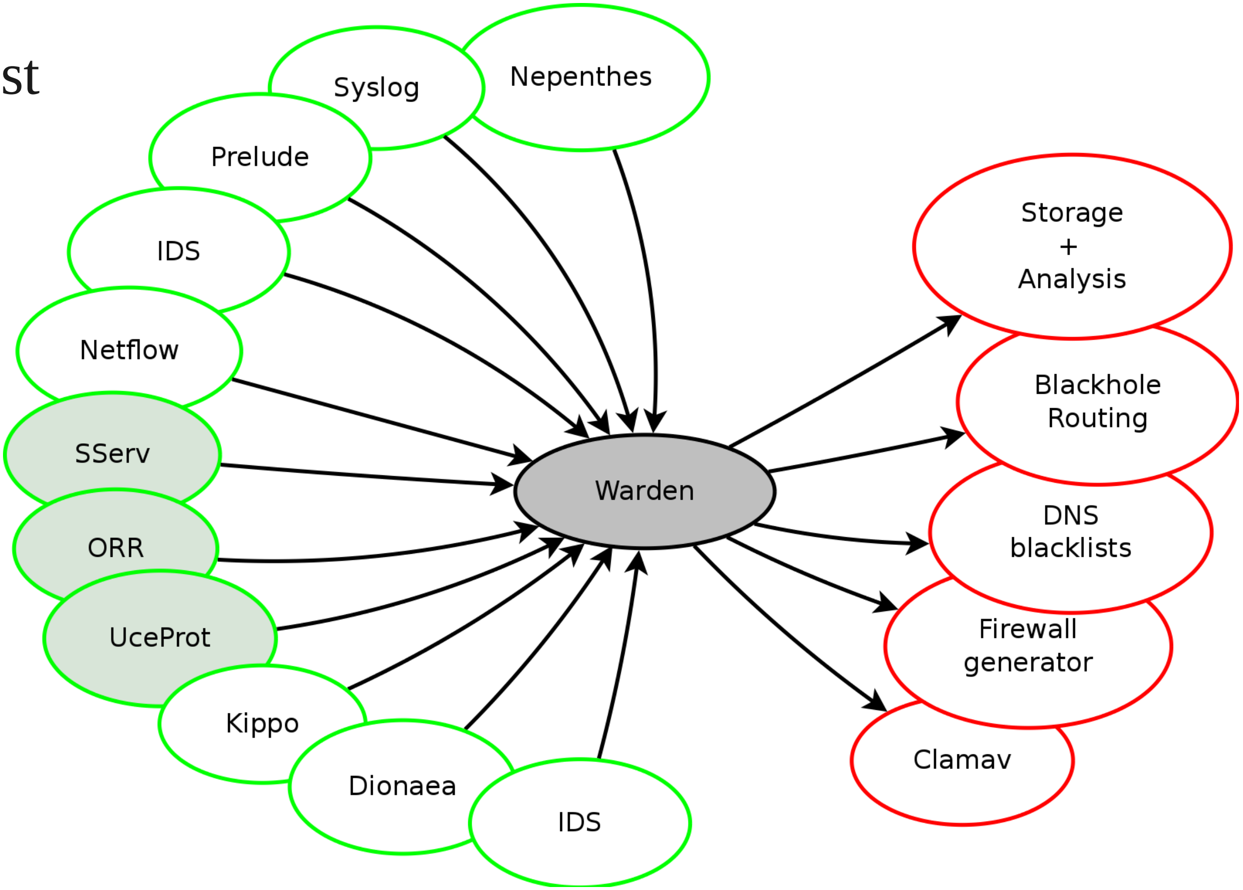
Automated information exchange in CESNET

Ing. Pavel Kácha
<ph@cesnet.cz>

CESNET-CERTS Computer Security Incident Response Team
CESNET
Prague
CZECH REPUBLIC

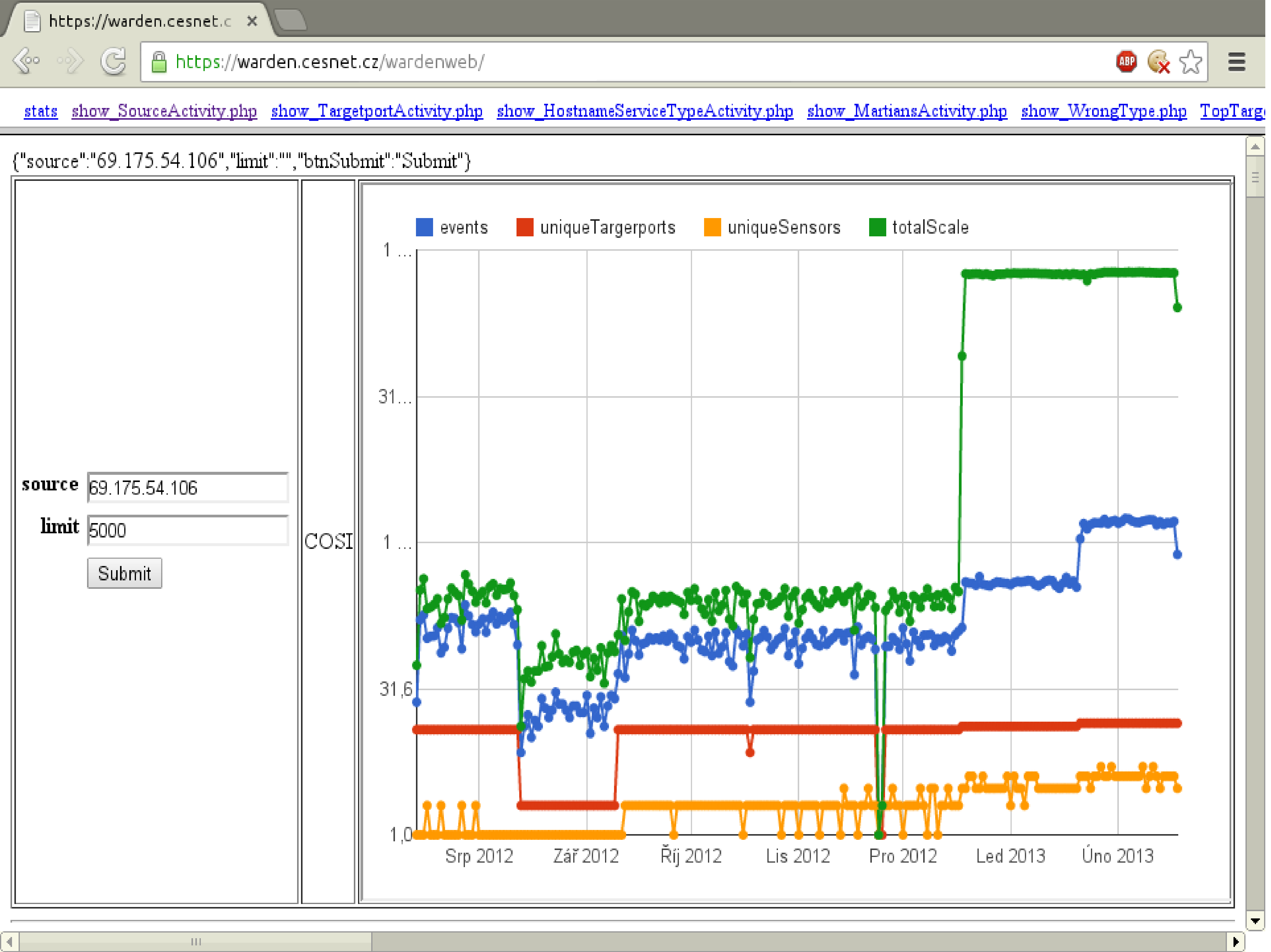
Warden Concepts

- Client/server architecture
- Events, not processes (we don't know end)
- Glorified queue
  - Only new events, no past
- Security
  - Authentication (X509)
  - Encryption
  - Tests of “saneness”
  - Peer review



Event

- *Hostname*, *Service*: e.g. ids.cesnet.cz, CESNET_IDS
- *Detection time, arrival time*
- *Event type*
  - Portscan, bruteforce, spam, phishing, botnet_c_c, dos, malware, copyright, webattack, other
- *Source*: IP/URL/Reply-To
  - 195.113.134.190, http://www.example.org/something
- *Aim*: protocol TCP, port 22
- *Scale*: scan 666 ports, sweep 66 machines
- *Note*: Free text note
- *Client tags:* Network, Connection, Honeypot, LaBrea



stats show_SourceActivity.php show_TargetportActivity.php show_HostnameServiceTypeActivity.php show_MartiansActivity.php show_WrongType.php TopTarg

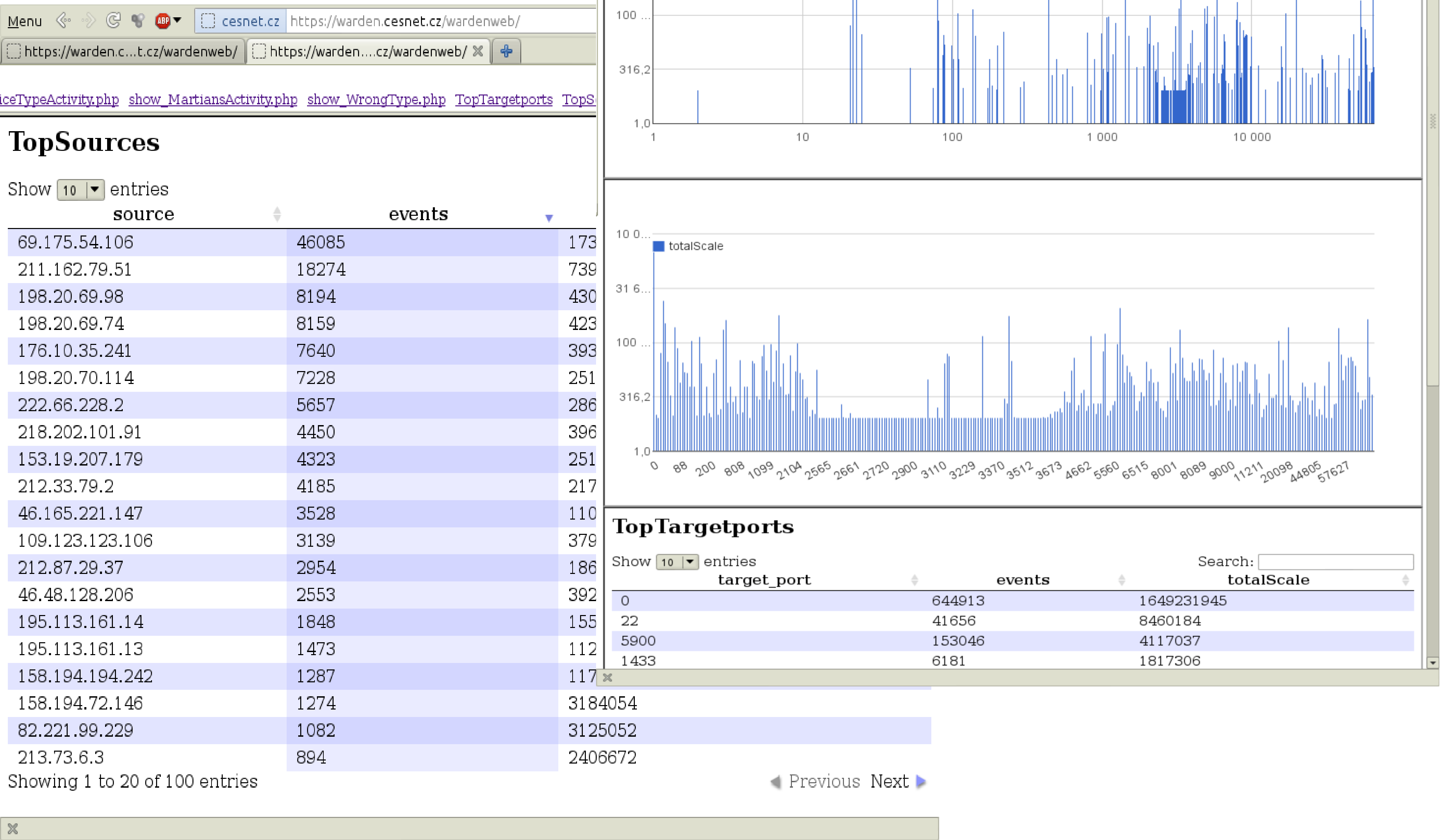
{"source":"69.175.54.106","limit":"","btnSubmit":"Submit"}

source 69.175.54.106

limit 5000

Submit

COSI



TopSources

Show 10 entries

source	events	
69.175.54.106	46085	173
211.162.79.51	18274	739
198.20.69.98	8194	430
198.20.69.74	8159	423
176.10.35.241	7640	393
198.20.70.114	7228	251
222.66.228.2	5657	286
218.202.101.91	4450	396
153.19.207.179	4323	251
212.33.79.2	4185	217
46.165.221.147	3528	110
109.123.123.106	3139	379
212.87.29.37	2954	186
46.48.128.206	2553	392
195.113.161.14	1848	155
195.113.161.13	1473	112
158.194.194.242	1287	117
158.194.72.146	1274	3184054
82.221.99.229	1082	3125052
213.73.6.3	894	2406672

Showing 1 to 20 of 100 entries

TopTargetports

target_port	events	totalScale
0	644913	1649231945
22	41656	8460184
5900	153046	4117037
1433	6181	1817306

Connected organizations

- CESNET *(LaBrea, Dionaea, Kippo, SSHbruteforce , netflow, 3rd party)*
- Masaryk University Brno *(netflow scans, honeypots, SSH bruteforce)*
- Technical University of Ostrava *(Kippo, SSH bruteforce)*
- Brno University of Technology *(honeypots)*
- University of West Bohemia *(HiHat, LaBrea)*
- Silesian University in Opava *(Kippo)*
- Technical University of Liberec *(honeypots)*

4 mil. of events last year, cca. 80 events per minute
28 mil., i.e. 332 malicious connections or attacks per second

Pitfalls

- Rigid format
  - Single attacker, single target
  - Not extensible
  - No voluntary anonymization
  - Cannot usably map most of the information from external sources
  - No common taxonomy
  - Standards (or lack of them)

- SOAP
  - Fragile in Perl
  - Dependencies from hell
  - Problems with X509

- NOW WHAT?
  - IDMEF? IODEF? X-ARF? AbuseHelper format?

IDEA – Intrusion Detection Extensible Alert

- Keys at the same places, same types, at most two level depth
  Friendly to relational database guys
- JSON data model
  Friendly to nosql/document database guys
- Extensibility (we're out of crystal balls)
  Producers free to include new non colliding keys
- Incompleteness, anonymisation, spoofing
  We do not know precise IP, it just belongs into specified range
  We do not want to disclose precise IP, it just belongs into range
  This IP/hostname/whatever is spoofed
- Machine parseable, human readable
- Standards
  - JSON, mkII, RFC 3339 – timestamps, RFC6335 – protocols, RFC2141, RFC 1738, RFC 1818 – URI, RFC 2046 – media types

IDEA example

```
{

   "Format": "IDEA0",
   "ID": "4390fc3f-c753-4a3e-bc83-1b44f24baf75",
   "DetectTime": "2012-11-03T10:00Z",
   "WindowStartTime": "2012-11-03T05:00Z",
   "WindowEndTime": "2012-11-03T10:00Z",
   "CreateTime": "2012-11-03T10:02Z",
   "FirstSeenTime": "2012-11-03T07:36Z",
   "LastSeenTime": "2012-11-03T09:55Z",
   "Category": "Phishing",
   "Reference": "cve:CVE-1234-5678",
   "Description": "Phishing on IMP",
   "Source": [
      {
         "Type": "PhishingURL",
         "IP4": ["192.0.43.10"],
         "URL": "http://www.example.com/cgi-bin/killemall",
         "Netname": "arin:ICANN-MDR"
      },
      {
         "Type": "PhishingSpamMTA",
         "IP": "10.0.0.5",
         "Hostname": "spammer.example.com",
      },
   ],
```

```
   "Target": [
      {
         "Type": "BackscatterEmail",
         "Email": "innocent@example.com",
         "Spoofed": 1,
      }
   ],
   "Attach": [
      {
         "ID": "att1",
         "FileName": "killemall",
         "Type": "malware",
         "Hash": "sha1:0c4a38c3569f0cc632e74f4c",
         "Size": 46,
         "Reference": "Trojan-Spy:W32/FinSpy.A"
      }
   ] ,
   "Node": [
      {
         "Name": "Kippo-sensor",
         "Realm": "example.org",
         "Tags": ["Network", "Honeypot", "Kippo"],
         "Software": "Kippo",
         "AggregationInterval": "0000-00-00T00:05Z",
      }
   ]
}
```

IDEA example (simplified)

```
Format:     IDEA0
ID: 4390fc3f-c753-4a3e-bc83-1b44f24baf75
DetectTime: 2012-11-03T10:00Z
WindowStartTime: 2012-11-03T05:00Z
WindowEndTime: 2012-11-03T10:00Z
CreateTime: 2012-11-03T10:02Z
FirstSeenTime: 2012-11-03T07:36Z
LastSeenTime: 2012-11-03T09:55Z
Category: Phishing
Reference: cve:CVE-1234-5678
Description: Phishing on IMP

Source:
        Type: PhishingURL
        IP4: 192.0.43.10
        URL: http://www.example.com/cgi-bin/killemall
        Netname: arin:ICANN-MDR

Source:
        Type: PhishingSpamMTA
        IP: 10.0.0.5
        Hostname: spammer.example.com
```

```
Target:
        Type: BackscatterEmail
        Email: innocent@example.com
        Spoofed: 1

Attach:
        ID: att1
        FileName: killemall
        Type: malware
        Hash: sha1:0c4a38c3569f0cc632e74f4c
        Size: 46
        Reference: Trojan-Spy:W32/FinSpy.A

Node:
        Name: Kippo-sensor
        Realm: example.org
        Tags: Network, Honeypot, Kippo
        Software: Kippo
        AggregationInterval: 0000-00-00T00:05Z
```

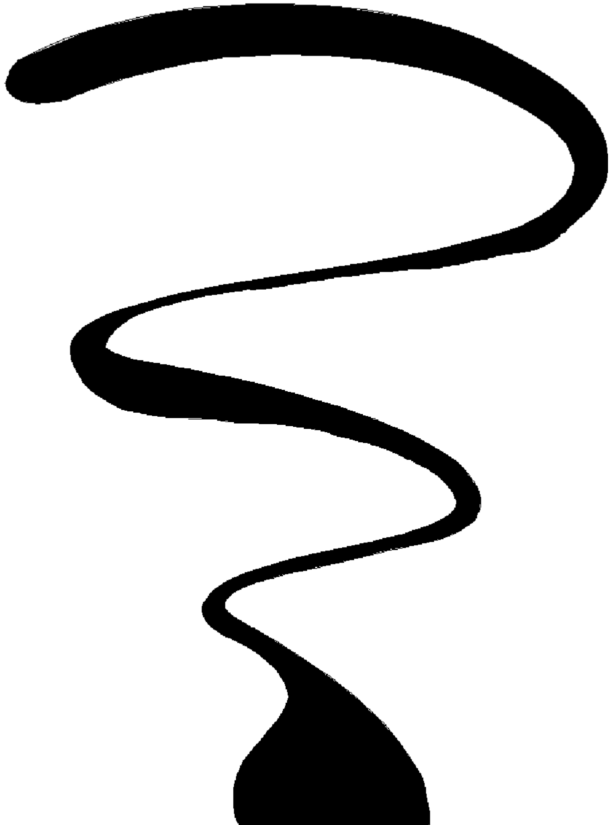
Taxonomies

- Incident classification
  - "mkII" taxonomy (by Don Stikvoort from SURFcert, itself based on eCSIRT.net taxonomy, and formerly Jimmi Arvidsson's taxonomy from Telia CERTCC)
  - Presented by Don at 39th TF-CSIRT meeting in Bucharest
- Protocols
  - RFC 6335 – IANA
- Sources of attack, detection nodes, payload classifications
  - See https://csirt.cesnet.cz/IDEA/Classifications

Links

- Website
  - https://csirt.cesnet.cz/Warden/Intro
- Download
  - ftp://homeproj.cesnet.cz/tar/warden
- IDEA
  - https://csirt.cesnet.cz/IDEA
- CESNET-CERTS
  - https://csirt.cesnet.cz/About%20us
- CESNET
  - http://www.cesnet.cz/?lang=en

Questions



Acknowledgment

- CESNET, z. s. p. o.
- Project “Large Infrastructure CESNET” (LM2010005) of the Ministry of Education, Youth and Sports of the Czech Republic
- MetaCentrum (load testing)