The following were the steps I took in order to find the user affected:

1. With a given botnet alert notices folder, paths of alert notices were retrieved.
2. These notices had post NAT IP & Port of the user that visited malicious website. Since these notices had data in an XML format, XML parser was used to retrieve data.
3. In order to find the pre NAT IP and Port, a class NATAnalyser which has an interface to scan through NAT logs using zgrep command was created.
4. NATAnalyser would give us the pre NAT IP, Port, and the range of time of interest.
5. Information from (4), was fed to DHCPAnalyser which is a class that has an interface to scan through logs\_db (a MySQL DB) that has dhcp table which provided macaddress corresponding to pre NAT IP in the given time range.
6. MACAnalyser class was created to read radacct and contactinfo tables in logs\_db, to get infected username. In order to provide that username, IP address and MAC address were given as input.
7. If IP address provided to MACAnalyser was in the subnet ‘172.19.\*.\*’, then radacct table was scanned to get the username. If it was not in that subnet, contactinfo table was searched.