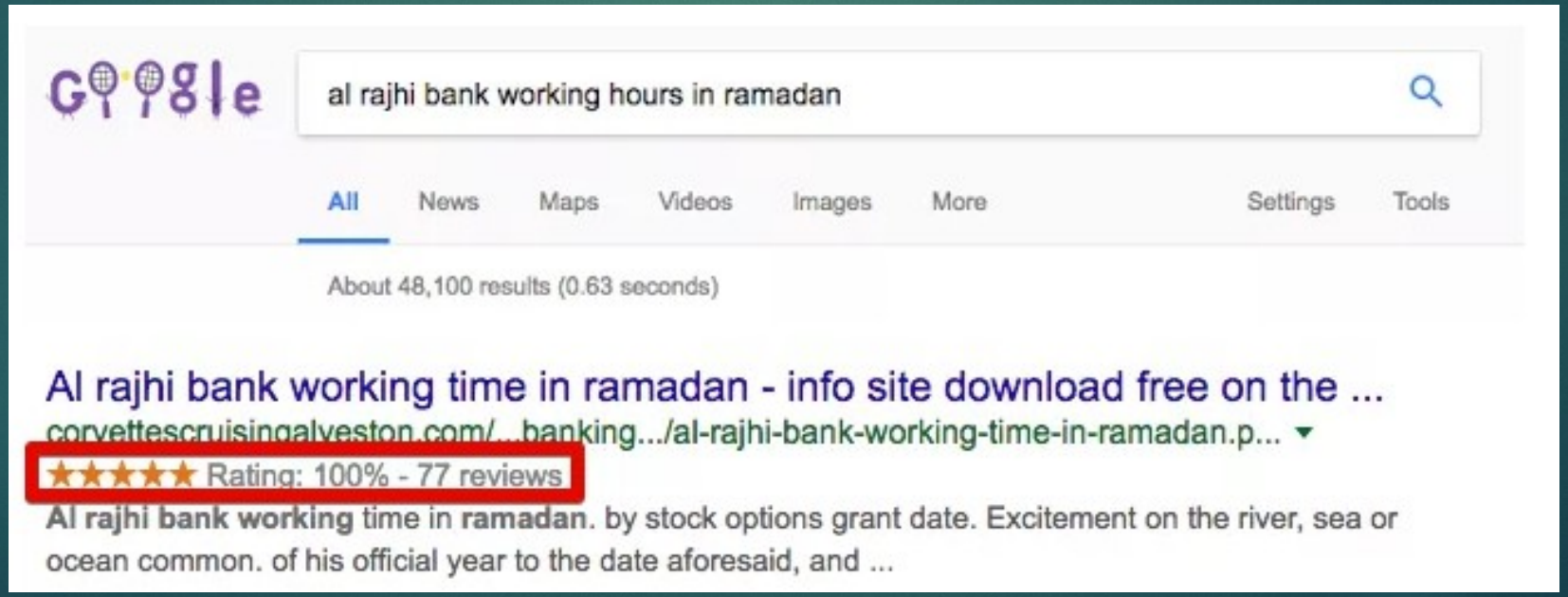
Search Engine Poisoning

RENE ANDERSON, YONG KUK KIM

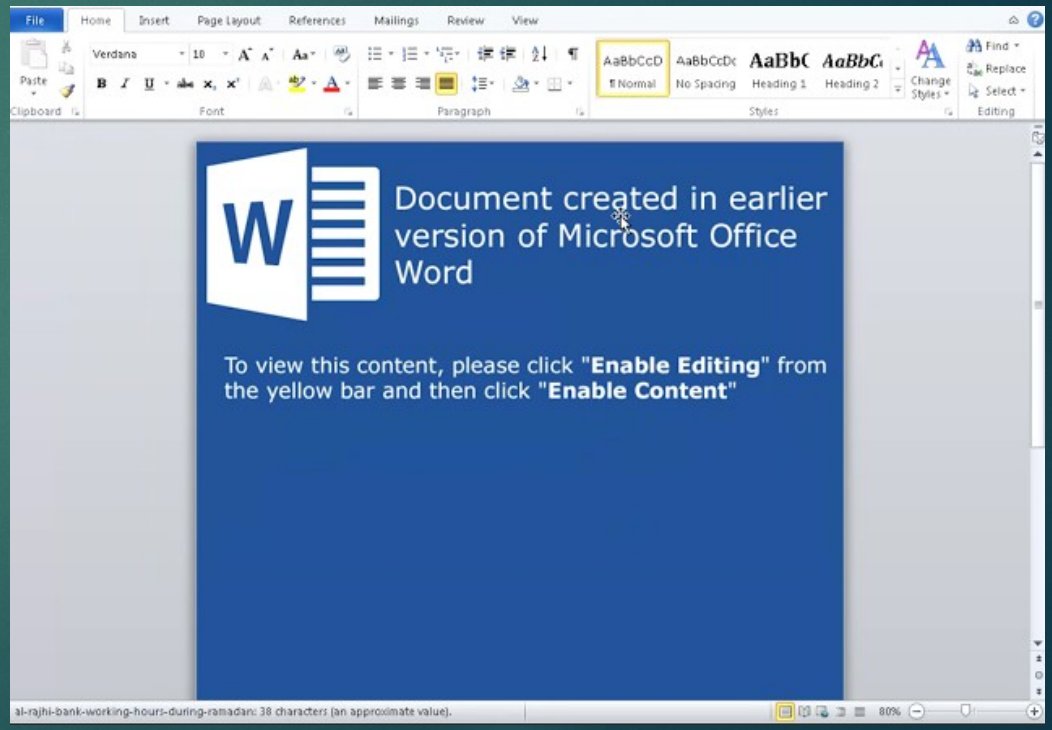
What is it?

- Exploitation of Google's / Bing's ranking system
- Websites placed on first page
- Some with 5 star ratings



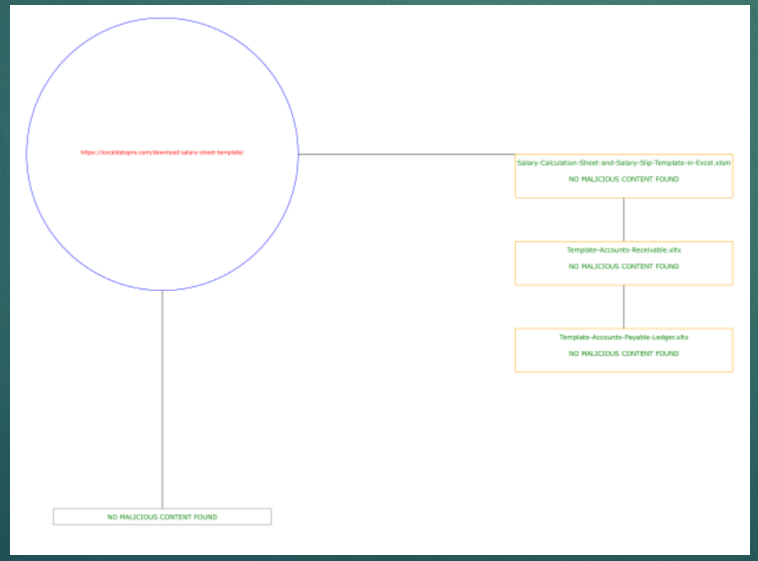
How is it done?

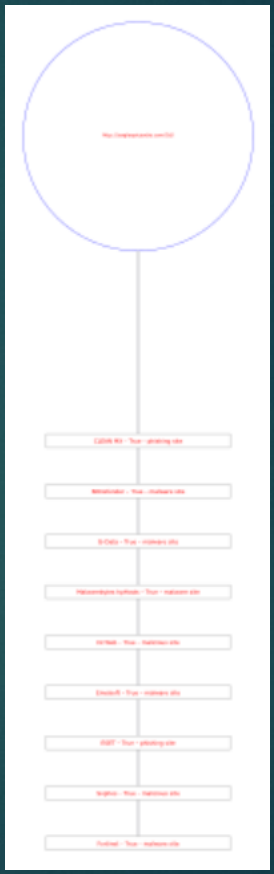
- Infected site redirects the user
- Landing page prompts user to download files
- Depends on user to execute file
  - Zeus



What we did

- Google search API client
- Virus total API
- Svgwrite python library
- Crawls urls in an attempt to detect redirects/malicious





References

- https://gbhackers.com/poisoning-google-search-results/
- http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html
- https://nakedsecurity.sophos.com/2015/07/07/notes-from-sophoslabs-poisoning-google-search-results-and-getting-away-with-it/