hosting.de

About us

Jean

As DevOps Jean connects the software developer and administrator teams. He is looking at problems through both lenses - availability, robustness and system stability are the important topics he is concerned with.

Michael

As Co-Founder and CSO Michael is designing and developing software for over 15 years. He is responsible for the hosting.de software stack focusing on software / system architecture and improving security of user websites.

Who we are

- Domains / DNS
- Webhosting / SSL
- E-Mail
- Virtual Machines / Managed LAEMP servers

Who we are

Public API

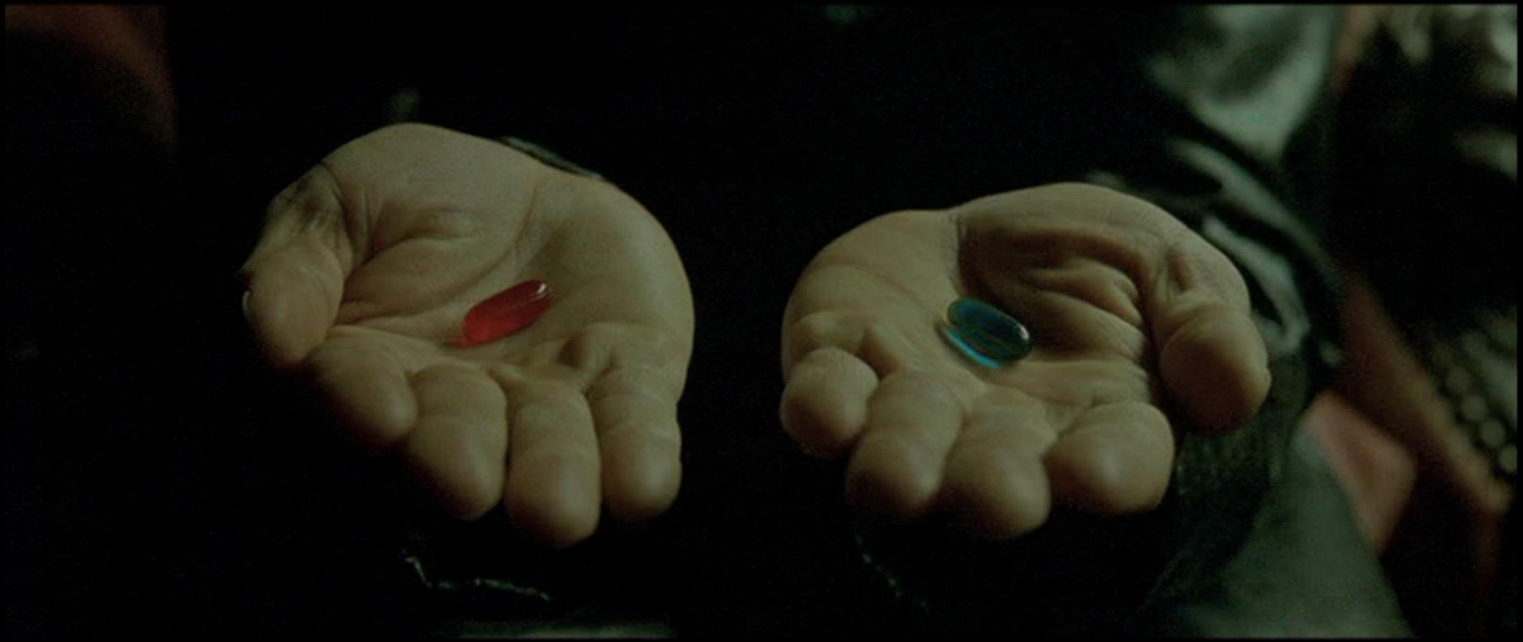
API doc: https://www.hosting.de/api

Who we are

Some figures:

- ca. 30 employees
- > 35.000 customers
- > 250.000 active vHosts
- > 5.000 virtual machines

Take the blue pill to stay sane, otherwise come with us



What are YOU doing..?

- How are customers using our services?
- How can we further support our customers?
- How can we optimize our infrastructure?

How are customers using our services?

How to detect what is happing on our webservers

- Look at files / webspaces manually
- Automatic scripts (grep, find)
- Existing tools, e.g. CMS Garden Scanner

  (https://github.com/CMS-Garden/cmsscanner)

How are customers using our services?

Issues

- Wtf… who wants to check things manually?!
- Application specific adaption
- Syntax might break between versions
- Version file might not be there or empty
- Version file might not tell the truth

Our findings

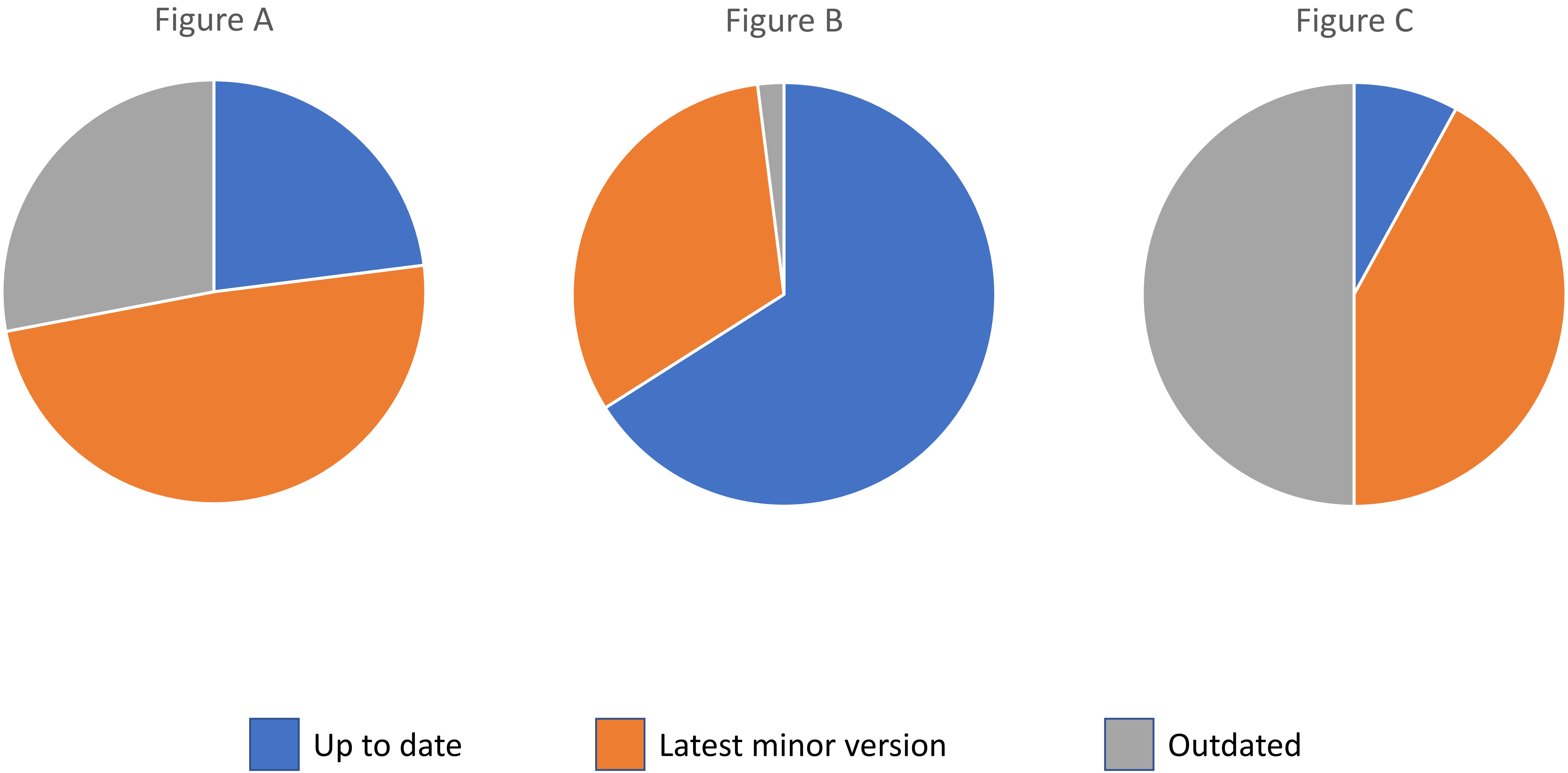
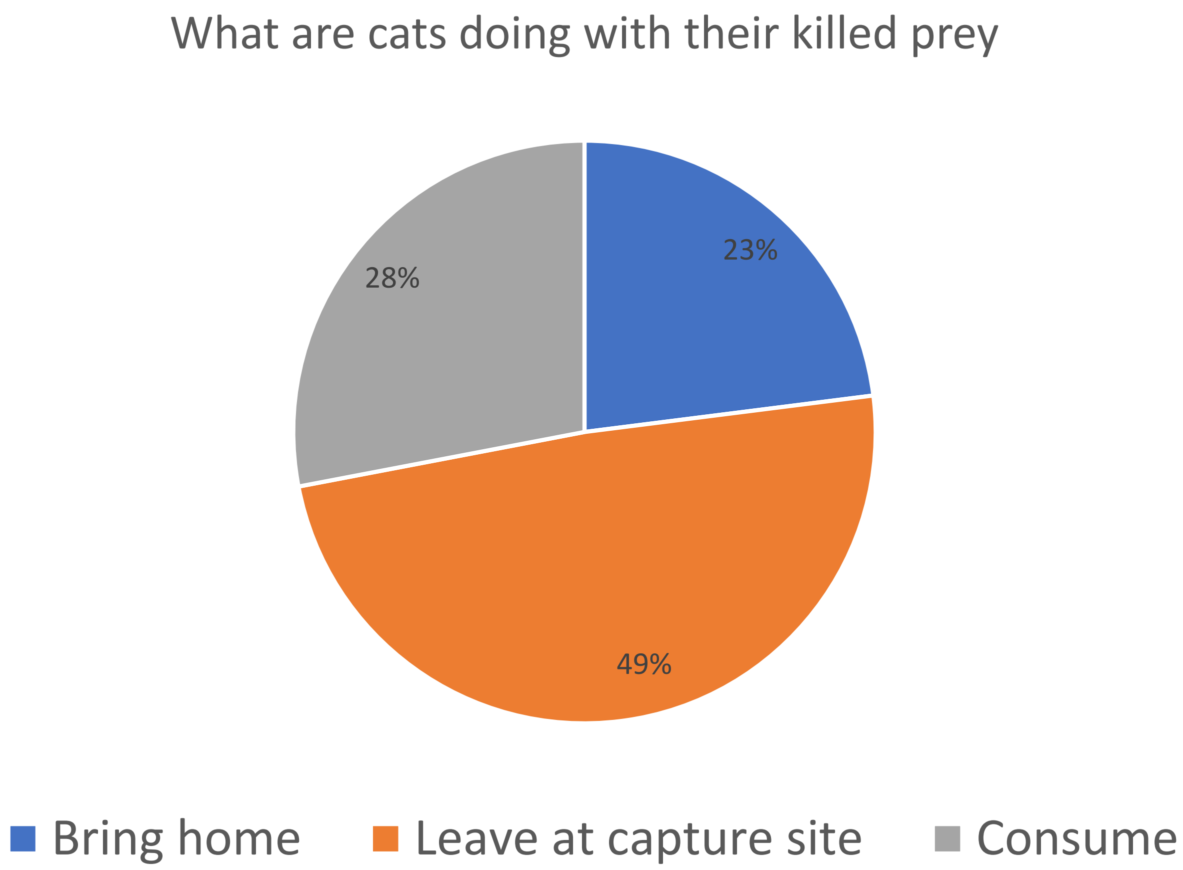


Figure A
Figure B
Figure C
Up to date
Latest minor version
Outdated

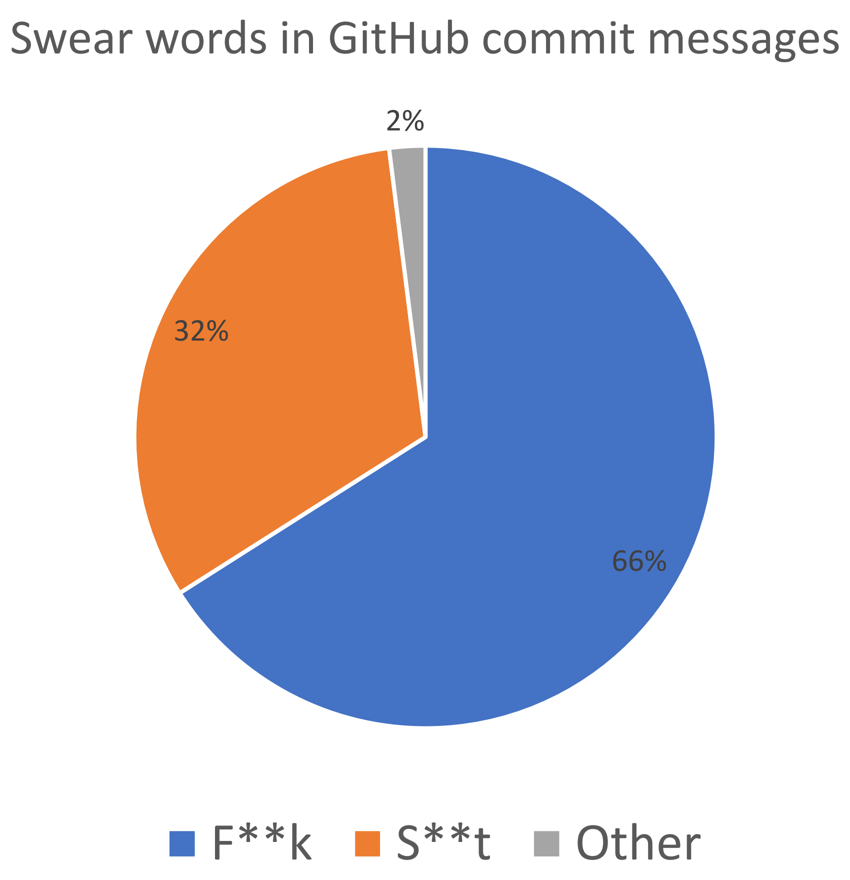
hosting.de

Figure A



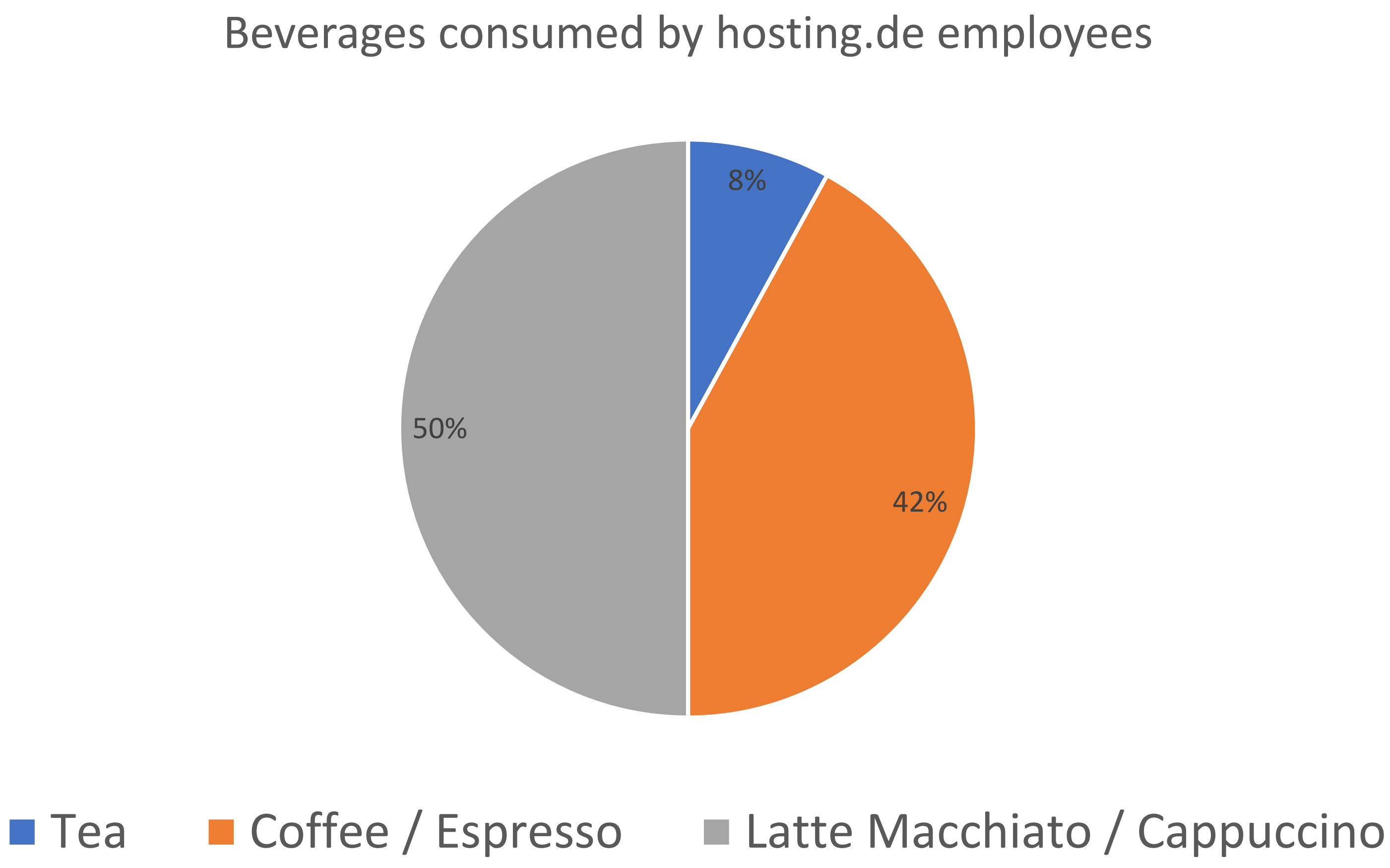
Source: http://www.kittycams.uga.edu/research.html

Figure B



Source: http://andrewvos.com/2011/02/21/amount-of-profanity-in-git-commit-messages-per-programming-language

Figure C

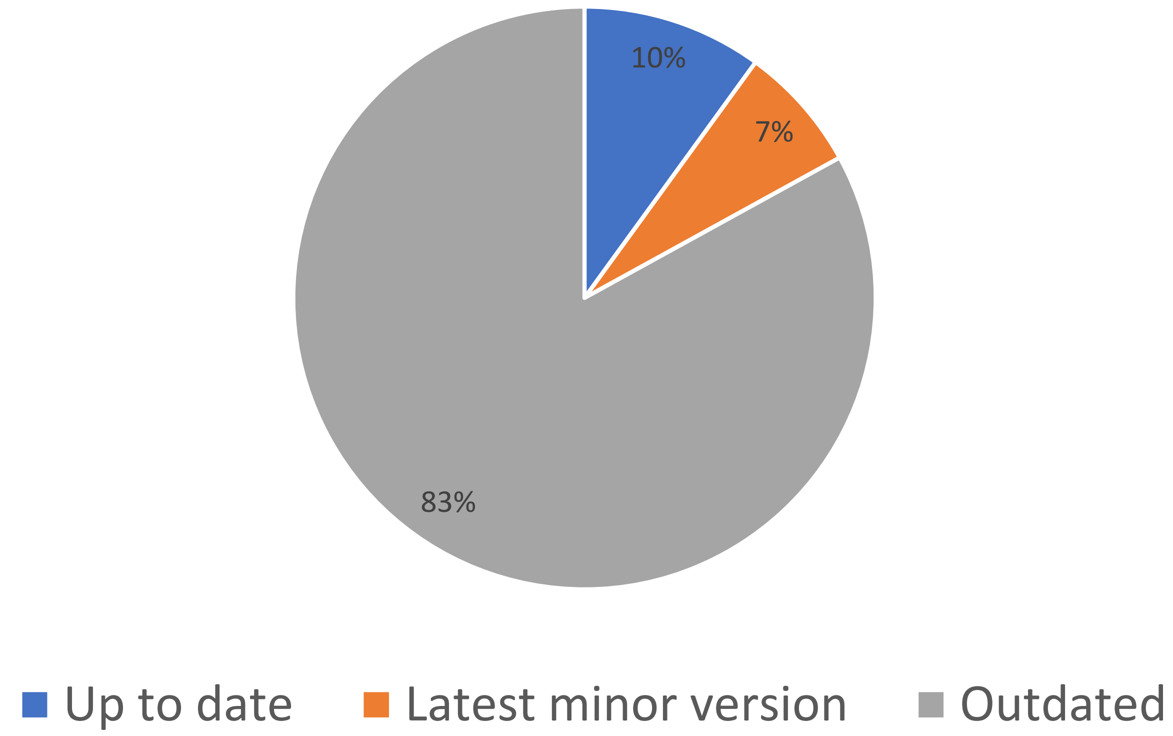


Beverages consumed by hosting.de employees

Source: https://www.hosting.de/unternehmen/

hosting.de

Actual result



Actual result in numbers

- Latest as of now – 3.8.7 (10%)
- Latest minor release – 3.8 (7%)
- Between 3.0 and 3.7 (30%)
- Below 3.0 (53%)

Distribution of outdated versions

- 3.0 and above (37%)
- Below 3.0 (63%)

Consequences

- Customers
  - Loss of reputation
  - Loss of availability
  - Restore to uncompromised state (everyone has backups..!)
- Hoster
  - Blacklisting
  - Performance, impacting other customers
  - DDoS

What to do, what to do..?

→Keep application up-to-date and always have a clean backup

Who takes care of it?!

- Customer!
- Web agency managing your site
- Webservices (e.g. myJoomla, Watchful.li, Sucuri, Sitelock)
    - Prices range from 1 Euro to 20 Euro per months
    - Check for malware in intervals between 24 hours and 30 minutes or even manually

Okay, we are done..?

Öhm, nope – some of the issues

- Integration (Addon / expose credentials)
- Time!

Our goal: real-time detection!

We need guns… A lot of them!

hosting.de

We need guns… A lot of them!

- Application independent approach
- Hash based fingerprinting instead of relying on the content of e.g. a version.php
- Monitoring file modifications in real-time
- Categorize modifications
- React to malicious changes

Our approach: hash-based fingerprinting

- Collect softwares / versions
  - No standards for releasing software (I am looking at YOU)
  - GitHub release vs. release on project website
  - Packaging is a pain…
- Build index

Monitoring file modifications in real-time

- No available tooling that just can be used
  - ionotify: does not scale, limit of files that can be watched
  - fanotify: no events on creating / renaming files
- Linux to the rescue
  - Just ask the kernel
  - Monitor the required events

React to modifications

- Recognize the new fingerprint (e.g. software update)
- Unknown fingerprint
  - Analyze modification
  - Send notification to the customer
  - Update index in case of malicious modifications

DEMO

What might the future bring..?

- Analyze HTTP-Request payload
- Discover new exploits
- Opensource the project..? Make the internet a safer place

Thank you!

Slides available at https://github.com/hosting-de-labs/talks