

Forum:[Hack Forums](#)

Thread: [Ultimate Doxing - Ep. 4 - Doxing by 2G/3G/4G Ip's](#)

?Criminal - January 17, 2016, 7:41 pm

So alot of people think phone tower ips are undoxable cause there shared well im here to kill off that misconception:

"On or about August 5, 2015 Verizon Wireless provided telephone numbers accessed by IP addresses #2 through #9 at the specific dates and times accessed by twitter account #1. The common telephone number that accessed IP addresses #2 through #9 was [CENSORED NUMBER]."

"Twitter provided IP addresses #2 through #9 were identified as verizon wireless."

After reading a criminal complaint recently I noticed LE is able to get whats known as the common telephone number that was assigned that specific verizion wireless phone tower IP address using breadcrumb timestamps(down to the nanosecond usually) and exact dates. As a social engineer you can take advantage of this by calling a specific phone carriers network department that handles these searches and social the info, theres many pretexts you can come up with and use but the most common one is the employee one just as it is in normal ISP doxing. Chances are PI's out in the field already obtain info from phone tower ips's although its not a very common method of obtaining info. Once you get the common phone number from the phone tower IP you can call the normal phone carriers customer support line and social info on the cell number normally. This also includes 4G dongles you can get any info tied to one of those as well. I would make it more indepth but this tutorial is spoonfed free and I condone people figuring stuff out on their own to get better at it. I hope you guys enjoyed this quick write up.

minimalist - January 17, 2016, 7:43 pm

Nobody serious about what they're doing should be doing anything that leads back to their online persona over a cellular network to begin with.

sinmar - January 18, 2016, 1:21 pm

should be pretty obvious to anyone who isn't retarded, but afaik most regular CSR's for carriers can't lookup tower information. if you can't make a fake subpoena you can try to S.E. via the normal employee pretext by calling the legal dept. or the NOC.

Linux™ - January 20, 2016, 8:01 pm

The fun thing is E911 systems come in handy for general mobile devices, but you're right using a phone doesn't hide someone. However some people could still use falsified registrant information on prepaid devices. IE

AT&T smartphones have a hotspot function, someone can register a gophone account without an SSN, so it really doesn't matter, but the E911 service can't be disabled without a rooted/jailbroken device/phone, and runs on GPS.

If they can manage this, then I'd say they're somewhat solid.

Good tutorial.

sinmar - January 22, 2016, 6:08 pm

(Jan 20, 2016 09:01 PM)Linux™ Wrote: [\[CITE\]](#) The fun thing is E911 systems come in handy for general mobile devices, but you're right using a phone doesn't hide someone. However some people could still use falsified registrant information on prepaid devices. IE

AT&T smartphones have a hotspot function, someone can register a gophone account without an SSN, so it really doesn't matter, but the E911 service can't be disabled without a rooted/jailbroken device/phone, and runs on GPS.

If they can manage this, then I'd say they're somewhat solid.

Good tutorial.

what do E911 functions have anything to do with mobile connections / doxing them