Telegram anonymity fails in desktop

Telegram anonymity fails in desktop - Dhiraj Mishra, inputzero.io.

- Published: date not stated
- Original: <https://www.inputzero.io/2018/09/bug-bounty-telegram-cve-2018-17780.html>
- Preserved from: https://www.inputzero.io/2018/09/bug-bounty-telegram-cve-2018-17780.html (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Hi Internet,

Summary: Strangely tdesktop 1.3.14 and Telegram for windows (3.3.0.0 WP8.1) leaks end user private and public IP address while making calls. This bug was awarded €2000 by Telegram security team. (Sweeet..)

|

| | | Img Src: https://telegram.org/img/tl_card_synchronize.gif | |

Telegram is supposedly a secure messaging application, but it forces clients to only use P2P connection while initiating a call, however this setting can also be changed from "Settings **>** Privacy and security **>** Calls **>** peer-to-peer" to other available options. The tdesktop and telegram for windows breaks this trust by leaking public/private IP address of end user and there was no such option available yet for setting "P2P **>** nobody" in tdesktop and telegram for windows.

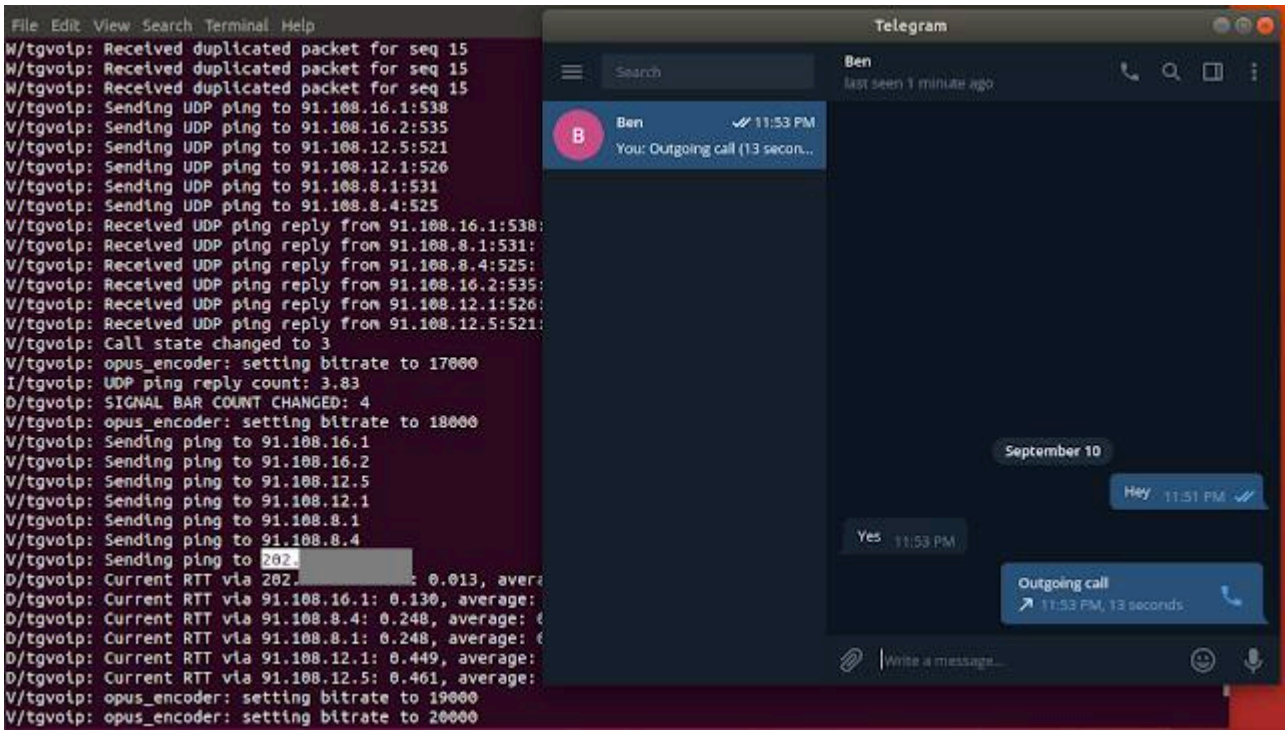
PS: Even telegram for android will also leak your IP address if you have not set "Settings **>** Privacy and security **>** Calls **>** peer-to-peer **>** nobody" (But Peer-to-Peer settings for call option already exists in telegram for android).

To view this in action in tdesktop:

1. Open tdesktop,

1. Initiate a call to anyone,

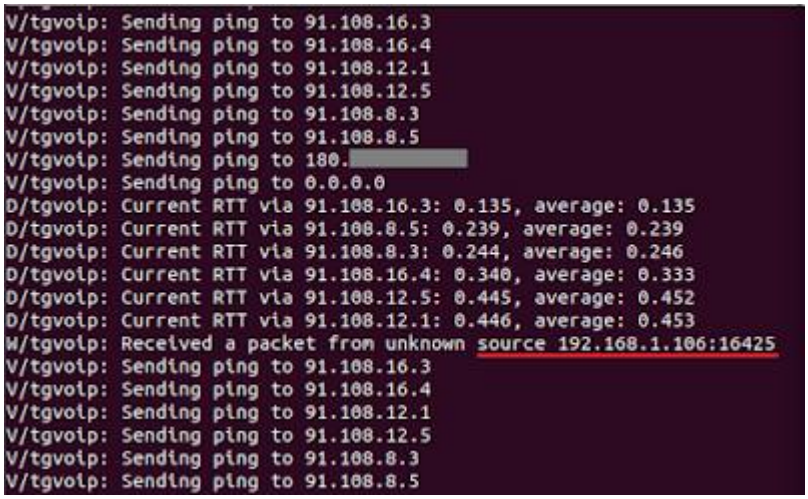
1. You will notice the end user IP address is leaking.



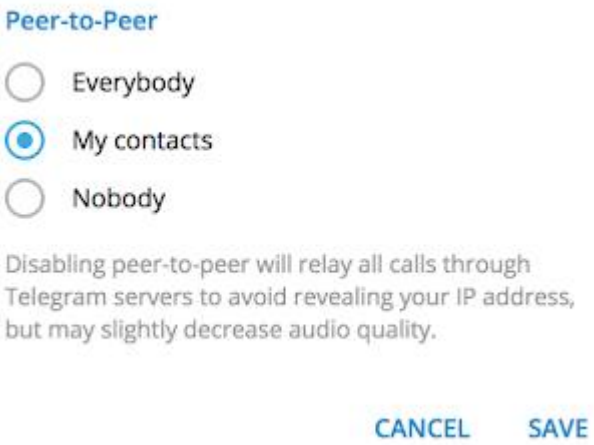
Other scenario:**

1. Open tdesktop in Ubuntu and login with user A

1. Open telegram in windows phone login with user B
2. Let user B initiate the call to user A
3. While user A access log will have public/private IP address of user B.



Not only the MTProto Mobile Protocol fails here in covering the IP address, rather such information can also be used for OSINT. This issue was fixed in 1.3.17 beta and v1.4.0 which have an option of setting your "P2P to Nobody/My contacts", Later CVE-2018-17780 was assign to this vulnerability.



Regards

Dhiraj
