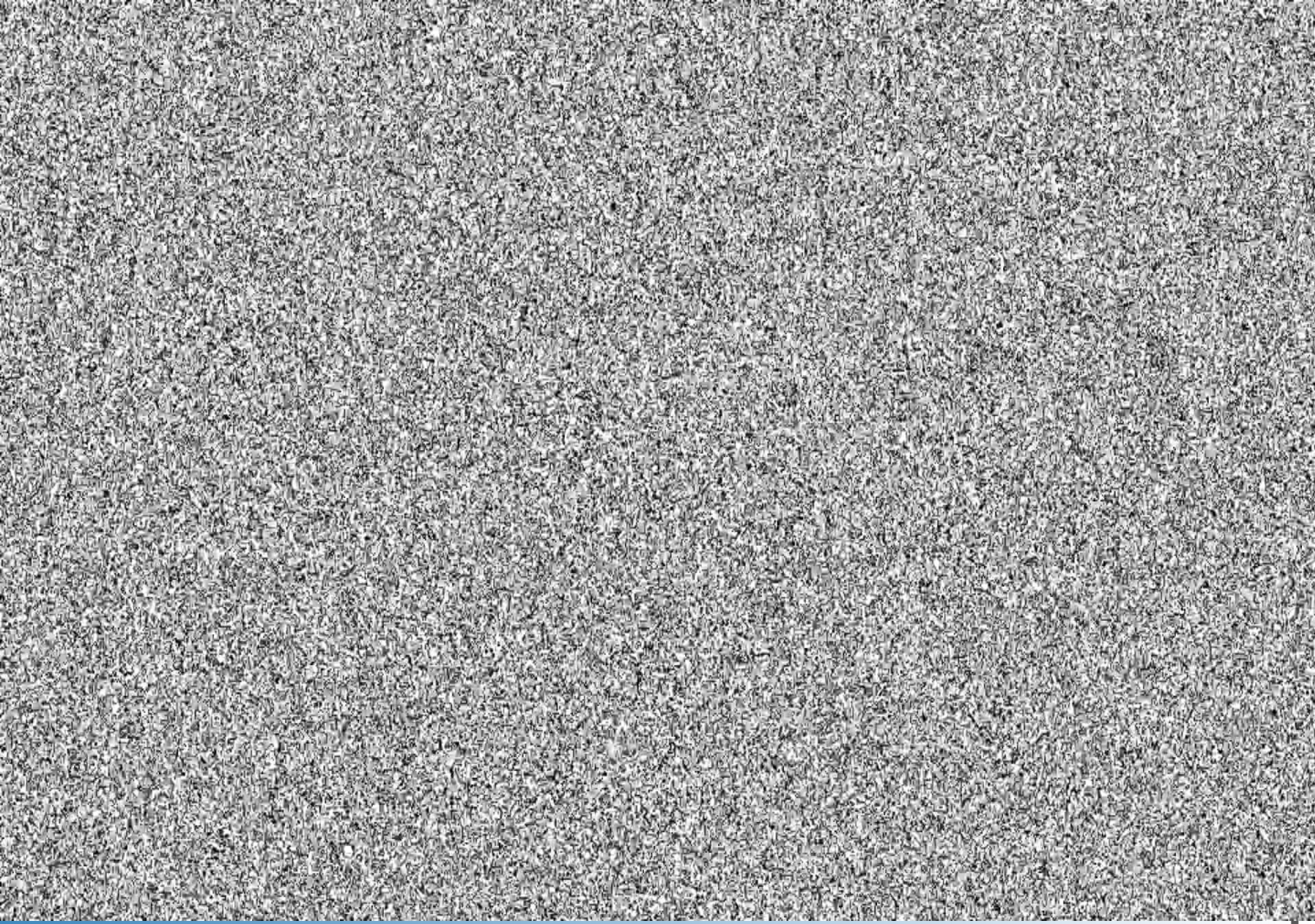
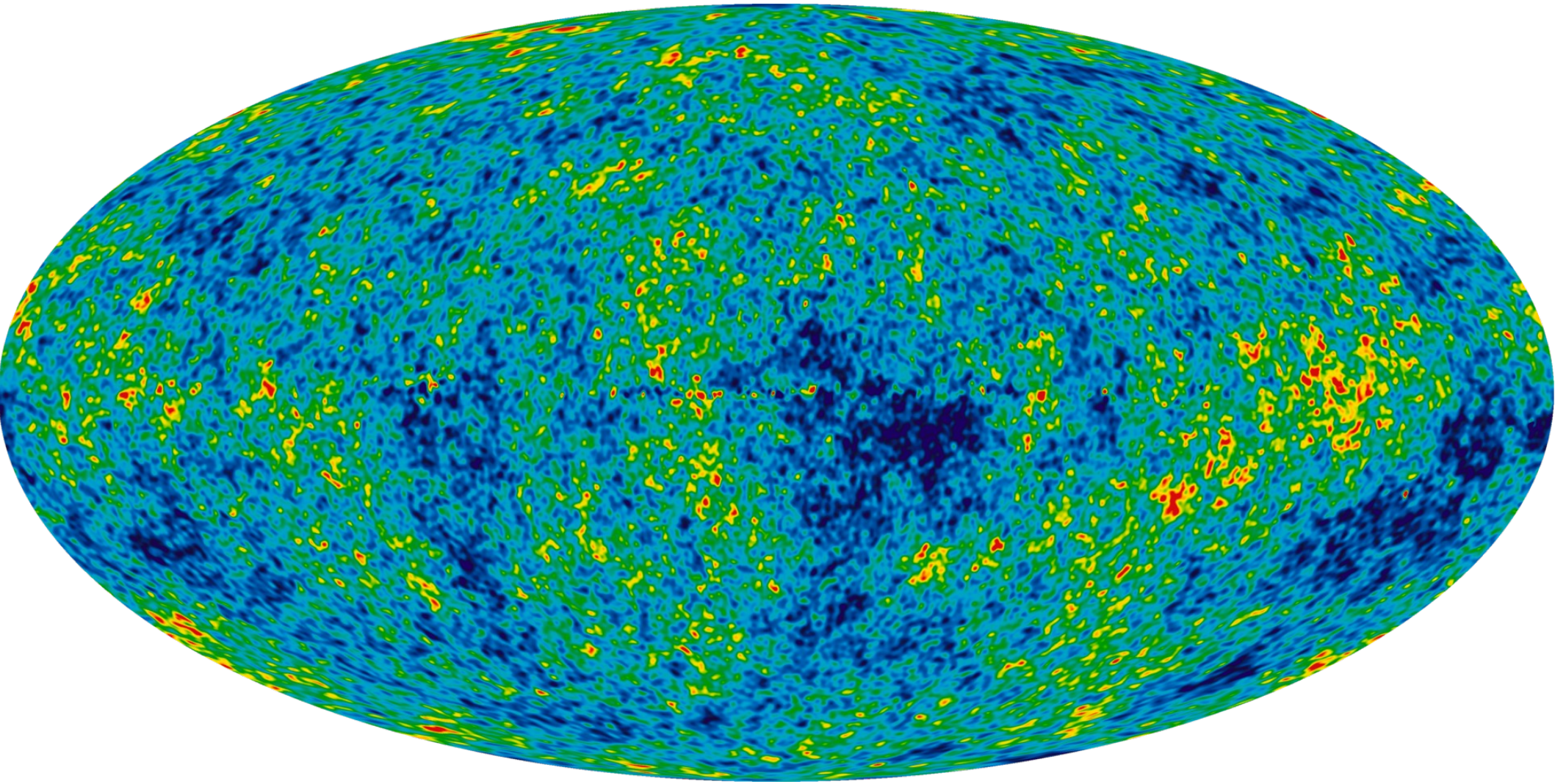
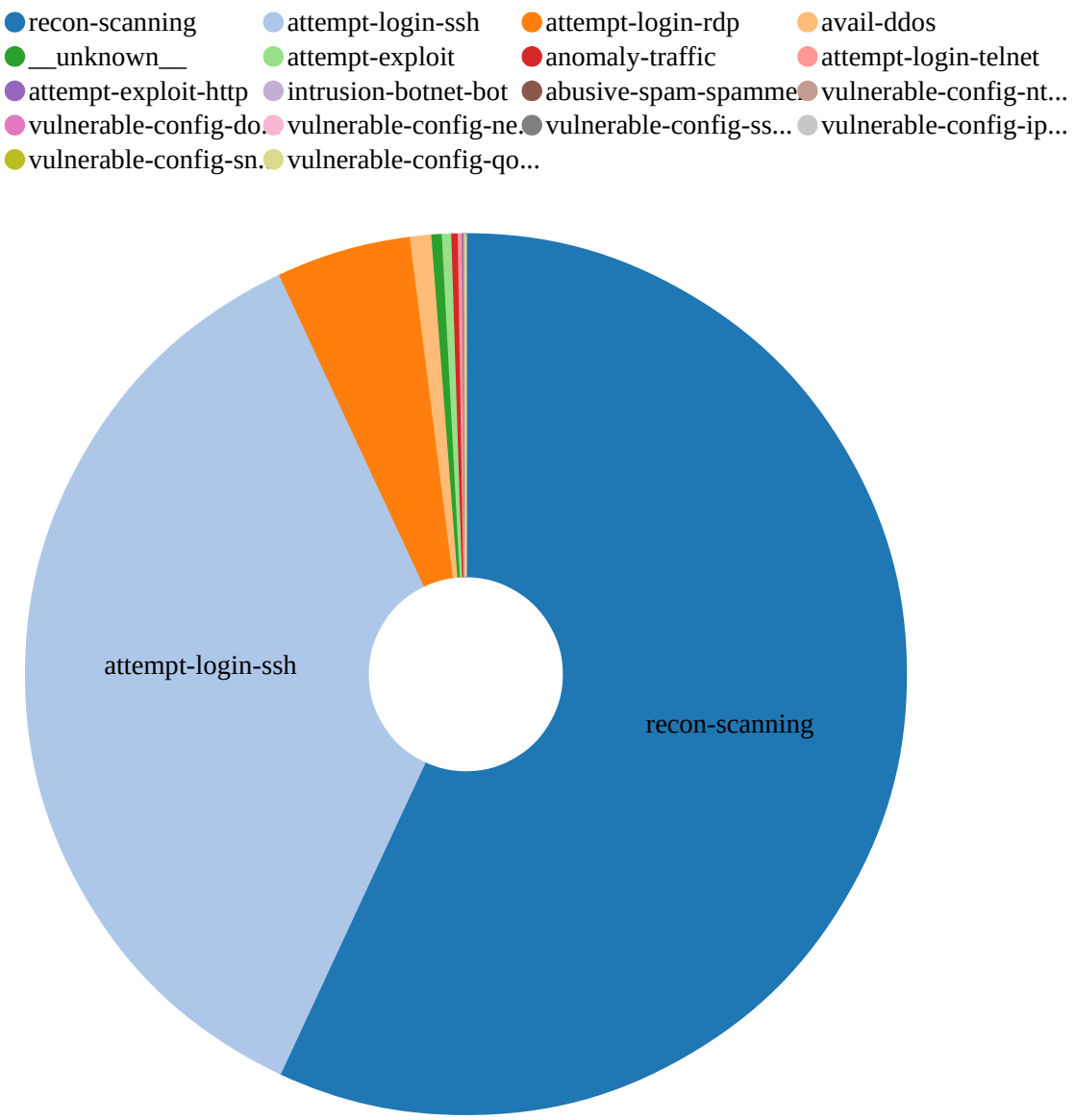
fail2ban

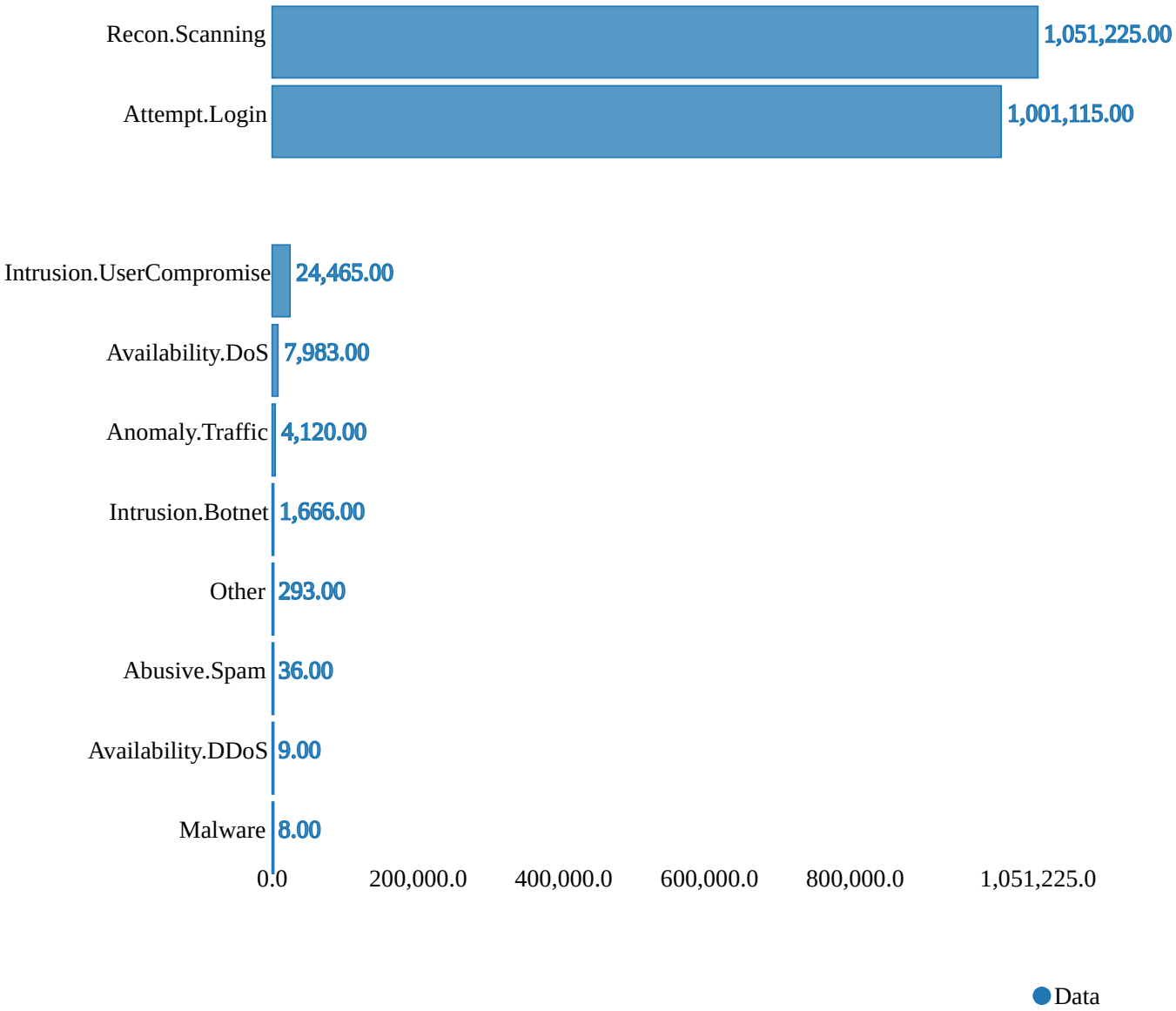
Jak na statický šum internetu?

Pavel Kácha
ph@cesnet.cz






recon-scanning
attempt-login-ssh
attempt-login-rdp
avail-ddos
__unknown__
attempt-exploit
anomaly-traffic
attempt-login-telnet
attempt-exploit-http
intrusion-botnet-bot
abusive-spam-spamme...
vulnerable-config-nt...
vulnerable-config-do...
vulnerable-config-ne...
vulnerable-config-ss...
vulnerable-config-ip...
vulnerable-config-sn...
vulnerable-config-qo...
attempt-login-ssh
recon-scanning


Recon.Scanning
1,051,225.00
Attempt.Login
1,001,115.00
Intrusion.UserCompromise
24,465.00
Availability.DoS
7,983.00
Anomaly.Traffic
4,120.00
Intrusion.Botnet
1,666.00
Other
293.00
Abusive.Spam
36.00
Availability.DDoS
9.00
Malware
8.00
0.0
200,000.0
400,000.0
600,000.0
800,000.0
1,051,225.0
Data

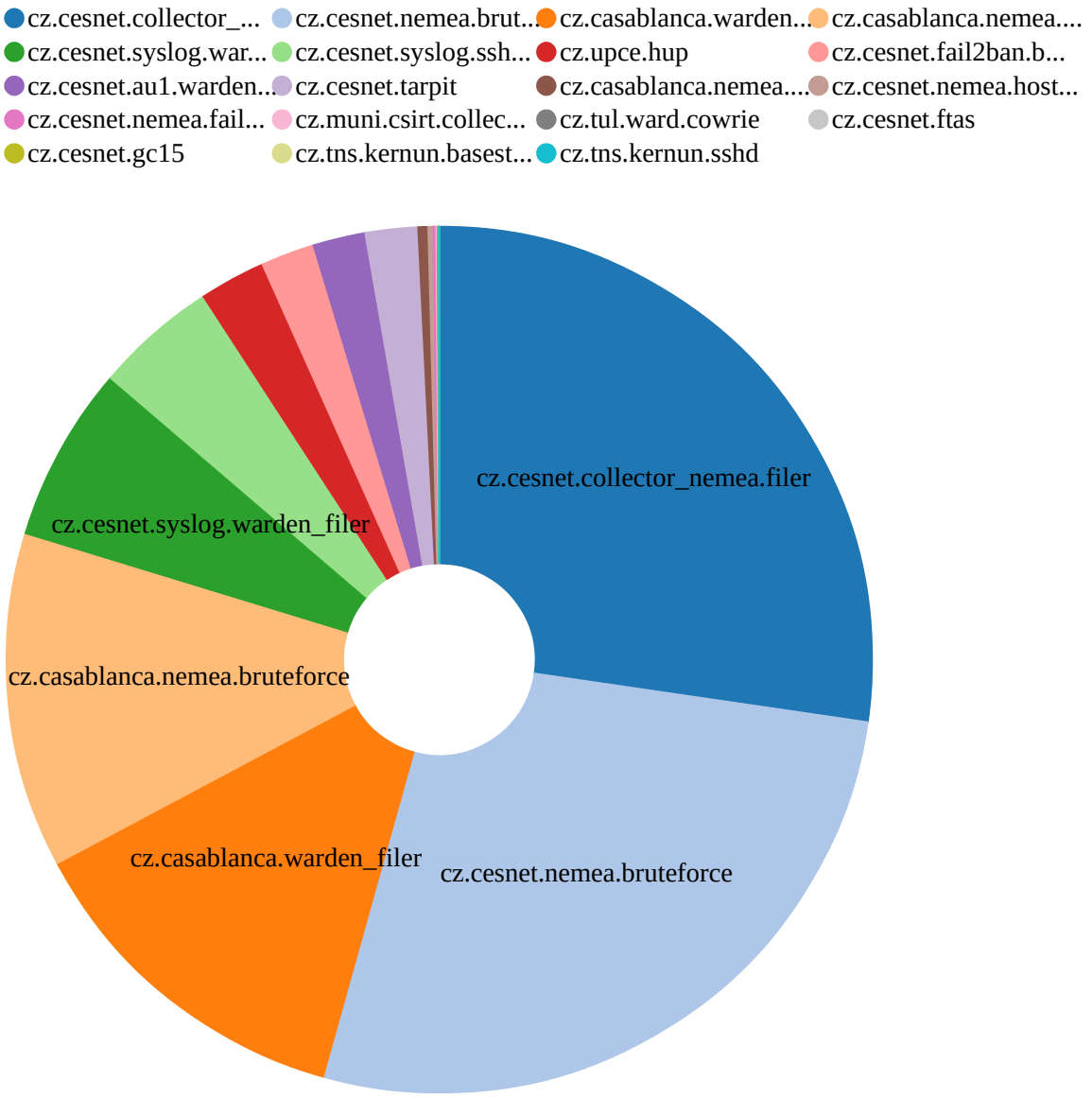
Feb 8 13:42:47 mucholapka sshd[17235]:
Invalid user appserver from 175.106.82.81 port 57742

Feb 8 13:42:48 mucholapka sshd[17235]:
Received disconnect from 175.106.82.81 port 57742:11: Bye Bye [preauth]

Feb 8 13:42:48 mucholapka sshd[17235]:
Disconnected from invalid user appserver 175.106.82.81 port 57742 [preauth]

Feb 8 13:42:48 fail2ban.actions[3661]:
NOTICE [sshd-from-mc] Ban 175.106.82.81

```
{
   "Category": ["Attempt.Login"],
   "DetectTime": "2021-02-08T13:56:40.116798Z",
   "Format": "IDEA0",
   "ID": "d102a152-c422-42a2-9c14-43cc60388586",
   "Description": "SSH dictionary/bruteforce attack",
   "Note": "Banned by fail2ban",
   "Source": [
      {
         "IP4": ["175.106.82.81"],
         "Port": [30394],
         "Proto": ["tcp", "ssh"]
      }
   ],
   "Node": [
      {
         "Name": "cz.cesnet.cool.detector",
         "Type": ["Connection", "Auth", "Statistical"]
      }
   ]
}
```


cz.cesnet.collector_...
cz.cesnet.nemea.brut...
cz.casablanca.warden...
cz.casablanca.nemea....
cz.cesnet.syslog.war...
cz.cesnet.syslog.ssh...
cz.upce.hup
cz.cesnet.fail2ban.b...
cz.cesnet.au1.warden...
cz.cesnet.tarpit
cz.casablanca.nemea....
cz.cesnet.nemea.host...
cz.cesnet.nemea.fail...
cz.muni.csirt.collec...
cz.tul.ward.cowrie
cz.cesnet.ftas
cz.cesnet.gc15
cz.tns.kernun.basest...
cz.tns.kernun.sshd
cz.cesnet.collector_nemea.filer
cz.cesnet.syslog.warden_filer
cz.casablanca.nemea.bruteforce
cz.casablanca.warden_filer
cz.cesnet.nemea.bruteforce

Děkuji za pozornost.

warden-info@cesnet.cz

SABU:	https://sabu.cesnet.cz/
Warden:	https://warden.cesnet.cz
Mentat:	https://mentat.cesnet.cz/
IDEA:	https://idea.cesnet.cz