Do bad guys work weekends?

Stephen Quinney <squinney@inf.ed.ac.uk>
Senior Computing Officer
University of Edinburgh School of Informatics

Background

- School of Informatics has:
  - ~2800 user accounts
  - ~1100 managed Linux machines:
    - 310 student lab
    - 490 office machines
    - 280 servers

SSH Service

- SSH access only permitted through 2 hosts:
  - One available for all
  - One restricted to staff and postgrads
- SSH servers tightly controlled & monitored
- Logs go to central log server:
  - logs processed into database
  - daily reports generated

You do use a central log server, right?

Login Failure Classification

- *root* – `root, r00t, ROOT, root@inf,` etc
- *real* – Associated with a real person, or looks like real account name (i.e. a likely typo)
- *non-personal* – exists in passwd DB but not associated with real person; a known daemon account; a generic team account name
- *others* – everything else
- *malicious* – *root* + *non-personal*

Login Failure Types

User Type	All Failures	Without Top Real	Without Real
root	45.2%	46.8%	64.3%
real	29.7%	27.3%	
non-personal	14.2%	14.7%	20.2%
others	10.9%	11.2%	15.4%

1st Commandment

- NEVER permit SSH access for root.

```
PermitRootLogin no
```

2nd Commandment

- Know your users

```
AllowGroups people
```

Non-Personal Username Targets

Rank	Username	%
1		14.1
2		6.0
3		5.5
4		5.4
5		4.8
6		4.4
7		4.0
8		3.0
9		2.9
10		2.8

The top ten (out of 279) non-personal usernames targetted account for 52.9% of all attacks of this type.

Non-Personal Username Targets

Rank	Username	%
1	test	14.1
2	ftp	6.0
3	oracle	5.5
4	web	5.4
5	nagios	4.8
6	admin	4.4
7	support	4.0
8	mysql	3.0
9	guest	2.9
10	www	2.8

The top ten (out of 279) non-personal usernames targetted account for 52.9% of all attacks of this type.

3rd Commandment

- Treat test / temporary accounts carefully.

```
DenyUsers testuser1
```

```
DenyGroup testusers
```

Login failures – further classification

User Type	Informatics	UoE	External
root	1	11	7150
Non-Personal	6	2	2194
Others	121	130	1462
Real	481	757	3445

Attempts to login as root or a non-personal account from your local or wider area network MUST always be investigated.

4th Commandment

- Store and analyse your logs

Top Ten Source Countries

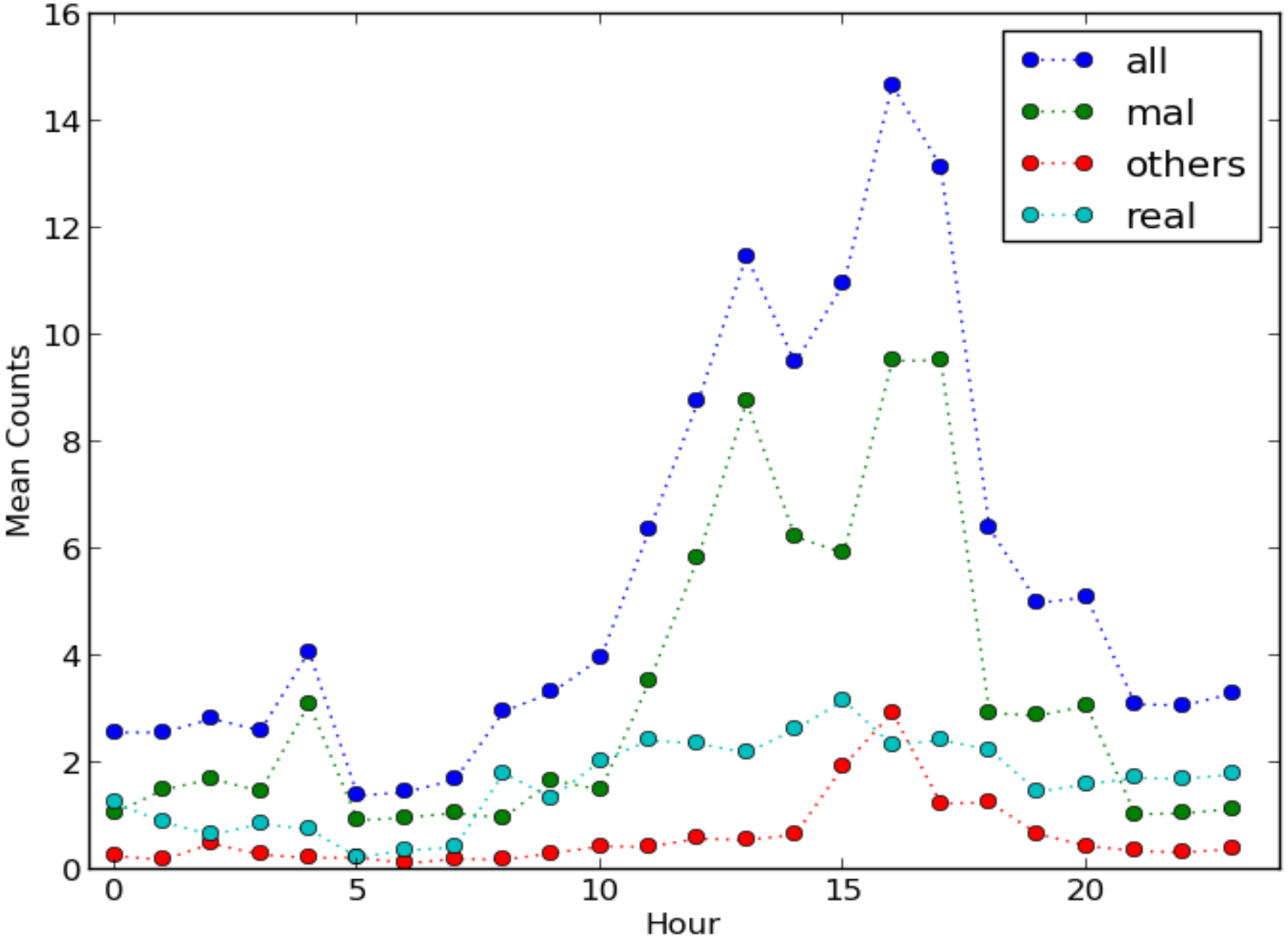
Rank	All	%	Malicious	%
1		20.2		30.8
2		20.1		21.3
3		13.6		8.3
4		7.2		8.3
5		5.8		6.9
6		5.7		6.7
7		5.5		3.1
8		5.0		2.0
9		3.9		1.9
10		2.0		1.9

Top Ten Source Countries

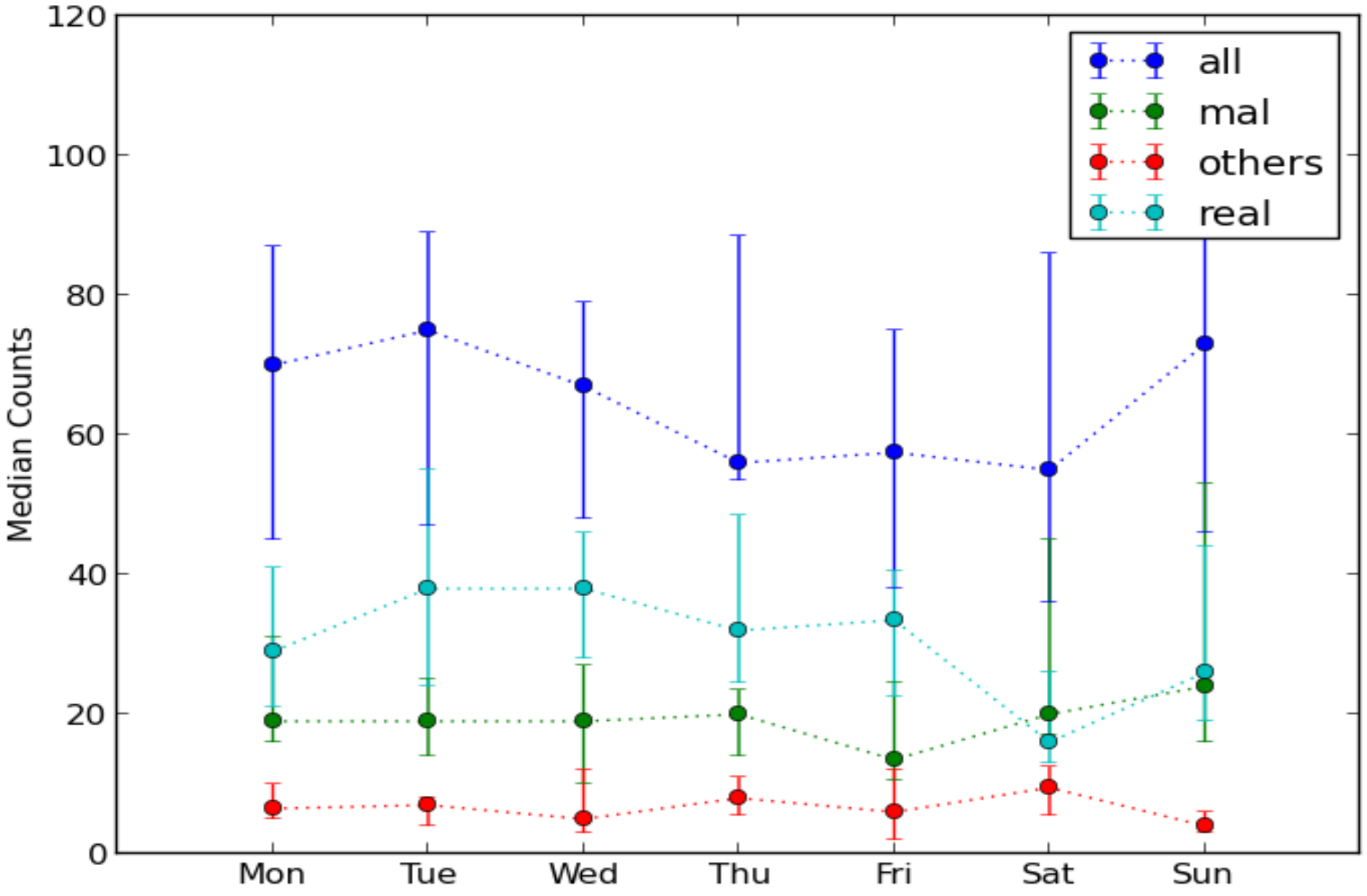
Rank	All	%	Malicious	%
1	United Kingdom	20.2	China	30.8
2	China	20.1	Cambodia	21.3
3	Cambodia	13.6	South Korea	8.3
4	Germany	7.2	Italy	8.3
5	United States	5.8	United States	6.9
6	UoE	5.7	Germany	6.7
7	South Korea	5.5	Netherlands	3.1
8	Italy	5.0	Russian Federation	2.0
9	Informatics	3.9	Turkey	1.9
10	Netherlands	2.0	Brazil	1.9

This, of course, does not show the country of origin for the attacker. Many attacks will come from previously compromised machines.

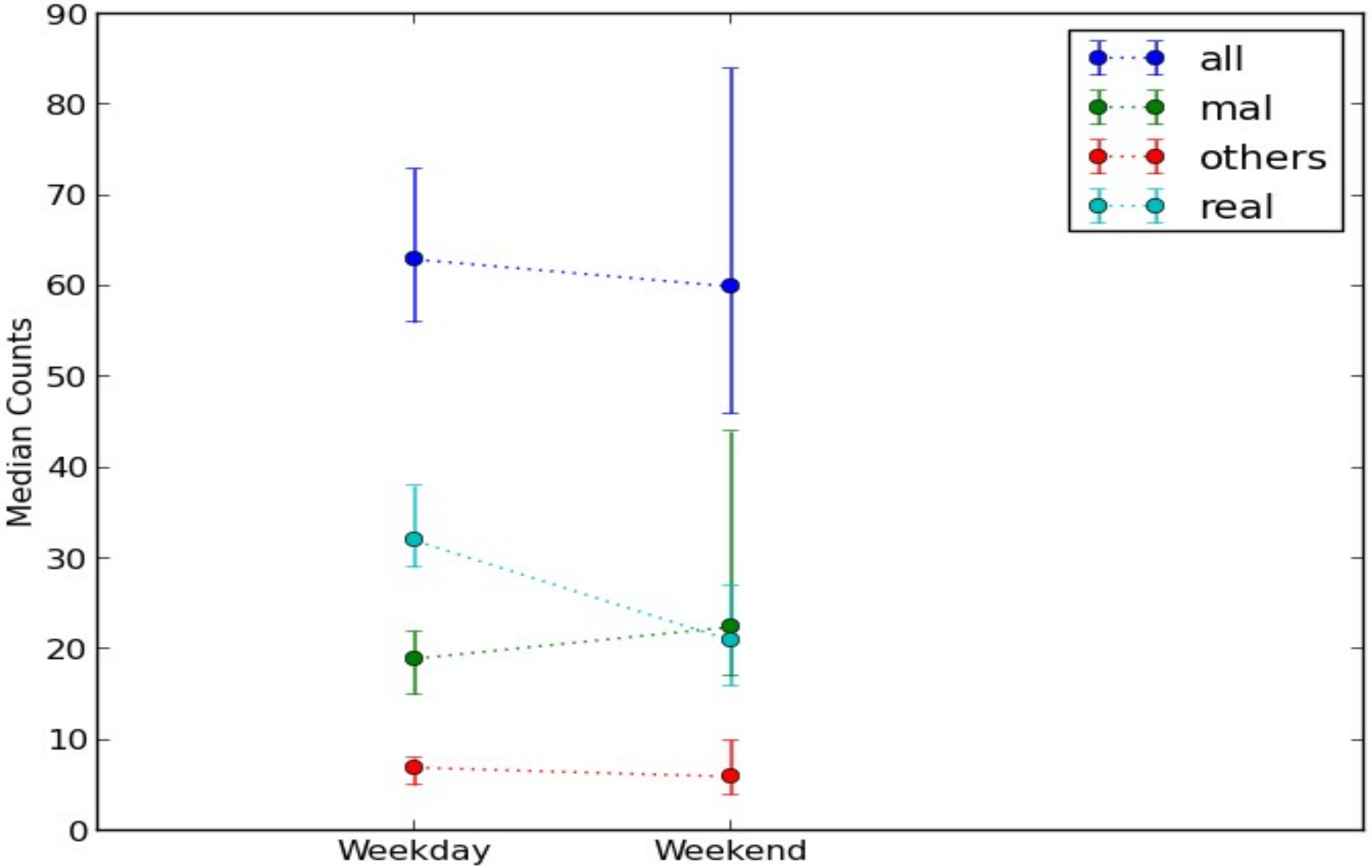
Login Failures - Hourly



Login Failures - Daily



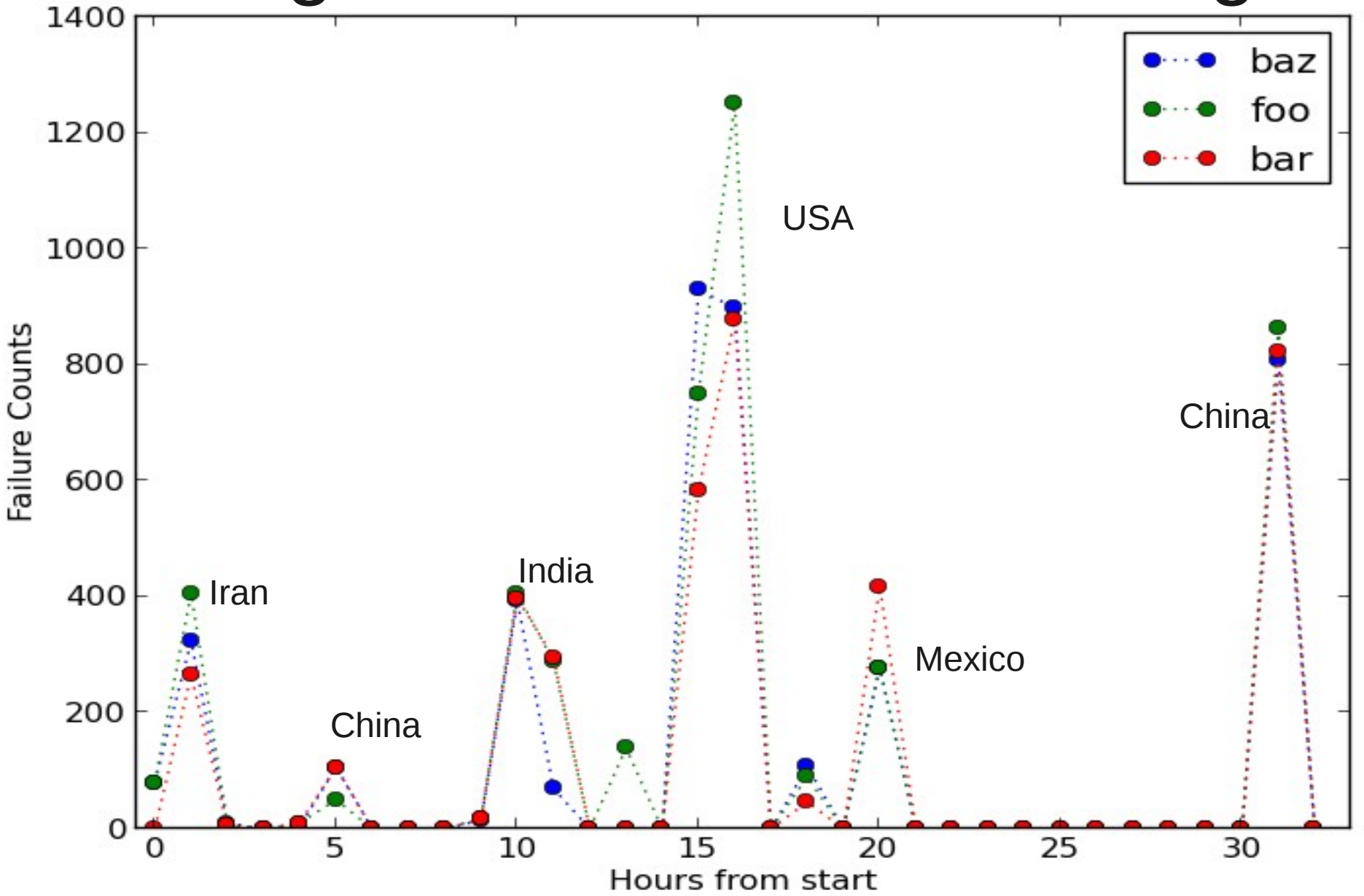
Login Failures - Weekends



Do bad guys work weekends?

- Yes!
- Probably because most attacks come from automated botnets.
- Don’t forget to analyse your logs from the weekends!

Login Failures – no blocking



Login Failures – no blocking

Rank	Country	# IP	%
1	USA	3	43.80
2	China	5	25.64
3	India	1	14.79
4	Iran	1	7.95
5	Mexico	1	7.79

5th Commandment

- Monitor login failures and block attacks

Summary

1. Never permit SSH access for root.
2. Know your users.
3. Treat test and temporary accounts carefully.
4. Store and analyse your logs.
5. Monitor login failures and block attacks.