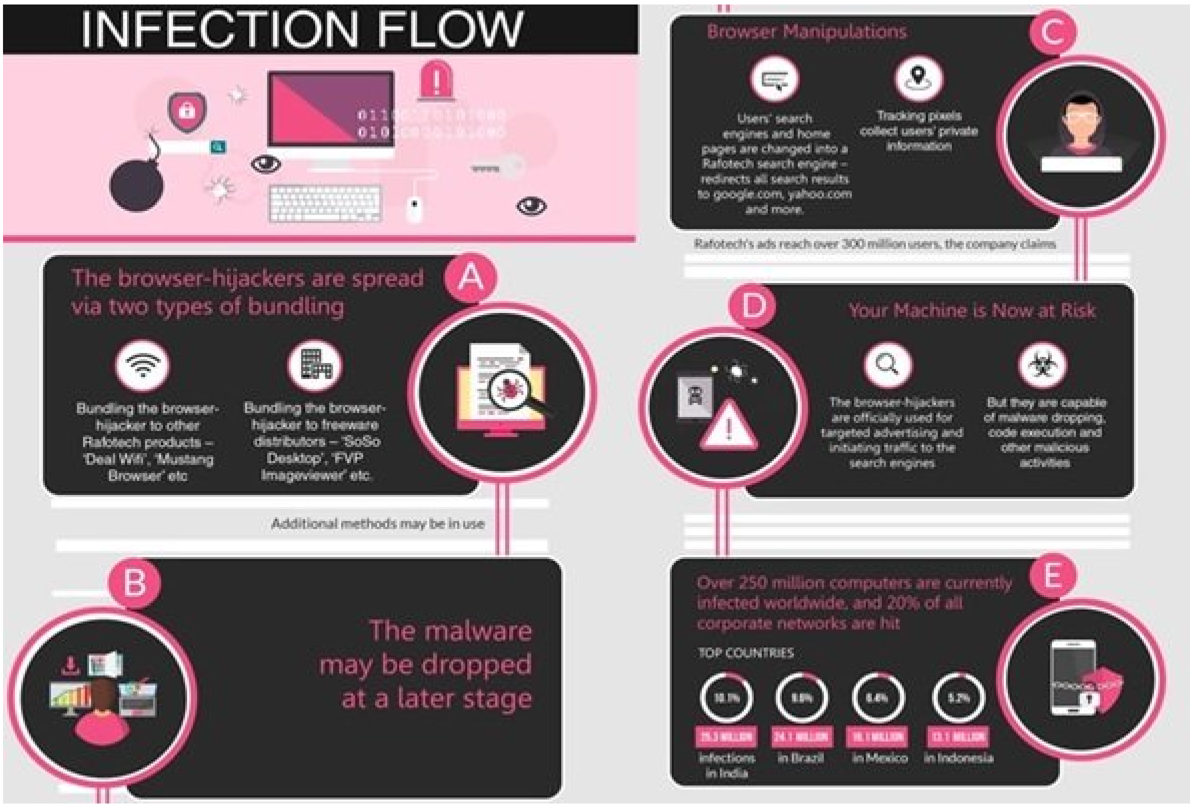
[illegible]


INFECTION FLOW
Browser Manipulations
C
Users' search engines and home pages are changed into a Rafotech search engine – redirects all search results to google.com, yahoo.com and more.
Tracking pixels collect users' private information
Rafotech's ads reach over 300 million users, the company claims
The browser-hijackers are spread via two types of bundling
A
Bundling the browser-hijacker to other Rafotech products – 'Deal Wifi', 'Mustang Browser' etc
Bundling the browser-hijacker to freeware distributors – 'SoSo Desktop', 'FVP Imageviewer' etc.
Additional methods may be in use
D
Your Machine is Now at Risk
The browser-hijackers are officially used for targeted advertising and initiating traffic to the search engines
But they are capable of malware dropping, code execution and other malicious activities
B
The malware may be dropped at a later stage
E
Over 250 million computers are currently infected worldwide, and 20% of all corporate networks are hit
TOP COUNTRIES
10.1%
9.6%
8.4%
5.2%
25.3 MILLION infections in India
24.1 MILLION in Brazil
16.1 MILLION in Mexico
13.1 MILLION in Indonesia

[illegible] Fireball [illegible] 250 [illegible] 5 [illegible] Fireball [illegible].

[illegible] Fireball [illegible] fireball [illegible] (Home Page) [illegible].

[illegible] 250 [illegible] 5.5 [illegible] fireball [illegible] 20 [illegible].

[illegible] fireball [illegible] (sandbox) [illegible].

[illegible].

[illegible]:

[illegible]

[illegible]:

[illegible]

[illegible]:

09:50 - 13/01/1398

[illegible]:

[illegible] - [illegible] - [illegible] - [illegible] - Fireball

---

[illegible]

[illegible]: https://www.shabakeh-mag.com/security/14191/%D8%B3%D8%B1%D9%82%D8%AA-%D9%86%D8%B4%D8%B3%D8%AA%E2%80%8C%D9%87%D8%A7-%D9%88-%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%D9%85%D8%B1%D9%88%D8%B1%DA%AF%D8%B1-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%AF%D8%B1-%D9%82%D8%A7%D9%84%D8%A8-%DB%8C%DA%A9-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87-%D9%85%D8%B9%D8%AA%D8%A8%D8%B1