I Survived a Bruteforce Attack

Jan Grosser, TroLUG, 2019/07/04

Bruteforce Attack

- Raspberry Pi Server an ADSL Leitung mit DynDNS Remote Zugriff und einigen offenen Ports:
  - http(s)
  - ssh
  - OpenVPN
  - MariaDB
- Bruteforce attack http(s)+ssh seit 2019/04/08
  - ~ 228.000 ssh error logs (ssh Login Versuche)
  - ~ 125 apache error logs (Zugriff auf php-Skripte)

Typische Logs

```
journalctl -u ssh
```

```
May  6 16:47:20 host sshd[4068]: Invalid user zj from
211.24.xxx.xxx port 37215
```

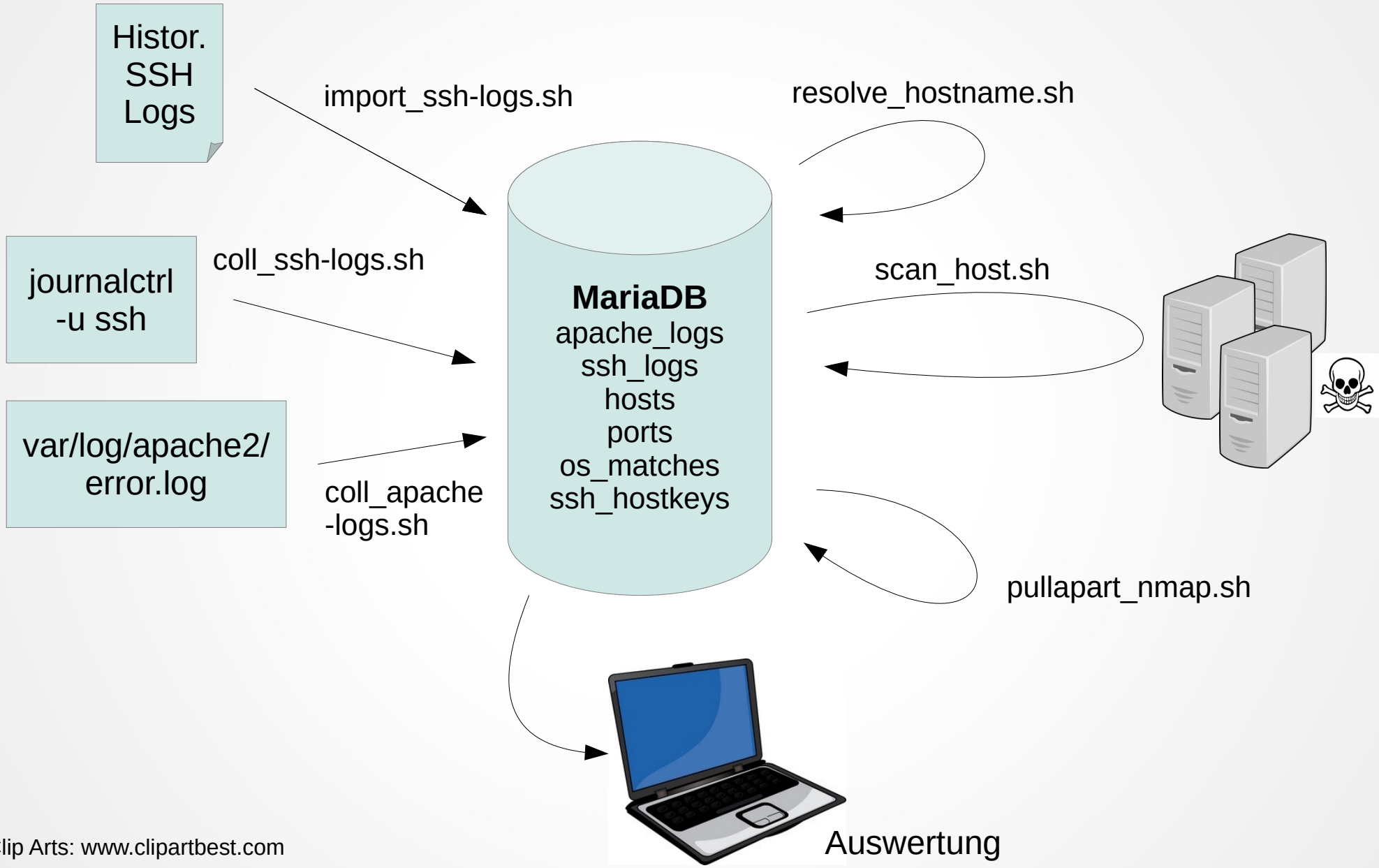
```
/var/log/apache2/error.log
```

```
[Thu Jun 20 09:04:28.180720 2019] [:error] [pid 11936]
[client 14.119.xxx.xx:58959] script
'/var/www/html/Appbf57f9d9.php' not found or unable to stat
```

Analyse der Logs: Tools

- Tools
  - Bash
  - MariaDB - Datenspeicher
  - EXTReMe-IP-Lookup.com – IP Informationen
  - Nmap – Port Scanner
  - xmllint, xpath - XML Tools
  - GnuPlot, R - Darstellung

Tools und Skripts



Clip Arts: www.clipartbest.com

Tabelle ssh_logs

```
> describe ssh_logs;
+-------------+---------+------+-----+---------+-------+
| Field       | Type    | Null | Key | Default | Extra |
+-------------+---------+------+-----+---------+-------+
| time        | double  | YES  | UNI | NULL    |       |
| user        | text    | YES  |     | NULL    |       |
| source_ip   | text    | YES  |     | NULL    |       |
| source_port | int(11) | YES  |     | NULL    |       |
+-------------+---------+------+-----+---------+-------+
4 rows in set (0.006 sec)

> select count(*) as 'Anzahl Logs' from ssh_logs;
+-------------+
| Anzahl Logs |
+-------------+
|      228068 |
+-------------+
1 row in set (0.844 sec)
```

Beliebteste ssh Benuternamen

```
> select user as User,count(user) as Anzahl from ssh_logs group by user
order by Anzahl desc limit 10;
+---------+--------+
| User    | Anzahl |
+---------+--------+
| admin   |   5979 |
| temp    |   4379 |
| test    |   3508 |
| ubuntu  |   3263 |
| nagios  |   3152 |
| ansible |   2877 |
| ftpuser |   2868 |
| ts3     |   2811 |
| dev     |   2781 |
| www     |   2743 |
+---------+--------+
10 rows in set (7.814 sec)
```

Beliebteste ssh Benuternamen

```
> select user as User,count(user) as Anzahl from ssh_logs group by user
order by Anzahl desc limit 10;
+---------+--------+
| User    | Anzahl |
+---------+--------+
| admin   |   5979 |
| temp    |   4379 |
| test    |   3508 |
| ubuntu  |   3263 |
| nagios  |   3152 |
| ansible |   2877 |
| ftpuser |   2868 |
| ts3     |   2811 |
| dev     |   2781 |
| www     |   2743 |
+---------+--------+
10 rows in set (7.814 sec)
```

Benutzername %test% (1/2)

```
> select user as User, count(*) as Anzahl from ssh_logs where user like
"%test%" group by user order by Anzahl desc limit 10;
+----------+--------+
| User     | Anzahl |
+----------+--------+
| test     |   3508 |
| testuser |   2141 |
| testftp  |   2125 |
| test3    |    569 |
| test4    |    455 |
| test2    |    454 |
| teste    |    107 |
| ftptest  |     96 |
| testing  |     83 |
| test1    |     70 |
+----------+--------+
10 rows in set (1.431 sec)
```

Benutzername %test% (2/2)

```
> select count(*) as Anzahl from ssh_logs where user like "%test%";
+--------+
| Anzahl |
+--------+
|   9814 |
+--------+
1 row in set (1.133 sec)
```

Tabelle apache_logs

```
> describe apache_logs;
+-------------+---------+------+-----+---------+-------+
| Field       | Type    | Null | Key | Default | Extra |
+-------------+---------+------+-----+---------+-------+
| time        | double  | YES  | UNI | NULL    |       |
| script      | text    | YES  |     | NULL    |       |
| source_ip   | text    | YES  |     | NULL    |       |
| source_port | int(11) | YES  |     | NULL    |       |
+-------------+---------+------+-----+---------+-------+
4 rows in set (0.007 sec)

> select count(*) as 'Anzahl Logs' from apache_logs;
+-------------+
| Anzahl Logs |
+-------------+
|         125 |
+-------------+
1 row in set (0.481 sec)
```

Gefragte Skripte

```
> select script as Skript, count(*) as Anzahl from apache_logs group by
script order by Anzahl desc limit 10;
+---------------------------------+--------+
| Skript                          | Anzahl |
+---------------------------------+--------+
| '/var/www/html/index.php'       |     25 |
| '/var/www/html/help.php'        |     22 |
| '/var/www/html/java.php'        |     14 |
| '/var/www/html/Appbf57f9d9.php' |     14 |
| '/var/www/html/elrekt.php'      |     11 |
| '/var/www/html/App8295f5d9.php' |      9 |
| '/var/www/html/echo.php'        |      6 |
| '/var/www/html/App129ff5d9.php' |      6 |
| '/var/www/html/_query.php'      |      4 |
| '/var/www/html/xmlrpc.php'      |      3 |
+---------------------------------+--------+
10 rows in set (0.014 sec)
```

Tabelle hosts (1/2)

```
> describe hosts;
+-----------------+-------------+------+-----+---------+-------+
| Field           | Type        | Null | Key | Default | Extra |
+-----------------+-------------+------+-----+---------+-------+
| businessName    | text        | YES  |     | NULL    |       |
| businessWebsite | text        | YES  |     | NULL    |       |
| city            | text        | YES  |     | NULL    |       |
| continent       | text        | YES  |     | NULL    |       |
| country         | text        | YES  |     | NULL    |       |
| countryCode     | text        | YES  |     | NULL    |       |
| ipName          | text        | YES  |     | NULL    |       |
| ipType          | text        | YES  |     | NULL    |       |
| isp             | text        | YES  |     | NULL    |       |
| lat             | double      | YES  |     | NULL    |       |
| lon             | double      | YES  |     | NULL    |       |
| org             | text        | YES  |     | NULL    |       |
| ipAddr          | varchar(15) | YES  | UNI | NULL    |       |
```

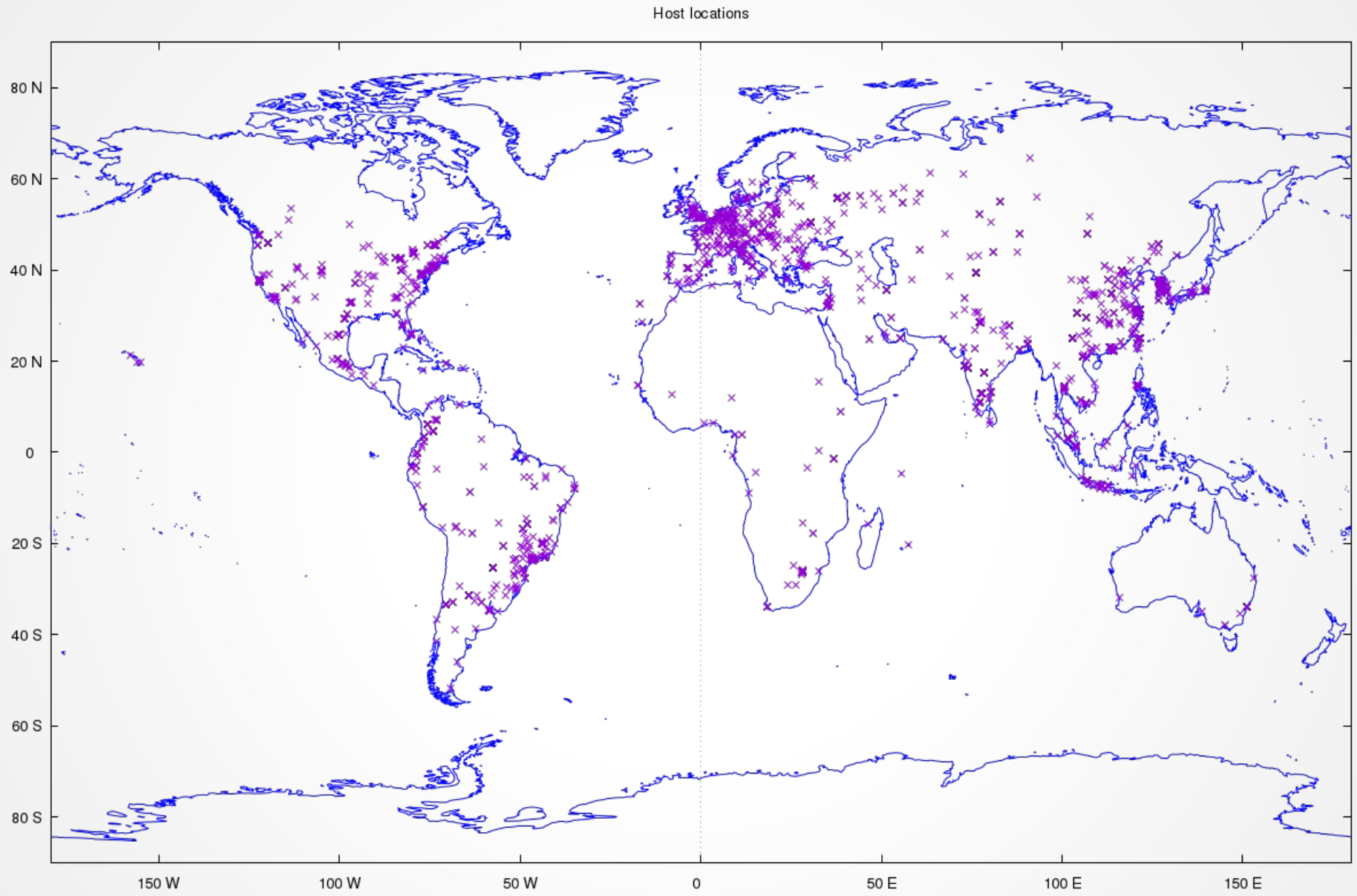
Tabelle hosts (2/2)

```
| region          | text         | YES  |     | NULL    |       |
| status          | text         | YES  |     | NULL    |       |
| lookupTime      | double       | YES  |     | NULL    |       |
| nmap            | text         | YES  |     | NULL    |       |
| nmapCmd         | text         | YES  |     | NULL    |       |
| nmapVer         | text         | YES  |     | NULL    |       |
| nmapXMLVer      | text         | YES  |     | NULL    |       |
| nmapStart       | double       | YES  |     | NULL    |       |
| nmapEnd         | double       | YES  |     | NULL    |       |
| nmapHostName    | text         | YES  |     | NULL    |       |
| nmapUptime      | bigint(20)   | YES  |     | NULL    |       |
| nmapProcessed   | tinyint(1)   | NO   |     | 0       |       |
| nmapInvalid     | tinyint(1)   | YES  |     | 0       |       |
+-----------------+--------------+------+-----+---------+-------+
26 rows in set (0.008 sec)
```

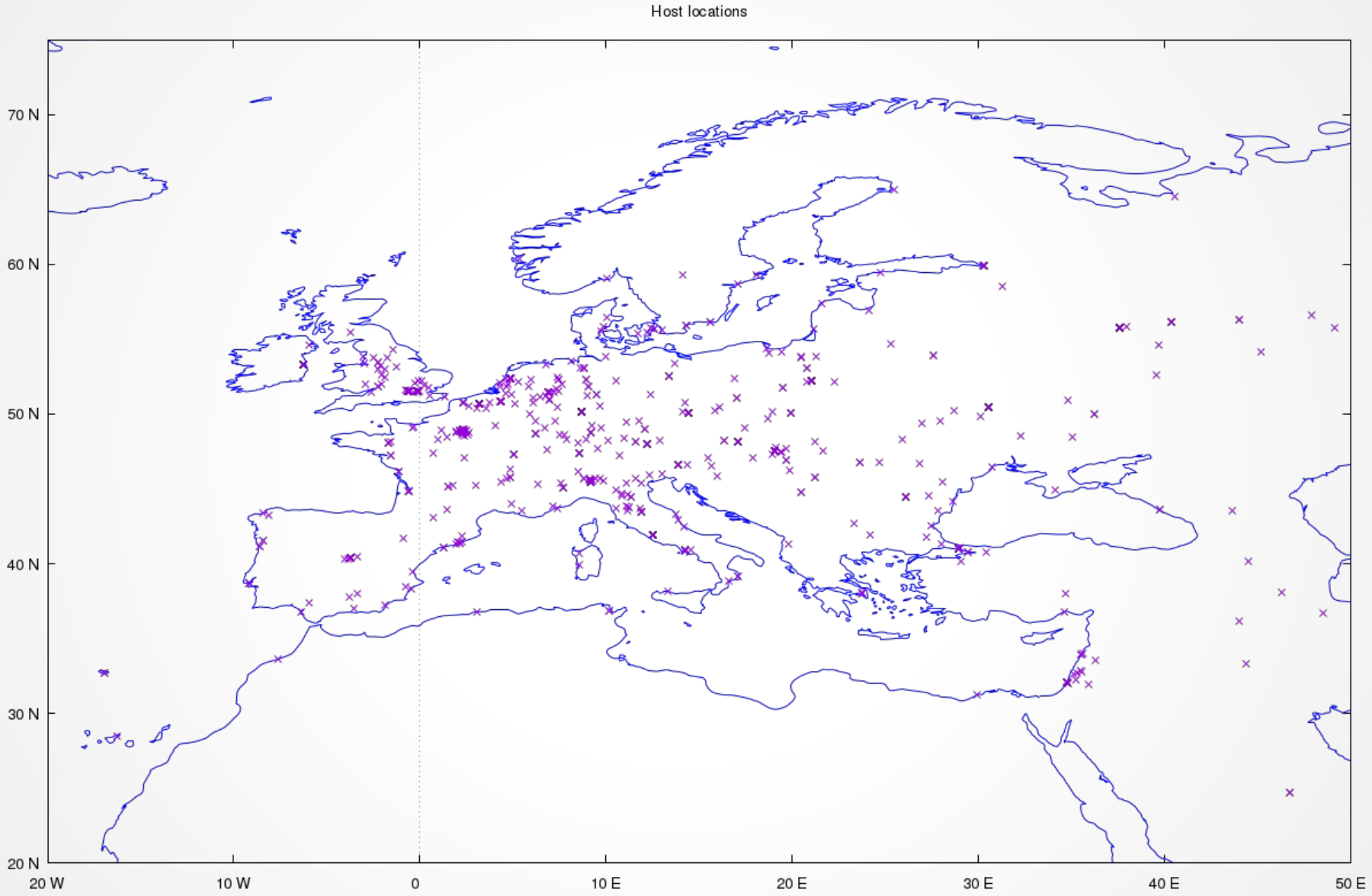
Woher kommen die Bösewichte?

```
> select country as Land, count(*) as Anzahl from hosts group by country
order by Anzahl desc limit 10;
+---------------+--------+
| Land          | Anzahl |
+---------------+--------+
| China         |    952 |
| United States |    504 |
| France        |    252 |
| Japan         |    180 |
| Singapore     |    157 |
| India         |    151 |
| Brazil        |    146 |
| South Korea   |    123 |
| Germany       |    121 |
| Canada        |     89 |
+---------------+--------+
10 rows in set (0.177 sec)
```

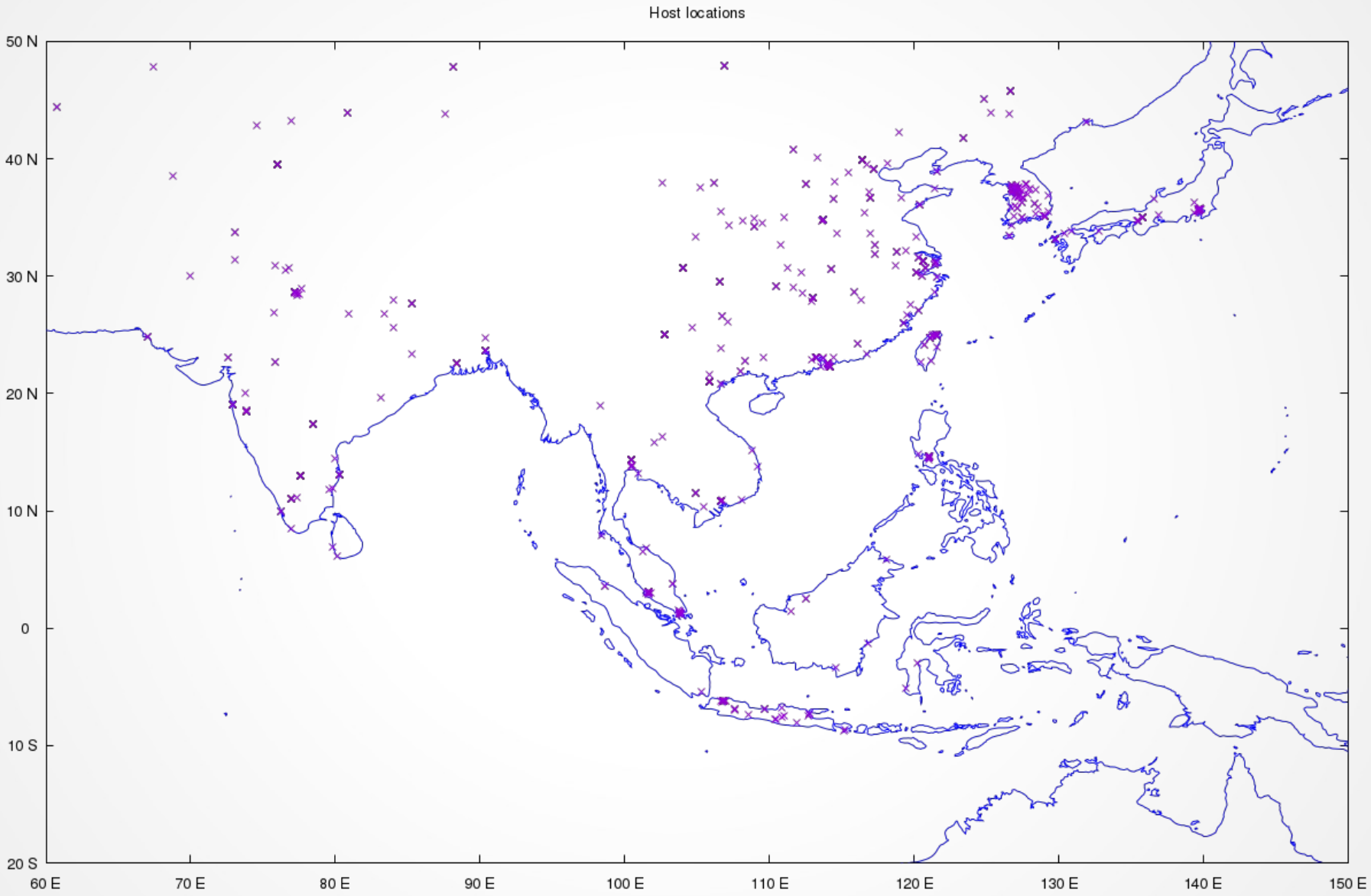
Globale Verteilung der Hosts



Hosts aus Europa



Hosts aus Asien



Aktivste ssh Schüffler

```
> select hosts.ipAddr as IP, count(ssh_logs.time) as Anzahl, hosts.country as
Land from hosts inner join ssh_logs on (hosts.ipAddr=ssh_logs.source_ip)
group by IP order by Anzahl desc limit 10;
+-----------------+--------+---------------+
| IP              | Anzahl | Land          |
+-----------------+--------+---------------+
| 213.57.xx.xxx   |   2837 | Israel        |
| 54.85.xx.xx     |   1090 | United States |
| 220.158.xxx.xxx |    804 | Cambodia      |
| 52.21.xxx.x     |    687 | United States |
| 145.239.xxx.xxx |    588 | France        |
| 94.191.xx.xxx   |    564 | China         |
| 13.127.xxx.xxx  |    544 | India         |
| 193.112.xxx.xx  |    524 | China         |
| 165.22.xxx.xxx  |    517 | United States |
| 18.208.xxx.xxx  |    512 | United States |
+-----------------+--------+---------------+
10 rows in set (27.691 sec)
```

Tabelle ssh_hostkeys

```
> describe ssh_hostkeys;
+-------------+--------------+------+-----+---------+-------+
| Field       | Type         | Null | Key | Default | Extra |
+-------------+--------------+------+-----+---------+-------+
| ipAddr      | varchar(15)  | YES  | MUL | NULL    |       |
| fingerprint | varchar(255) | YES  |     | NULL    |       |
| type        | text         | YES  |     | NULL    |       |
| sshkey      | text         | YES  |     | NULL    |       |
| bits        | int(11)      | YES  |     | NULL    |       |
+-------------+--------------+------+-----+---------+-------+
5 rows in set (0.008 sec)

> select count(*) as 'Anzahl Hostkeys' from ssh_hostkeys;
+-----------------+
| Anzahl Hostkeys |
+-----------------+
|            2731 |
+-----------------+
1 row in set (0.019 sec)
```

Bitlänge der SSH-RSA Keys

```
> select bits, count(*) as Anzahl from ssh_hostkeys where type="ssh-rsa" group by bits order by Anzahl desc;
+------+--------+
| bits | Anzahl |
+------+--------+
| 2048 |   1228 |
| 1024 |     13 |
| 1039 |      2 |
| 1040 |      2 |
+------+--------+
4 rows in set (0.042 sec)
```

Wiederholung von Hostkeys?

```
> select fingerprint, type, count(*) as Anzahl from ssh_hostkeys group
by fingerprint order by Anzahl desc limit 10;
+----------------------------------+---------------------+--------+
| fingerprint                      | type                | Anzahl |
+----------------------------------+---------------------+--------+
| 2249b25c7c8f735689298abd56497466 | ecdsa-sha2-nistp256 |     33 |
| a68d6ff2b5a949340718cd734984a0c4 | ssh-rsa             |     32 |
| 6f237d680ec4cdedfeca9ebb8e7df4e8 | ssh-rsa             |     15 |
| 915c3ff45e77464926bb91626d0f7a09 | ssh-dss             |     14 |
| 06b92486c46def94f5d3f544e2fe2392 | ecdsa-sha2-nistp256 |     13 |
| ae70015e05d9da8f75e723e55f2d3d89 | ssh-rsa             |     12 |
| dd60934f7a86868a18ffa4e4d05ee2a1 | ecdsa-sha2-nistp256 |     12 |
| bf5edc03908c47b086510c56126ecbec | ssh-rsa             |     11 |
| b92f9c979166b44b2a895d28f306062d | ecdsa-sha2-nistp256 |     11 |
| 0443e3bcafa3645ae6ad7dcc41239b61 | ssh-dss             |      9 |
+----------------------------------+---------------------+--------+
10 rows in set (0.390 sec)
```

Fingerprint 2249b25c7c... (1/2)

```
 select count(*) from ssh_hostkeys where fingerprint="2249b25c7c8f735689298abd56497466";
+----------+
| count(*) |
+----------+
|       33 |
+----------+
1 row in set (0.02 sec)


> select substr(hosts.isp,1,23) as Provider, count(*) as Anzahl from ssh_hostkeys inner
join hosts on hosts.ipAddr=ssh_hostkeys.ipAddr where
ssh_hostkeys.fingerprint="2249b25c7c8f735689298abd56497466" group by Provider order by
Anzahl desc;
+-------------------------+--------+
| Provider                | Anzahl |
+-------------------------+--------+
| Tencent Cloud Computing |     33 |
+-------------------------+--------+
1 row in set (0.02 sec)
```

Fingerprint 2249b25c7c... (2/2)

```
> create temporary table top_os as (select ipAddr, name, line, type,
vendor, family, portUsed, max(accuracy) from os_matches group by ipAddr);
Query OK, 2849 rows affected (16.76 sec)
Records: 2849  Duplicates: 0  Warnings: 0


> select top_os.name, top_os.family, count(*) as Anzahl from top_os inner
join ssh_hostkeys on top_os.ipAddr=ssh_hostkeys.ipAddr where
ssh_hostkeys.fingerprint="2249b25c7c8f735689298abd56497466" group by
top_os.name order by Anzahl desc;
+-----------------------------+---------+--------+
| name                        | family  | Anzahl |
+-----------------------------+---------+--------+
| Asus RT-AC66U WAP           | Linux   |     28 |
| Linux 3.11 - 3.14           | Linux   |      3 |
| Infomir MAG-250 set-top box | Linux   |      1 |
| Android 4.1.1               | Android |      1 |
+-----------------------------+---------+--------+
4 rows in set (0.14 sec)
```

Tabelle Ports

```
> describe ports;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| ipAddr      | varchar(15) | YES  | MUL | NULL    |       |
| type        | varchar(15) | YES  |     | NULL    |       |
| portID      | int(11)     | YES  |     | NULL    |       |
| state       | text        | YES  |     | NULL    |       |
| reason      | text        | YES  |     | NULL    |       |
| reasonTTL   | int(11)     | YES  |     | NULL    |       |
| serviceName | text        | YES  |     | NULL    |       |
| product     | text        | YES  |     | NULL    |       |
| version     | text        | YES  |     | NULL    |       |
| extrainfo   | text        | YES  |     | NULL    |       |
| osType      | text        | YES  |     | NULL    |       |
| method      | text        | YES  |     | NULL    |       |
| conf        | text        | YES  |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
13 rows in set (0.009 sec)
```

Offene Ports

```
> select type, portID, serviceName, count(*) as Anzahl from ports group by serviceName
order by Anzahl desc limit 10;
+------+--------+--------------+--------+
| type | portID | serviceName  | Anzahl |
+------+--------+--------------+--------+
| tcp  |     80 | http         |   3760 |
| tcp  |     22 | ssh          |   2684 |
| tcp  |    445 | microsoft-ds |    988 |
| tcp  |   8181 | unknown      |    806 |
| tcp  |     21 | ftp          |    664 |
| tcp  |   3306 | mysql        |    637 |
| tcp  |    135 | msrpc        |    513 |
| tcp  |    139 | netbios-ssn  |    466 |
| tcp  |    443 | https        |    448 |
| tcp  |     25 | smtp         |    427 |
+------+--------+--------------+--------+
10 rows in set (0.623 sec)
```

Welcher SSH Server?

```
> select product, version, ostype, count(*) as Anzahl from ports where servicename="ssh"
group by product order by Anzahl desc;
+-------------------------------------+-------------------------+--------+--------+
| product                             | version                 | ostype | Anzahl |
+-------------------------------------+-------------------------+--------+--------+
| OpenSSH                             | 7.2p2 Ubuntu 4ubuntu2.1 | Linux  |   1357 |
|                                     |                         |        |   1306 |
| Dropbear sshd                       | 0.46                    | Linux  |      7 |
| MikroTik RouterOS sshd              |                         | Linux  |      5 |
| Cyberoam firewall sshd              |                         |        |      4 |
| Cisco SSH                           | 1.25                    | IOS    |      3 |
| DrayTek Vigor 2820n ADSL router sshd | 2.0                     |        |      1 |
| SunSSH                              | 1.5                     |        |      1 |
+-------------------------------------+-------------------------+--------+--------+
8 rows in set (0.239 sec)
```

Tabelle os_matches

```
> describe os_matches;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| ipAddr   | varchar(15)  | YES  | MUL | NULL    |       |
| name     | varchar(255) | YES  |     | NULL    |       |
| accuracy | int(11)      | YES  |     | NULL    |       |
| line     | int(11)      | YES  |     | NULL    |       |
| type     | text         | YES  |     | NULL    |       |
| vendor   | text         | YES  |     | NULL    |       |
| family   | text         | YES  |     | NULL    |       |
| portUsed | int(11)      | YES  |     | NULL    |       |
+----------+--------------+------+-----+---------+-------+
8 rows in set (0.009 sec)

MariaDB [bruteforce]> select count(*) from os_matches;
+----------+
| count(*) |
+----------+
|    17389 |
+----------+
1 row in set (1.202 sec)
```

Bsp: OS Matches für eine IP

```
> select name as Betriebssystem, accuracy from os_matches where
ipAddr="98.246.xx.xx" order by accuracy desc;
+------------------------+----------+
| Betriebssystem         | accuracy |
+------------------------+----------+
| Linux 3.11 - 3.14      |       94 |
| Linux 2.6.26 - 2.6.35  |       92 |
| Linux 2.6.32 - 3.10    |       92 |
| Linux 3.2 - 3.8        |       91 |
| Linux 2.6.23 - 2.6.38  |       91 |
| Linux 2.6.32           |       90 |
| Linux 3.11 - 3.13      |       89 |
| Linux 3.0              |       89 |
| HP P2000 G3 NAS device |       89 |
| Linux 3.10             |       88 |
+------------------------+----------+
10 rows in set (0.006 sec)
```

Häufigste OS

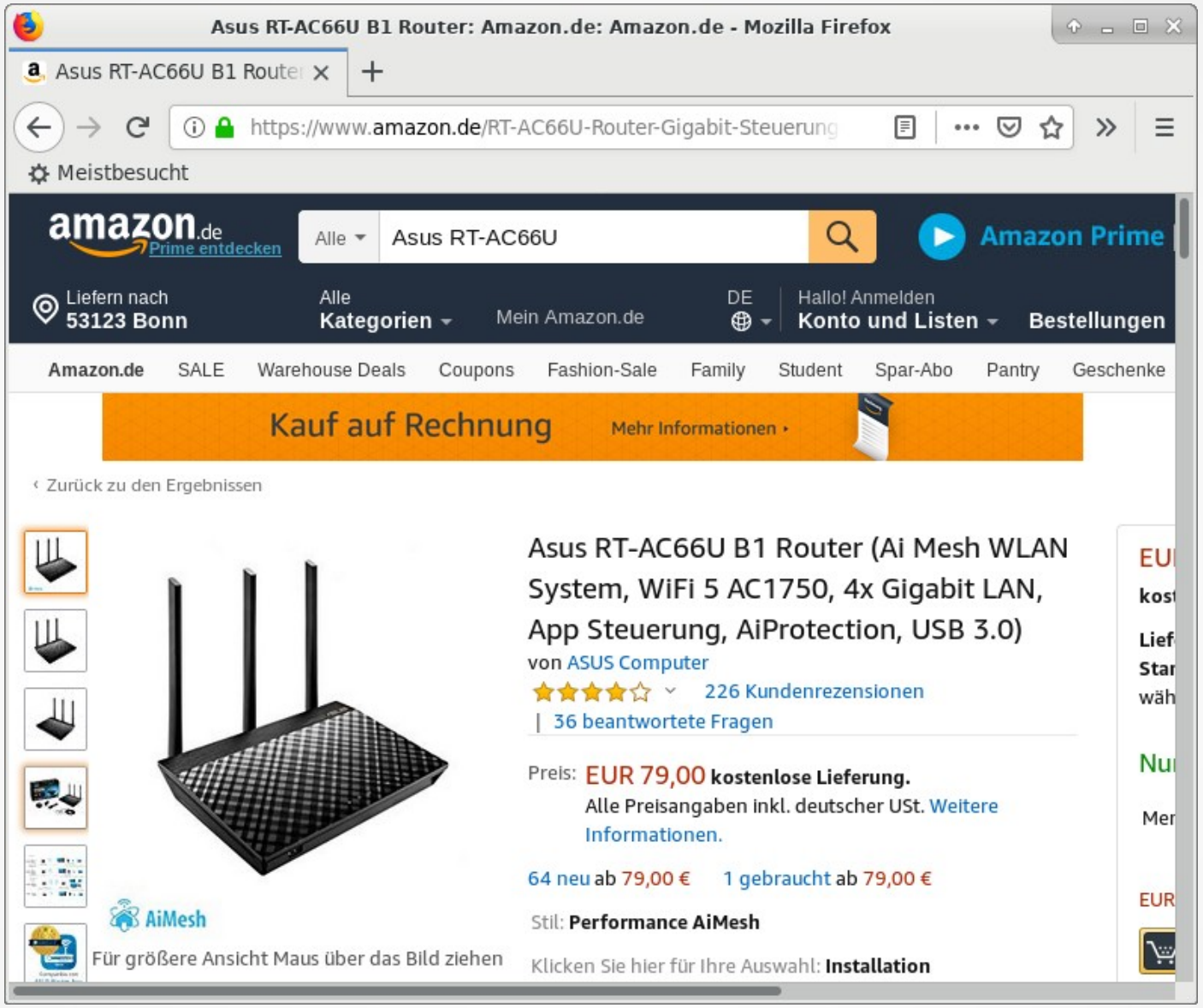
```
> create temporary table top_os as (select ipAddr, name, line, type, vendor, family, portUsed, max(accuracy) from os_matches group by ipAddr);
Query OK, 2871 rows affected (5.928 sec)
Records: 2871  Duplicates: 0  Warnings: 0


> sselect family as Familie, count(*) as Anzahl from top_os group by family order by Anzahl desc limit 10;
+----------+--------+
| Familie  | Anzahl |
+----------+--------+
| Linux    |   2220 |
| embedded |    407 |
| 2-Series |     74 |
| Windows  |     61 |
| Android  |     61 |
| FreeBSD  |     15 |
| iPXE     |     11 |
| Mac OS X |      8 |
| IOS      |      5 |
| PIX OS   |      3 |
+----------+--------+
10 rows in set (0.351 sec)
```

Häufigste Linux-Versionen

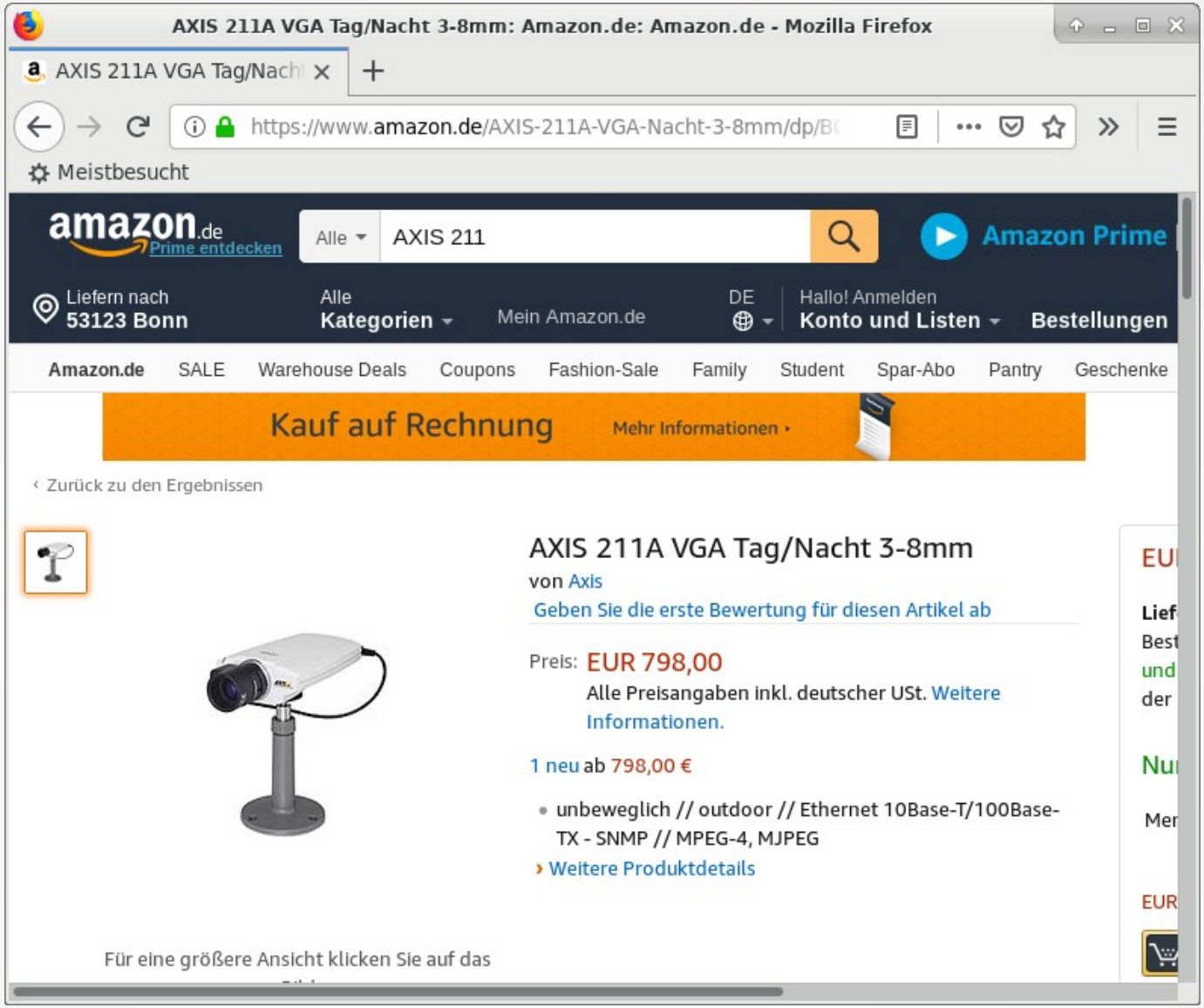
```
> select family as Familie, name, type, count(*) as Anzahl from top_os where
family="Linux" group by name order by Anzahl desc limit 10;
+---------+-----------------------------------------------+-----------------+--------+
| Familie | name                                          | type            | Anzahl |
+---------+-----------------------------------------------+-----------------+--------+
| Linux   | Linux 3.11 - 3.14                             | general purpose |    755 |
| Linux   | Asus RT-AC66U WAP                             | WAP             |    713 |
| Linux   | Linux 2.6.32 - 3.10                           | general purpose |    144 |
| Linux   | 2.6.32                                        | general purpose |    132 |
| Linux   | Linux 2.6.18 - 2.6.22                         | general purpose |     58 |
| Linux   | Linux 2.6.22 - 2.6.36                         | general purpose |     52 |
| Linux   | Asus RT-AC66U router (Linux 2.6)              | router          |     50 |
| Linux   | Linux 2.6.23 - 2.6.38                         | general purpose |     41 |
| Linux   | Linux 3.11 - 3.13                             | general purpose |     41 |
| Linux   | AXIS 210A or 211 Network Camera (Linux 2.6.17) | webcam          |     17 |
+---------+-----------------------------------------------+-----------------+--------+
10 rows in set (0.151 sec)
```

Asus RT-AC66U



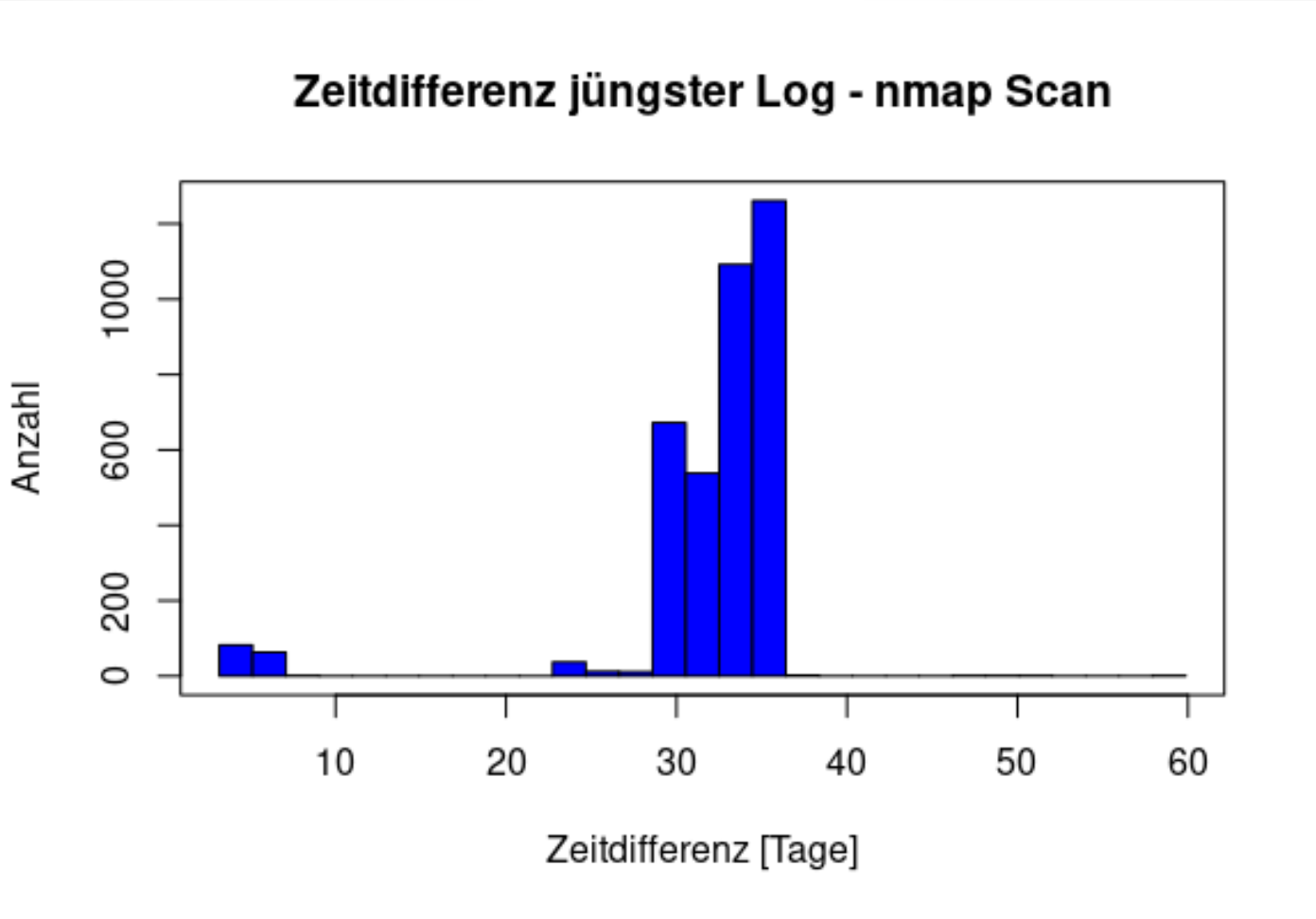
Asus RT-AC66U Security Vulnerabilities

AXIS 211 Webcam



Methodische Schwäche

```
> select (hosts.nmapStart-min(ssh_logs.time))/86400 as dt from
ssh_logs inner join hosts on ssh_logs.source_ip=hosts.ipAddr group by
ipAddr order by dt desc;
```



Tipps

- Monitoring Tool verwenden, z.B. Munin
- fail2ban installieren und einrichten
- Absichern des SSH
  - Nur ausgewählte User ssh-Zugriff erlauben, z.B.: Gruppe ssh_allow anlegen
  - Passwort Auth → Public Key Auth
  - Keine erratbaren Usernamen verwenden, z.B.: test, admin, pi, ...
  - IP Range einschränken (z.B. bestimmte ISPs)

Vielen Dank!