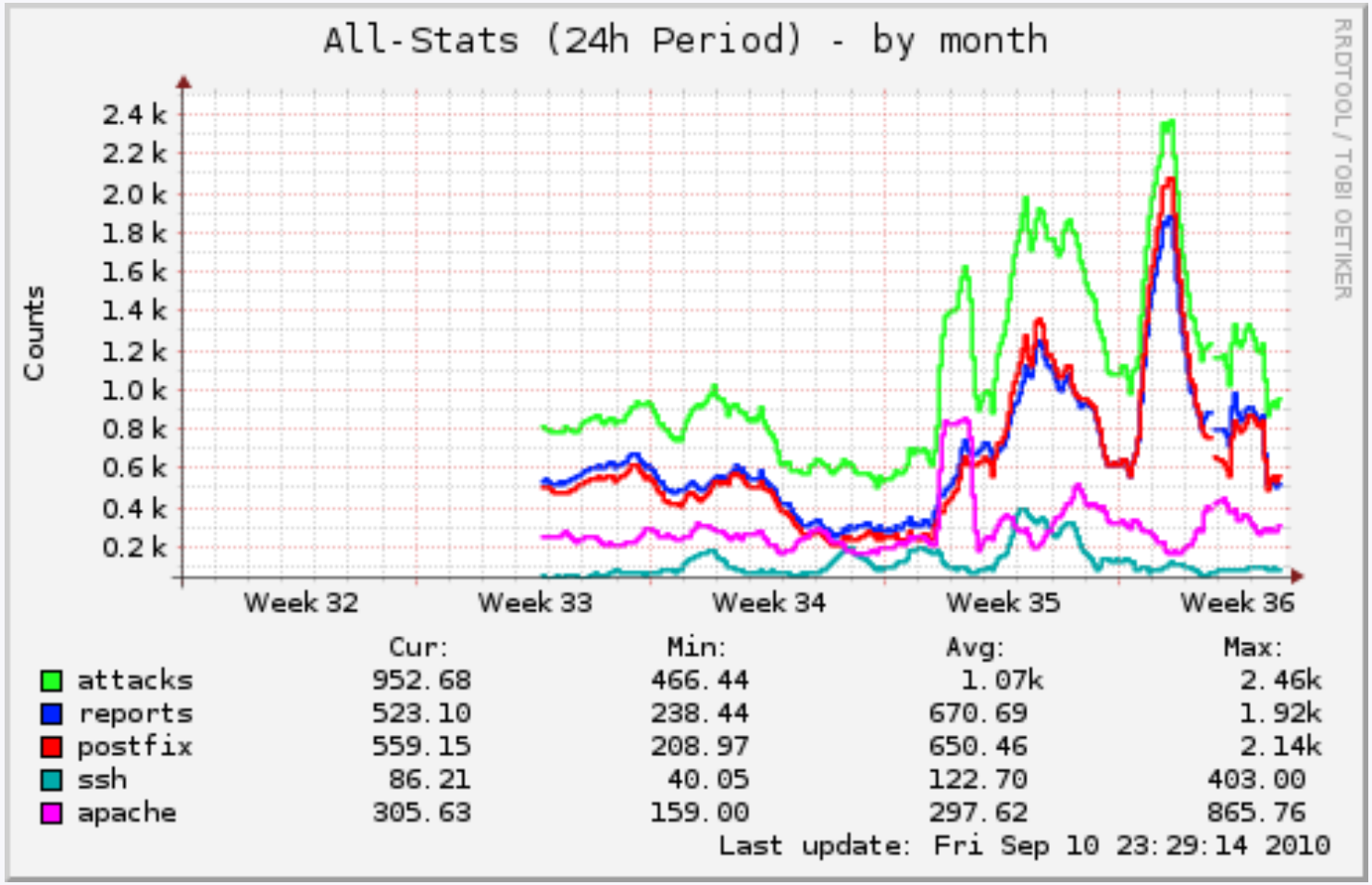
X-ARF Reports von blocklist.de

1. Was ist blocklist.de?
2. Warum blocklist.de (Vorteile)?
3. X-ARF allgemein
4. Generierung von X-ARF Reports
5. Mögliche Verarbeitung

1. Was ist blocklist.de?

- Freier Service zum melden von Attacken
- Prüft Fail2Ban-Mails auf benötigte Daten
- Statistiken pro Server/User und im Vergleich
- Vergleichbar mit spamcop.net für Angriffe
- Download der bösen IP‘s
- Kostenlos

1. Was ist blocklist.de?



2. Warum blocklist.de (Vorteile)?

- Reports werden nur alle 24 Stunden gesendet
- Alternative Abuse-Adresse möglich (abusix.org)
- Blacklisting von Empfängern
- Whitelisting von angreifenden IP‘s
- Reports in X-ARF
- Vollautomatische Verarbeitung
- Anonymisierung individuell/automatisch möglich

3. X-ARF allgemein

- X-ARF = Network Abuse Reporting 2.0
- X-ARF ist ein E-Mailformat , baut auf ARF auf
- Einfach zu lesen (Maschine & Menschen)
- Schnell erweiterbar durch neue Schema
- Offen und kostenlos
- Einfach zu generieren und zu parsen

4. Generierung von X-ARF Reports

- Haupt-Category finden: abuse, fraud, auth…
- Report-Type finden: login-attack, harvesting….
- Header: Auto-Submitted, X-ARF: yes
- Yaml-Report nach Schema erstellen
- Body mit Anhängen und Logs erstellen
- Versenden

5. Mögliche Verarbeitung

- Prüfen ob „X-ARF: yes“ im Header
- Yaml-Report laden und gegen Schema validieren
- Werte auslesen und bewerten -> Report-Type:
  - login-attack (alleine 50P)
  - malware (25P) + reported-from: x@xyz.tld (100P)
- Max-Punkte erreicht? Kunden informieren.

5. Mögliche Verarbeitung

```
Auto-Submitted: auto-generated
Content-Transfer-Encoding: 7bit
Content-Type: multipart/mixed;
        boundary="Abuse-9659d956f8b3694965099d0f98f1371a";
X-Arf: yes
X-Report-ID: 190000
Message-Id: <20100910225109.667321801E0F@server5.customer-config.de>
Date: Sat, 11 Sep 2010 00:51:09 +0200 (CEST)
```

```
---
Reported-From: autogenerated@blocklist.de
Category: abuse
Report-Type: login-attack
Service: rfi-attack
```

Fragen und Beispiel

- Beispiele zum generieren und verarbeiten:
  http://www.x-arf.org/tools.html
  – Generierung-> genxarf-php.tar.gz
  – Validierung -> validatexarf-php.tar.gz

- Fragen zu X-ARF, blocklist.de oder Fail2Ban?