Practical Exploitation of the VPN 'PortFail' IP Leak against Torrent Users.

Nov 26, 2015

Today there was a critical vulnerability in various VPN providers disclosed by the Perfect Privacy VPN's security team. This vulnerability can lead to "unmasking" or "decloaking" of VPN users under certain conditions, and after some analysis of how it works, I determined that this issue is of utmost importance to those who use VPN services to mask their bittorrent traffic from MAFIAA scum, as it can allow for 'uncloaking' of Bittorrent users quite readily.

In the spirit of openness, and now that the bugs details are public, I have decided to outline an example attack which would allow for someone to decloak Torrent users hiding behind vulnerable VPN's. While I am not providing some automated deanonymizing toolkit for getting the job done, the instructions below should suffice for someone else to reproduce the attack and demonstrate its effectiveness in deanonymizing users.

How to be evil:

1. Sell your soul to the devil and become the kind of wanker who wants to help sue bittorrent users.
2. Bulk register accounts on VPN's that have been found to be vulnerable to this attack.
3. For torrents of interest, become a peer in the peer swarm, to gather IP's that are "protected" by VPN's.
4. Match IP's of peers in the swarm against a list of known-vulnerable VPN exit IP's.
5. Spin up a VPN connection using the same exit server as the client(s) you wish to "uncloak".
6. Port forward torrent port using the VPN and then join the peer swarm. You want to look like a good peer. Perhaps even deny non-interesting peers access, or whatever method you need to do to be attractive to your victim(s) of interest.
7. When the peers of interest connect to you, they will reveal their real IP address.

8. Summon your evil lawyer subpeona teams, and take a good, hefty dose of whatever it is that kills your conscience enough to permit you to work for evil copyright scum.

As you can see, this attack is well within the capabilities of almost anyone - no nation state capabilities needed. You would simply need to have the budget to buy accounts on multiple VPN services (to identify vulnerable ones, and also for the deanonymizing step), a list of torrents that were of interest to you (i.e. ones that you are 'protecting' the copyright of, or some such bullshit. You could just use the top 100 on any given day if you were just generally being a bastard though), a computer, and a minimal amount of technical knowledge.

I believe this kind of attack is probably going to be used heavily by copyright-litigation firms trying to prosecute Torrent users in the future, so it is probably best to double check that the VPN provider you are using does not suffer this vulnerability. If they do, notify them, and make sure they fix it.

0x27 Finger Discount

0x27 Finger Discount

0x27
info_dox

The adventures and exploits of a student/developer as they explore wonderous new lands of unsanitized inputs, programming languages, and Computer Science 3.