CERT POLSKA

NASK

CERT R&D projects: handling the dynamic evolution of threats

Piotr Kijewski, Mirosław Maj, Krzysztof Silicki
NASK / CERT Polska
Warsaw, POLAND

piotr.kijewski@cert.pl, miroslaw.maj@cert.pl, krzysztof.silicki@nask.pl

22nd ANNUAL FIRST CONFERENCE MIAMI
JUNE 13-18, 2010

Introduction

- *CERTs (Computer Emergency Response Teams) as security incident handlers have hands-on experience with the latest attack techniques on the Internet.*
- *This is the result of direct contact with their constituency and other CERT teams, which often serve as the first line of support when faced with new threats.*
- *The dynamic development of threats remains a never ending challenge not just for them, but the entire security industry.*
- *Research and development projects that are launched in response to analyzing threats often have a problem keeping up and developing adequate tools that can be applied in practice. Nevertheless, creating new platforms that can facilitate detection and improve situation awareness is critical in order to stop these threats.*

Content

- We present technical issues concerning national and international research and development projects conducted by the CERT Polska team, operating in NASK structures. It gives an overview of:
  - how these projects support the operational activity of CERT, which determines the requirement for new tools and research – namely for projects having practical application in e.g. :
    - threat monitoring, correlation, early warning, malware analysis or effective transfer of information to proper recipients.
  - a few examples of building synergy between projects being implemented

The main technical projects of CERT Polska team

- ARAKIS Project
- HoneySpider Network Project
- WOMBAT Project
- FISHA Project

ARAKIS Project

www.arakis.pl

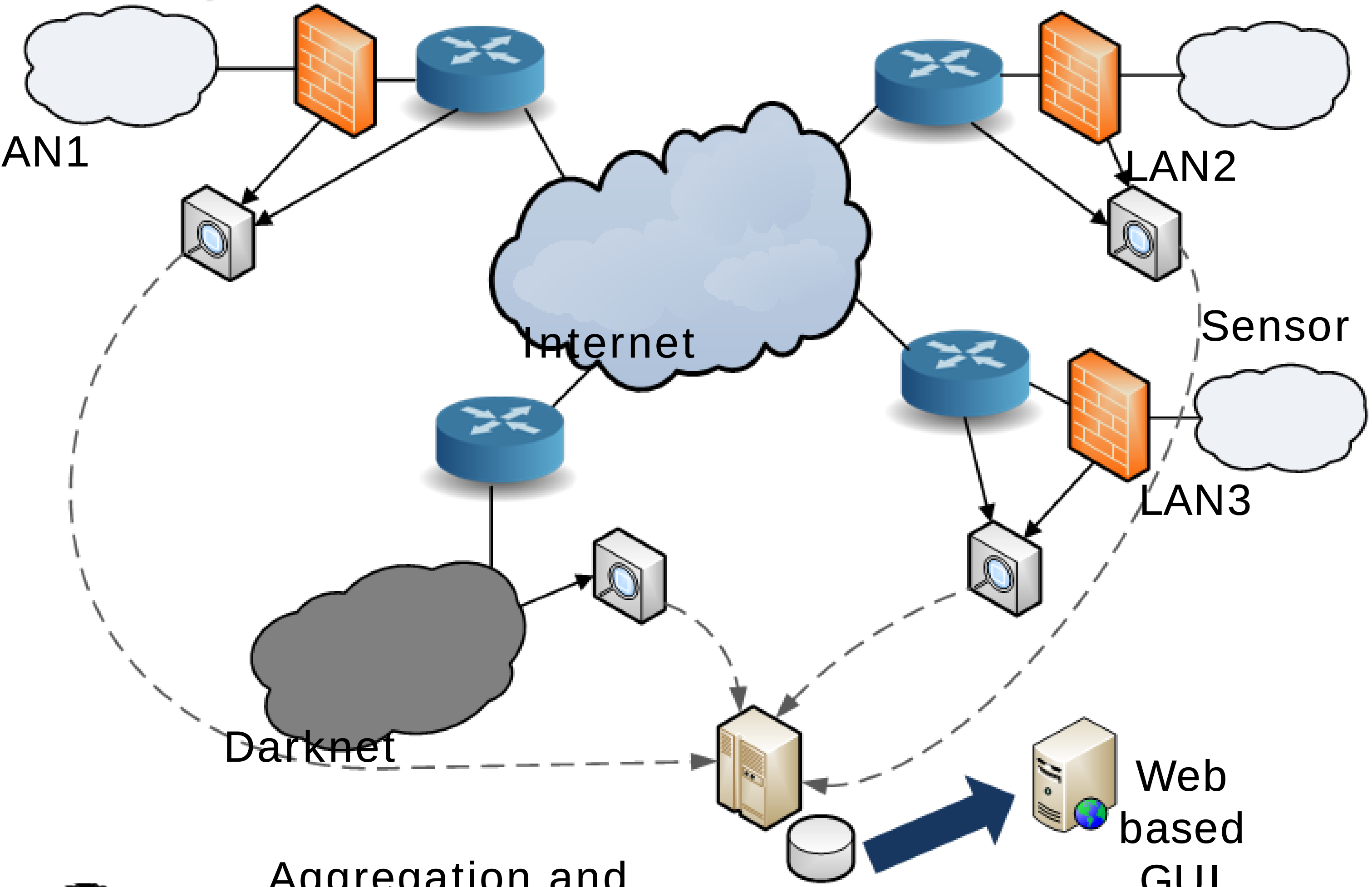
ARAKIS
agregacja, analiza i klasyfikacja incydentów sieciowych

- ARAKIS is a CERT Polska (NASK) project that aims to create an early warning and information system concerning novel network threats.
- The system developed as part of the project focuses on detection and characterization of new automated threats with a focus primarily, though not only, on exploits used in the wild, not malware.
- Currently the system detects threats that propagate actively through scanning.
- ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems. Each of these sources gives a different perspective on what is happening on the network.

ARAKIS Project

www.arakis.pl

ARAKIS
agregacja, analiza i klasyfikacja incydentów sieciowych



Aggregation and Analysis Center

Honey Spider Network Project

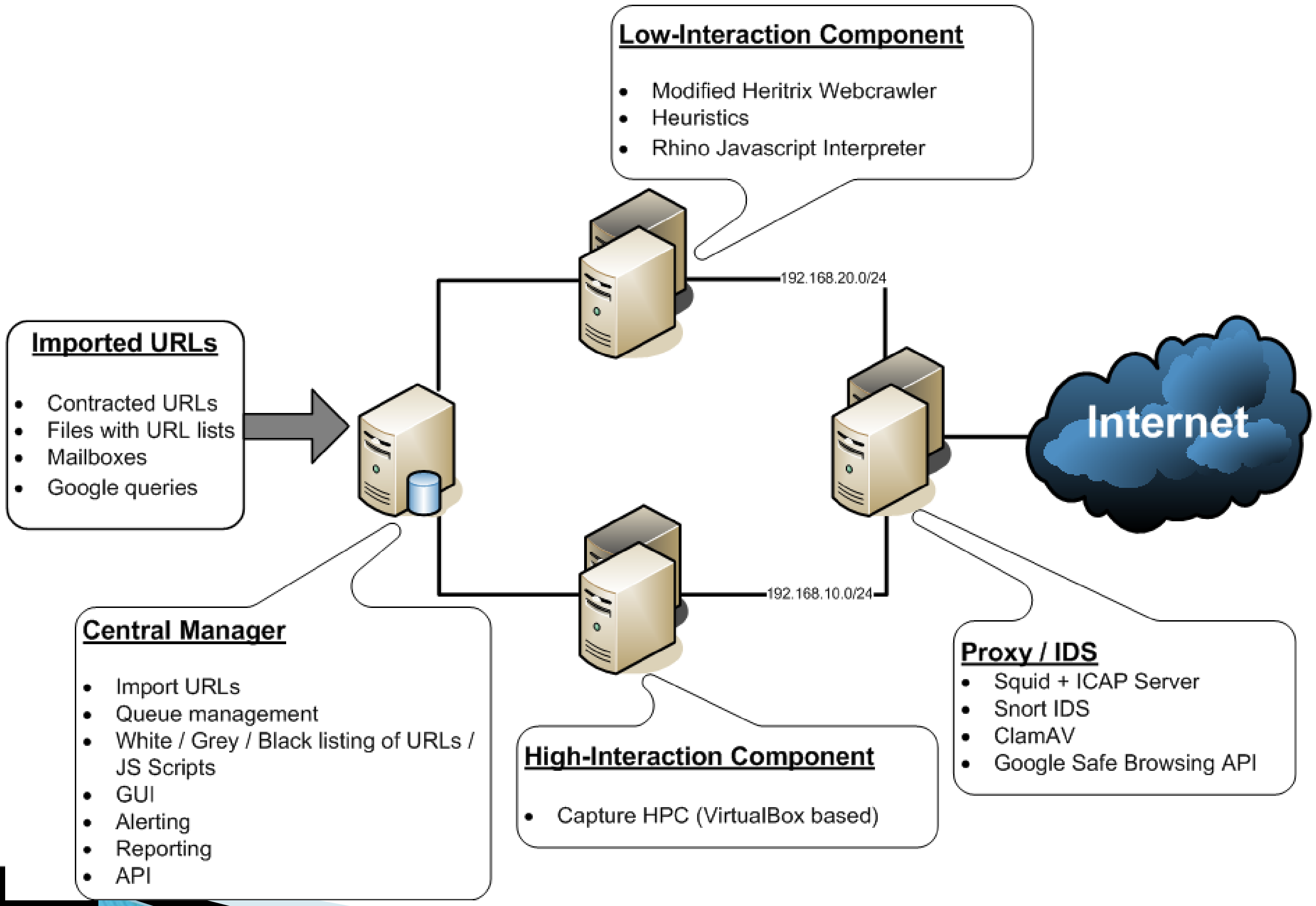
www.honeyspider.net

- HoneySpider Network Project is a joint venture between NASK/CERT Polska, GOVCERT.NL and SURFnet.
- Major incentive to start this project is the rapidly growing number of browser exploits involving varying degrees of user interaction.
  - These types of attacks lie outside the scope of current monitoring systems in use by the three parties.
  - we view this system as an expansion of our current monitoring and early warning abilities.
- The goal is to develop a complete client honeypot (or honeyclient) system, based on existing state-of- the-art client honeypot solutions and a novel crawler application specially tailored for the bulk processing of URLs.
- The system focuses primarily on attacks against, or involving the use of, Web browsers. These include the detection of
  - drive-by downloads,
  - malicious binaries
  - phishing attempts.
- Initially, the main area of exploration is drive-by downloads.
- Apart from identifying browser exploits (including oday attacks), the system is expected to automatically obtain and analyze the attacking malware and ultimately generate its signature.

Honey Spider Network Project

www.honeyspider.net

HONEYSPIDER
network



Low-Interaction Component

- Modified Heritrix Webcrawler
- Heuristics
- Rhino Javascript Interpreter

Imported URLs

- Contracted URLs
- Files with URL lists
- Mailboxes
- Google queries

Central Manager

- Import URLs
- Queue management
- White / Grey / Black listing of URLs / JS Scripts
- GUI
- Alerting
- Reporting
- API

High-Interaction Component

- Capture HPC (VirtualBox based)

Proxy / IDS

- Squid + ICAP Server
- Snort IDS
- ClamAV
- Google Safe Browsing API

WOMBAT Project

(the 7th Framework Program of the European Union)

www.wombat-project.eu

WOMBAT

Worldwide Observatory of Malicious Behavior and Attack Threats

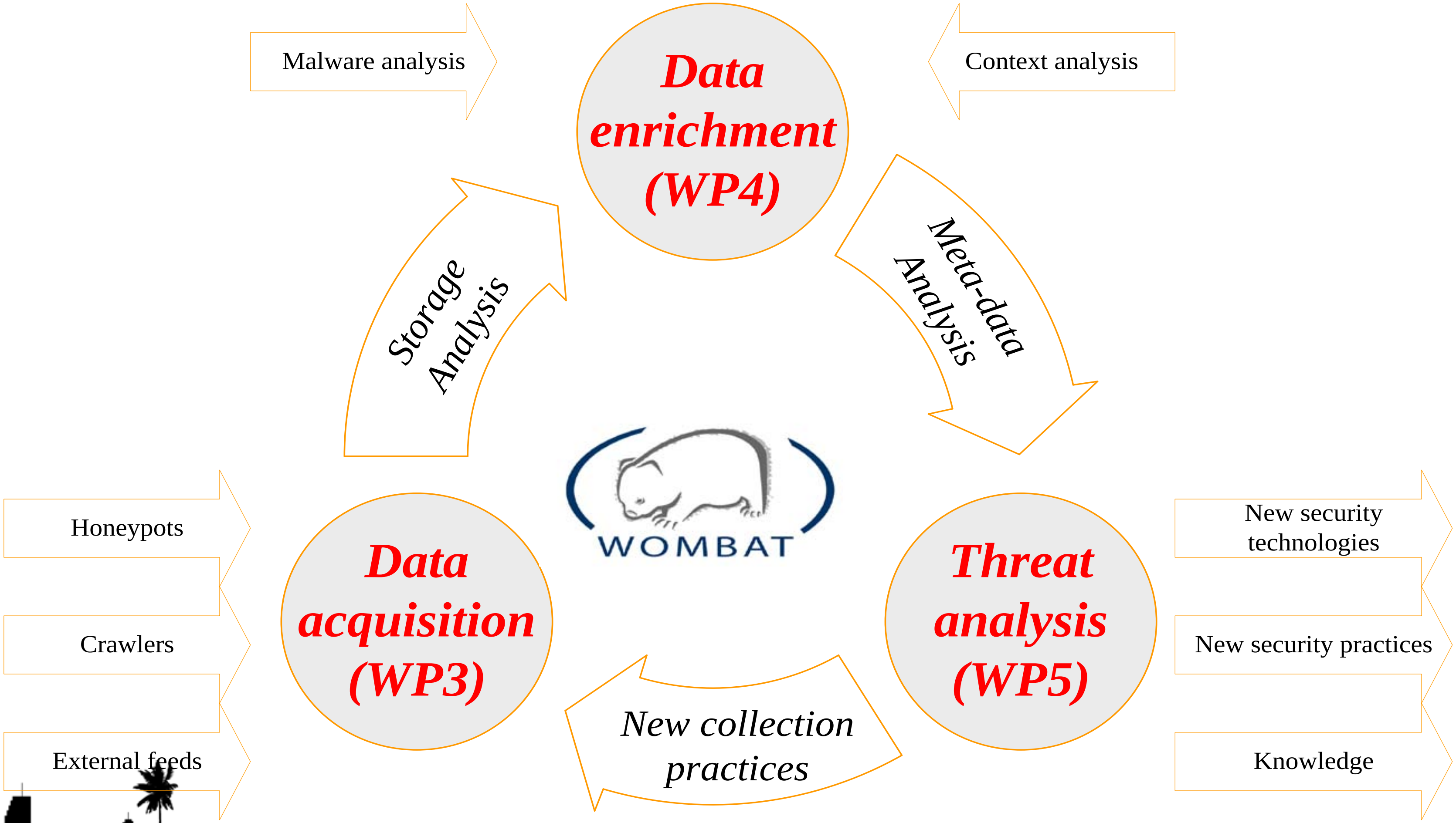
- The goal of the WOMBAT project is to create a global system of monitoring and analysis of online threats, with particular focus on malicious software,
- The research within the WOMBAT project focuses on
  - the creation of new methods of analysing the threats appearing on the Internet on a mass scale,
  - the identification of their sources and reasons for their occurrence.
- The necessity of ensuring privacy of data has so far made it impossible to share and use for such research the details of data possessed by different subjects dealing with security. The project is intended to break this barrier.
- Also, as trends of threats are changing, there is a special need for novel sources of data, located all over the world and analysed in a wide context. This includes information registered by the
  - global dispersed system of honeypots SGNet operated by the Eurecom Institute,
  - data from the world’s biggest collection of malicious software gathered by Hispasec Company (within the framework of the Virustotal project),
  - data made available by the CERT Polska team originating from the HoneySpider Network honeyclient system
  - data from the Anubis system operated by the Vienna Technical University
  - data from the Shelia honeyclient from Vrije Universiteit Amsterdam

WOMBAT Project

(the 7th Framework Program of the European Union)

www.wombat-project.eu

Worldwide Observatory of Malicious Behavior and Attack Threats



Malware analysis

Context analysis

Data enrichment (WP4)

Storage Analysis

Meta-data Analysis

Honeypots

Crawlers

External feeds

Data acquisition (WP3)

New collection practices

Threat analysis (WP5)

New security technologies

New security practices

Knowledge

FISHA Project

www.fisha-project.eu

fisha

A Framework for Information Sharing and Alerting

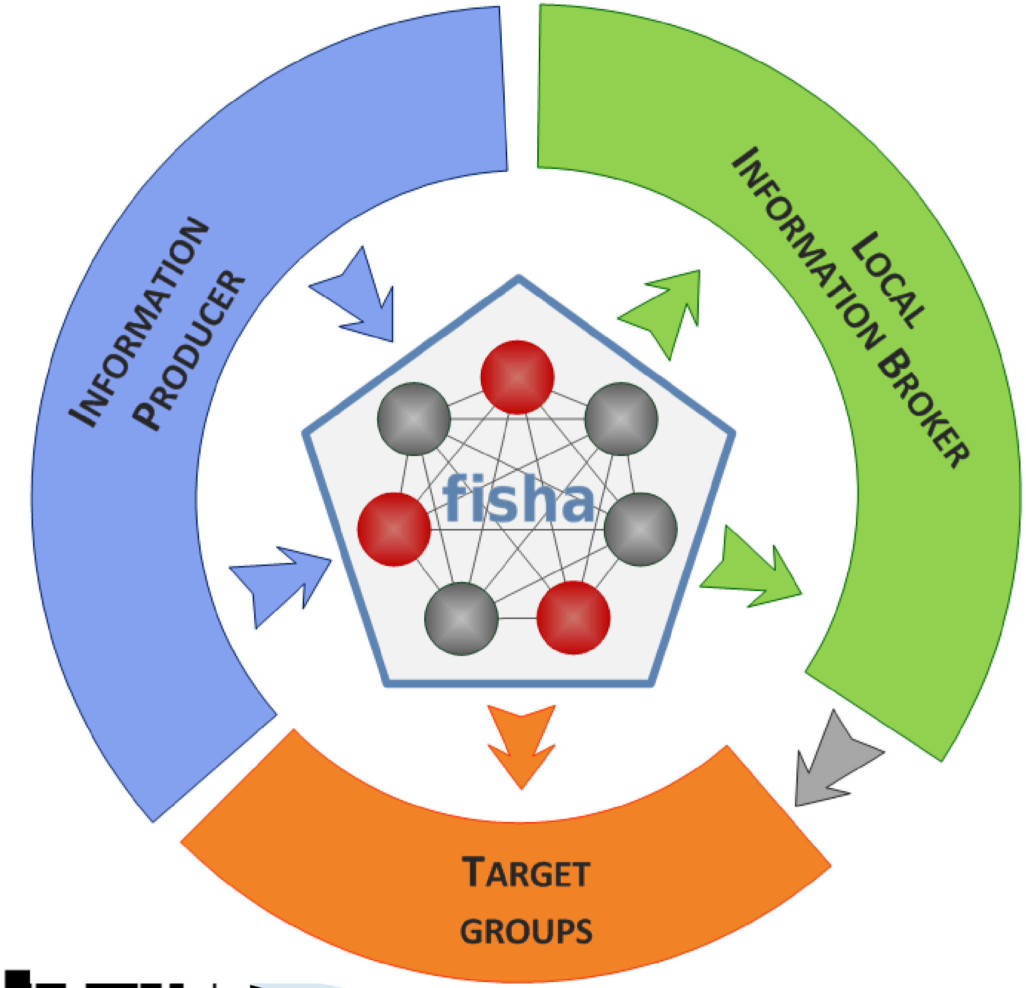
- The goal of the FISHA project is to develop a prototype of **the European Information Sharing and Alerting System (EISAS).**
- EISAS system is intended to operate on the basis of existing national and private sector information and alert sharing systems. The major purpose of EISAS is to **raise awareness on IT security issues among home users and staff of small and medium-sized enterprises**.
- One of the project main tasks is to design a **prototype of a dedicated web portal**, addressed to those target groups.
- Ultimately, it is planned that each EU Member State will have its own, national portal where up-to-date and easy-to-understand information on various IT computer security aspects, collected under EISAS, will be published.
- In addition to portals, special information and education campaigns are planned to effectively reach those particular communities.
- The project started in February 2009 and is being developed under the special **"Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" Program of the European Commission.** The project is scheduled for two years and created in collaboration between NASK, CERT-Hungary and the Institute for Internet Security at the University of Gelsenkirchen.

FISHA Project

www.fisha-project.eu

fisha

A Framework for Information Sharing and Alerting



● **SUPER NODE**
(to manage P2P network)

● BASIC NODE

Relations and synergy between projects

- As an example:

  - fully operational **early warning system ARAKIS**, based on monitoring the network in terms of threats that propagate through active means (e.g. network worms, botnets)

  - supplemented through new a **Honey Spider Network project – focused on "*drive-by-download*" attacks**. This is in response to the recent trends in observed attack techniques, as reported by CERT constituency.

  - information acquired in such a manner is used in another European (FP7) project – **WOMBAT, a global observatory of threats**, confronting locally observed processes with phenomena noticeable in other parts of the globe

- relations between projects are established,
- new modules and interfaces developed,
  - which bind existing solutions to new ones,
  - creating at the same time an area of research and development projects, which are used in practice in CERT environment and public administration units.

Projects and CERT services interactions

The evolution of threats and their influence on selection of projects

- natural evolution of online threats as observed by CERT Polska ,
  - has crucial impact on selection of applied R&D projects in which CERT Polska is engaged.
- next slide illustrates functionalities of each particular project implemented in response to group of threats they dealing with.

Characterisitics of CERT Polska projects in terms of functionality and threat categories

ARAKIS

THREATS

- NETWORK SCANNING
- VIRUSES
- WORMS
- 0-DAY EXPLOITS

FUNCTIONALITY

- DETECTION OF ANOMALIES
- WATCH AND WARNING
- DATA COLLECTION
- ALERTING
- TREND OBSERVATION

HoneySpider Network

THREATS

- MALWARE
- DRIVE-BY-DOWNLOAD INFECTIONS
- INFECTED WEBSITES
- CLIENT APPLICATION ATTACKS

FUNCTIONALITY

- THREAT CRAWLING
- ACTIVE MALWARE SEARCHING
- DATA COLLECTION

WOMBAT

THREATS

- MALICIOUS SOFTWARE
- ONLINE THREATS
- UNDERGROUND ECONOMY

FUNCTIONALITY

- GLOBAL SYSTEM
- DATA COLLECTION
- MONITORING
- THREAT ANALYSIS
- IDENTIFICATION OF THREAT SOURCES
- DATA SHARING

FISHA

THREATS

- LACK OF AWARENESS
- LACK OF COOPERATION
- LACK OF INFORMATION SHARING

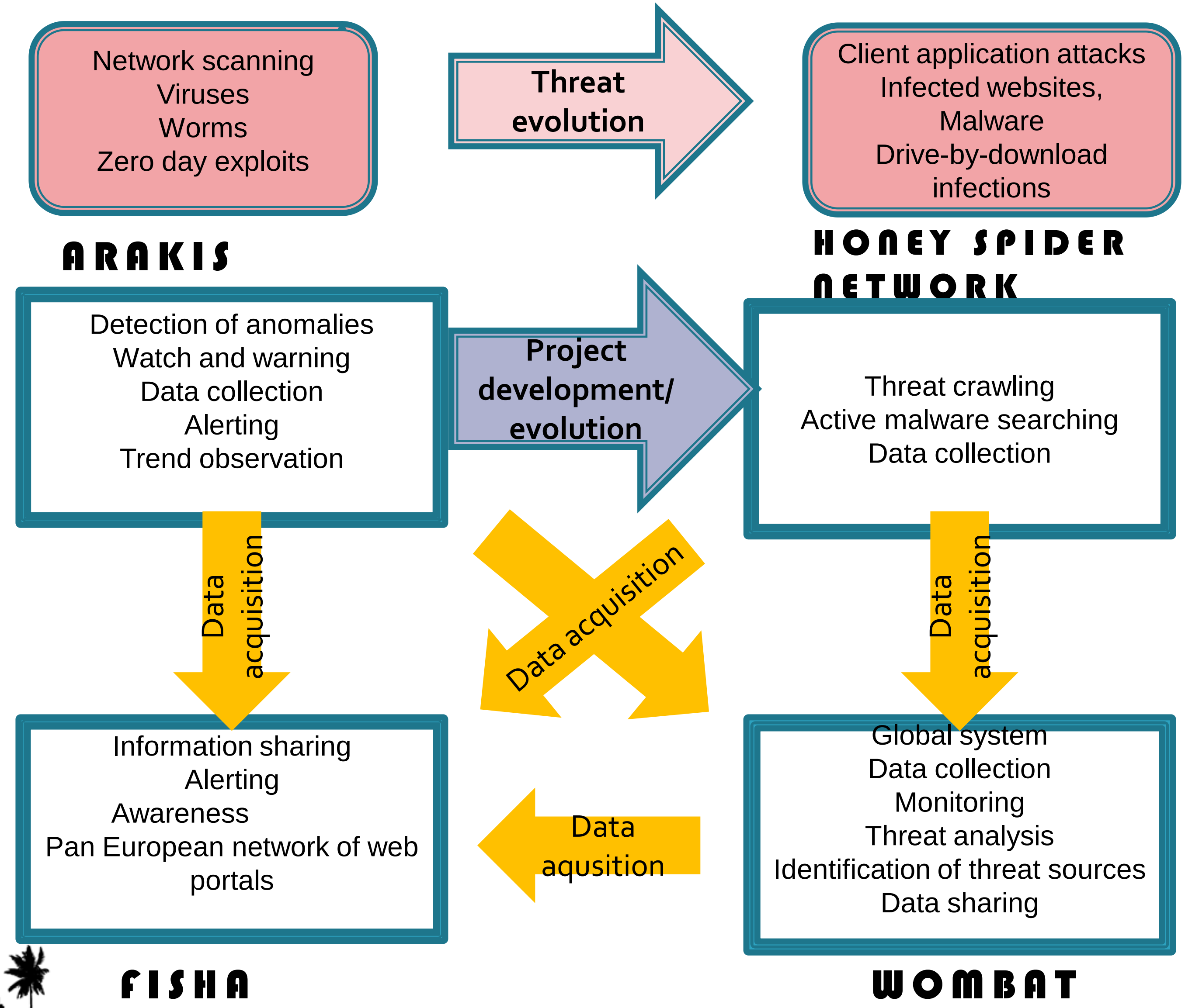
FUNCTIONALITY

- INFORMATION SHARING
- ALERTING
- AWARENESS RAISING
- PANEUROPEAN NETWORK OF WEBPORTALS

The evolution of threats and their influence on selection of projects (2)

- Following slide illustrates
  - how the evolution of threats influenced development and evolution of projects
    - (eg. HoneySpider Network project was launched in response to client side threats not covered by ARAKIS project)
  - as well as benefits one project had from other projects (in terms of possibility of data acquisition).

The evolution of threats and their influence on selection of projects



Network scanning
Viruses
Worms
Zero day exploits

Threat evolution

Client application attacks
Infected websites,
Malware
Drive-by-download infections

ARAKIS

HONEY SPIDER NETWORK

Detection of anomalies
Watch and warning
Data collection
Alerting
Trend observation

Project development/ evolution

Threat crawling
Active malware searching
Data collection

Data acquisition

Data acquisition

Data acquisition

Information sharing
Alerting
Awareness
Pan European network of web portals

Data aqusition

Global system
Data collection
Monitoring
Threat analysis
Identification of threat sources
Data sharing

FISHA

WOMBAT

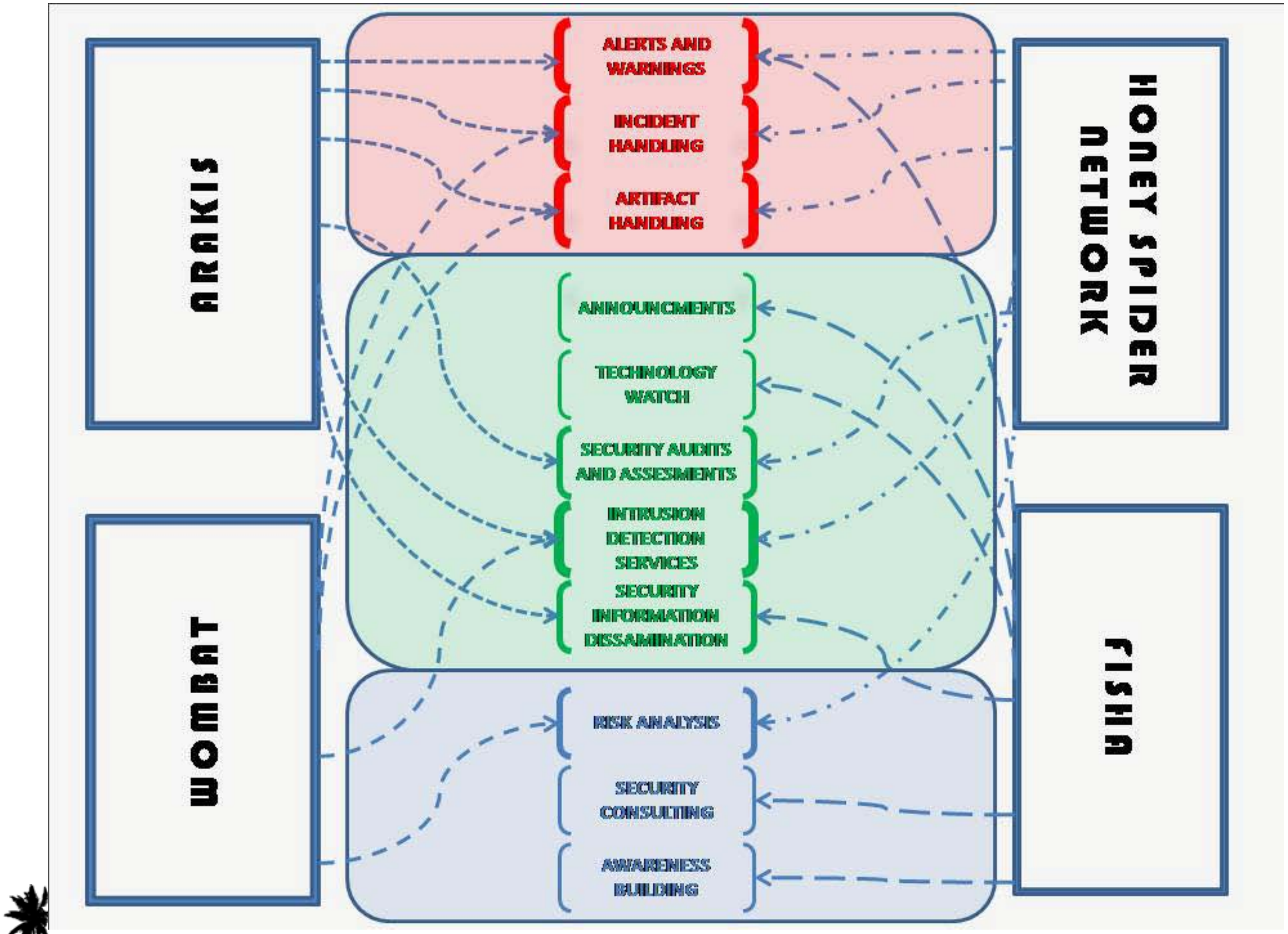
Relations between technical projects and CERT services

- R&D projects have a direct influence on CERT services
- They improve the quality of existing services but also allow for the launching of new services for the CERT constituency.
- Very often the decision about entering a new project is a consequence of needs identified by CERT staff who provide a particular service.
- The table and a schema on the next slide show the relationship between CERT Polska projects and some services.
  - The list of services is not complete. The entire list has more positions and was developed by experts from CERT Coordination Center at Carnegie Mellon University (http://www.cert.org./csirts/services.html)

Relationship between CERT Polska projects and common CERT services

CERT SERVICES / CERT POLSKA PROJECTS	ARAKIS	HSN	WOMBAT	FISHA
REACTIVE SERVICES				
ALERTS AND WARNINGS	●	●		●
INCIDENT HANDLING	●	●	●	
ARTIFACT HANDLING	●	●	●	
PROACTIVE SERVICES				
ANNOUNCEMENTS				●
TECHNOLOGY WATCH				●
SECURITY AUDITS AND ASSESMENTS	●	●		
INTRUSION DETECTION SERVICES	●	●	●	
SECURITY-RELATED INFORMATION DISSEMINATION	●	●	●	●
SECURITY QUALITY MGMT SERVICES				
RISK ANALYSIS		●	●	
SECURITY CONSULTING				●
AWARENESS BUILDING	●	●	●	●

Influence of particular CERT Polska projects on services the team provides



ARAKIS

WOMBAT

HONEY SPIDER NETWORK

FISHA

ALERTS AND WARNINGS

INCIDENT HANDLING

ARTIFACT HANDLING

ANNOUNCMENTS

TECHNOLOGY WATCH

SECURITY AUDITS AND ASSESMENTS

INTRUSION DETECTION SERVICES

SECURITY INFORMATION DISSAMINATION

RISK ANALYSIS

SECURITY CONSULTING

AWARENESS BUILDING

Conclusions

- The presented examples of projects show the significant role of a well organized process of knowledge exchange within a CERT type team. It could be recognized as a potential model for implementation between any operational and R&D units within the same organization.
- It is important to point out some important aspects of organization of such cooperation:
  - The process of information exchange and decisions about the implementation of new functionalities and abilities should be fast. This condition is very important because of a very dynamic network environment.
  - The development of new abilities should go hand in hand with a continuous process of Internet threat trends analysis, from both operational and network monitoring point of view.

Conclusions (cont.)

- Finally it is worth listing a number of benefits coming from close cooperation between operational and research and development experts. The fruit of this cooperation allows to:
  - Tighten international cooperation and use different views and observations in resolving problems
  - Maximize projects and knowledge dissemination, based on concrete and practical examples
  - Extend contacts between security experts, on how to improve both operational and R&D activities
  - Create tools for systematic monitoring and discovering of new Internet threats

Conclusions (cont.)

- Establish an educational and training platform for the new CERT teams members, who have a possibility to learn about Internet network threats using systems developed in response to them as well as particular technologies and security tools (e.g. honeypots, intrusion detection systems etc)
- Establish permanent systems which are able to present a picture of network security for particular constituencies.
  - Thanks to this fact a team becomes independent from other opinions and assessments, which may not universal and true for its constituency.

22nd ANNUAL FIRST CONFERENCE MIAMI
JUNE 13-18, 2010

Questions?