Wie man SSH-Angreifern mit Linux Honeypots nachstellt

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

Bild: Fir0002/Flagstaffotos

Agenda

- SSH Account Probes
- Was ist ein Honeypot?
- Verschiedene Typen von SSH Honeypots
- Zusammenfassung
- Wie werde ich nicht Opfer?

SSH Account Probes

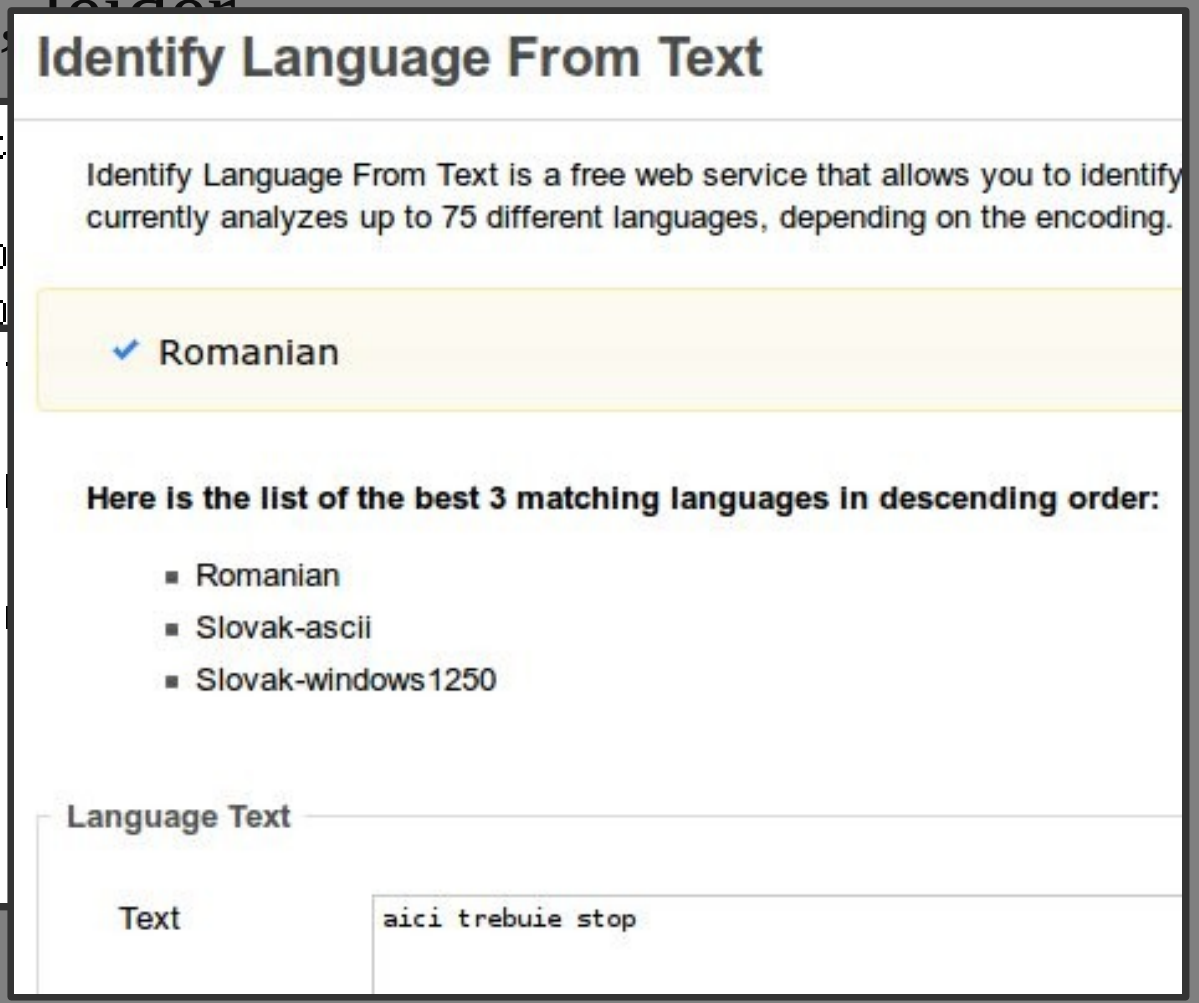
- Passwort-Rate-Angriff / Brute-Force-Angriff / ...
- Ist das normal? Ja, leider.
- Warum ist das interessant?
  - Wir sehen immer wieder die gleichen Angriffs-Tools
  - Es scheinen sehr oft die gleichen Angreifer zu sein

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
```

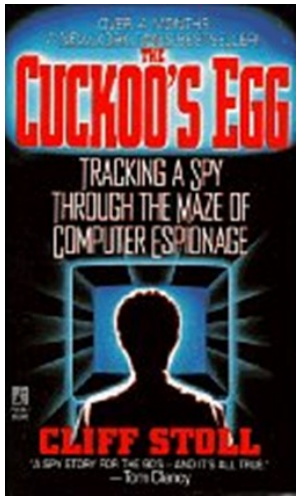


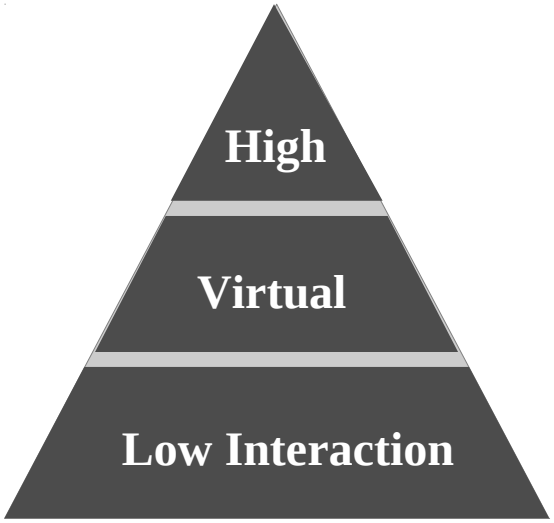
SSH Account Probes (II)

- 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?

Was ist ein Honeypot?

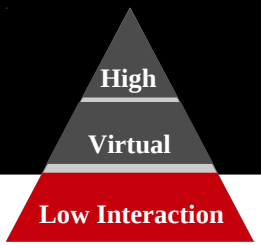
- „The Cuckoo's Egg“ - Clifford Stoll (1990)
- Ur-Idee: Angreifer verbinden sich zu echtem System und werden beobachtet
- „*A honeypot is a ressource whose value lies in it's illicit use.*“ - Lance Spitznes
- Typen von Honeypots:
  - High Interaction Honeypots
  - Virtuelle Honeypots
  - Low Interaction (effiziente Simulation)





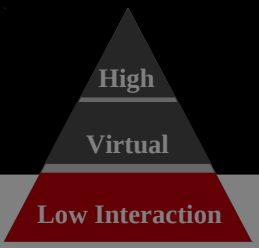
Andreas Bunten
Torsten Voss

Low Interaction Honeypot



- Nur ein kleiner Linux-Server, der so tut als ob ...
- Basierend auf Cisco NAS & Debian
- Modifizierter OpenSSH Server
  - Kein Login möglich
  - Mehr Protokollierung
    (Passwörter, Client ID, KEX, ...)
- Skripte (Perl/Bash)
  - Ergebnisstransport / Überwachung / ...

Low Interaction Honeypot



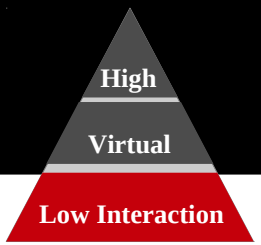
- Nur ein kleiner … ut als ob ...
- Basierend auf …
- Modifizierter …
  - Kein Login m…
  - Mehr Protokol… (Passwörter, …
- Skripte (Perl/B…
  - Ergebnisstrans…

Andreas Bunten
Torsten Voss

Low Interaction Honeypot

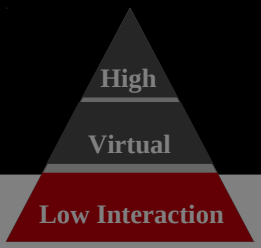
- Nur ein kleiner Linux-Server, der so tut als ob ...

Low Interaction Honeypot (II)

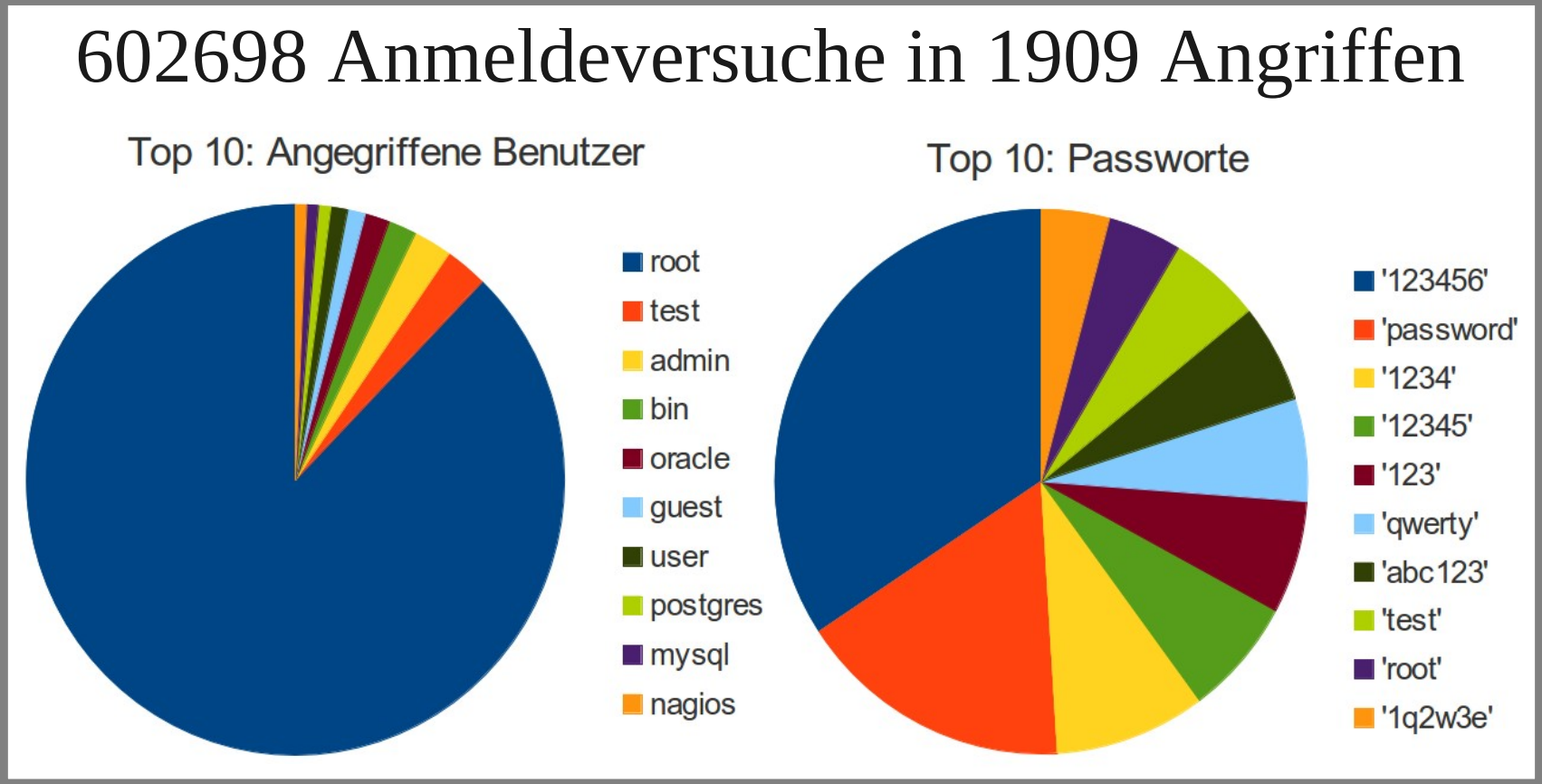


- Ergebnisse!
  - Statistiken bzgl. Benutzern & Passworten

Low Interaction Honeypot (II)

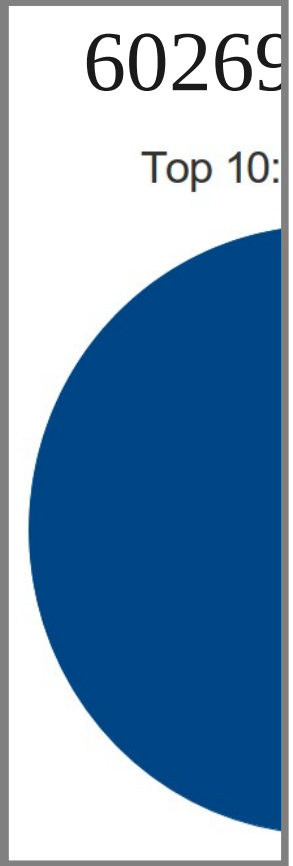


- Ergebnisse!
  - Statistiken bzgl. Benutzern & Passworten

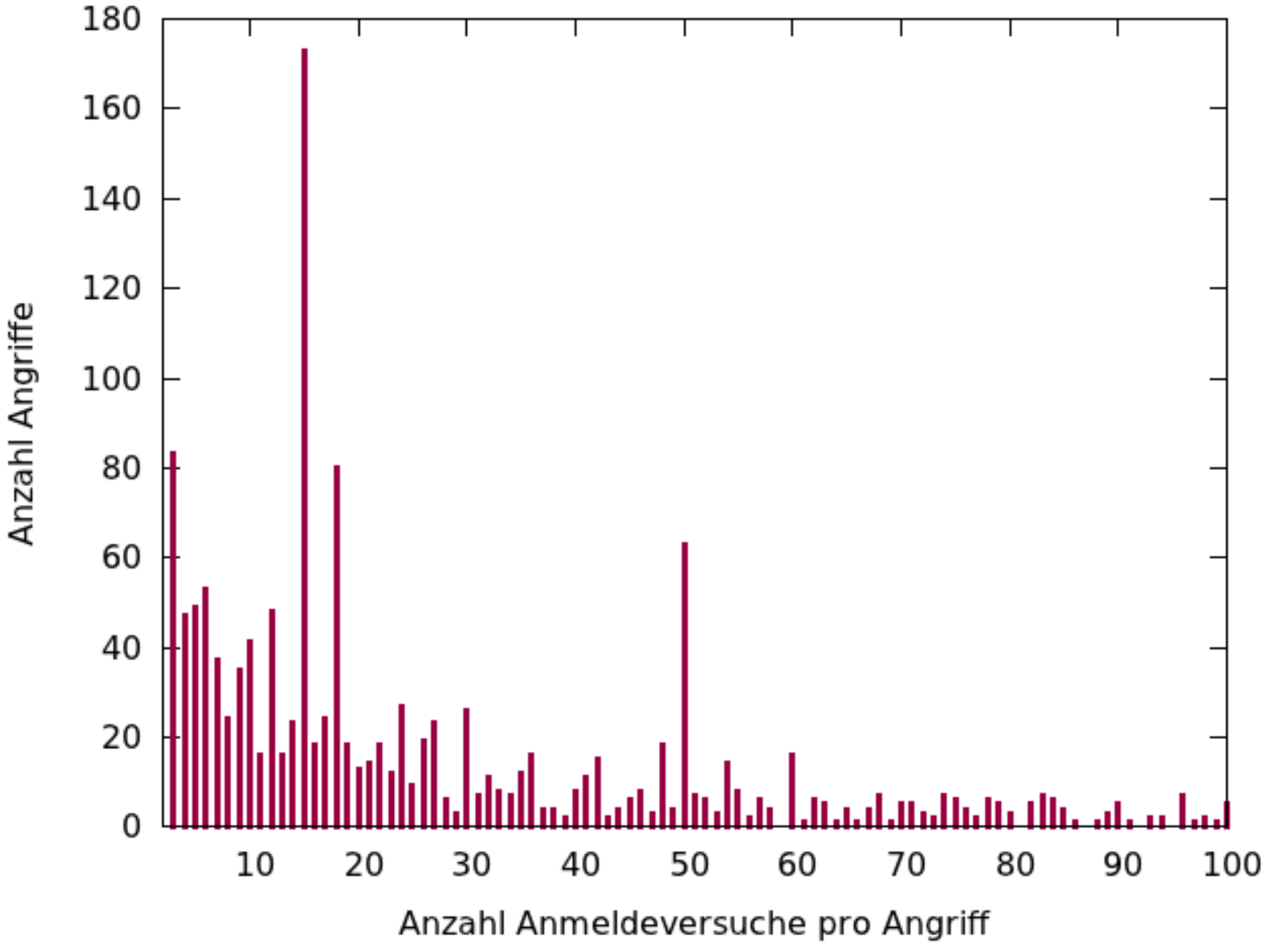


Low Interaction Honeypot (II)

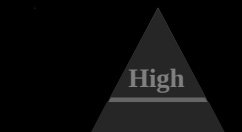
- Ergebn
  - Stati



Wie viele Anmeldeversuche pro Angriff?



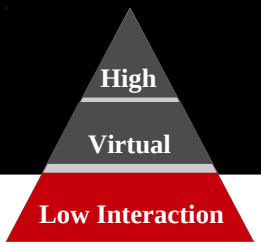
Low Interaction Honeypot (II)



Wie viele Anmeldeversuche pro Angriff?

- In den Daten stecken viele skurile Dinge …
  - 226377 Versuche mit Username == Passwort
  - 30689 Versuche in einem Angriff
  - 177 Versuche mit Passworten der Länge > 30
  - 3358 Versuche mit 1-Zeichen Passworten
  - 705 Versuche mit Passwort, das 'fuck' enthält
  - … dabei kamen 61 Passwort-Varianten vor
  - Seltsame Konten: 'Terminator', 'Tolkien', 'U5a6d7d8u', 'username', 'thisisalongusername', …
  - Seltsame Passworte: '!#EWDYUWU*(&@#YEDS', '!@##@!@#$#@#$%^&*^%$%^&*(&^%&', ...

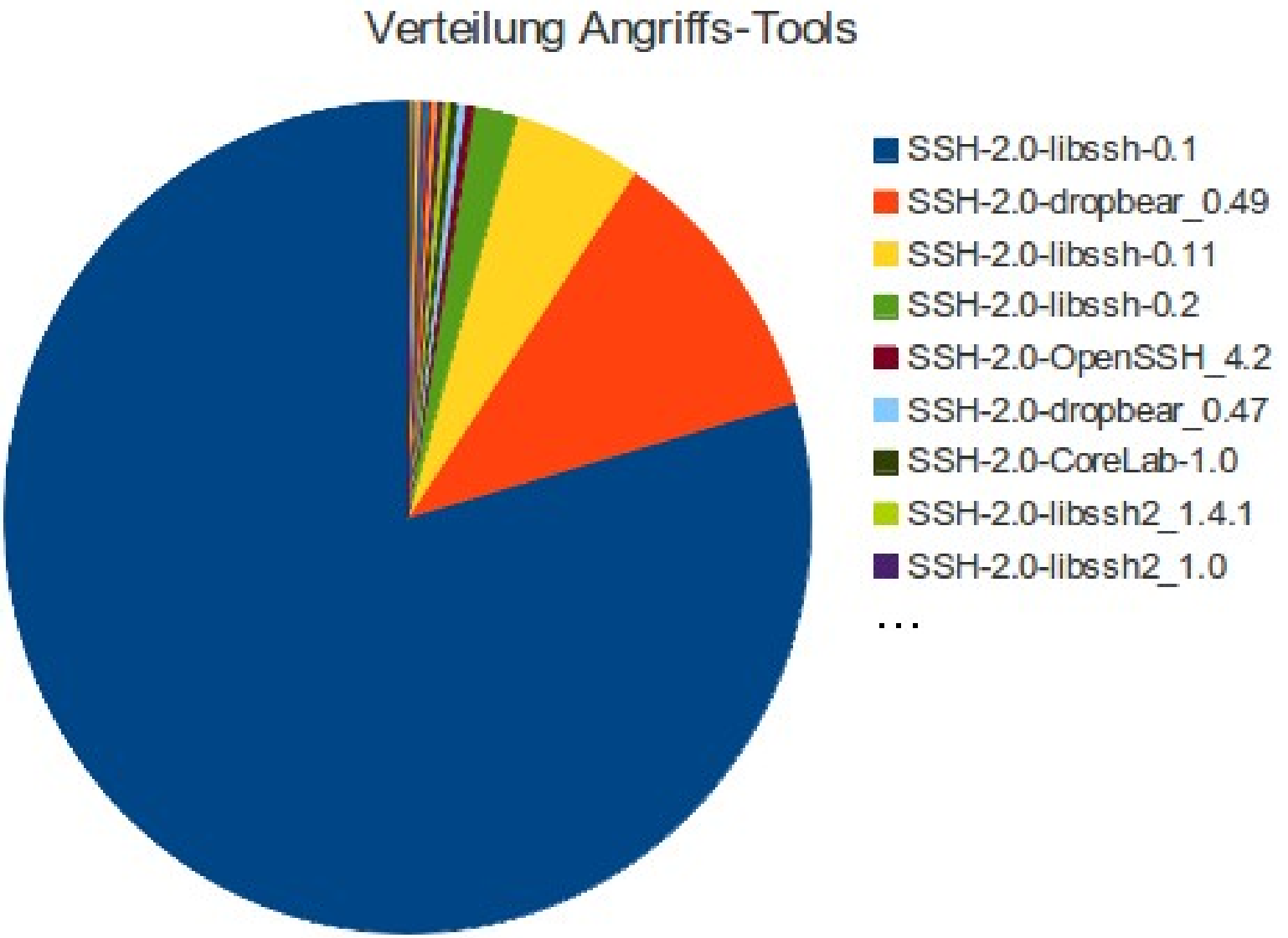
Low Interaction Honeypot (II)



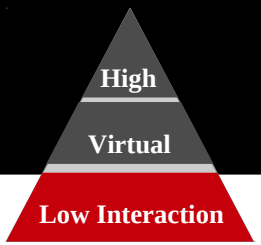
- Ergebnisse!
  - Statistiken bzgl. Benutzern & Passworten
  - Fingerprints der Angriffs-Tools

Low Interaction Honeypot (II)

Wie meldet sich die SSH Client-SW der Angreifer?



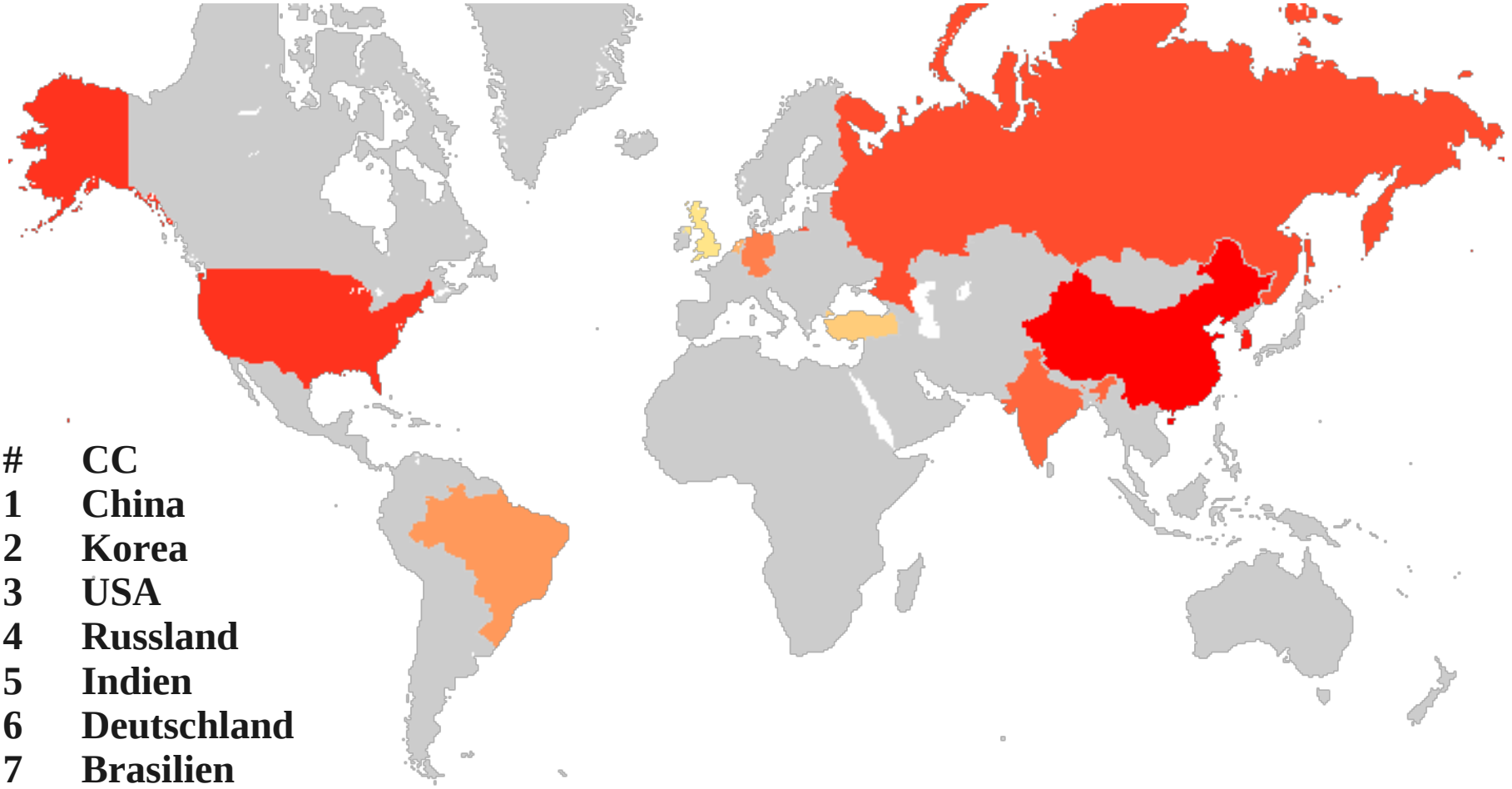
Low Interaction Honeypot (II)



- Ergebnisse!
  - Statistiken bzgl. Benutzern & Passworten
  - Fingerprints der Angriffs-Tools
  - Woher die Angreifer kommen

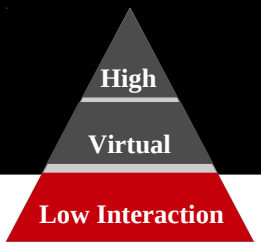
Low Interaction Honeypot (II)

Von IP-Adressen welcher Länder erfolgen Angriffe?



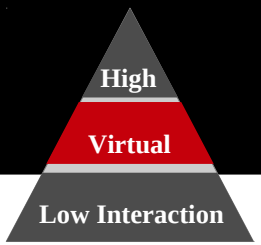
#	CC
1	China
2	Korea
3	USA
4	Russland
5	Indien
6	Deutschland
7	Brasilien
8	Niederlande
9	Türkei
10	Großbritannien

Low Interaction Honeypot (II)



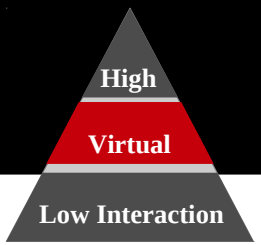
- Ergebnisse!
  - Statistiken bzgl. Benutzern & Passworten
  - Fingerprints der Angriffs-Tools
  - Woher die Angreifer kommen
- Was fehlt?
  - Das sind alles kompromittierte Systeme.
    Woher kommen die Angreifer?
  - Wie war das mit Ost-Europa?
  - Was machen die Angreifer, wenn sie könnten?

Virtuelle Honeypot



- Und wenn wir so tun, als ob das Passwort stimmt?
- Ein erfolgreiches Login wird vorgetäuscht
- Software Kippo (früher Kojonne)
  - Linux Shell wird simuliert
  - Download weitere Tools möglich
  - … aber kein Start fremder Software
- Skripte (Perl/Bash)
  - Ergebnisstransport / Überwachung / ...

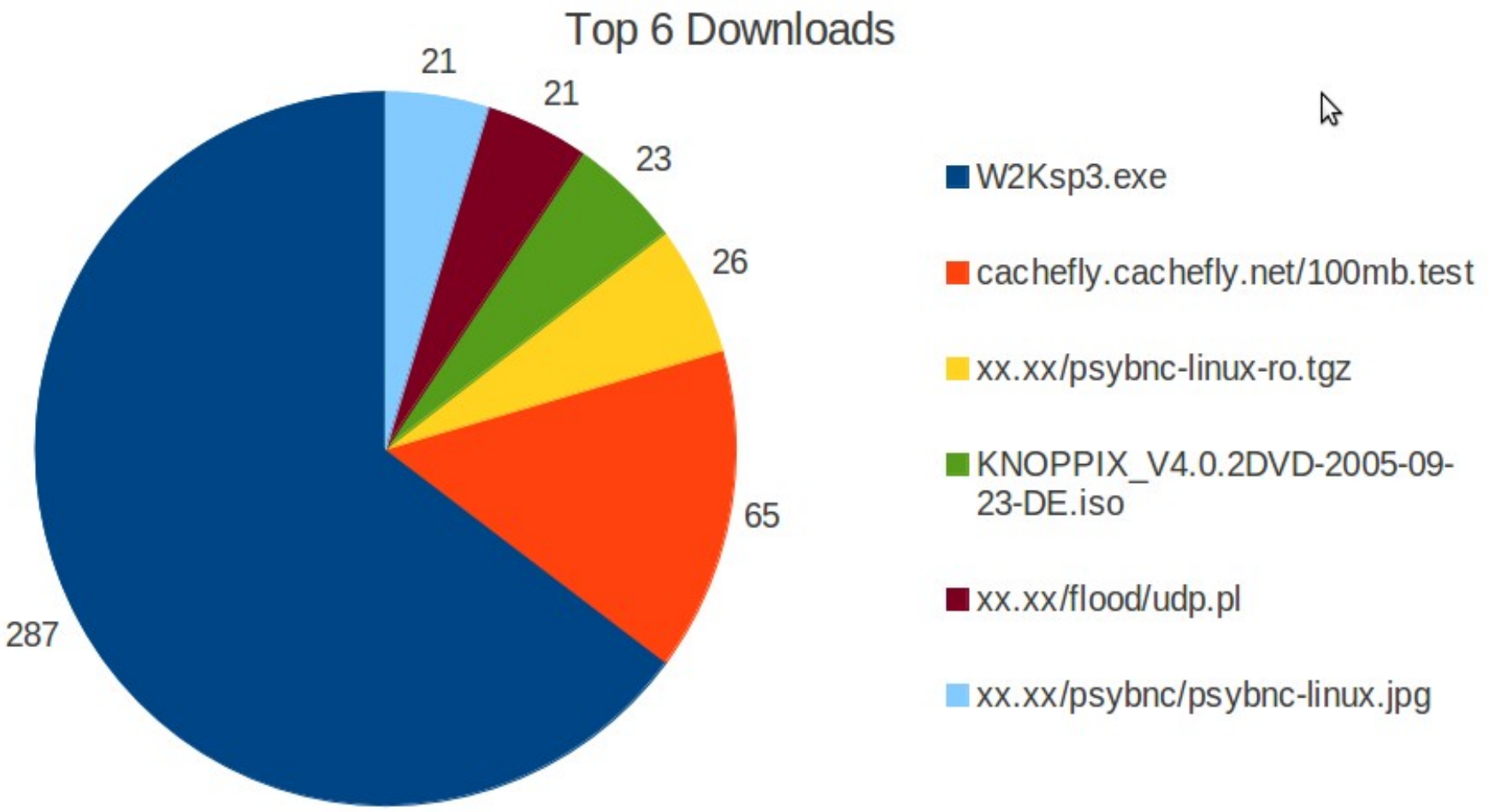
Virtueller Honeypot (II)



- Ergebnisse!
  - Wir sehen was die Angreifer nach dem Login treiben
  - Viele Angreifer sind weniger geschickt als erwartet
  - Wir sehen Malware-Downloads

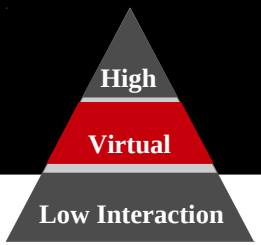
Virtueller Honeypot (II)

Was laden die Angreifer nach?



Skurilste Downloads: Teamspeak, webmin, XAMPP, pine, Half-Life Gameserver

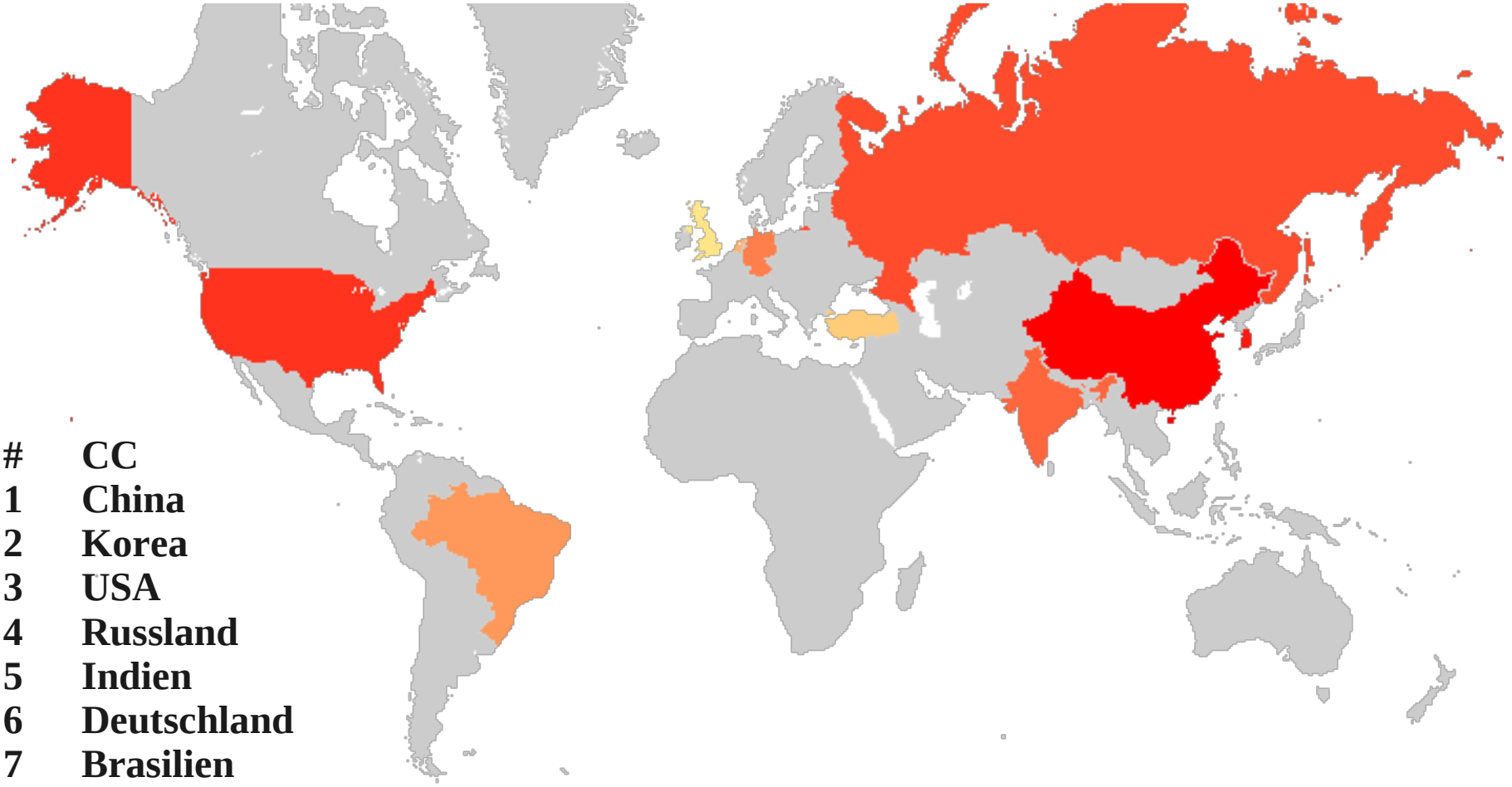
Virtueller Honeypot (II)



- Ergebnisse!
  - Wir sehen was die Angreifer nach dem Login treiben
  - Viele Angreifer sind weniger geschickt als erwartet
  - Wir sehen Malware-Downloads
  - Wir sehen die Angreifer-Systeme und nicht nur Scanner!

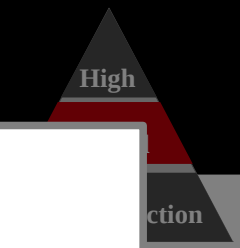
Virtueller Honeypot (II)

Länder aus denen die Brute Force Angriffe kamen

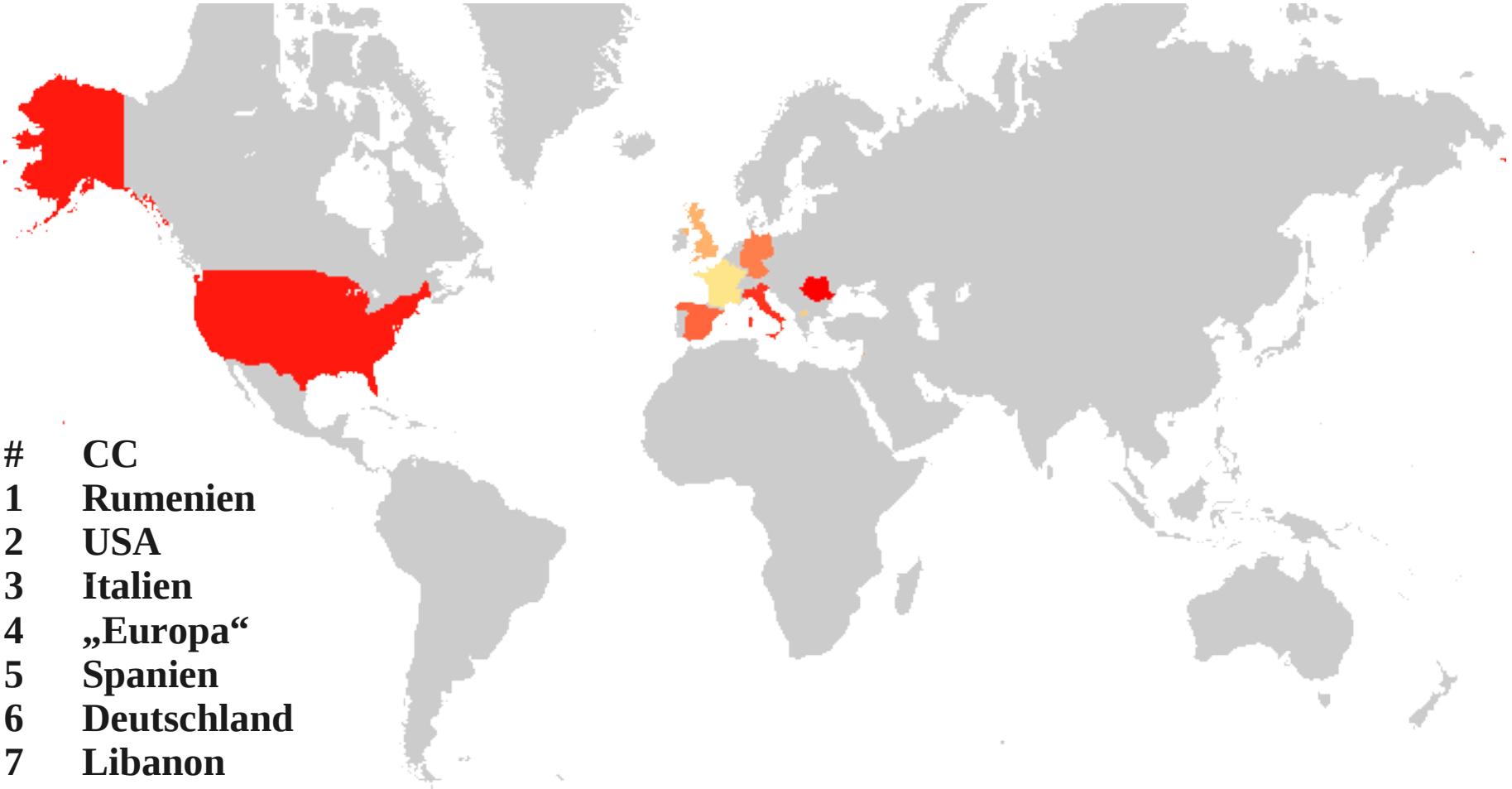


#	CC
1	China
2	Korea
3	USA
4	Russland
5	Indien
6	Deutschland
7	Brasilien
8	Niederlande
9	Türkei
10	Großbritanien

Virtueller Honeypot (II)



Länder aus denen interaktive Sessions kamen



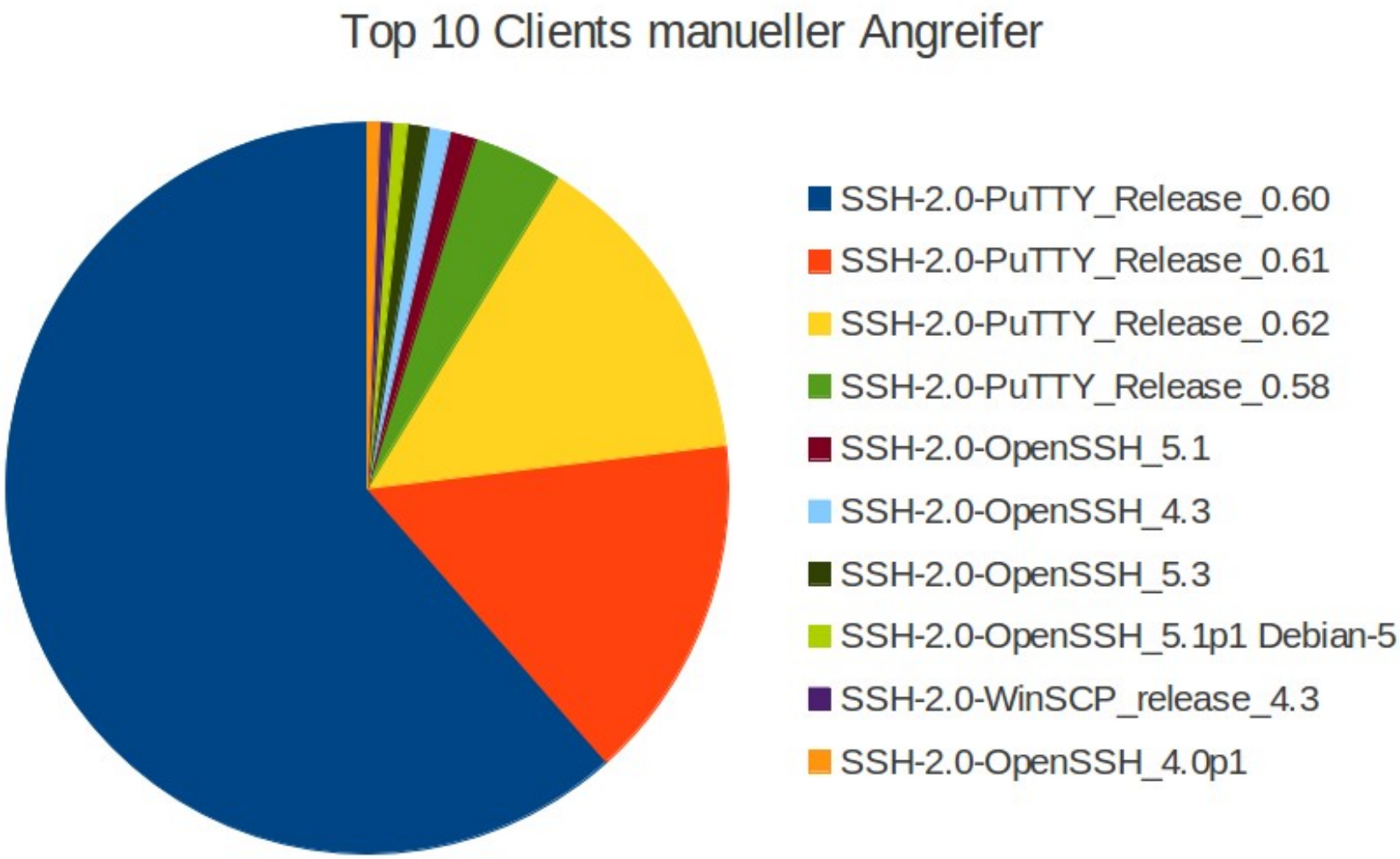
#	CC
1	Rumenien
2	USA
3	Italien
4	„Europa“
5	Spanien
6	Deutschland
7	Libanon
8	Großbritannien
9	Mazedonien
10	Frankreich

Virtueller Honeypot (II)

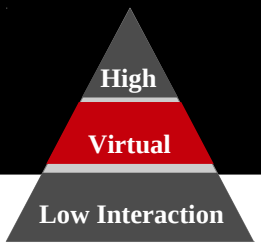
High

ction

Welche Clients verwenden die *echten* Angreifer?

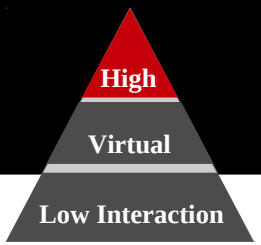


Virtueller Honeypot (II)



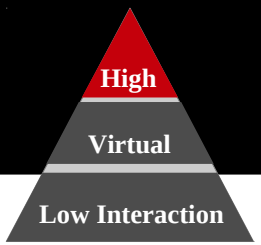
- Ergebnisse!
  - Wir sehen was die Angreifer nach dem Login treiben
  - Viele Angreifer sind weniger geschickt als erwartet
  - Wir sehen Malware-Downloads
  - Wir sehen die Angreifer-Systeme und nicht nur Scanner!
- Was fehlt?
  - Der Honeypot zu schnell erkannt :-/
    Was wäre danach passiert?

High Interaction Honeypot



- Wir wollen einen Schritt weiter gehen ...
- Angreifer erhält Kontrolle über ein echtes System
- Das System ist entsprechend vorbereitet ...
- Risiken und Nebenwirkungen!
  - Auch Honeypot-Software enthält Fehler
  - Ausbruch aus dem Honeypot-Netzwerk
  - Angriffe ausgehend von unseren Systemen
  - Angreifer sperrt uns aus
  - Der Honeypot oder wir werden erkannt
  - Mehrfache Angreifer zur gleichen Zeit oder kein sauberes Image

High Interaction Honeypot (II)



- Ergebnisse!
  - Wir sehen was „danach“ passiert
  - Wir sehen mehr Malware und wie sie konfiguriert wird
  - Angriffs-Muster – wie wird die Malware eingesetzt
- Was wir gelernt haben
  - Alarmierung ist wichtig!
  - Es ist nicht ganz so einfach wie wir uns es vorstellten …
  - Checklisten helfen (Forensik, Incident Response, Status des Systems, Dokumentation, ...)

Zusammenfassung

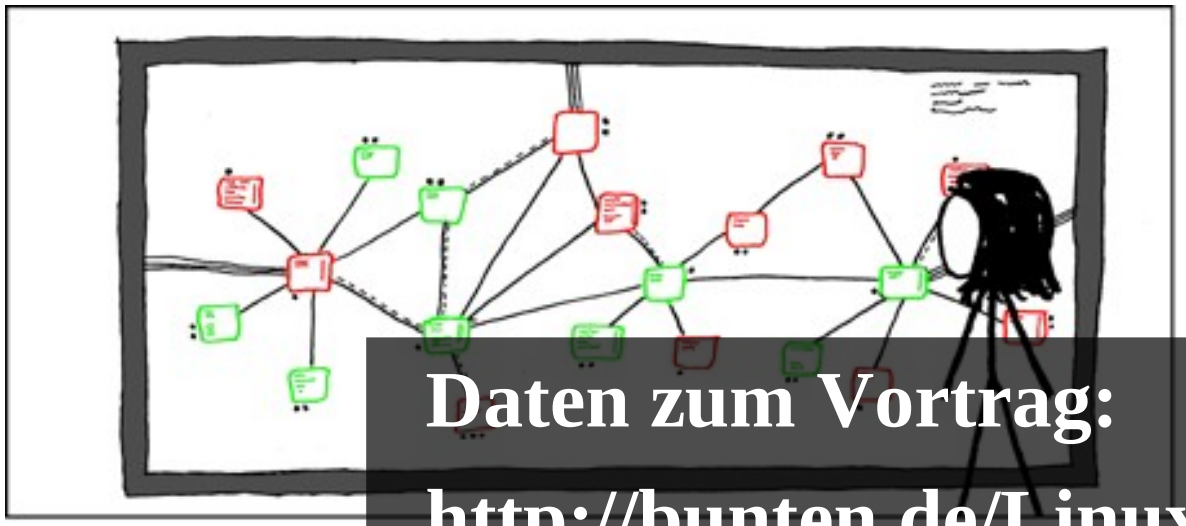
- Work in Progress!
  - Es sind scheinbar wirklich nicht viele Angreifer-Gruppen
  - Es lassen sich Signaturen zu den Angriffs-Tools erstellen
  - Die initialen Angriffe kommen von kompromittierten Systemen
  - Die eigentlichen Angreifer sitzen eher nicht in China!
- Honeypots sind cool! Zusätzliche Vorteile:
  - Kombination der Daten verschiedener Honeypots gibt Tiefe & Breite
  - Wir erhalten Zugriff auf die Tools der Angreifer
  - Forensische Images für Test von Tools / Ausbildung
- „Normale Leute“ halten sich Hamster oder Goldfische …

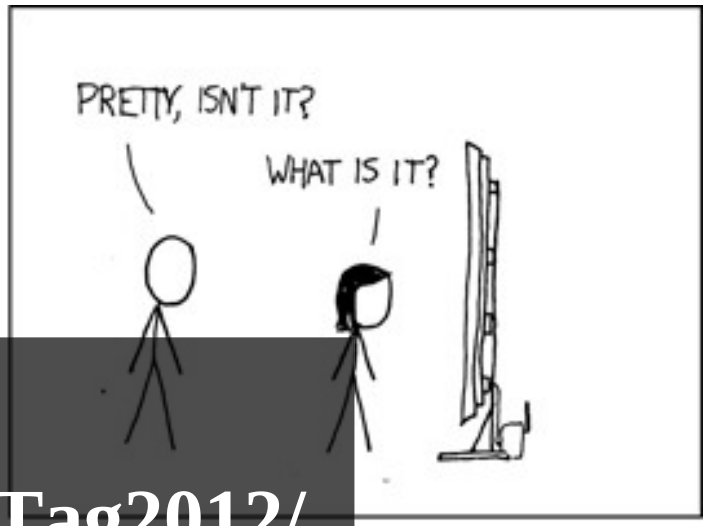
Bild: pukeycow / sxc.hu

Wie werde ich nicht Opfer?

- 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
- Wieviele SSH-Server betreiben Sie? Testen!
- Zentrale Log-Auswertung hilft weiter
- Scans und Angriffe lassen sich per Signatur erkennen
- Kompromittierte Systeme immer neu aufsetzen!

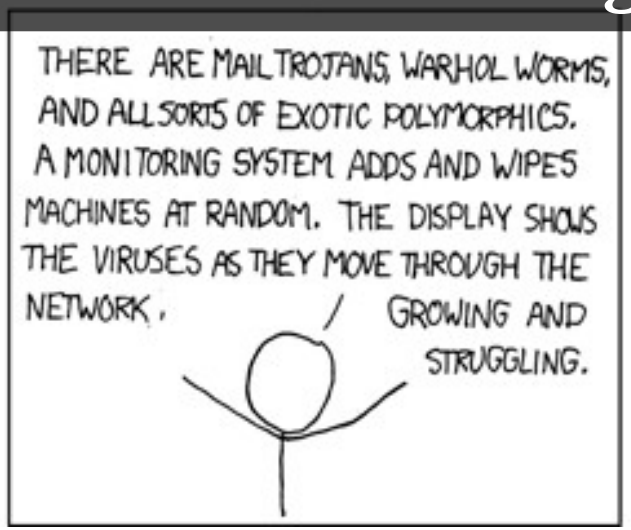
Vielen Dank! Fragen?





Daten zum Vortrag:

http://bunten.de/LinuxTag2012/



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

Comic: www.xkcd.com

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