LITNET CERT
Team update

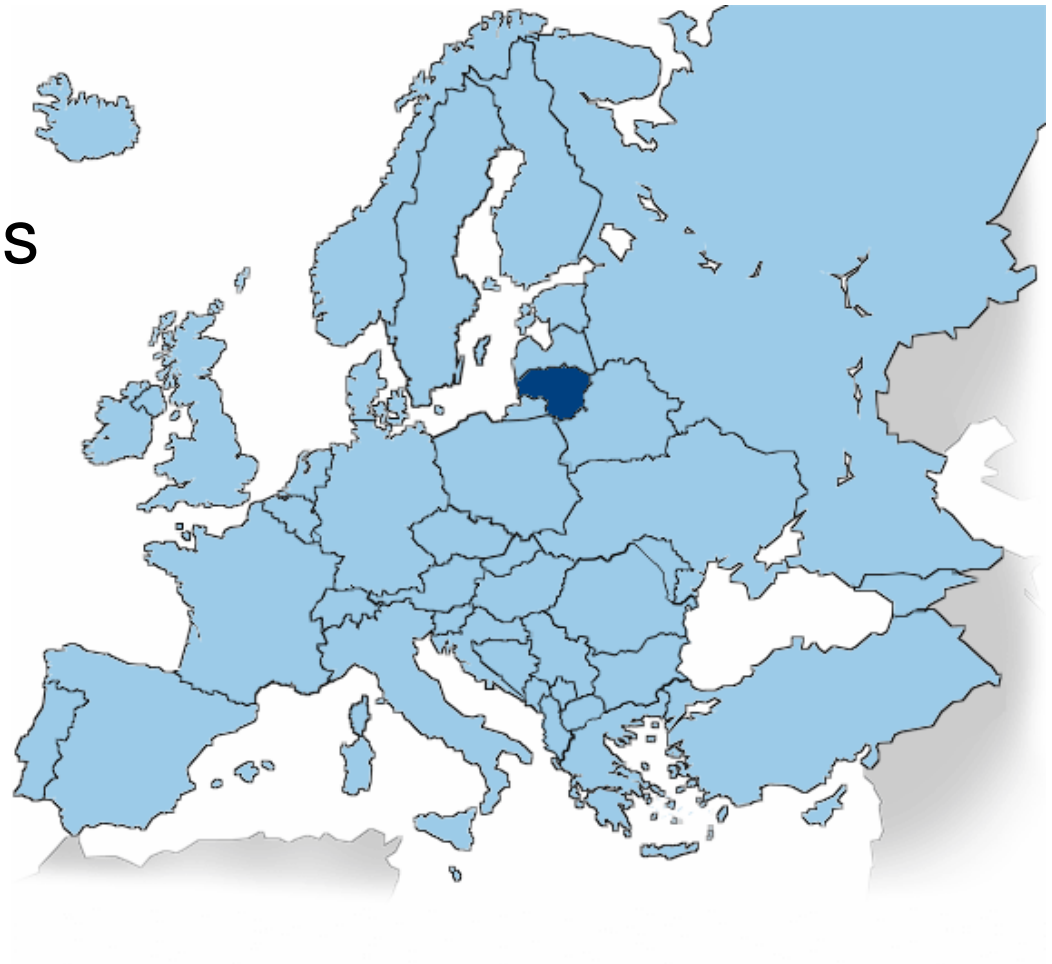
Vytautas Krakauskas

2008-01-29, Prague

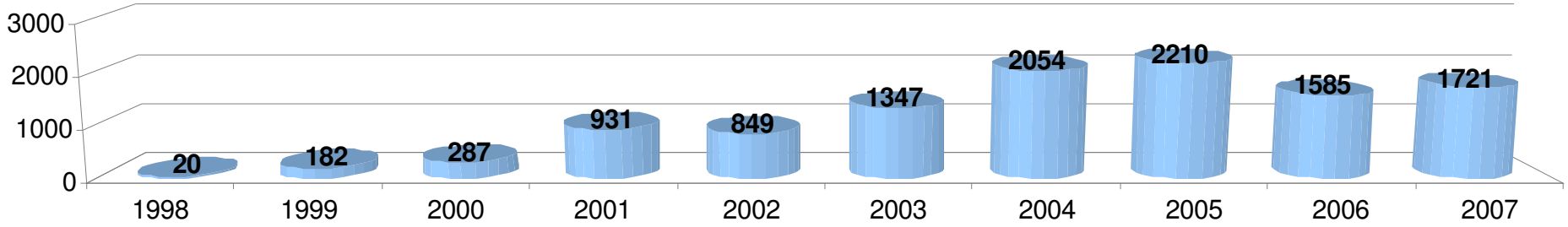
LITNET

- http://www.litnet.lt
- NREN in Lithuania
- ~1300 Organizations
- ~200 000 Users

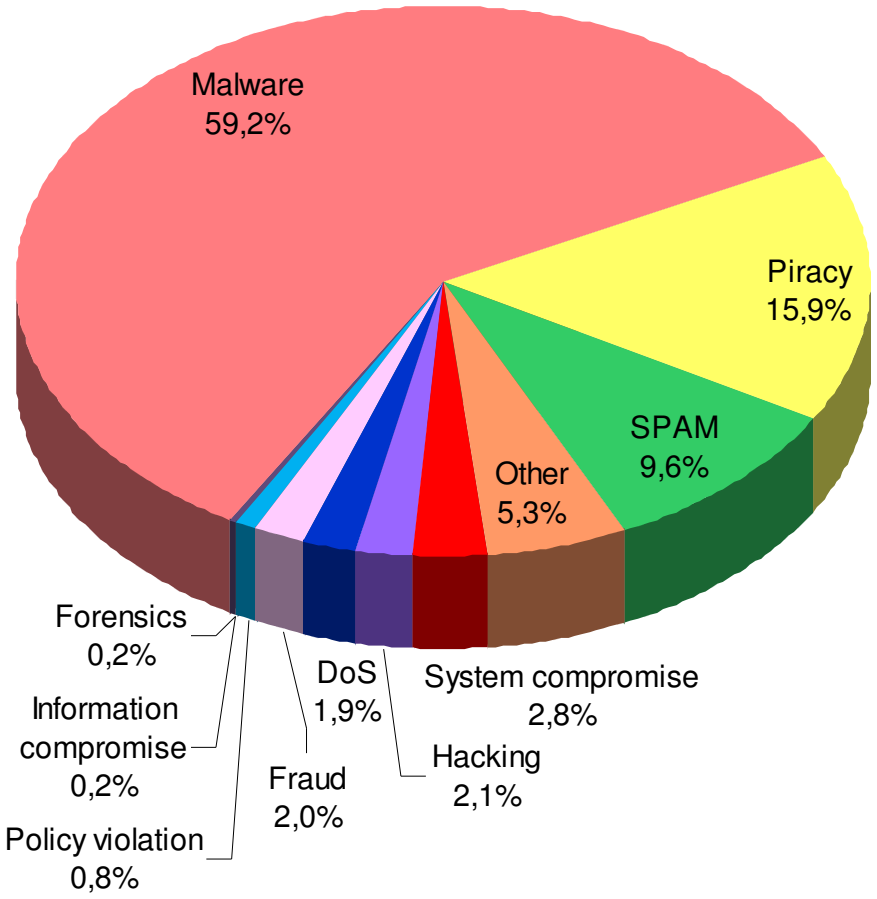
- LITNET CERT
- http://cert.litnet.lt
- 16 persons
- 8 major nodes



Statistics


3000
2000
1000
0
20
182
287
931
849
1347
2054
2210
1585
1721
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007

Statistics


Malware
59,2%
Piracy
15,9%
SPAM
9,6%
Other
5,3%
System compromise
2,8%
Hacking
2,1%
DoS
1,9%
Fraud
2,0%
Forensics
0,2%
Information
compromise
0,2%
Policy violation
0,8%

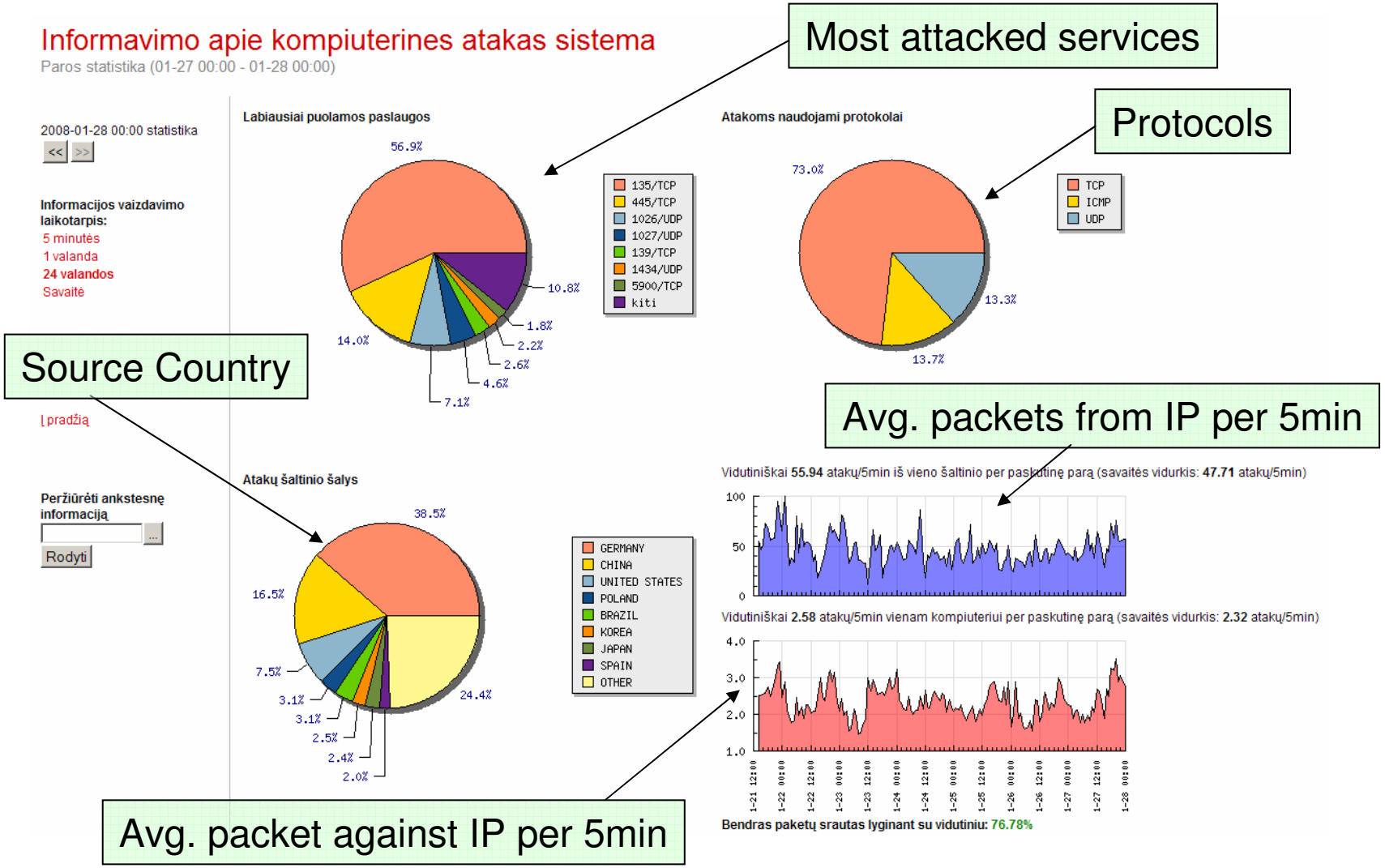
LITNET

- Everyday incident handling
- Activities
  - Advisories in lithuanian
  - Lithuanian ISP abuse forum
- Projects
  - Warning System
  - Automatic malware blocking

Warning System

- Kind of early warning system
- Monitors traffic coming to a darknet
- http://ews.litnet.lt
  - Currently in lithuanian only, sorry ☹
- Work in progress

Warning System



Warning System

Informavimo apie kompiuterines atakas sistema

Paskirties portų pasiskirstymas - 5 minučių statistika (01-28 17:50 - 01-28 17:55)

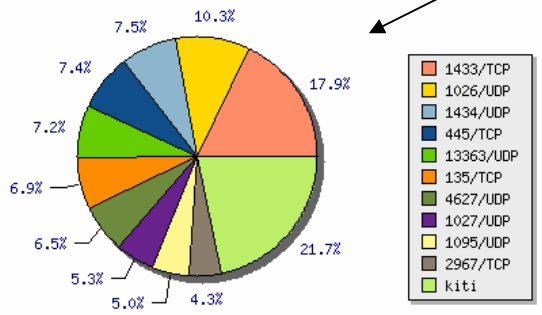
5min stats

2008-01-28 17:55 statistika

<< >>

Informacijos vaizdavimo laikotarpis:

5 minutės
1 valanda
24 valandos
Savaitė



| pradžią

Peržiūrėti ankstesnę informaciją

...

Rodyti

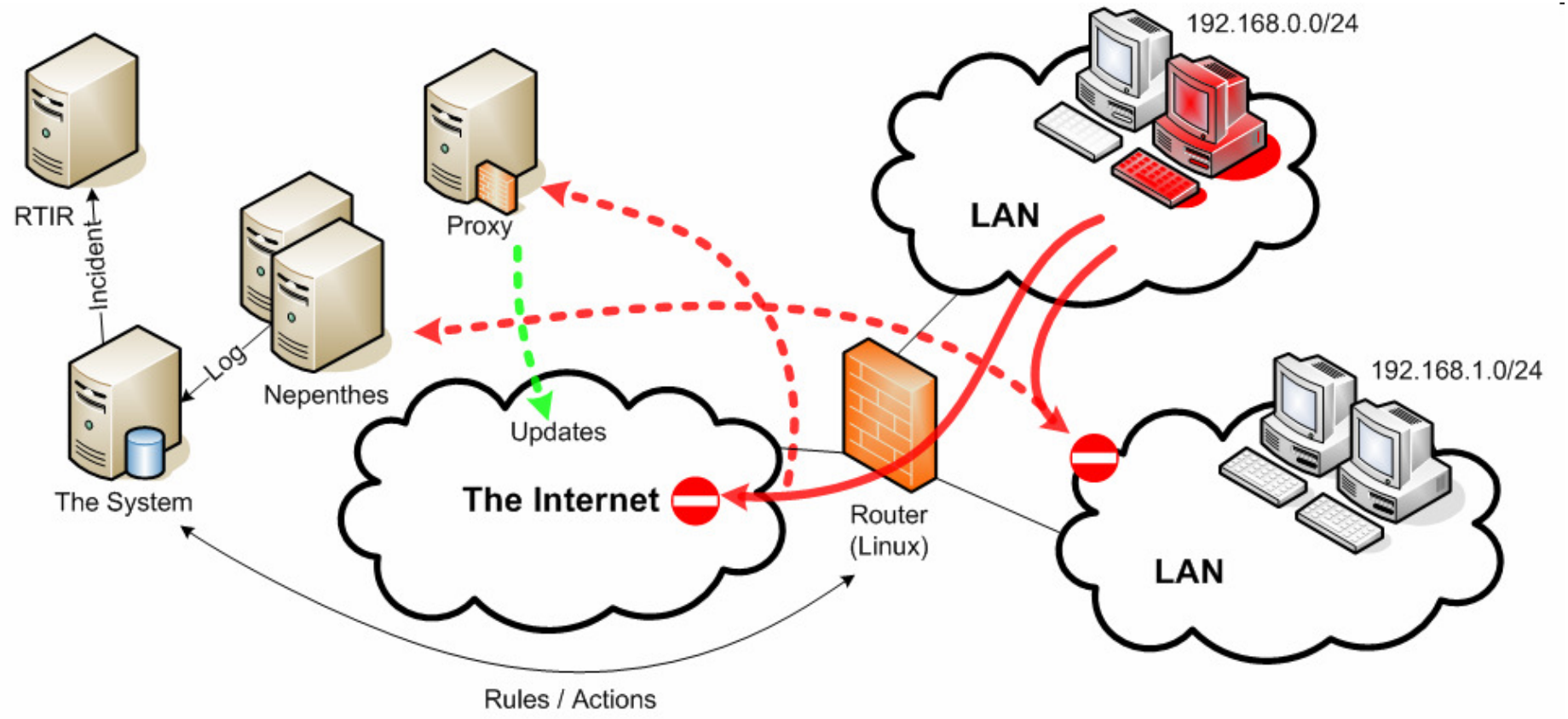
Details about ports

Portas	Paketų skaičius	Procentai	Pokytis	Rodyti porto aktyvumo grafiką
1433/TCP	1213	17.872%	+9.08%	... ... Rodyti
1026/UDP	698	10.284%	+491.53%	... ... Rodyti
1434/UDP	508	7.485%	-1.17%	... ... Rodyti
445/TCP	501	7.382%	+2.66%	... ... Rodyti
13363/UDP	491	7.234%	-8.40%	... ... Rodyti
135/TCP	465	6.851%	-4.91%	... ... Rodyti
4627/UDP	439	6.468%	+98.64%	... ... Rodyti
1027/UDP	361	5.319%	+231.19%	... ... Rodyti
1095/UDP	340	5.010%	-42.08%	... ... Rodyti
2967/TCP	295	4.347%	-10.61%	... ... Rodyti
5900/TCP	177	2.608%	+4.73%	... ... Rodyti
137/UDP	142	2.092%	-10.69%	... ... Rodyti
45306/UDP	141	2.078%	+187.76%	... ... Rodyti
13193/UDP	136	2.004%	+209.09%	... ... Rodyti
3662/TCP	109	1.606%	-4.39%	... ... Rodyti
3127/TCP	77	1.135%	+∞	... ... Rodyti
15118/TCP	58	0.855%	0.00%	... ... Rodyti
4662/TCP	55	0.810%	-30.38%	... ... Rodyti
5505/TCP	49	0.722%	-32.88%	... ... Rodyti
53/UDP	38	0.560%	-19.15%	... ... Rodyti
Kiti	494	7.279%		

Automatic malware blocking

- Goals
  - Automagically block
  - Create an incident in RTIR
  - Allow to get updates
- Work in progress

Automatic malware blocking



The END