Vytvoření bezpečnostního týmu CSIRT-CUNI

Vladimír Horák vhor@cuni.cz

Seminář správců sítí UK

Brandýs nad Labem, 14. 4. 2016

Computer **S**ecurity **I**ncident **R**esponse **T**eam

- Tým pro koordinaci řešení bezpečnostních incidentů
- Účel:
  - Incident response & incident handling
    - Vyhodnocení, profiltrování
    - Vyřízení (předání správcům konkrétní sítě)
    - Odpovídání, archivace
  - Proaktivní činnost (analýza dat)
    - Souvislosti v rámci univerzitní sítě
  - Podpora správců univerzitní sítě

Praktická realizace

- 3 zaměstnanci ÚVT
  - Vladimír Horák
  - Michal Voců
  - Jan Víšek
- Týdenní služby, během pracovní doby
- V pilotním provozu od května 2015 (330 dní)
- Kontakt a hlášení incidentů
  - abuse@cuni.cz
  - 224 491 235
  - http://csirt.cuni.cz

Prostředky

- Ticketovací systém (OTRS)
- NetFlow na rozhraní PASNET/CESNET
  - Invea FlowMon, ADS
  - CESNET FTAS
- Nessus
- CESNET Warden/Mentat

Formální ustanovení CSIRT-CUNI

- Pravidla provozování a užívání počítačové sítě Univerzity Karlovy
- Registrace u národního centra kybernetické bezpečnosti podle zákona č. 181/2014 Sb
- Ustanovení CSIRT-CUNI v rámci řešení projektu FR CESNETu

Projekt FR CESNETu:

Vytvoření bezpečnostního týmu CSIRT (CSIRT-CUNI pracoviště), vybudování monitorovacích systémů pro podporu řešení bezpečnostních incidentů a detekci anomálií v datových sítích Univerzity Karlovy v Praze, zapojení Univerzity Karlovy do systému pro sdílení informací o detekovaných bezpečnostních událostech Warden (http://warden.cesnet.cz).

Cíle projektu

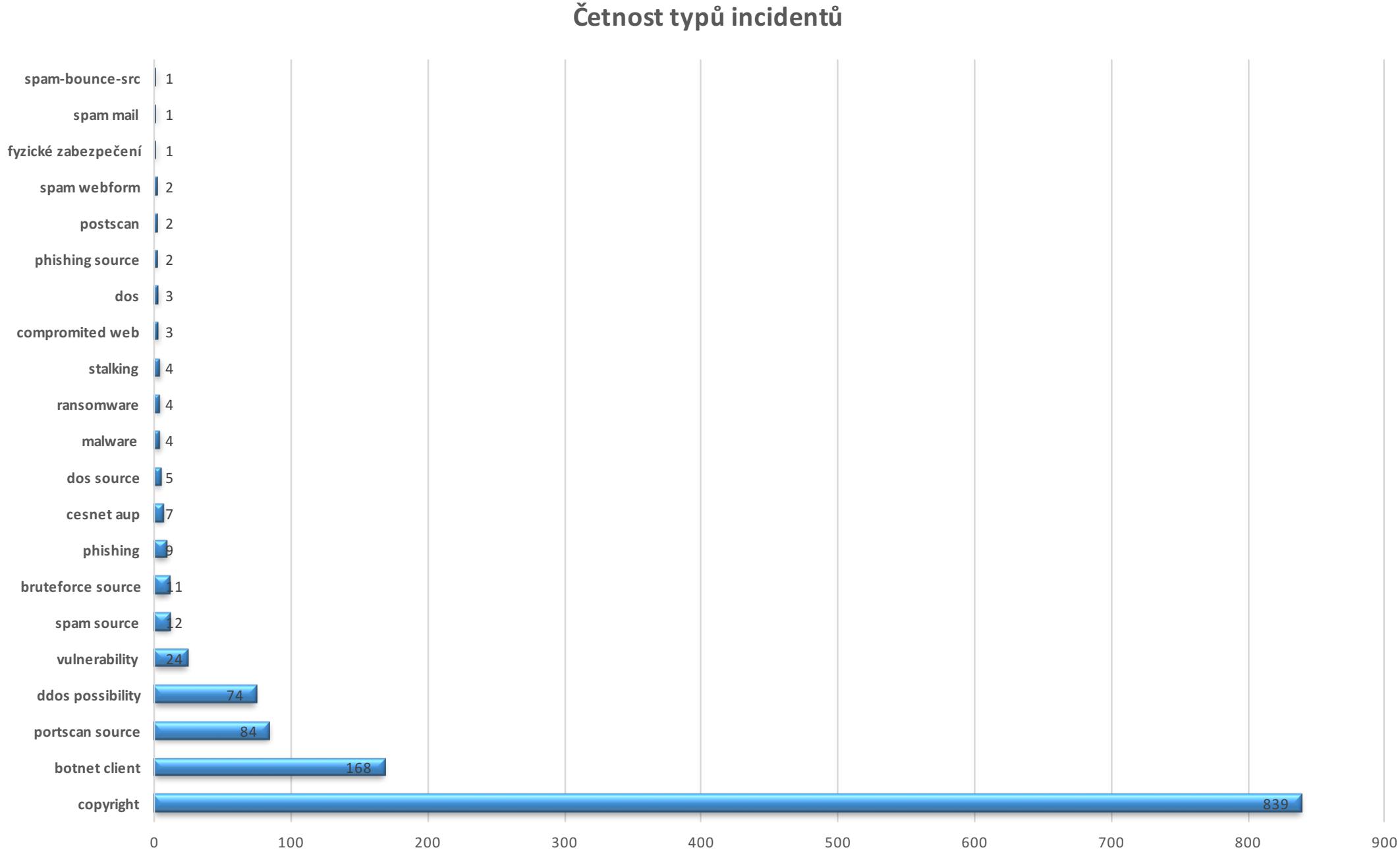
- Vytvoření CSIRT týmu
- Pilotní detekce anomálií systémem FlowMon ADS
- Detekce zranitelností systémem Nessus
- Provázání se systémem Warden

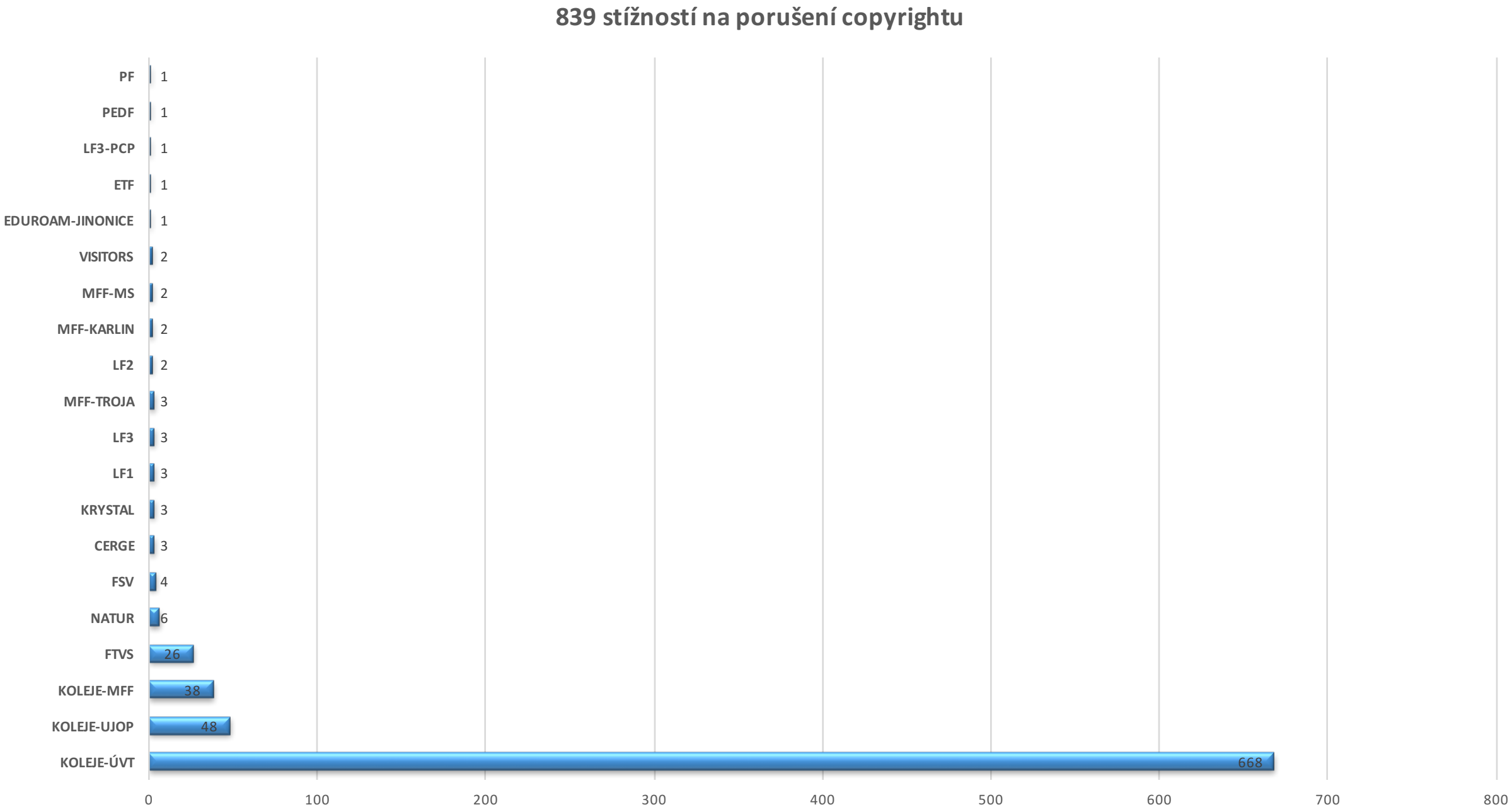
Přehled incidentů během pilotního provozu

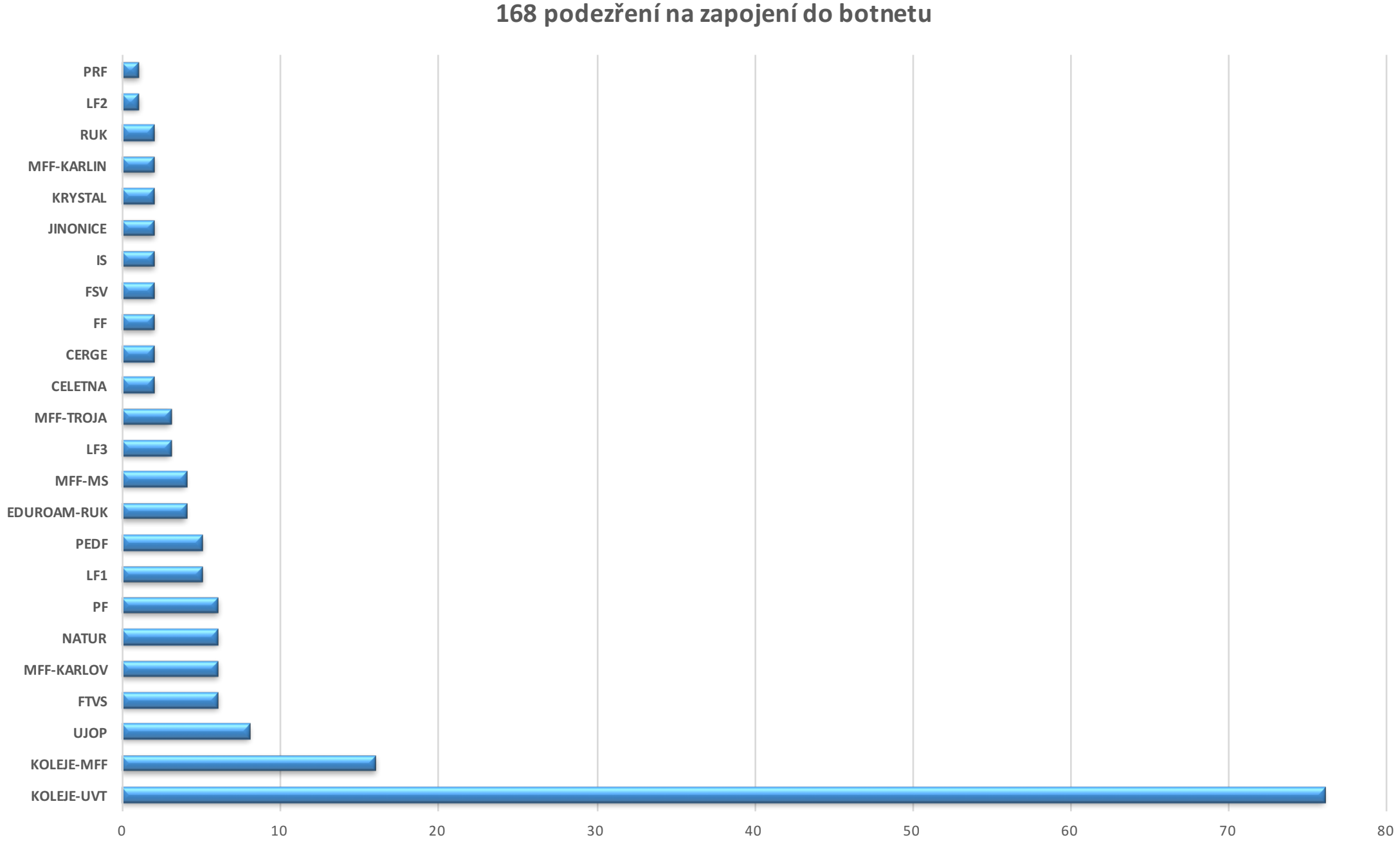
- Pilotní provoz od května 2015 (330 dní)
- 1261 ticketů/incidentů
- 8 žádostí policie o informace

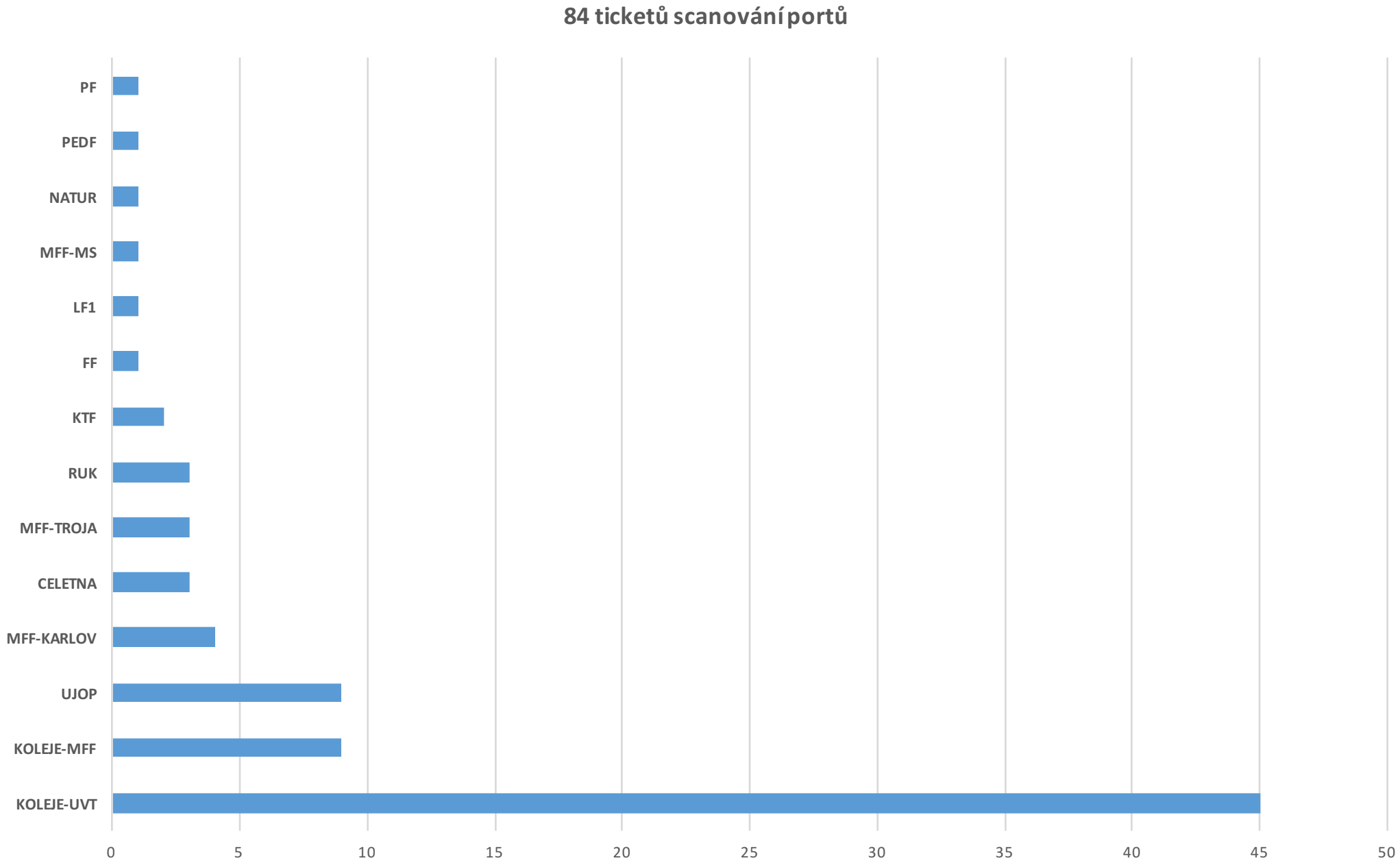
Počty incidentů podle sítí

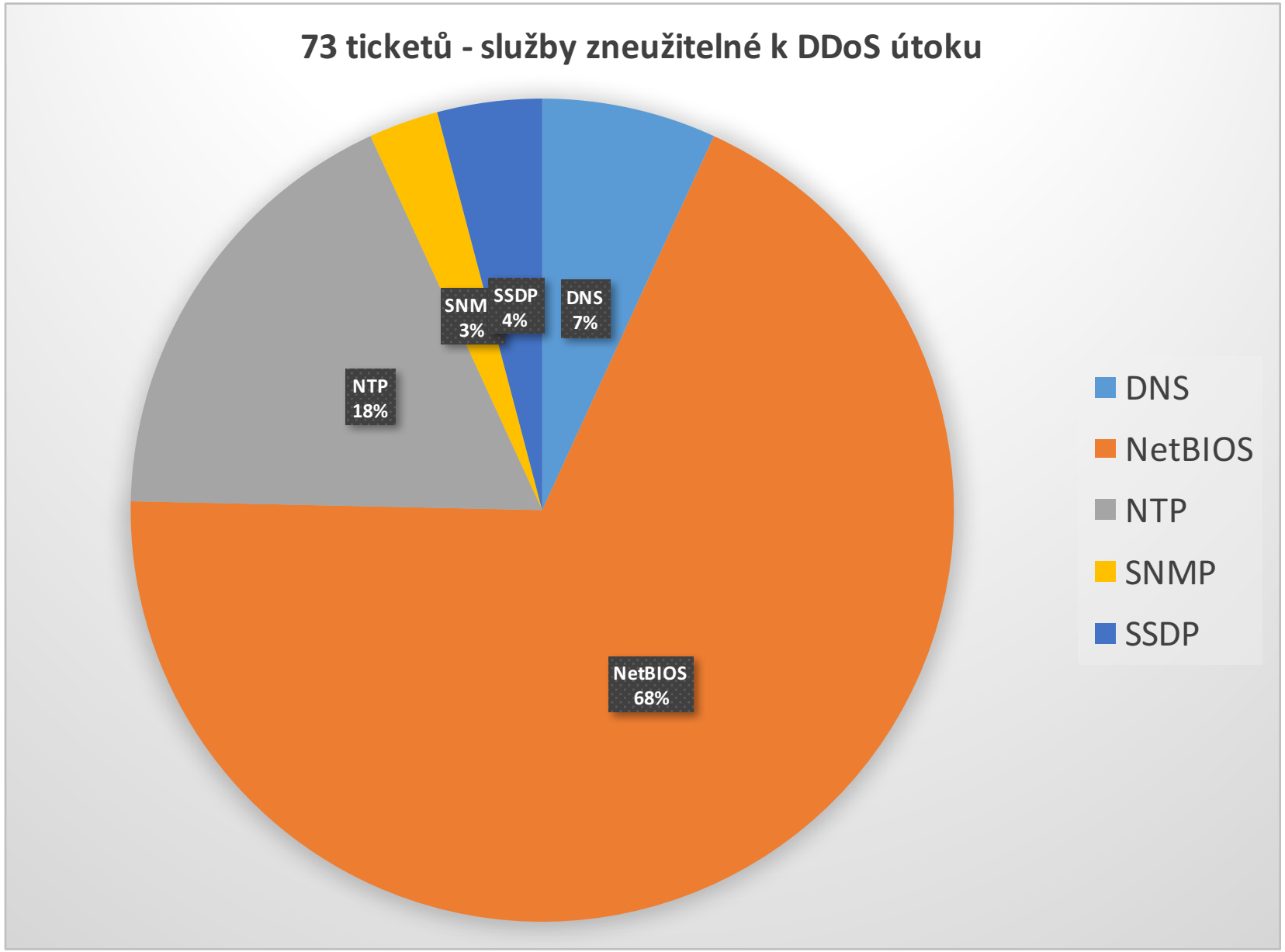
CELETNÁ	12	**IS**	3	**LF2**	9	**PEDF**	12
CERGE	7	**JINONICE**	7	**LF3**	12	**PF**	11
EDUROAM	5	**KOLEJE-MFF**	65	**LF3-PCP**	26	**RUK**	24
ETF	2	**KOLEJE-ÚVT**	824	**LFHK**	1	**UJOP**	66
FF	9	**KRYSTAL**	5	**MFF**	47	**VISITORS**	1
FSV	16	**KTF**	7	**NATUR**	18	**-**	20
FTVS	34	**LF1**	12	**PASNET**	4		

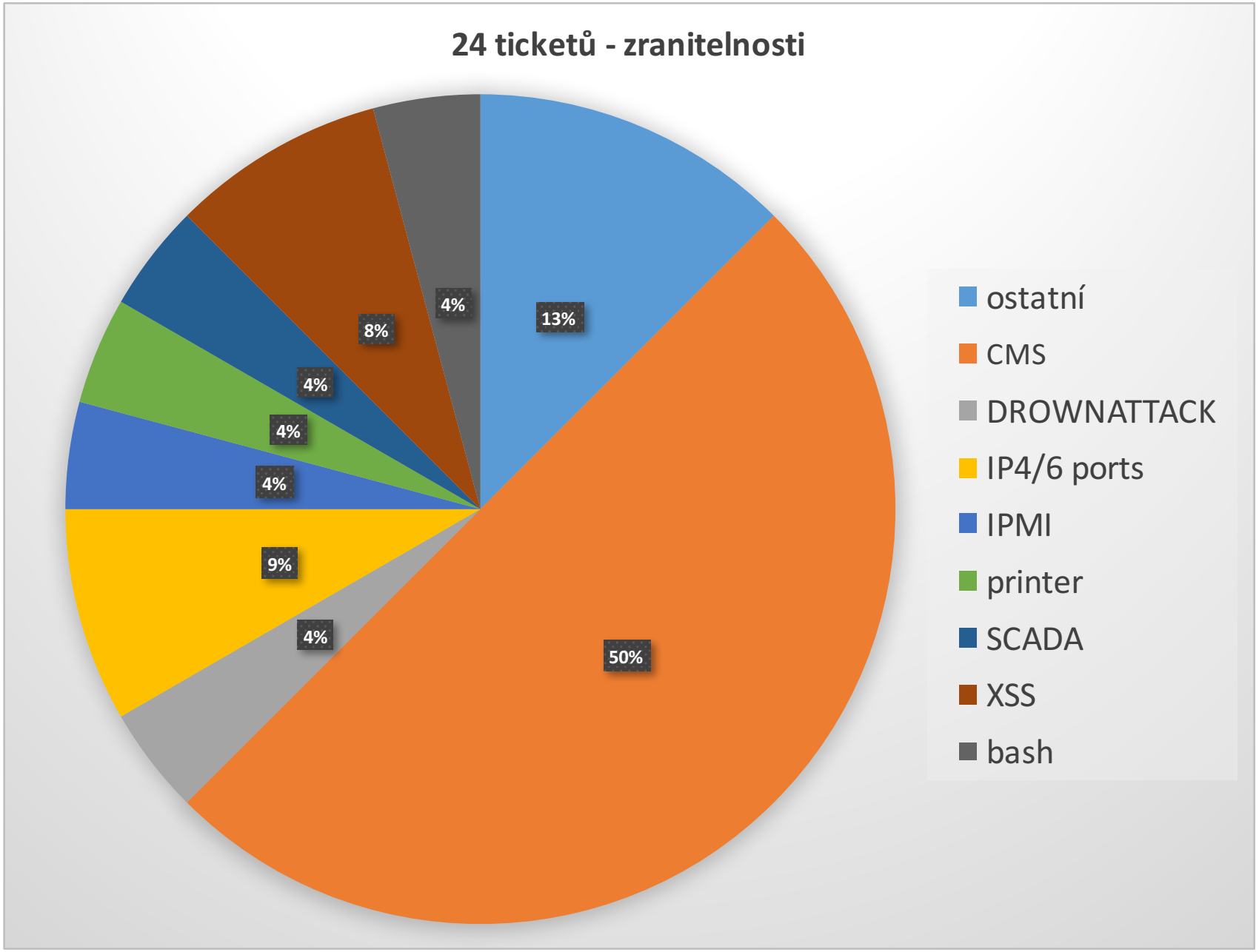

Četnost typů incidentů
spam-bounce-src 1
spam mail 1
fyzické zabezpečení 1
spam webform 2
postscan 2
phishing source 2
dos 3
compromited web 3
stalking 4
ransomware 4
malware 4
dos source 5
cesnet aup 7
phishing 9
bruteforce source 11
spam source 12
vulnerability 24
ddos possibility 74
portscan source 84
botnet client 168
copyright 839
0 100 200 300 400 500 600 700 800 900


839 stížností na porušení copyrightu
PF 1
PEDF 1
LF3-PCP 1
ETF 1
EDUROAM-JINONICE 1
VISITORS 2
MFF-MS 2
MFF-KARLIN 2
LF2 2
MFF-TROJA 3
LF3 3
LF1 3
KRYSTAL 3
CERGE 3
FSV 4
NATUR 6
FTVS 26
KOLEJE-MFF 38
KOLEJE-UJOP 48
KOLEJE-ÚVT 668
0 100 200 300 400 500 600 700 800


168 podezření na zapojení do botnetu
PRF
LF2
RUK
MFF-KARLIN
KRYSTAL
JINONICE
IS
FSV
FF
CERGE
CELETNA
MFF-TROJA
LF3
MFF-MS
EDUROAM-RUK
PEDF
LF1
PF
NATUR
MFF-KARLOV
FTVS
UJOP
KOLEJE-MFF
KOLEJE-UVT
0
10
20
30
40
50
60
70
80


84 ticketů scanování portů
PF
PEDF
NATUR
MFF-MS
LF1
FF
KTF
RUK
MFF-TROJA
CELETNA
MFF-KARLOV
UJOP
KOLEJE-MFF
KOLEJE-UVT
0
5
10
15
20
25
30
35
40
45
50


73 ticketů - služby zneužitelné k DDoS útoku
SNM 3%
SSDP 4%
DNS 7%
NTP 18%
NetBIOS 68%
DNS
NetBIOS
NTP
SNMP
SSDP


24 ticketů - zranitelnosti
13%
50%
4%
9%
4%
4%
4%
8%
4%
ostatní
CMS
DROWNATTACK
IP4/6 ports
IPMI
printer
SCADA
XSS
bash

Ukázky z nástrojů

- NetFlow na rozhraní PASNET/CESNET
  - Invea FlowMon, ADS
- Nessus
- CESNET Warden/Mentat

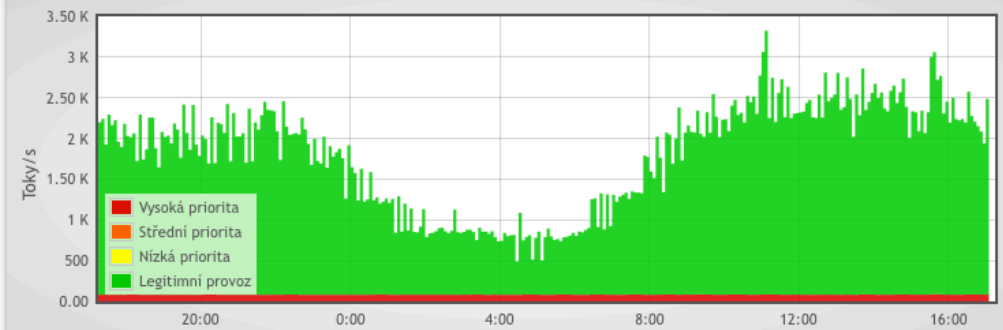
Vyhledávací kritéria

Od 2016-04-12 17:17 Do 2016-04-13 17:17 Vyhledat Reset

Perspektiva UK Zdroj NetFlow Default

Přehledový graf | Události

Provoz dle toků



Toky | Bajty | Pakety

Statistika provozu (2016-04-12 17:17 - 2016-04-13 17:20)

✔	Priorita	Toky	Průměr toků	Bajty	Průměr bajtů	Pakety	Průměr paketů
☑	Vysoká priorita	144.6 K toků	1.668 toků/s	823.9 MiB	9.7 KiB/s	3.9 M paketů	45.5 paketů/s
☑	Střední priorita	0.0 toků	0.000 toků/s	0.0B	0.0B/s	0.0 paketů	0.0 paketů/s
☑	Nízká priorita	0.0 toků	0.000 toků/s	0.0B	0.0B/s	0.0 paketů	0.0 paketů/s
☑	Legitimní provoz	150.3 M toků	1.733 K toků/s	11.7 TiB	141.3 MiB/s	12.0 G paketů	138.2 K paketů/s
	Celkový provoz	150.4 M toků	1.735 K toků/s	11.7 TiB	141.4 MiB/s	12.0 G paketů	138.3 K paketů/s

10 nejprioritnějších typů událostí (8404) | Hrozby (Agregované události) (13)

2016-04-12 17:17 - 2016-04-13 17:17

- Malware infected device. (MALWARE) — 9 hrozeb
  - 78.128.185.86 (...) — 1 hrozeb
    - Event count: 2
      Čas: 2016-04-13 17:04:46 - 17:05:00, Neuzavřená

#	Zdroj	Typ události	Detail	Časová známka	Zdroj NetFlow dat	Cíle
1	78.128.185.86 (...)	BLACKLIST	Known botnet command & control center, attempts: 4, uploaded: 556.00 B, downloaded: 0.00 B, frequently used port(s): 80.	2016-04-13 17:10:56	Default	195.16.127.102 (...)
2	78.128.185.86 (...)	BLACKLIST	Known botnet command & control center, attempts: 3, uploaded: 404.00 B, downloaded: 0.00 B, frequently used port(s): 80.	2016-04-13 17:05:00	Default	195.16.127.102 (...)
3	78.128.185.86 (...)	BLACKLIST	Known botnet command & control center, attempts: 1, uploaded: 52.00 B, downloaded: 0.00 B, frequently used port(s): 80.	2016-04-13 17:04:46	Default	195.16.127.102 (...)

OS: Microsoft Windows Server 2003

Results Summary

Critical	High	Medium	Low	Info	Total
2	7	7	2	31	49

Results Details

0/tcp

- 84729 - Microsoft Windows Server 2003 Unsupported Installation Detection [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]
- 11936 - OS Identification [-/+]
- 54615 - Device Type [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 66334 - Patch Report [-/+]
- 19506 - Nessus Scan Information [-/+]

0/udp

- 10287 - Traceroute Information [-/+]

21/tcp

- 10079 - Anonymous FTP Enabled [-/+]
- 45112 - FileZilla Server < 0.9.31 Denial of Service [-/+]
- 34324 - FTP Supports Cleartext Authentication [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 22964 - Service Detection [-/+]
- 10092 - FTP Server Detection [-/+]

80/tcp

- 58987 - PHP Unsupported Version Detection [-/+]
- 50069 - Apache 2.0.x < 2.0.64 Multiple Vulnerabilities [-/+]
- 68914 - Apache 2.0.x < 2.0.65 Multiple Vulnerabilities [-/+]
- 57537 - PHP < 5.3.9 Multiple Vulnerabilities [-/+]
- 58966 - PHP < 5.3.11 Multiple Vulnerabilities [-/+]

Home
Group dashboards
Reports
Alerts
Event library
Whois
Group management

Reports

Report ID or type, abuse contact o | From: YYYY-MM-DD HH:MM:S | To: YYYY-MM-DD HH:MM:S | Search

Displaying items **1** to **30** (**30** items of **2,295** total) | Page **1** of **77**

1 2 3 4 5 6 7 › »

#	?	Time period	Report ID	Abuse contact	Node	ECNT | UNIQ | ACNT | CCNT	Delay
1	M	2016-04-13 08:00:00 - 2016-04-13 10:00:00	M20160413EM-ykMAI	abuse@cuni.cz	78.128.196.57	1 1 1 1	7m 45s
2	M		M20160413EM-oQRuV	abuse@cuni.cz	78.128.196.246	1 1 1 1	7m 45s
3	M		M20160413EM-mBVJG	abuse@cuni.cz	78.128.196.124	1 1 1 1	7m 45s
4	M		M20160413SM-4BvNS	abuse@cuni.cz	78.128.196.57 (3 total)	3 3 1 1	7m 45s
5	M	2016-04-13 06:00:00 - 2016-04-13 08:00:00	M20160413EM-nmm7H	abuse@cuni.cz	78.128.173.147	1 1 1 2	7m 53s
6	M		M20160413EM-hcYVk	abuse@cuni.cz	78.128.160.7	1 1 1 2	7m 53s
7	M		M20160413SM-xl0uU	abuse@cuni.cz	78.128.173.147 (2 total)	2 2 1 2	7m 53s
8	L	2016-04-12 02:00:00 - 2016-04-13 02:00:00	M20160413EL-SLZ1R	abuse@cuni.cz	78.128.166.140	1 1 1 1	8m 5s
9	L		M20160413EL-X0luK	abuse@cuni.cz	195.113.20.68	1 1 1 1	8m 5s
10	L		M20160413SL-ZVENV	abuse@cuni.cz	195.113.20.68 (2 total)	2 2 1 1	8m 5s
11	M	2016-04-12 08:00:00 - 2016-04-12 10:00:00	M20160412EM-nNG8d	abuse@cuni.cz	78.128.196.229	1 1 1 1	8m 22s
12	M		M20160412EM-dBslQ	abuse@cuni.cz	78.128.195.235	1 1 1 1	8m 22s
13	M		M20160412EM-loME3	abuse@cuni.cz	195.113.40.5	1 1 1 1	8m 22s
14	H	2016-02-01 15:20:00 -	M20160202EH-dJZ0E	abuse@cuni.cz	195.113.53.91	1 1 1 1	4m 15s

Home
Group dashboards
Reports
Alerts
Event library
Whois
Group management

Report detail

Home / Reports / Detail

Report M20160413EM-ykMAI

Unprotected access: https://mentat-hub.cesnet.cz/mentat/unauth/report/ID8HxqYmGZtFVK8HGpA3

Severity	Abuse	Created
medium	abuse@cuni.cz	2016-04-13 10:07:45

Report timing

Time period	2016-04-13 08:00:00 - 2016-04-13 10:00:00 (2h)
Report sent	2016-04-13 10:07:45 | Report mailed to abuse contact 'abuse@cuni.cz'
Delay	7m 45s

Report magnitude

Event count	1 (1 entered filtering, 0 blocked, 0 thresholded)
IP count	1 unique IP address
Diversisty	1 analyzer, 1 category

Actions

- Download report data in JSON
- Download report data in CSV

Report menu

- Report message
- Report statistics
- Applied filters
- Last 30 viewers

Report message

```
Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

 [1]     Hlášení o strojích poskytujících službu UDP NETBIOS Name Service, které
    lze zneužít k útokům typu DDoS (Scan NETBIOS):

    * Analyzer:  SSERV
    * Popis:     Scan NETBIOS
    * Kategorie: Vulnerable.Config
    ================================================================================
     IP             | Čas                                           | # událostí
    ================================================================================
    78.128.196.57   | 2016-04-12 03:45:25 - 2016-04-13 09:51:13 | 1
    --------------------------------------------------------------------------------
    * Celkem 1 událost, 1 unikátní IP adresa
```