

Fighting cyber threats – CERT perspective

Current issues and research areas

Piotr Kijewski (piotr.kijewski@cert.pl)

4th EU-Japan Symposium on New Generation Networks and Future Internet

19th January 2012, Tokyo, Japan

THREAT DETECTION & INTELLIGENCE

Threat detection & intelligence (I)



Network Early Warning System
based on honeypots
(Arakis 2.0 currently being
implemented)



System for the
automated detection
of malicious URLs
based on honeyclients
– included in
WOMBAT
(HSN 2.0 under
development since
January 2011)



Worldwide Observatory of
Malicious Behaviour and
Attack threats – EU FP7
(project completed April
2011)

SOPAS

System for protection against
network attacks

Threat detection & intelligence (II)

Analysis of large security datasets

Looking at algorithms for analysis of large security datasets, visualization

DNS sec. research

Looking at ways to detect malicious domains at the registry level, passive DNS

Botnet research

Research into ways of automating analysis of botnets

Mobile threats

Research into automating ways of detection and analysis of malware on smartphones

Threat detection & intelligence (III)

Underground economy

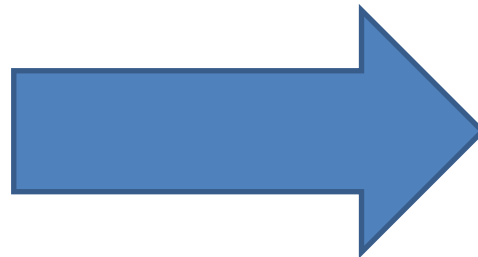
Key to understanding cybercrime, mobile threats give new dimension

Banking trojans

Classic „phishing” giving way to sophisticated threats – Zeus, ZITMO, SpyEye etc

Proactive Detection

Early warning services to the community



CERT FOCUS: PROACTIVE DETECTION

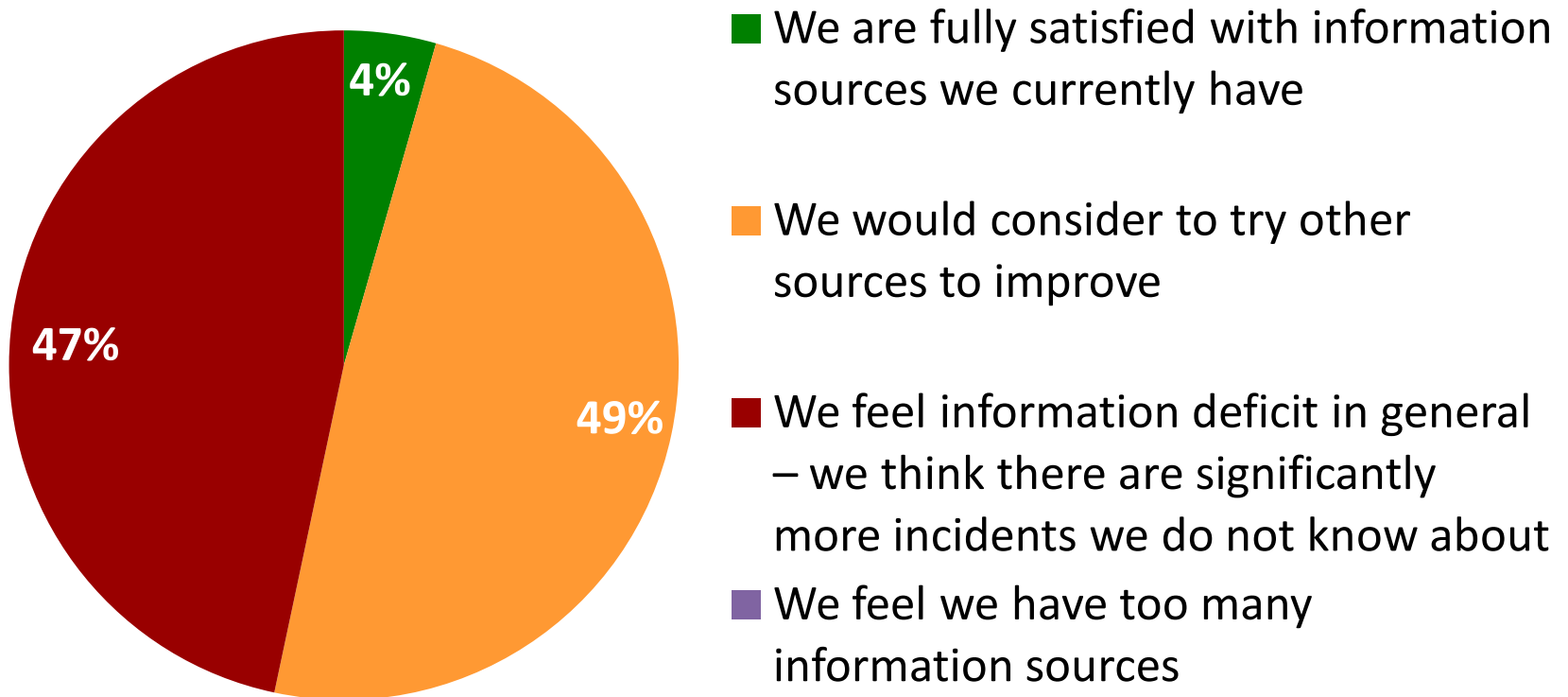
CERT Focus: Proactive Detection of Network Security Incidents

- ENISA commissioned survey & study (by CERT Polska)
- Mainly CERTs (national/governmental) but also others
- Major goals:
 - do a stocktaking of measures used by CERTs to proactively detect incidents
 - identify shortcomings and provide recommendations on how to mitigate them

CERT Focus: What is meant by proactive detection?

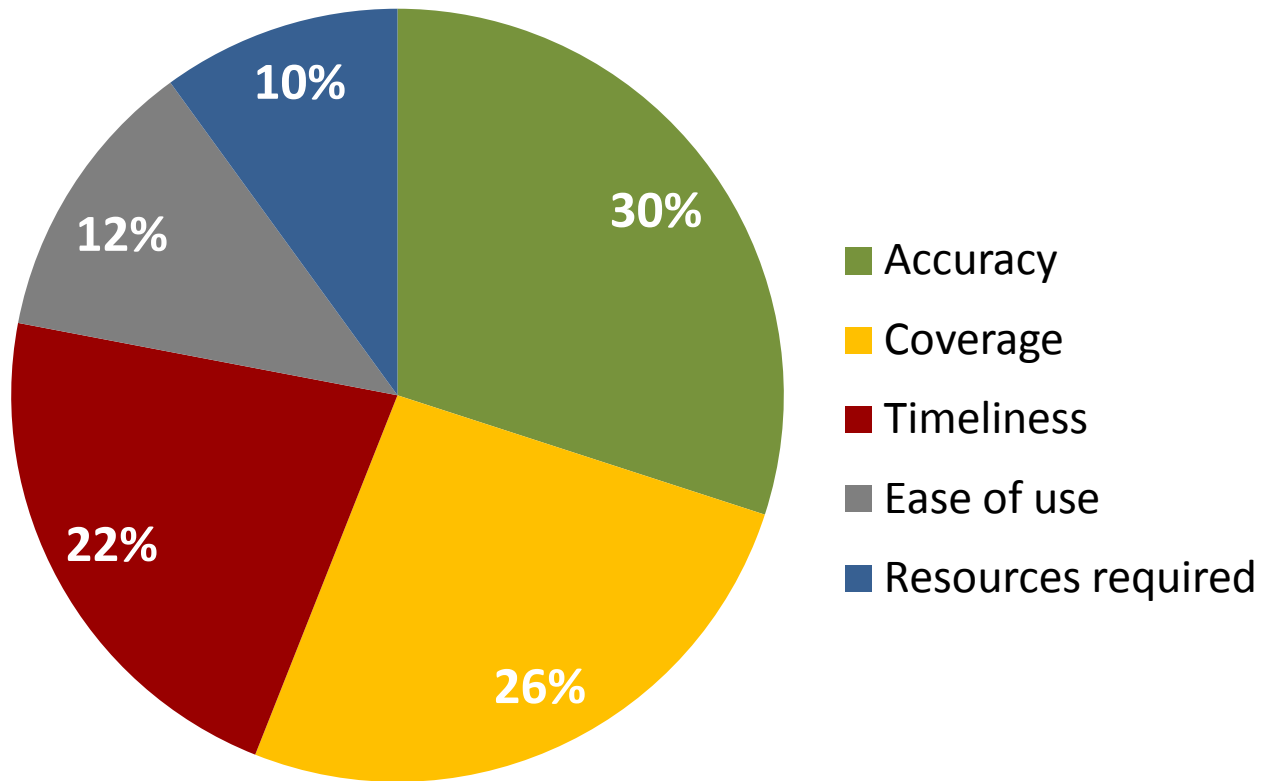
- Detection of malicious activity in a constituency before constituents become aware of the problem and report it themselves
- Effectively early warning for constituents
- Can be achieved by using external data feeds that report incidents or by deploying internal monitoring tools

CERT Focus: Feelings regarding info sources



Based on responses from 45 CERTs

CERT Focus: What would you like to improve?



Based on responses from 45 CERTs

CERT Focus: Some findings (I)

- Most popular source of information is used by only 40% CERTs
- Only 23,4% collect and share information about other constituencies
- Only 35,2% correlate automatically
- Lack of DDoS, data leak, targeted attack external information services ...
- Passive DNS underutilized

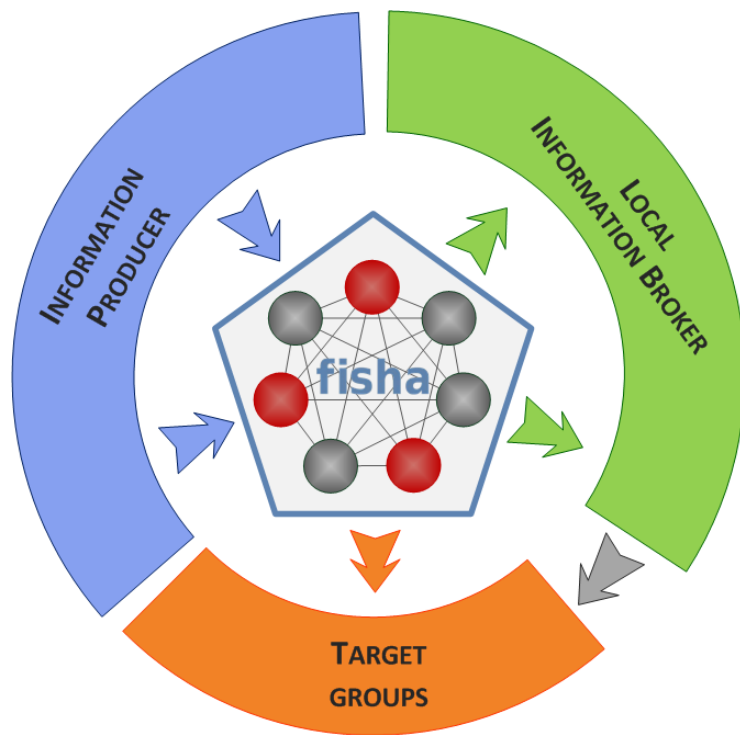
CERT Focus: Some findings (II)

- 30 external information sources identified and rated
- 16 shortcomings identified (technical/legal)
- 35 recommendations on improvements and potential research

More: <http://www.enisa.europa.eu/act/cert/support/proactive-detection/>

FACILITATING BETTER INFORMATION SHARING

Distribution of Security-related information



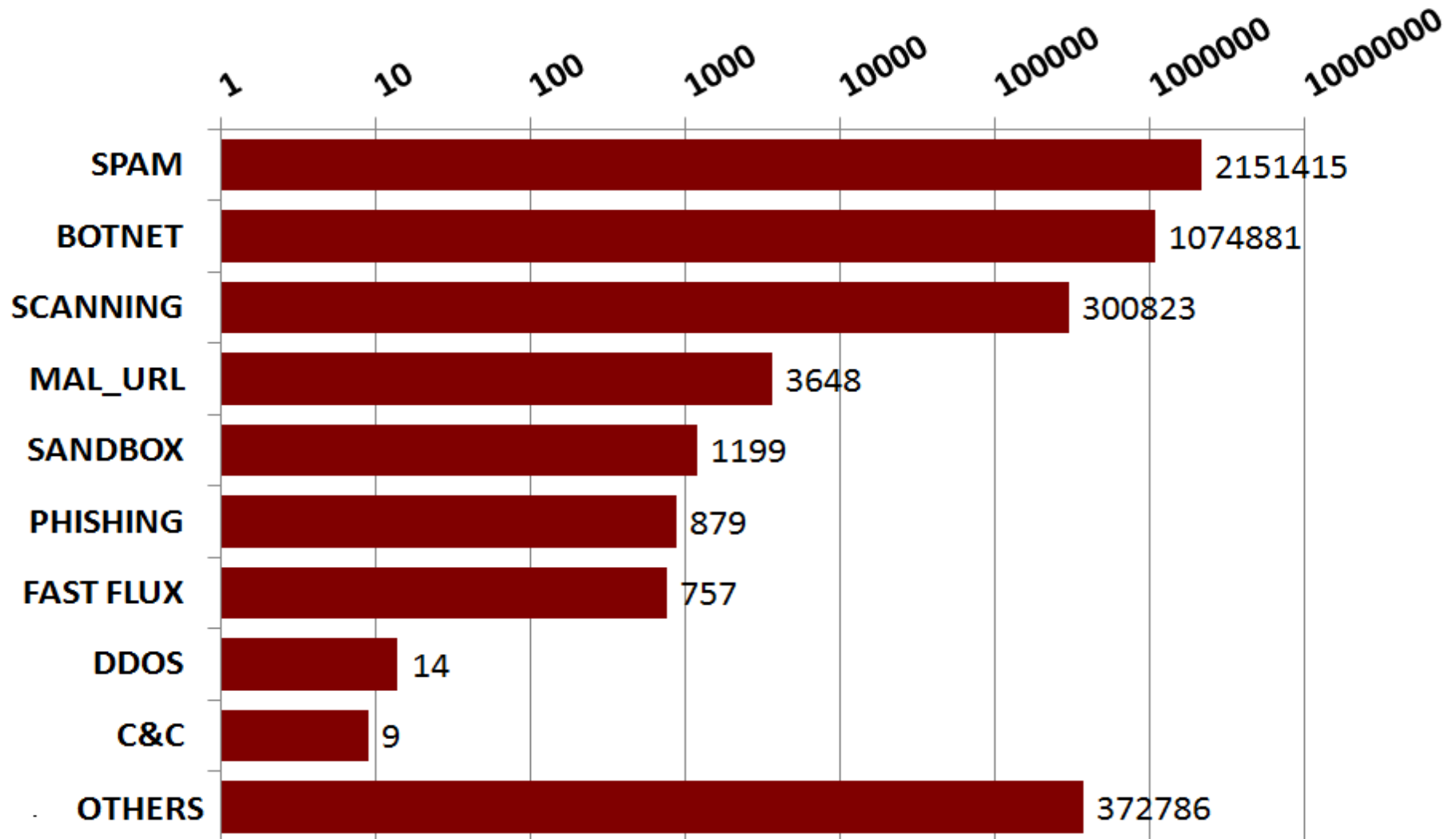
fisha 

Framework for Information
Sharing and Alerting
(completed Feb 2011)

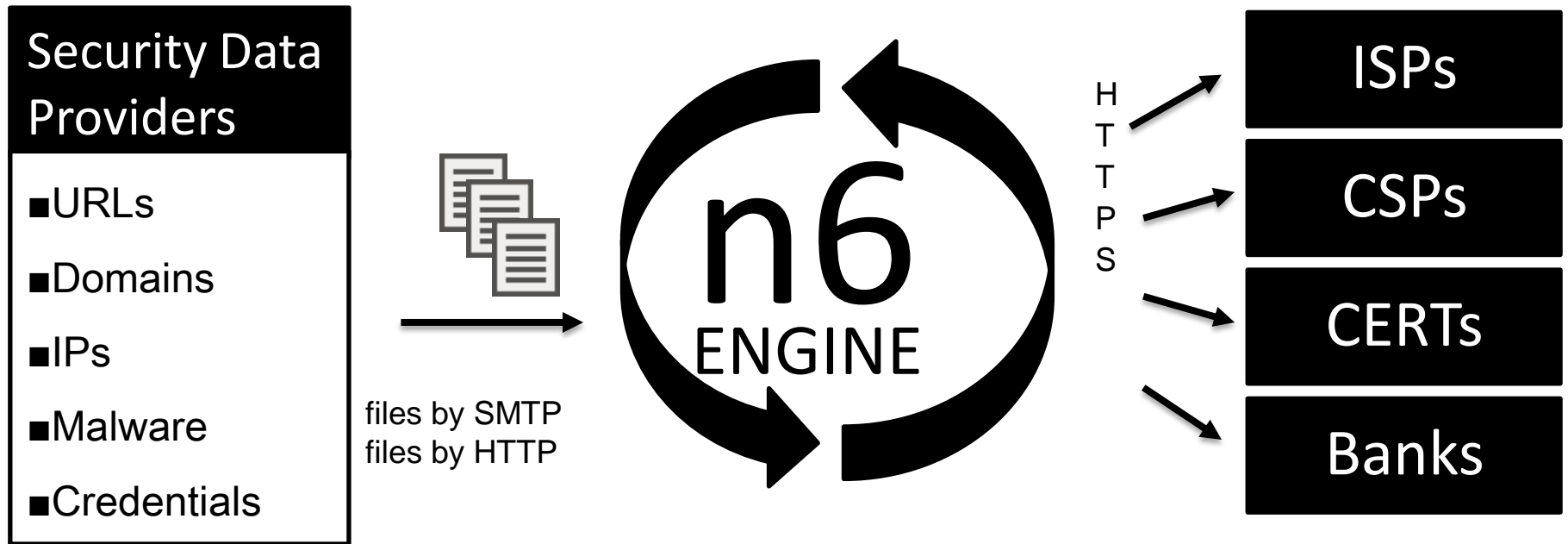
Followup project to
implement pilot: NISHA

(under EU programme
„Prevention, Preparedness
and Consequence
Management of Terrorism
and other Security Related
Risks” - CIPS)

Scale of incidents – Poland 1h2011



n6 PLATFORM – incident exchange



n6

What to share

Aggregated sources:

- our systems (ARAKIS, HSN, ...)
- external organizations - major data providers, including CERTs, vendors, other security organizations

Types of data

malicious URLs

malicious artifacts

infected hosts (bots)

scanning

C&C servers

DDoS

brute force

fast flux

phishing



Web: www.cert.pl

Facebook: facebook.com/cert.polska

Twitter: [@CERT_Polska_en](https://twitter.com/CERT_Polska_en)

Contact: info@cert.pl

THANK YOU!