SSH-Angreifern mit Honeypots über die Schulter schauen

Andreas Bunten <andreas.bunten@controlware.de>
Torsten Voss <voss@dfn-cert.de>

Agenda

- SSH Account Probes
- Was ist ein Honeypot?
- Vorgehen der Angreifer
- Erkennen der Malware
- Erkennen der Angreifer
- Zusammenfassung
- Wie schütze ich mich?

Andreas Bunten
Torsten Voss

SSH Account Probes

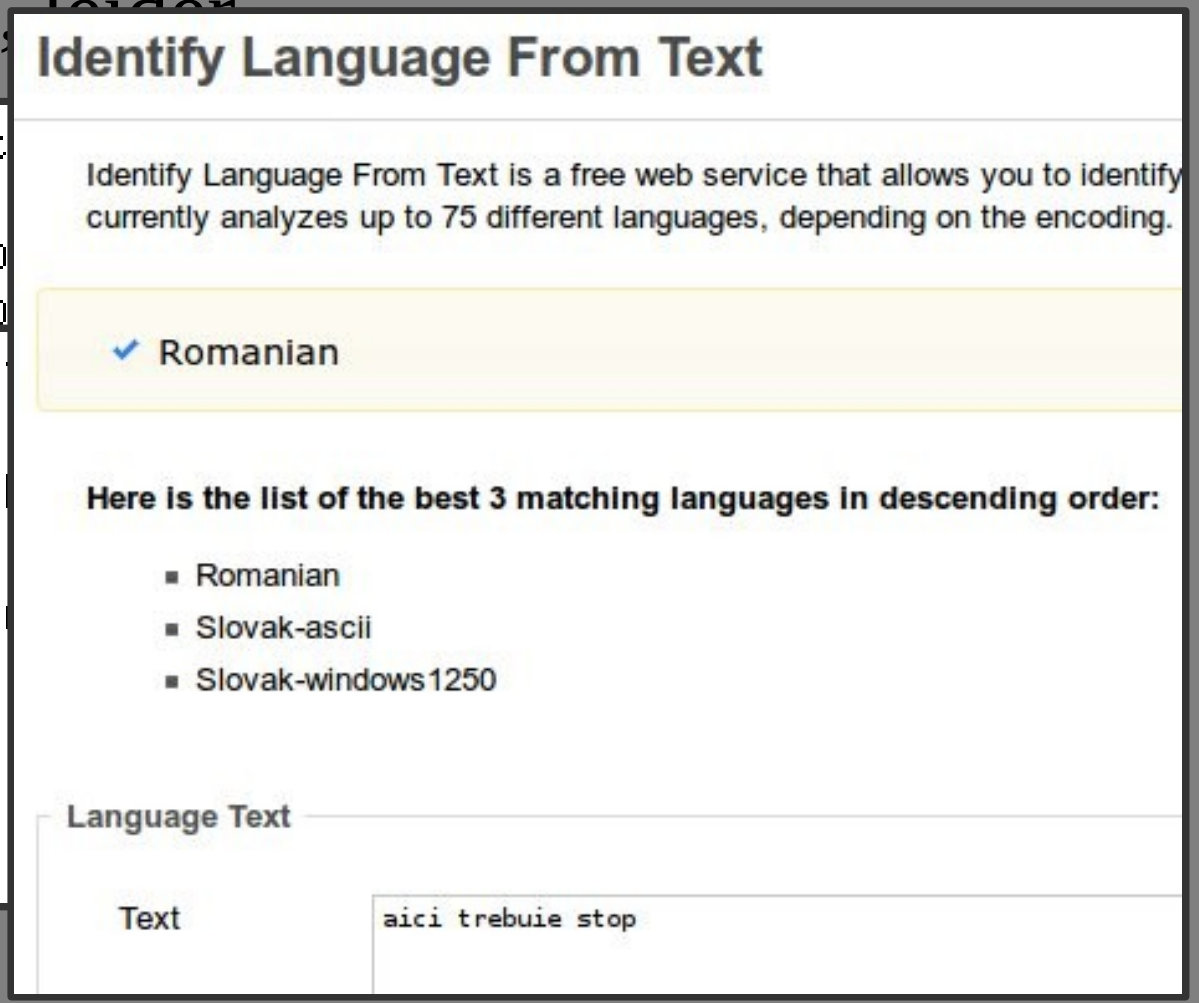
- Passwort-Rate-Angriff / Brute-Force-Angriff / ...
- Ist das normal? Ja, leider.
- Warum ist das interessant?
  - Wir sehen immer wieder die gleichen Angriffs-Tools
  - Es scheinen sehr oft die gleichen Angreifer zu sein

SSH Account Probes

- Passwort-Rate-Angriff / Brute-Force-Angriff / ...
- Ist das normal? Ja, leider

```
root@fileserver:/var/www/ht
total 1380
drwxr-xr-x 2 root root   40
drwxr-xr-x 4 root root   40
-rwxr
-rw-r
-rwxr
-rwxr
-rwxr
-rwxr
-rwxr
```

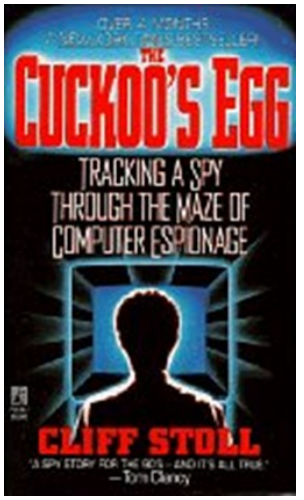
```
root@fileserver:/va
echo -e "\033[1;36m
./ss 22 -a $1 -i et
cat bios.txt |sort
oopsnr2=`grep -c .
echo "  "
echo "# $oopsnr2 ip
./ssh-scan 150
rm -rf bios.txt mfu
```



SSH Account Probes (II)

- Passwort-Rate-Angriff / Brute-Force-Angriff / ...
- Ist das normal? Ja, leider.
- Warum ist das interessant?
  - Wir sehen immer wieder die gleichen Angriffs-Tools
  - Es scheinen sehr oft die gleichen Angreifer zu sein
- Wir haben da ein paar Fragen ...
  - Sind das wirklich nur wenige Gruppen?
  - Kommen die alle aus Ost-Europa?
  - Was wollen die mit meinem System machen?
  - Wie kann ich mich besser schützen?

Was ist ein Honeypot?

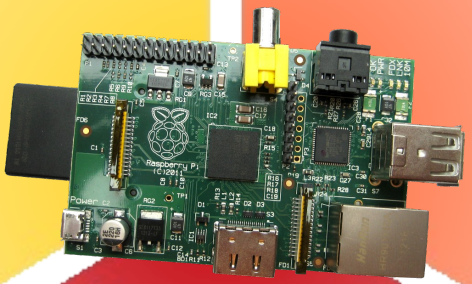


- „The Cuckoo's Egg“ - Clifford Stoll (1990)
- Angreifer verbinden sich zum Honeypot System und werden beobachtet
- „*A honeypot is a ressource whose value lies in it's illicit use.*“ - Lance Spitzner
- Es gibt verschiedene Typen von Honeypots
- Honeypots galten nach 2000 nicht als modern
- Werden aber durchgehend für Forschung eingesetzt
- Neue Popularität u.a. durch ENISA & auch für Firmen

Welche Honeypots verwenden wir?

Low Interaction

- Mini-Appliances
- Debian
- Protokolliert Anmeldeversuche



Virtual Honeypot

- Software Kippo
- Simuliert Linux System
- Anmeldung und etwas Interaktion möglich

High Interaction

- Modifiziertes reales System
- Angreifer erhält volle Kontrolle

Beispiel

```
TIME: 2013-02-18 12:57:59
OFFENDER IP: 223.4.
SENSOR ID: 12
SENSOR IP: 217.239.
BELEG1: Feb 18 12:57:59 skipper sshd[28366]: Failed password for invalid user apache from 2
BELEG2: Feb 18 12:58:02 skipper sshd[28369]: Failed password for invalid user sys from 223.
BELEG3: Feb 18 12:58:05 skipper sshd[28371]: Failed password for invalid user root from 223
COUNT ACCOUNTS: 96
COUNT TRIALS: 162
COUNT CONNECTS: 162
TRIAL PER CONNECT: 1
CLIENT ID: SSH-2.0-libssh-0.1
CLIENT ID UNIQUE: 1
KEX: diffie-hellman-group1-sha1
KEX HOST KEY: ssh-rsa
KEX ENC: aes128-cbc
KEX MAC: hmac-sha1
KEX COMP: none
KEX LANG:
TRIAL: 2013-02-18 12:57:59|apache|test123|0
TRIAL: 2013-02-18 12:58:02|sys|sys|0
TRIAL: 2013-02-18 12:58:05|root|root|0
TRIAL: 2013-02-18 12:58:08|share|share|0
TRIAL: 2013-02-18 12:58:10|root|admin|0
```

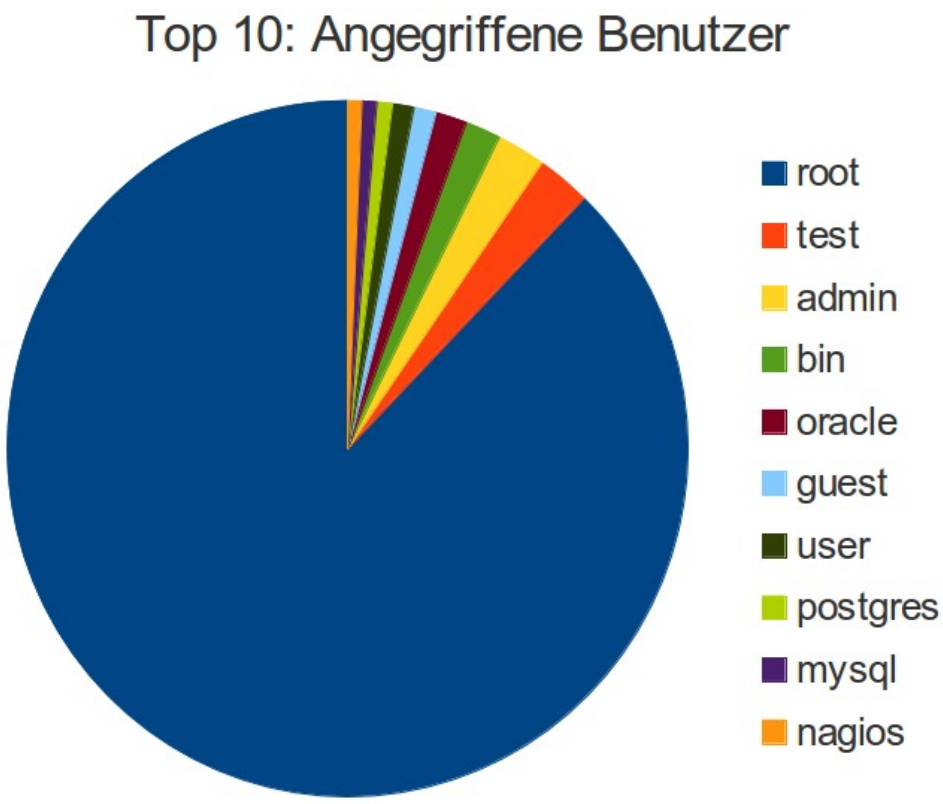
Beispiel (II)

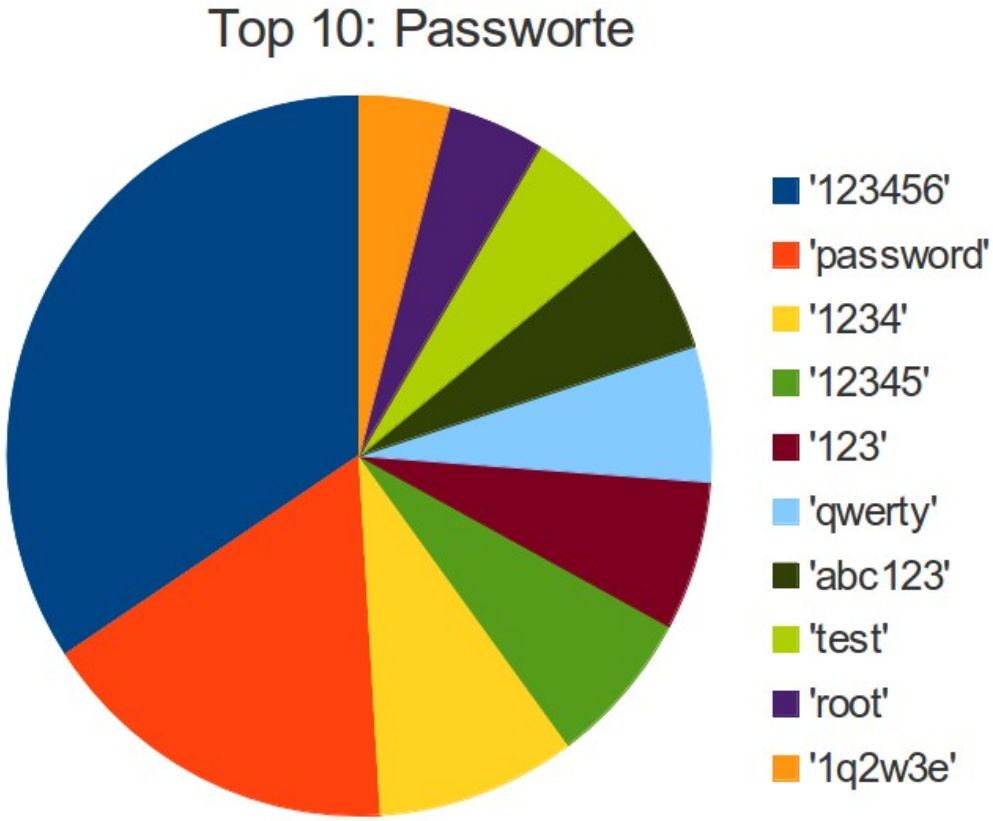
```
Welcome to XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX i686)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
root@fileserver:~# w
 01:12:41 up 2 days,  4:20,  1 user,  load average: 0,00, 0,01, 0,05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/2    XX.XXX.XXX.XXX   01:12    0.00s  0.43s  0.01s w
root@fileserver:~# asterisk -r
Die Anwendung »asterisk« ist momentan nicht installiert.  Sie können sie
olgende Eingabe installieren:
apt-get install asterisk
root@fileserver:~#
```


Andreas Bunten
Torsten Voss

Vorgehen der Angreifer

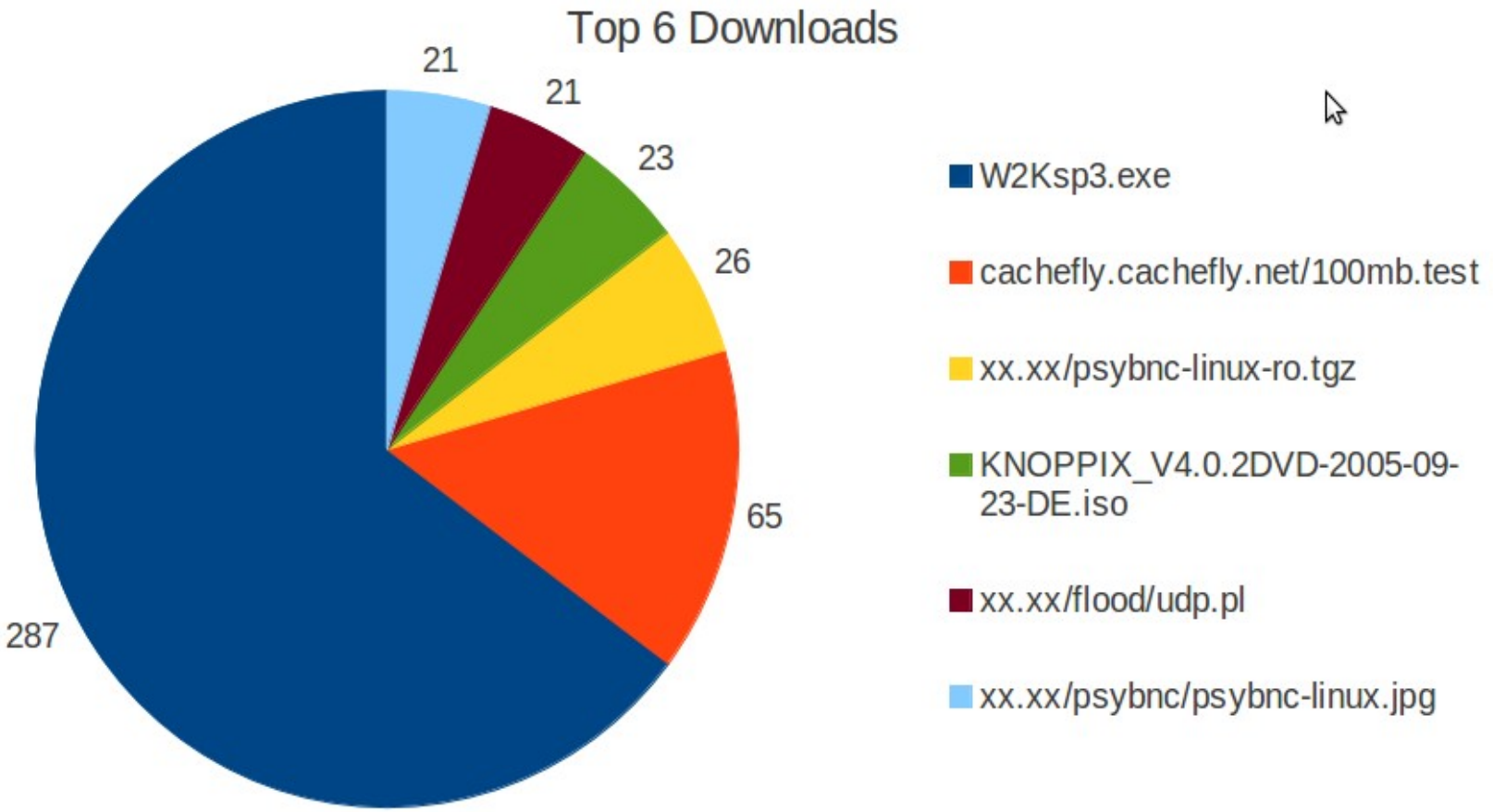
- 602698 Anmeldeversuche in 1909 Angriffen
- Typischerweise < 30 Versuche pro Angriff





Vorgehen der Angreifer (II)

- Meistens wird ein Test-Download durchgeführt



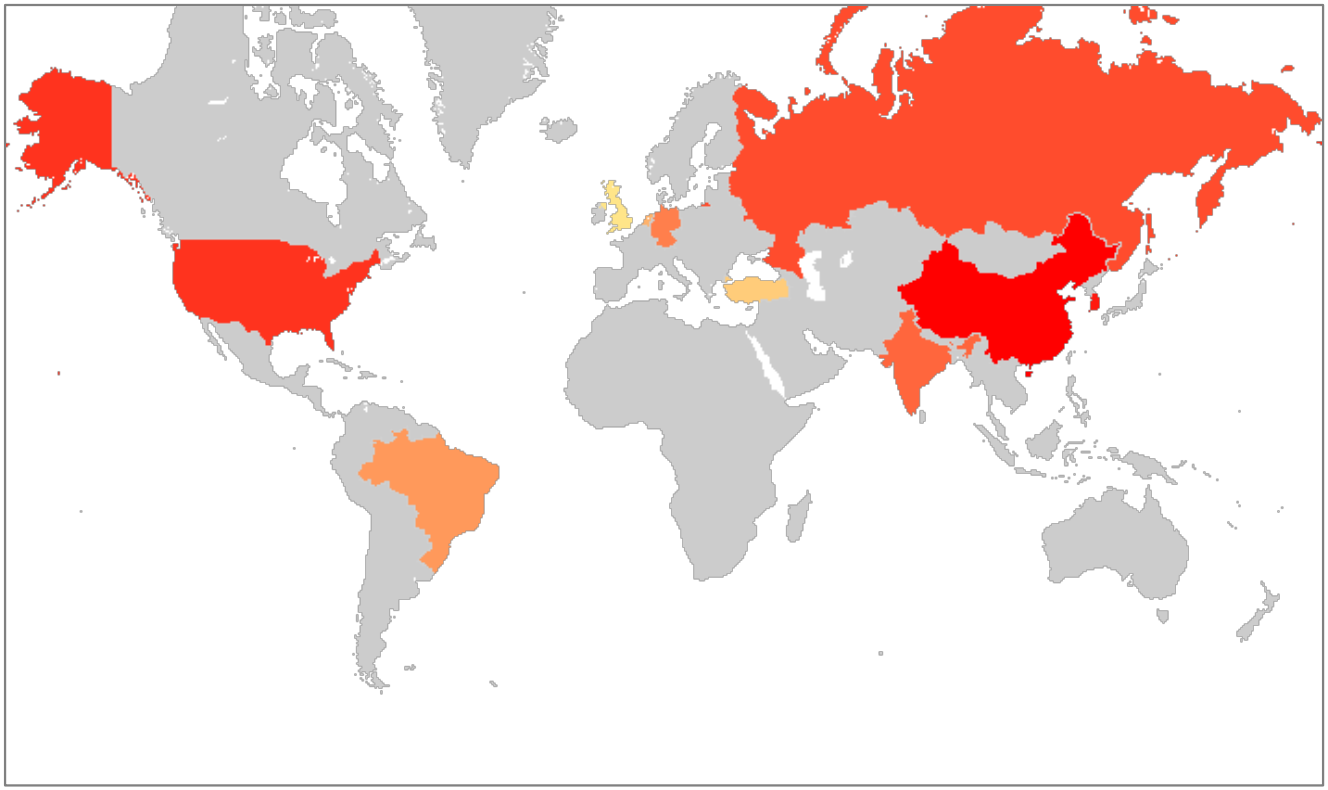
- Seltsame Downloads: Teamspeak, HL Gameserver, ...

Vorgehen der Angreifer (III)

- Standard-Vorgehen:
  - Brute Force Angriff von kompromittiertem Server
  - Interaktive Session später von anderer IP-Adresse

Brute Force Angriffe:

#	CC
1	China
2	Korea
3	USA
4	Russland
5	Indien
6	Deutschland
7	Brasilien
8	Niederlande
9	Türkei
10	Großbritanien

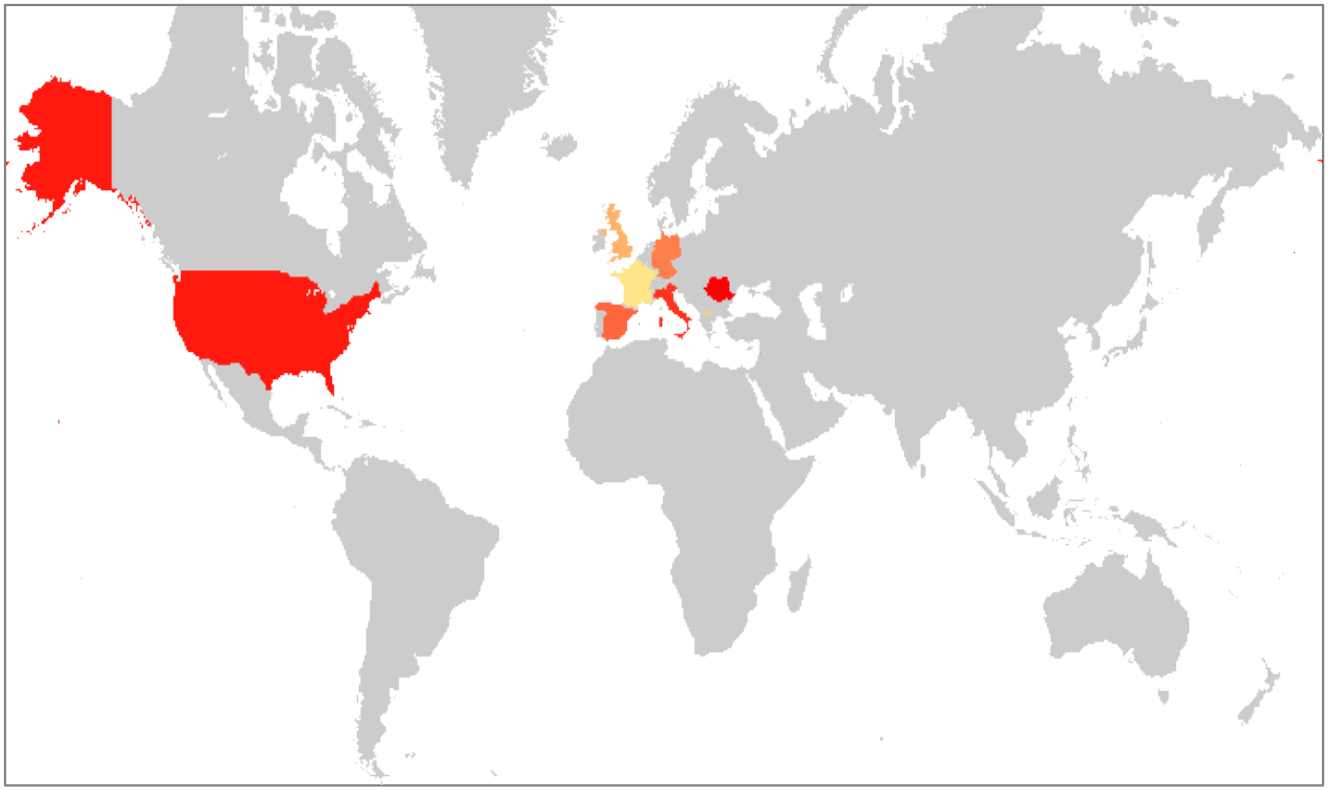


Vorgehen der Angreifer (IV)

- Standard-Vorgehen:
  - Brute Force Angriff von kompromittiertem Server
  - Interaktive Session später von anderer IP-Adresse

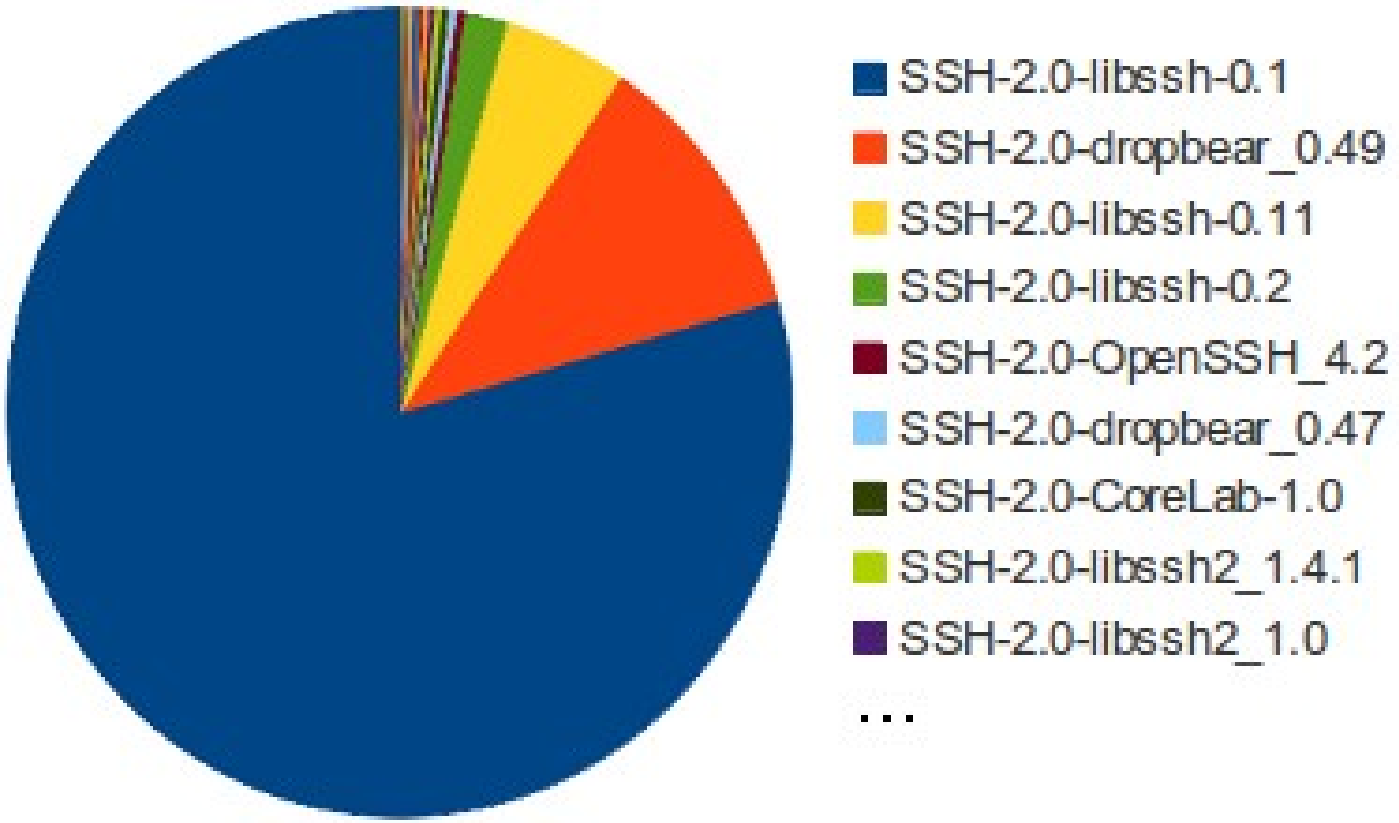
Interaktive Sessions:

#	CC
1	Rumenien
2	USA
3	Italien
4	„Europa“
5	Spanien
6	Deutschland
7	Libanon
8	Großbritannien
9	Mazedonien
10	Frankreich

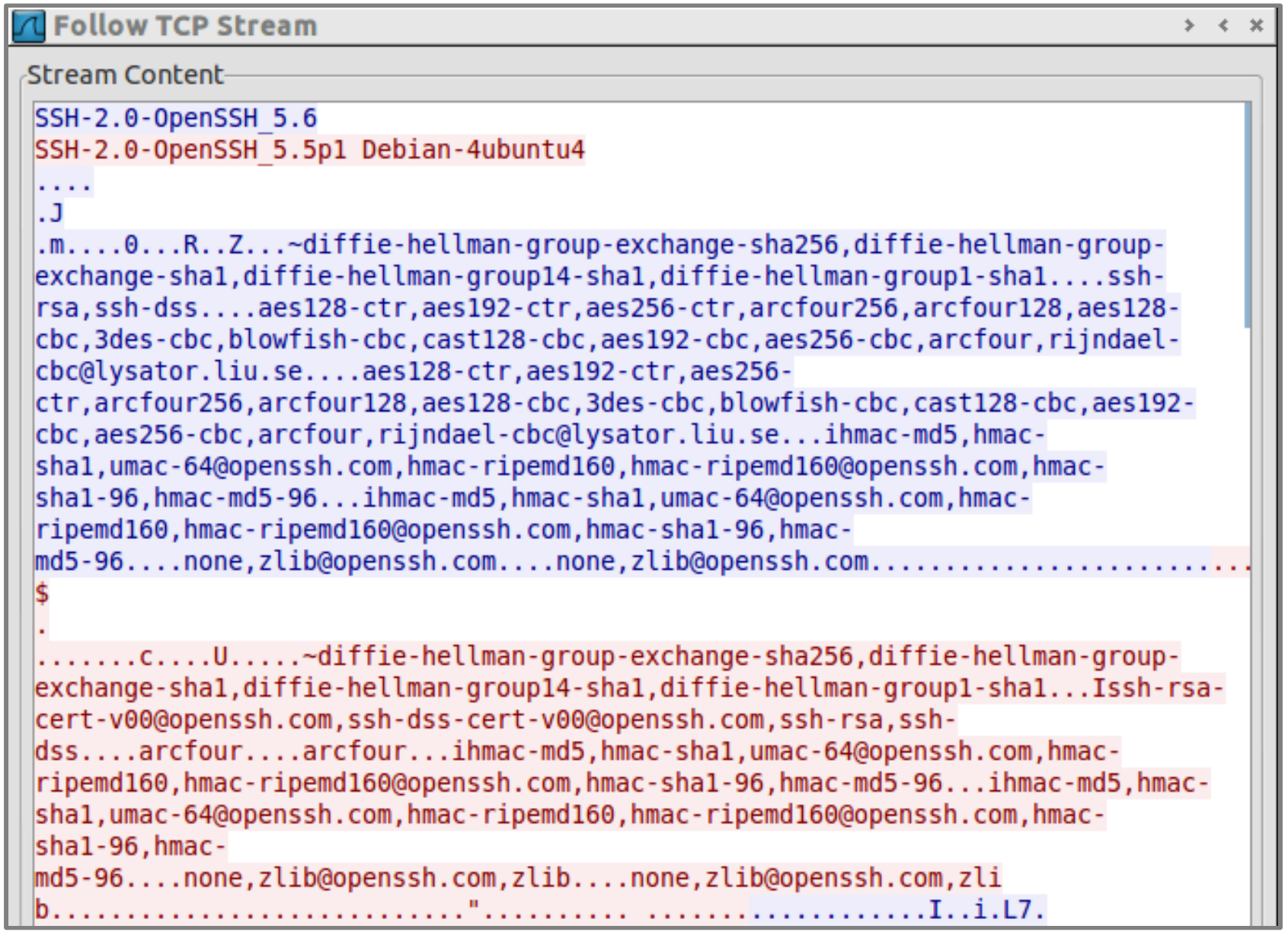


Erkennen der Malware

- Die Angreifer verwenden häufig das selbe Werkzeug
- Verteilung Client-IDs



Erkennen der Malware



Erkennen der Malware

```
TIME: 2013-02-18 12:57:59
OFFENDER IP: 223.4.
SENSOR ID: 12
SENSOR IP: 217.239.
BELEG1: Feb 18 12:57:59 skipper sshd[28366]: Failed password for invalid user apache from
BELEG2: Feb 18 12:58:02 skipper sshd[28369]: Failed password for invalid user sys from 223
BELEG3: Feb 18 12:58:05 skipper sshd[28371]: Failed password for invalid user root from 22
COUNT ACCOUNTS: 96
COUNT TRIALS: 162
COUNT CONNECTS: 162
TRIAL PER CONNECT: 1
CLIENT ID: SSH-2.0-libssh-0.1
CLIENT ID UNIQUE: 1
KEX: diffie-hellman-group1-sha1
KEX HOST KEY: ssh-rsa
KEX ENC: aes128-cbc
KEX MAC: hmac-sha1
KEX COMP: none
KEX LANG:
TRIAL: 2013-02-18 12:57:59|apache|test123|0
TRIAL: 2013-02-18 12:58:02|sys|sys|0
TRIAL: 2013-02-18 12:58:05|root|root|0
TRIAL: 2013-02-18 12:58:08|share|share|0
TRIAL: 2013-02-18 12:58:10|root|admin|0
```

Erkennen der Malware

- Die Client-ID korreliert mit KEX-Werten
- Anwendungen
  - IDS-Regel für verdächtige Client-IDs & KEX-Werte
  - Abbruch der Verbindung, bei zusätzlichem Verdacht (mehrfache Anmeldeversuche, seltsame Quell-IP, …)
- Nachteile
  - Client-ID alleine kann gefälscht werden
  - False Positives möglich bei ungewöhnlichen Clients

Erkennen der Angreifer

- Gängiges Vorgehen
  - Angreifer anhand vieler Fehlversuche erkennen
  - Sperren von IP-Adresen bekannter Angreifer
  - Beispiel: Projekt DenyH0STS
- Nachteile
  - Manche Angreifer wechseln ihre IP-Adresse
  - Aussperren legitimer Benutzer nach IP-Wechsel
  - Wurde Server bereinigt verbleibt seine IP auf Sperrliste

Erkennen der Angreifer

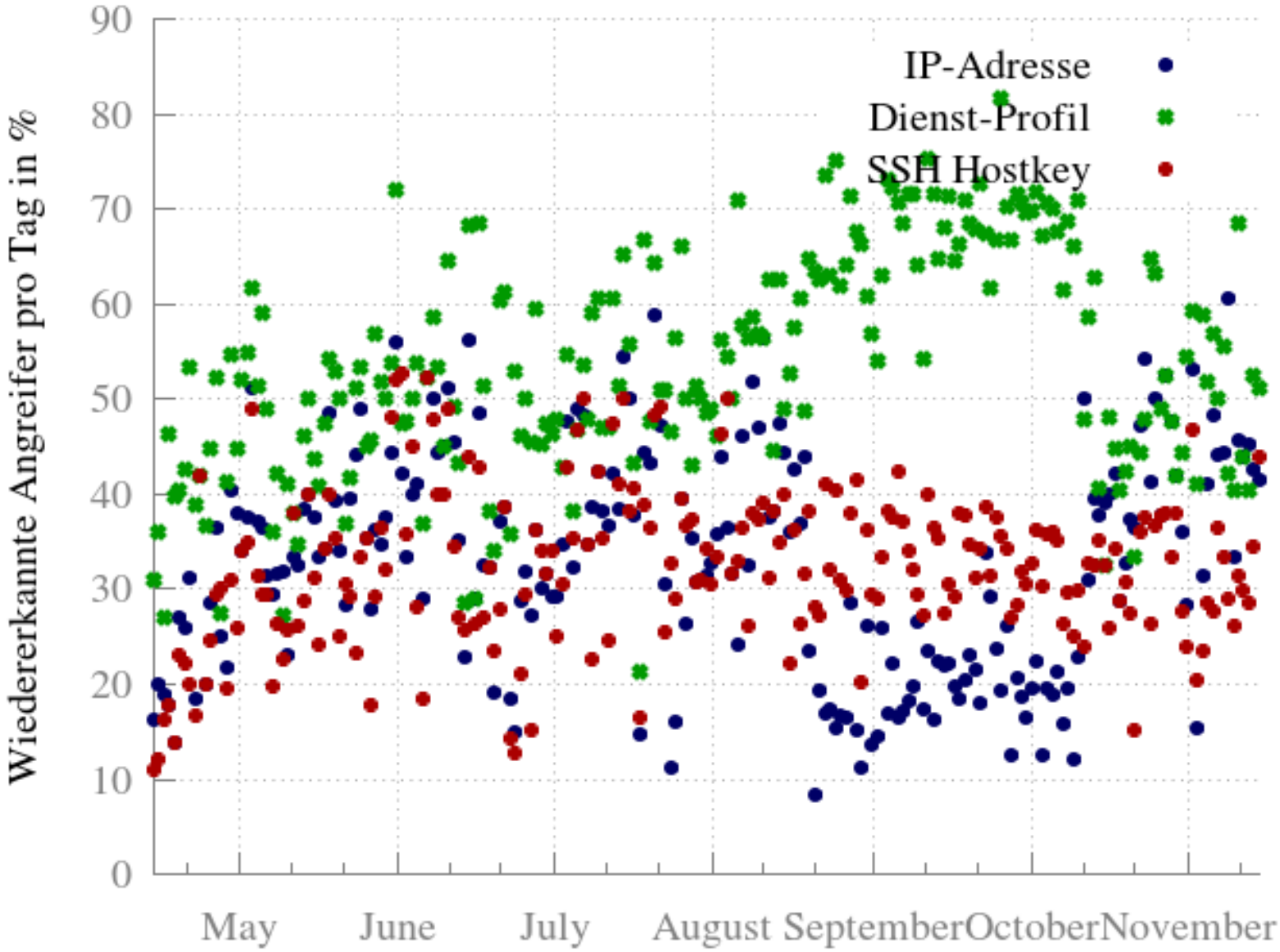
- Alle Angreifer wurden Port Scans unterzogen

```
Host is up (0.17s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE         VERSION
22/tcp    open  ssh             OpenSSH 4.3p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey: 2048 7a:9c:5d:1a:0b:75:84:1e:9f:fe:66:7a:5a:0f:f3:9e (RSA1)
| 1024 56:01:92:06:db:c2:8a:2d:8a:3f:9f:e9:ee:8f:41:96 (DSA)
|_2048 02:b6:2a:e7:b3:84:be:46:05:fa:fc:0b:ea:d5:06:40 (RSA)
80/tcp    open  http            Apache Tomcat/Coyote JSP engine 1.1
| http-methods: GET HEAD POST PUT DELETE TRACE OPTIONS
| Potentially risky methods: PUT DELETE TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: VOS3000
111/tcp   open  rpcbind
1300/tcp  open  h323hostcallsc?
1720/tcp  open  H.323/Q.931?
2000/tcp  open  cisco-sccp?
3306/tcp  open  mysql           MySQL (unauthorized)
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
```

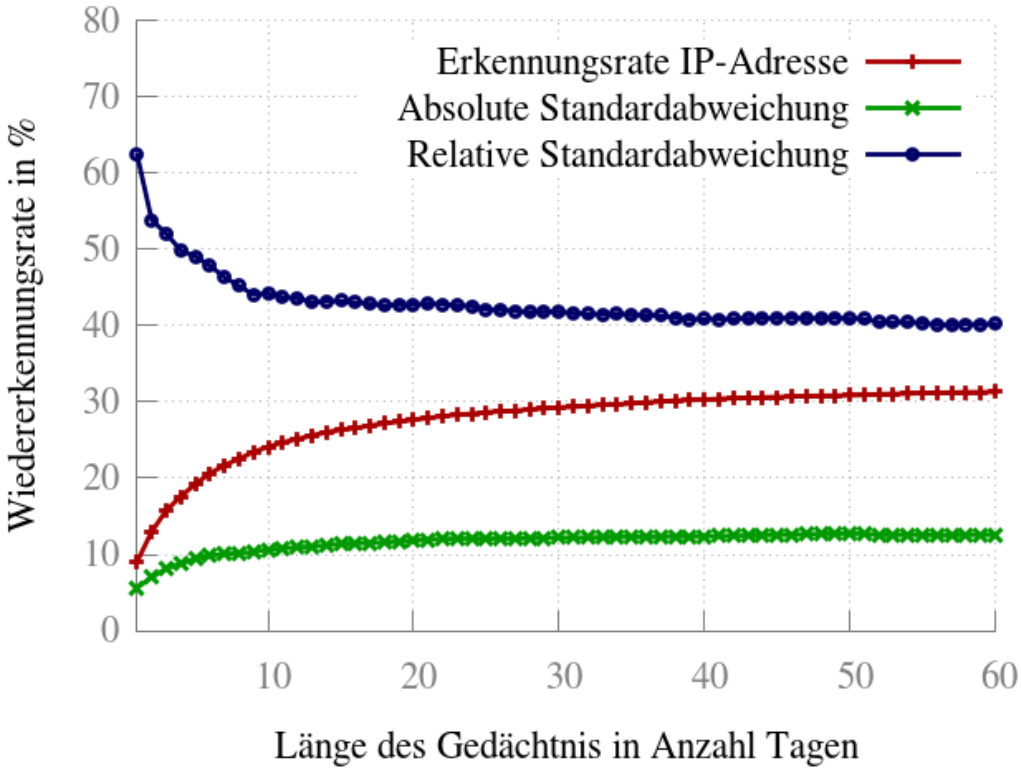
Erkennen der Angreifer

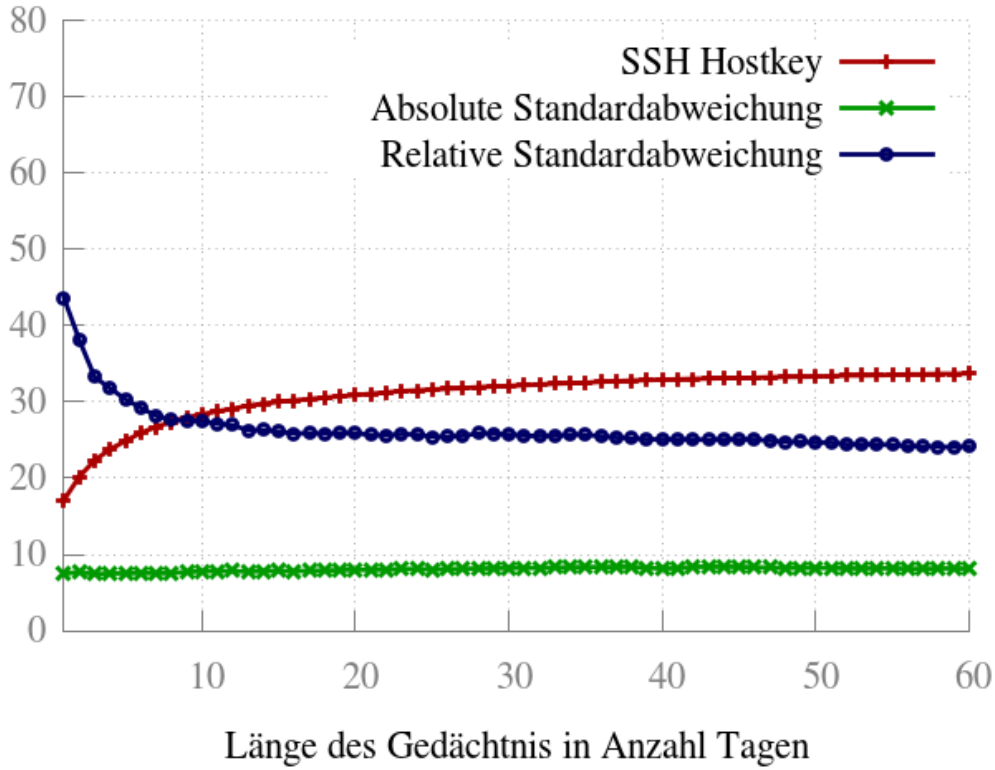
- Was eignet sich als Erkennungsmerkmal?
  - IP-Adresse **116.55.XXX.XX**
  - Dienst-Profil **22/tcp:open|80/tcp:open|111/tcp:open|443/tcp:open**
  - SSH Hostkey **e2:11:ee:0a:0a:28:02:ff:90:b4:25:55:df:41:17:ce**
- Test der Merkmale anhand von 12.858 Angriffen
  - Wieviele Angreifer können wiedererkannt werden?
  - Wie lang sollten Merkmale aufgehoben werden?
- Dienst-Profile ergeben leicht False Positives
  - Viele Angreifer haben nur Port 22 TCP geöffnet

Erkennen der Angreifer



Erkennen der Angreifer





- Gemittelte Erkennungsraten zeigen Unterschied
  - Hostkeys: bessere Erkennungsrate / kleine Std.abweichung
  - Gedächtnis muss in keinem Fall sehr lang sein

Andreas Bunten
Torsten Voss

Erkennen der Angreifer

- Warum funktioniert das?
  - Die Angriffe stammen von kompromittierten Servern
  - Dort ist fast immer ein SSH-Dienst vorhanden
- Vorteile Erkennung per SSH Hostkeys
  - IP-Wechsel stellen kein Problem dar
  - Neuinstallation kompromittierter Server: Neuer Hostkey
  - Keine False Positives möglich

    … sagt zumindest die Intuition!

Erkennen der Angreifer

- Offene Fragen
  - Ist ein Port Scan legitim?
  - Darf man einen Back Connect zu 22/TCP durchführen?
  - Hostkeys sind leider doch nicht eindeutig
- Ausprobieren!
  - Wir liefern tägliche Liste Angreifer Hostkeys
  - Skript kann z.B. auth.log parsen
  - Alarm, falls verbindendes System auf Angreifer-Liste

Wie geht es weiter?

- Verfahren verallgemeinerbar
  - z.B. Spezialisierte Angriffe auf SSL-geschützte Dienste
- Wir können Vorfälle dennoch nicht ganz verhindern
- Woher weiß ich, dass die Angreifer schon da sind?
- Honeypots anders einsetzen
  - Nicht nur zur Generierung von Daten
  - Im Produktiv-Netz als Falle für Angreifer
  - Als Server, Client-Workstation, Daten-Verzeichnis, ...

Zusammenfassung

- Vorgehen der SSH-Angreifer ist speziell
- Zusätzlicher Schutz möglich:
  - Erkennung der Malware z.B. per Netzwerk IDS
  - Erkennung der angreifenden Systeme
- Ausprobieren!
- Unterstützung in Form von IP-Adressen!
- Honeypots bieten weitere Möglichkeiten
  - Erkennung der Angreifer egal wie der Zugriff auf das System erfolgte!

Bild: pukeycow / sxc.hu

Wie schütze ich mich?

- Starke Passworte verwenden
  - Eigentlich muss man nur dumme PW vermeiden (Black List)
- Auch SSH-Keys werden gestohlen
  - Passworte auf Key-Dateien sollten Standard sein
  - Kennen Sie „Ihre“ Keys? Sperren sollten durchsetzbar sein
- Zentrale Log-Auswertung gibt Überblick
- Scans und ausgehende Angriffe per IDS erkennen
- Kompromittierte Systeme immer neu aufsetzen
- 2-Faktor-Authentifikation löst viele SSH-Probleme!

Ressourcen

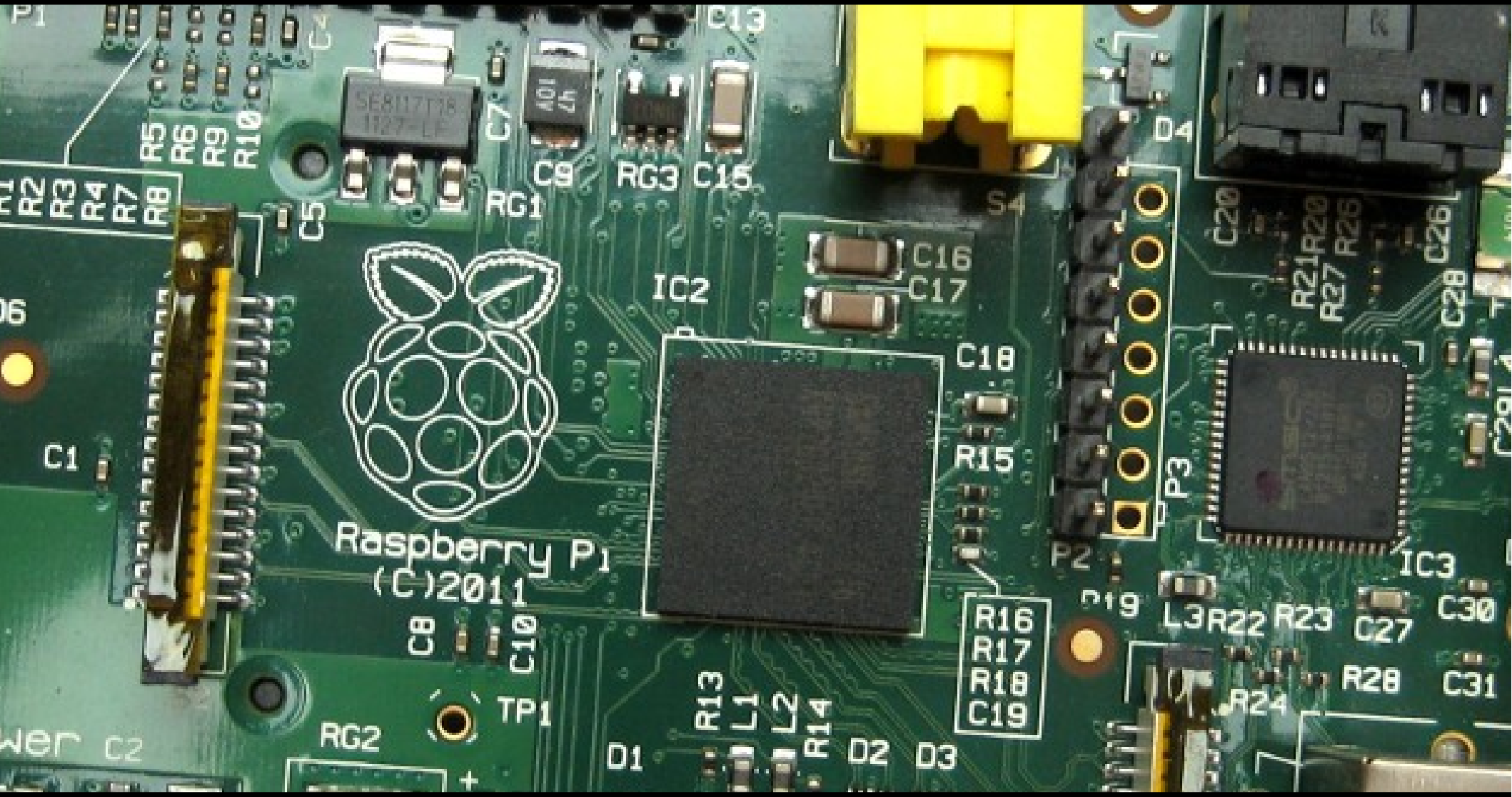
SSH Hostkeys der SSH-Angreifer
http://bunten.de/ssh-hostkeys.html

DenyH0STS Projekt Homepage
http://denyhosts.sourceforge.net/

„*SSH-Honeypots und neue Schutzmaßnahmen gegen Brute Force Angriffe*“
Im Tagungsband des 20. DFN Workshop „Sicherheit in vernetzten Systemen“, Februar 2013
http://bunten.de/paper/dfn-cert-workshop2013-ssh-angriffe.pdf

„*Wie man SSH-Angreifern mit Linux Honeypots nachstellt*“
Vortrag auf 18. LinuxTag in Berlin, Mai 2012
http://bunten.de/paper/LinuxTag2012-SSH-Honeypots-unter-Linux.pdf

Vielen Dank! Fragen?



Andreas Bunten (andreas.bunten@controlware.de)
Torsten Voss (voss@dfn-cert.de)

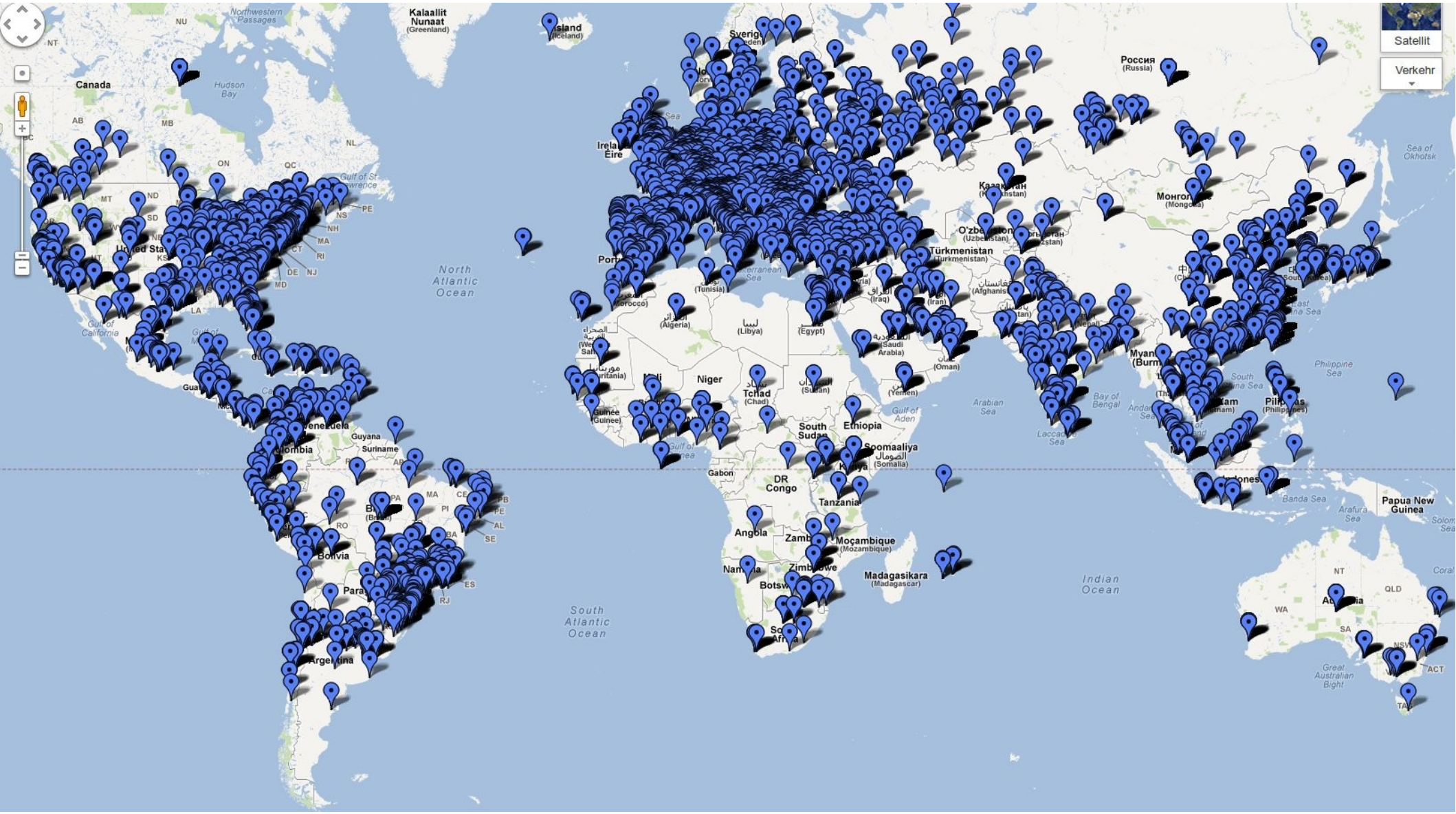
Vielen Dank an: Christel, Eve, Agnes, Josef, Sabine, Barbara, Guido, Controlware GmbH & DFN-CERT Services GmbH

Trivia

In den Daten stecken viele skurile Dinge …

- 226377 Versuche mit Username == Passwort
- 30689 Versuche in einem Angriff
- 177 Versuche mit Passworten der Länge > 30
- 705 Versuche mit Passwort, das 'fuck' enthält
- … dabei kamen 61 Passwort-Varianten vor
- Seltsame Konten: 'Terminator', 'Tolkien', 'thisisalongusername', …
- Seltsame Passworte:
  '!#EWDYUWU*(&@#YEDS',
  '!@##@!@#$#@#$%^&*^%$%^&*(&^%&', ...

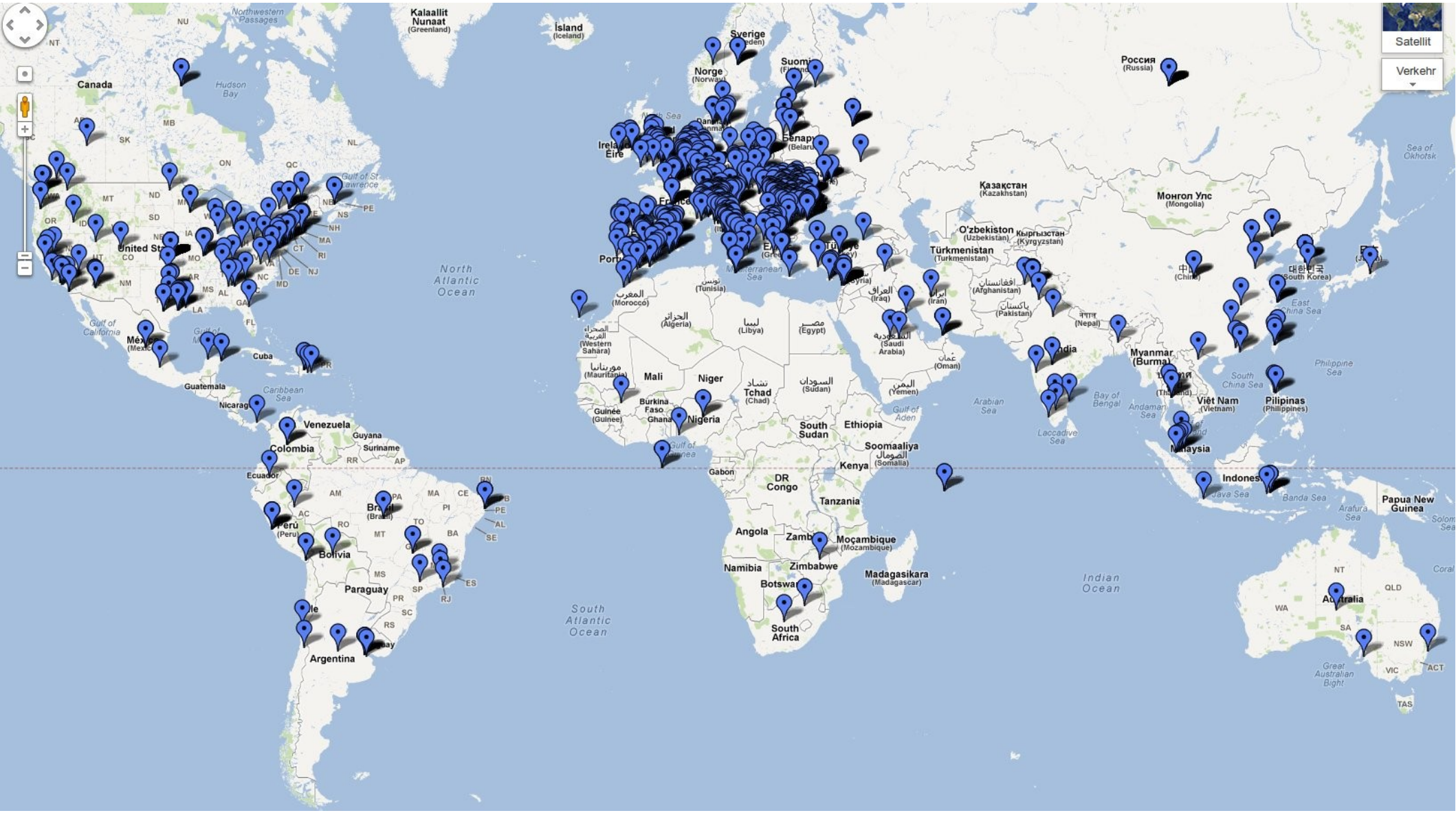
Virtueller Honeypot: Brute Force Angriffe



SSH-Angreifern mit Honeypots über die Schulter schauen
GUUG Frühjahrsfachgespräch 2013

Andreas Bunten
Torsten Voss

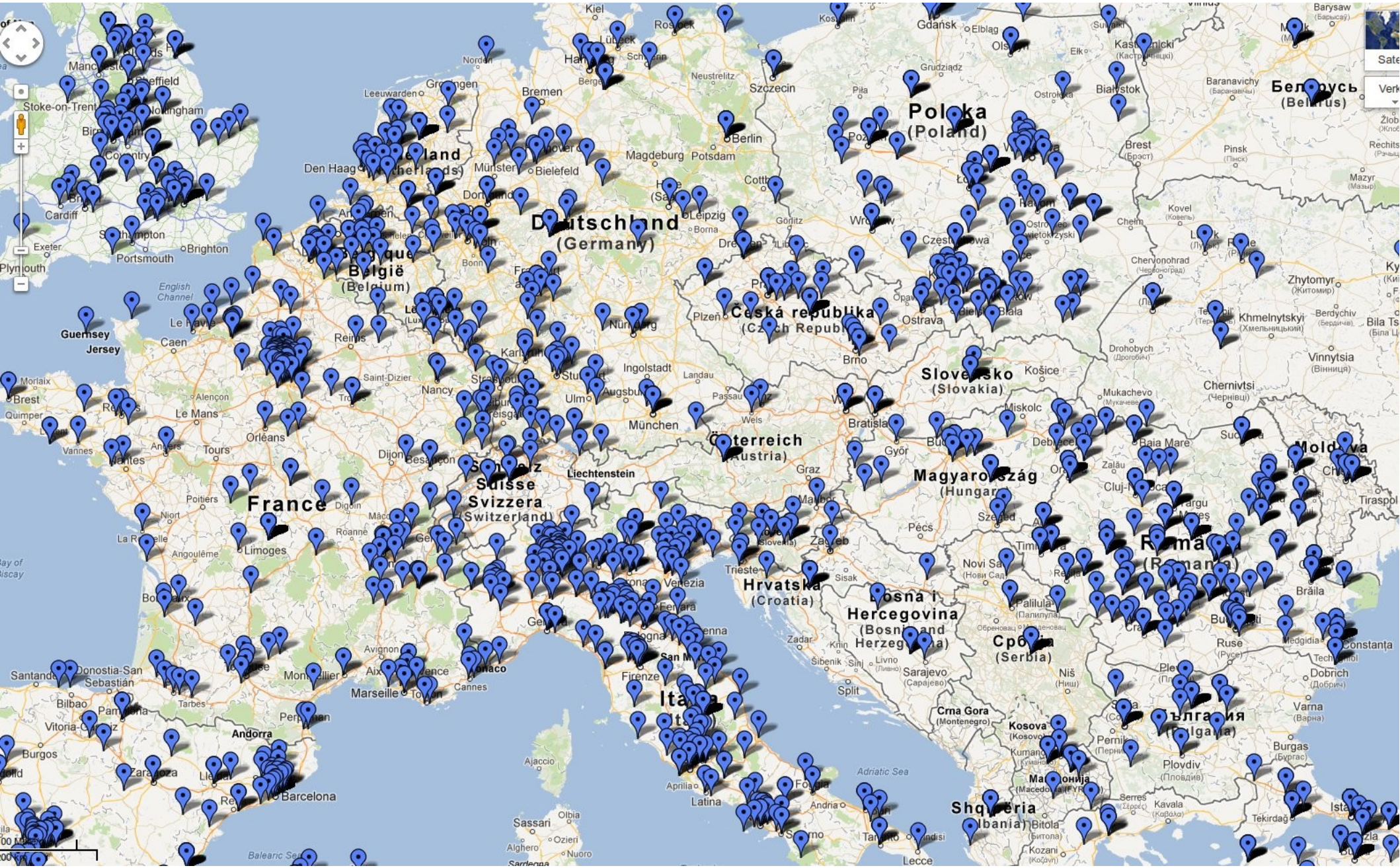
Virtueller Honeypot: Angreifer-Logins



SSH-Angreifern mit Honeypots über die Schulter schauen
GUUG Frühjahrsfachgespräch 2013

Andreas Bunten
Torsten Voss

Virtueller Honeypot: Brute Force Angriffe (II)



Virtueller Honeypot: Angreifer-Logins (II)