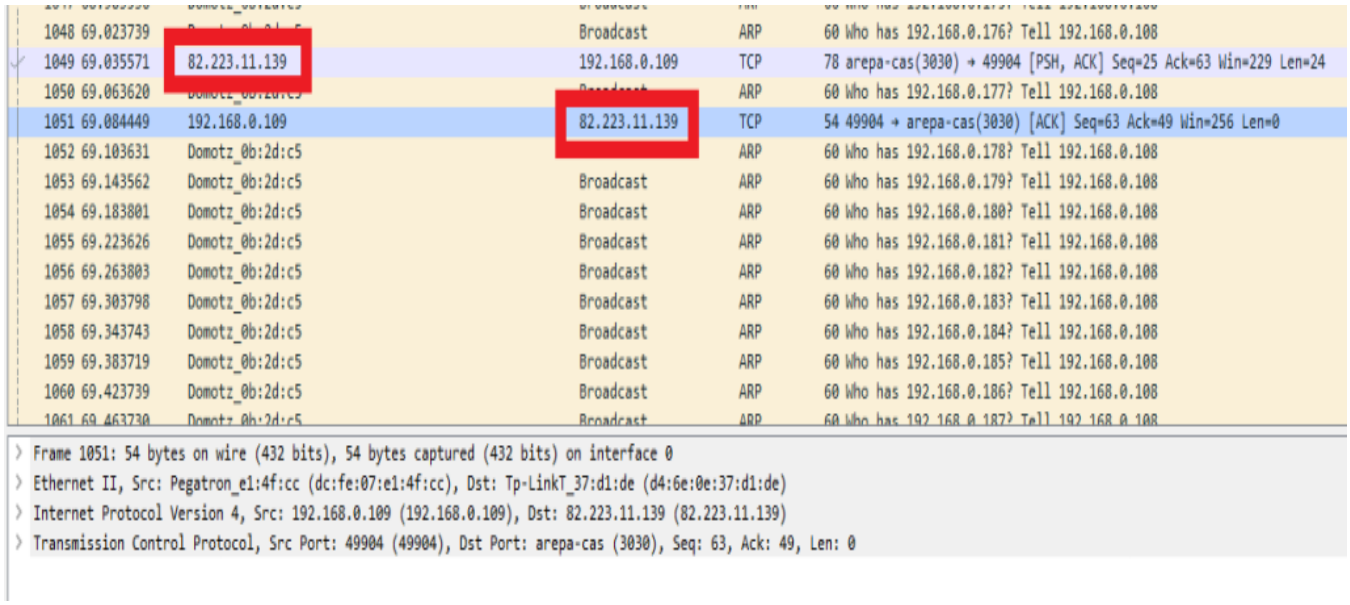
Downloading SID



SID servers in Madrid



Installation folder on PC



Testing SID with WireShark

6. Criteria used for testing.

• **Zero knowledge:** Only the sender and receiver can access their data. When stored on offline servers for backup or offline delivery, data is encrypted, only accessible to individuals holding the decryption keys on their devices. No alteration, reading, or analysis of sent data occurs for any purpose.

• **End-to-End encryption:** SID messenger employs robust encryption, differentiating itself from HTTPS, which secures only the connection between a device and a server. Unlike HTTPS, where data remains visible on the server side, SID encrypts the entire transfer chain, safeguarding data from service providers or cloud system access.

• **Encryption implementation:** SID combats weak number generator issues prevalent in other secure messengers by using its robust random number generators based on Whirlpool512 hash with a 4096-bit entropy pool. Device-generated and stored secret keys authenticate contacts, ensuring secure communication and data integrity without interception.

• **Peer-to-peer file transfer:** SID enables sending files of any size like documents, videos, or photos directly to recipients' devices. In group transfers, all devices act as senders, enhancing network backup availability. Local network file transfers operate swiftly, bypassing internet connectivity issues.

• **SID address:** Sign-up on SID doesn't necessitate personal data like email, phone numbers, or addresses. SID uses its addressing system, using a username appended with an asterisk (*) and a unique 5-digit number. This prevents spam and allows users to maintain preferred usernames while managing contacts.

• **Open source:** At present, SID's source code remains private. Future plans include publishing the source code and technology for auditing and review. Interested parties seeking code review can contact security@sid.co.

• **Multiplatform:** SID is accessible across various platforms, including desktop, Windows, Mac, Linux, iOS, and Android.

• **Resistance to state-sponsored criminals:** These individuals encompass law enforcement, prosecutors, and similar authorities. Their actions are deemed legal due to corruption within state institutions, resulting in a lack of oversight. These criminals pose significant threats to individuals and countries alike, as they can manipulate the legal system to cover up any illicit activities. They possess the capability to intercept and scrutinize IMAP, POP3, TLS, and SSL communications, along with the ability to spoof your email provider's SSL certificate. Access to SMS and emails makes recovery options susceptible to easy attacks. Hence, it is crucial to employ encryption software, secure your devices through encryption, and procure hardware from sources outside the country of operation.

7. Sources.

Download.com. (2018). Sid. [online] Available at: http://download.cnet.com/Sid/3000-2654_4-76641095.html [Accessed 28 Mar. 2018].

Sid. (2018). Sid | End-to-End Secure Team Communication. [online] Available at: https://sid.co/en/security-by-design [Accessed 28 Mar. 2018].