BitTorrent vulnerability to DRDoS attacks uncovered

August 18 2015, by Bob Yirka

Credit: Wikipedia

A quartet of researchers, two with City University of London and one each with PLUMgrid Inc. and THM Friedberg has released a paper first shown at the recent USENIX Woot '15, detailing what they claim is a major vulnerability of the BitTorrent protocol. The problem is that it opens up BitTorrent hosts to distributed reflective denial of service (DRDoS) attacks—by as few as one single perpetuator. Such attacks are becoming a bigger problem as BitTorrent communities have grown in size over the past several years—they now number in the millions.

BitTorrent, as most are aware, is a protocol under which a user community can share files among themselves. As part of the protocol, traffic among the people working together to share files and a host is monitored—like a traffic cop—otherwise, bottlenecks would occur, or worse, those with a bigger pipe would hog all the bandwidth preventing those with lower bandwidth from obtaining any files. Now, imagine if someone were to go in and mess with the traffic cop in such a way as to flag all traffic to flow at once, and to send a signal for some to actually send more requests than they actually need—the host would be overwhelmed and no one could get anywhere. That is the basis of DRDoS attacks. Perpetuators do not have to enlist large groups or collections of computers, instead, a single person can direct the host's own software to invite in so much traffic that the whole user community becomes bogged down and useless to anyone.

The authors of the paper claim that the vulnerability actually exists in uTP, DHT and Message Stream Encryption, in addition to BitTorrent Sync protocols. All that was needed to test the vulnerability on real systems, they write, was a valid info-hash, noting that pinging one message was enough to boost traffic by up to 120 percent.

The group also offers suggestions on how to prevent such an attack from occurring, the first is for internet providers to work together to come up with a scheme to prevent IP spoofing. The second is for a defense

mechanism to be added to the BitTorrent protocol, similar to that used for TCP—where a three-way handshaking protocol would prevent such attacks from working.

More information: P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks, PDF.

© 2015 Tech Xplore

Citation: BitTorrent vulnerability to DRDoS attacks uncovered (2015, August 18) retrieved 19 April 2024 from
https://techxplore.com/news/2015-08-bittorrent-vulnerability-drdos-uncovered.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.