OK, more on the nature of the 9/25-9/26 attack...

Much larger than the 10/09 attack, this appears to have also been going after the entire corpus, spawning sessions beginning with a particular DOI, and instructing the session to download articles sequentially. When a particular session fails, a new one is spawned at the # where the previous one died. The order in which journals were targeted was haphazard, but sessions follow the same pattern - beginning with a DOI, and increment it by 1, ad infinitum, until failure.

As there were 1.2MM sessions, with only ('only') 451K downloads, the session failure rate was obviously fairly high, which is likely a by-product of: 1) our abuse controls; and, b) gaps in the number sequence in our DOI list (i.e., the bot hits the next number in a sequence, but we have no article with that DOI).

Still working on a title-history roll-up version of the listing in the spreadsheet.

> Quantify MIT Abuse Cases
>  -------------------------
>  
>  Key: OPS-1843
>  URL: http://
>  Project: Operations
>  Issue Type: Task
>  Reporter: 
>  Assignee: 
>  Priority: Urgent
>  Attachments: mit_abuse_details.xlsx
>  
>  is requesting a summary of both recent MIT abuse incidents to include...
>  Start / Stop times
>  # of articles downloaded
>  IPs of origin
>  affects on servers
> ...any other relevant information as needed.

--
This message is automatically generated by JIRA.

- If you think it was sent incorrectly contact one of the administrators: 
  http://

- For more information on JIRA, see: http://www.atlassian.com/software/jira