Exploiting
MS Teams Metadata
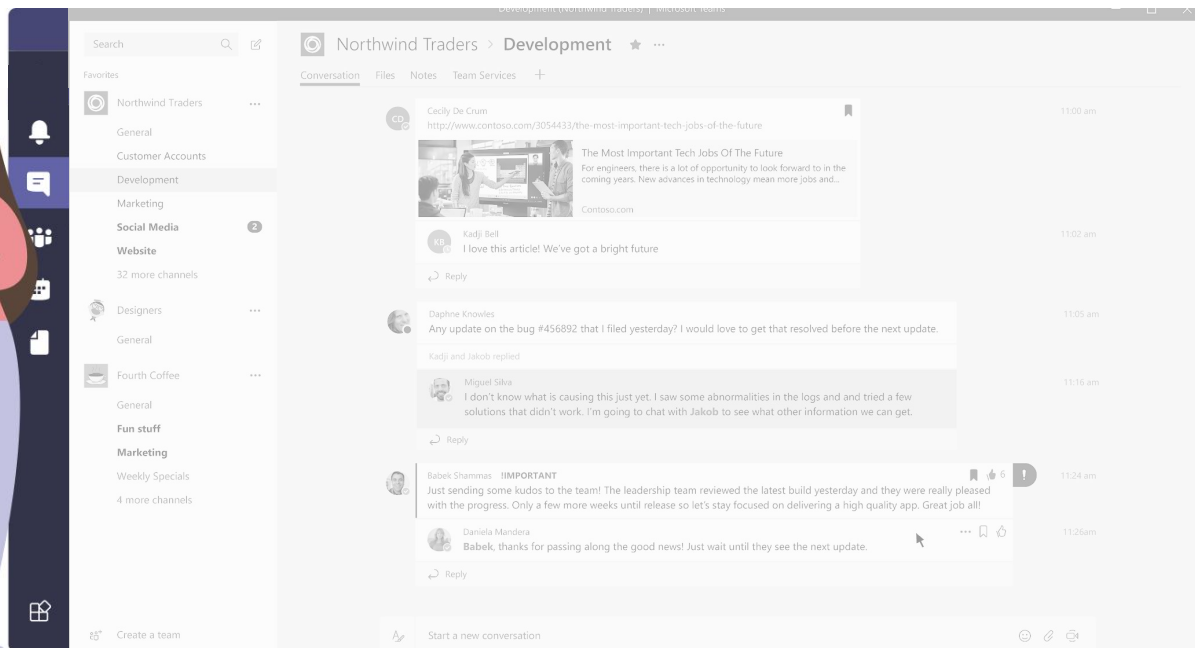
@botlabsDev

Microsoft Teams (Image: Microsoft)

Microsoft Teams (Image: Microsoft)

Microsoft Teams (Image: Microsoft)

Microsoft Teams (Image: Microsoft)

Microsoft Teams (Image: Microsoft)

Extraction Setup

- **Traffic redirected**
- **Replaced TLS certificate**
- **Extracted cookie und header data**
- **Extracted User IDs**

- **Intercepted traffic forwarded to MS Teams server**

Python mitmproxy

- Additional connections established:
  - **Query "user status" each 10 seconds**
  - **Query "user information" for each new User ID**

- Data stored in ElasticSearch:
  - User status and timestamp
  - User information

Elasticsearch Logstash Kibana

Dataset evaluated in February 2021

What Can We Expect ?

User Activity
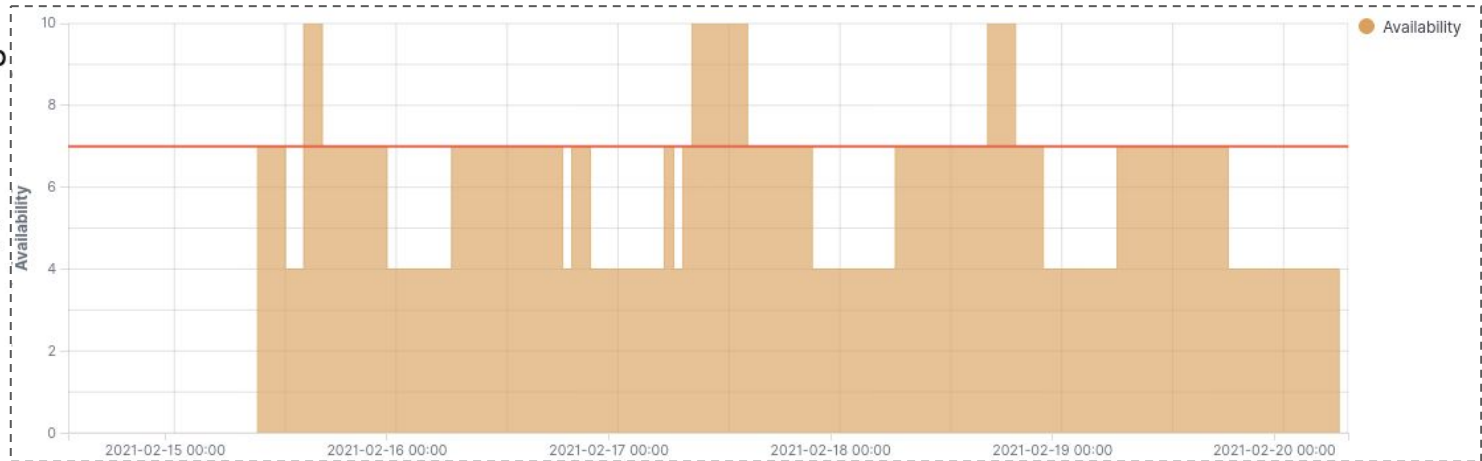
User Activity + Used Devices

Calls, Conference Calls, Team Meetings, ….

Desktop
Mobile
Web
Call
Screen share
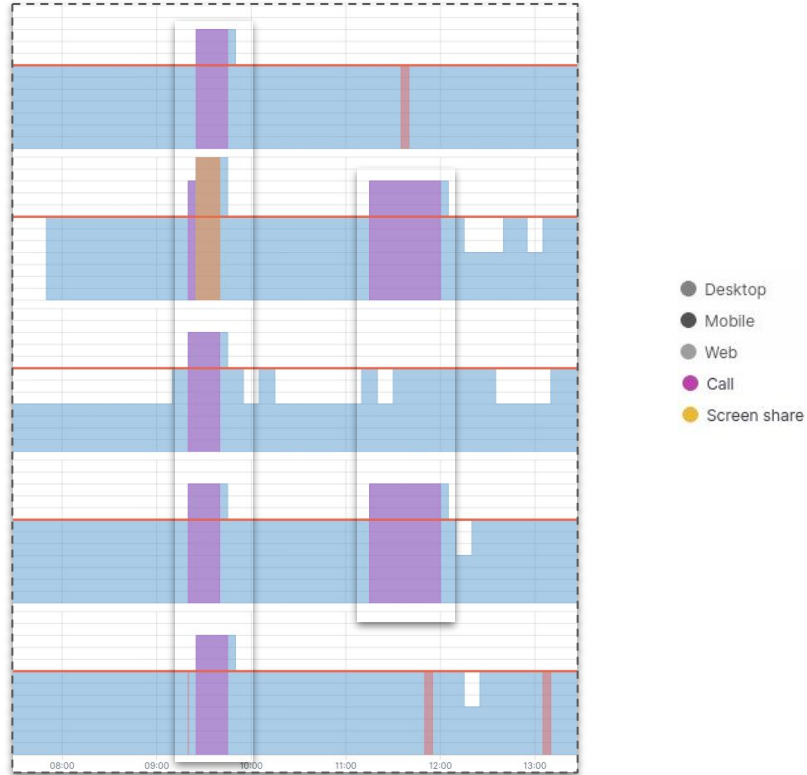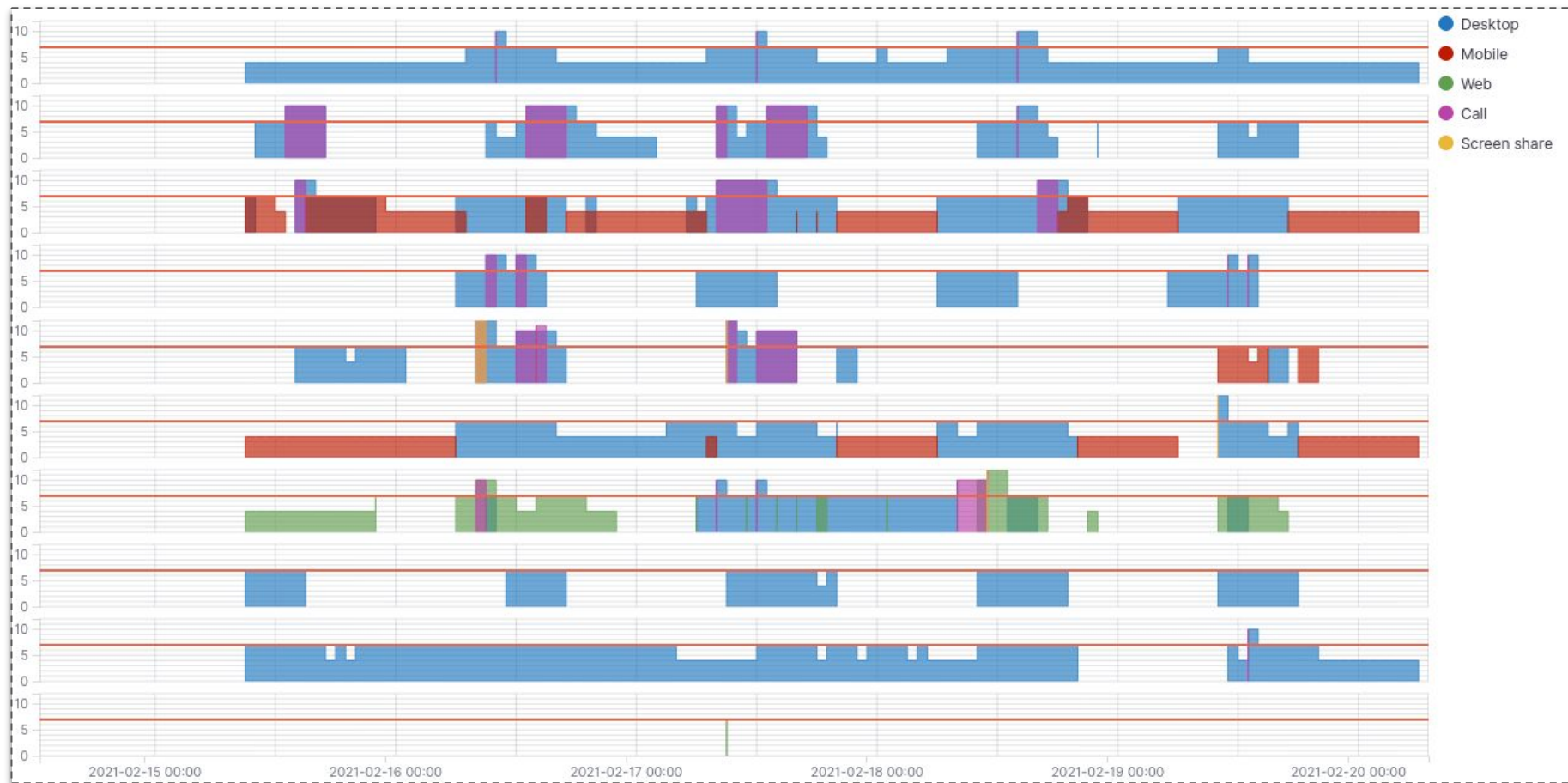
Team Overview

Department Overview
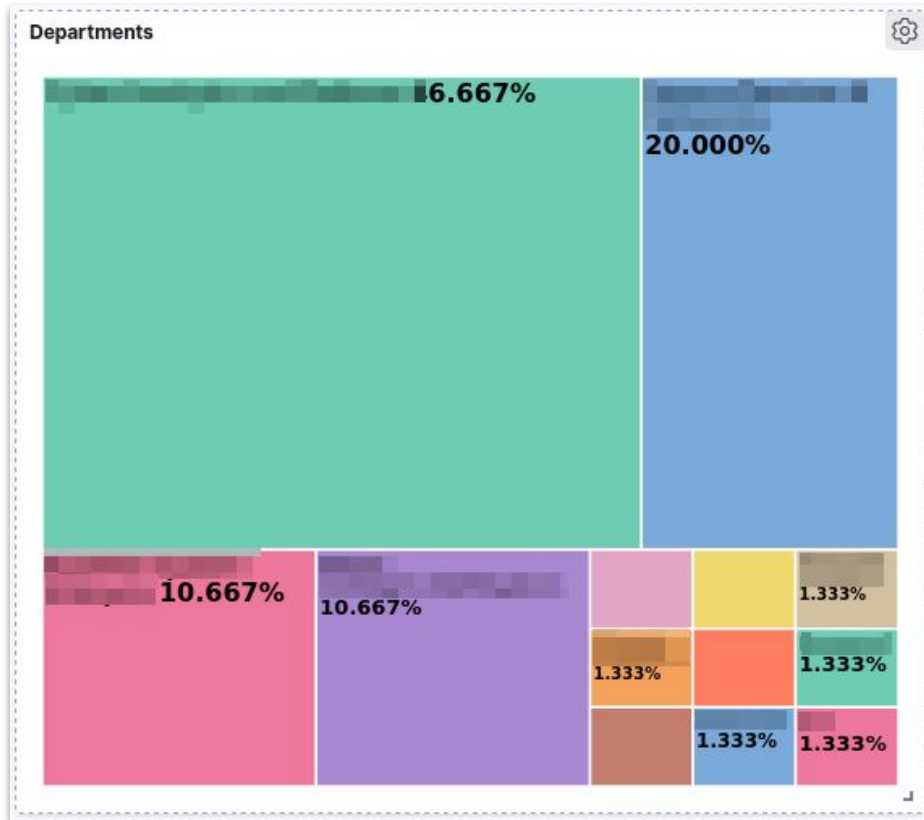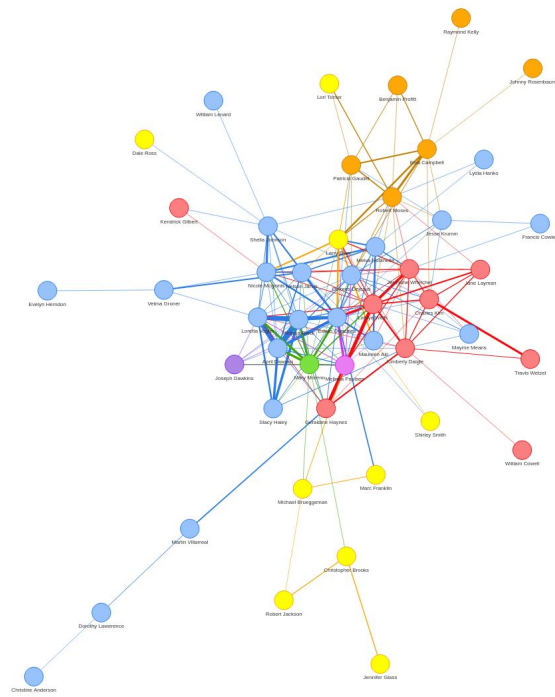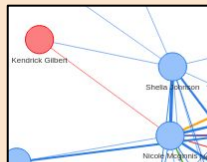

Departments

- Number of Departments
- Department sizes
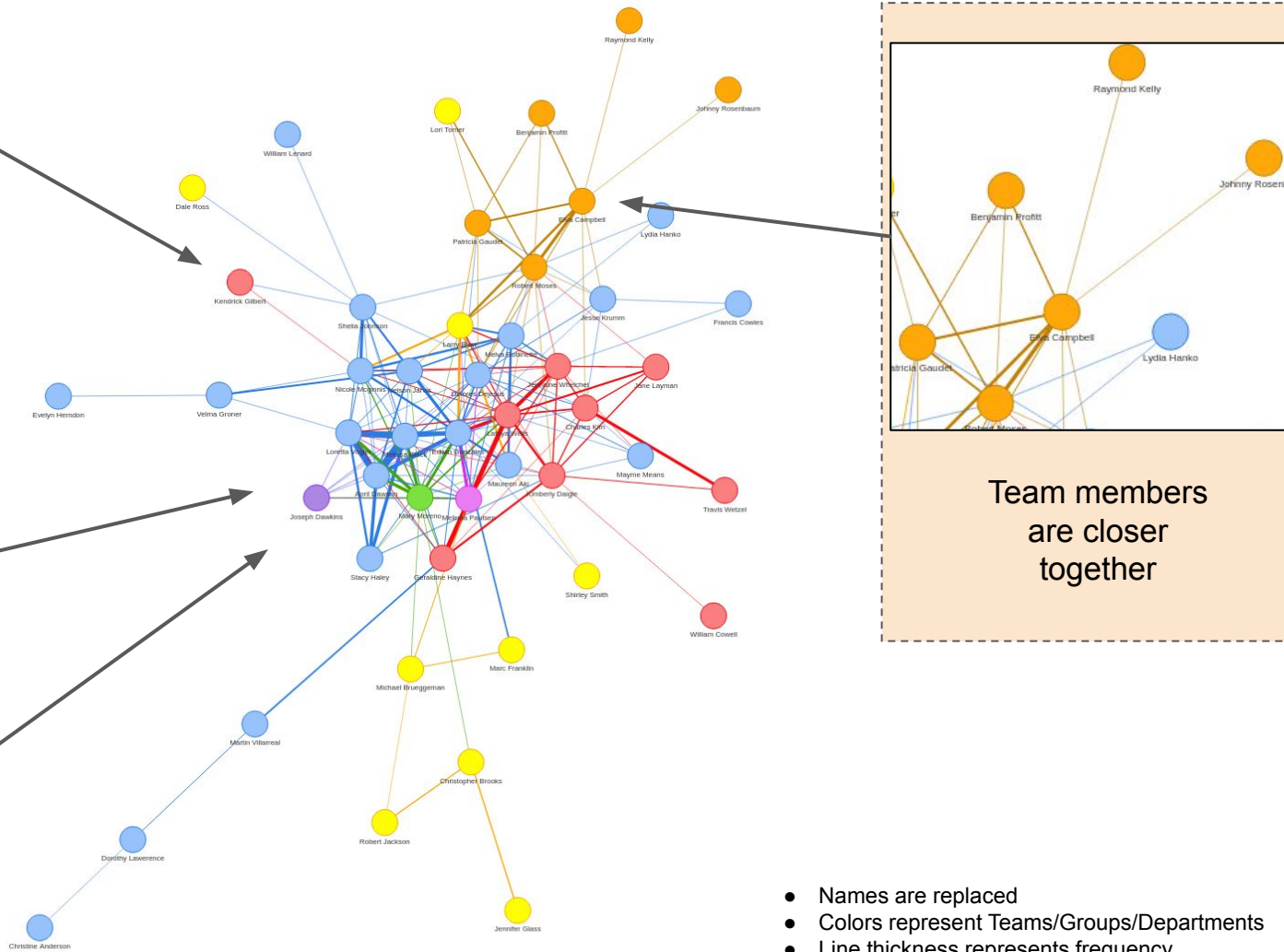- Employee movement between Departments
- Leaves / Hires

Common Call Groups

- Names are replaced
- Colors represent Teams/Groups/Departments
- Line thickness represents frequency
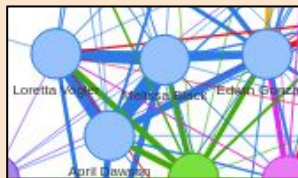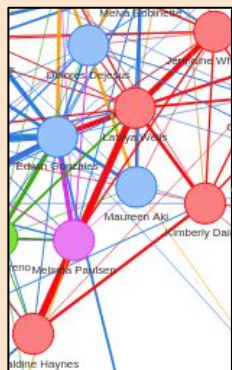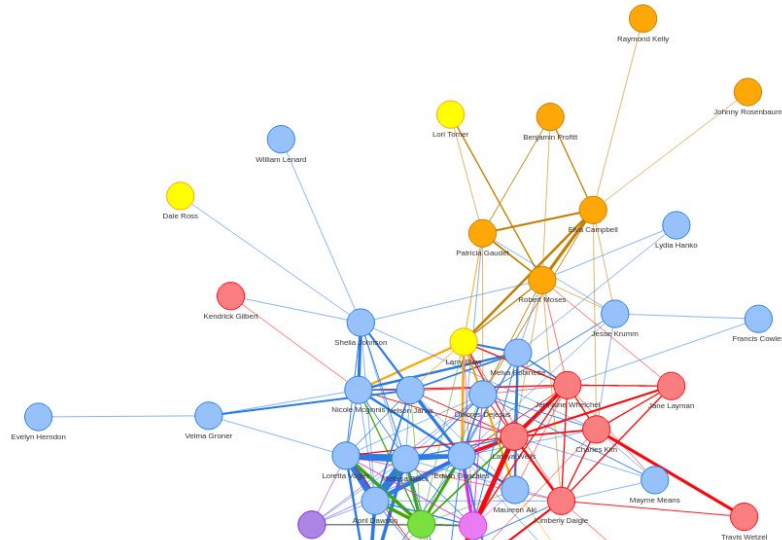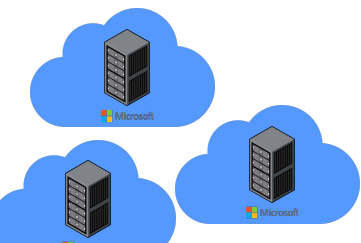
Cooperating teams

Common call groups

Team members are closer together

- Names are replaced
- Colors represent Teams/Groups/Departments
- Line thickness represents frequency

Conclusion

1. MS Teams API has no (noticeable) query limit in place.
2. Profound insights into the privacy of users is possible:
   a. Daily routines
   b. Holidays
   c. Meetings
   d. ...
3. Monitoring the whole company is possible.

Questions & Discussion