A CIP-PSP funded pilot action
Grant agreement n°325188

Deliverable	**D3.1 Planning reports of the experiments**
Work package Due date Submission date Revision Status of revision	WP3 Experiment Planning, Integration and Deployment M16 13.06.2014 0.1
Responsible partner Contributors	INTECO (Angela García, Gonzalo de la Torre, Jonás Ropero, Ana Santos)
Project Number Project Acronym Project Title Start Date of Project	CIP-ICT PSP-2012-6 / 325188 ACDC Advanced Cyber Defence Centre 01/02/2013

Dissemination Level	
PU: Public	
PP: Restricted to other programme participants (including the Commission)	X
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Version history

Rev.	Date	Author(s)	Notes
v.0.1	15/05/2014	Angela García (INTECO), Gonzalo de la Torre (INTECO), Jonás Ropero (INTECO), Ana Santos (INTECO).	Initial version to complete by all wp3 partners
v.0.1	19/05/2014	Darko Perhoc (CARNET)	Added comments and changes done to the initial version
v.0.1	23/05/2014	Dan Tofan (CERT-RO), Beatriz Gallego-Nicasio (ATOS), Paolo De Lutiis (TI-IT), Aleš Černivec (XLAB)	Added comments and changes done to the initial version
v.0.1	26/05/2014	Marc Rivero López (BDigital), Katia Velikova (BGPOST), Thomas King (DE-CIX)	Added comments and changes done to the initial version
v.0.1	28/05/2014	Antonio Pastor (TID)	Added comments and changes done to the initial version
v.0.1	02/06/2014	Michael Weirich (ECO), Edgardo Montesdeoca (Montimage)	Added comments and changes done to the initial version
v.0.1	03/06/2014	Christian Nordlohne (IF-IS), Andreas Fobian (GDATA)	Added comments and changes done to the initial version
v.0.1	04/06/2014	Jorge de Carvalho (FCCN) Thomas Fontvielle (Signal Spam)	Added comments and changes done to the initial version
v.0.1	05/06/2014	Tiziano Inzerilli (ISCTI), Roberto Cecchini (GARR), Christian Keil (DFN-CERT), Jochen Schöenfelder (DFN-CERT)	Added comments and changes done to the initial version
v.0.1	10/06/2014	Felix Stornig (TEC)	Added comments and changes done to the initial version
v.1.0	12/06/2014	Angela García (INTECO), Gonzalo de la Torre (INTECO), Jonás Ropero (INTECO), Ana Santos (INTECO).	New version (integrates all contribution from partners for final review)
V.1.0	12/06/2014	Paolo De Lutiis (TI-IT)	Added changes to version v.1.0

V.1.0	13/06/2014	Aleš Černivec (XLAB), Paolo Roccetti (EII), Will Rogofsky (CyDef)	Added changes to version v.1.0

Table of contents

Table of figures

Table of tables

1. Executive summary

This document describes the general planning for the experimentation phase under the scope of ACDC. The aim is to describe general information needed to be part and contribute to ACDC experiments and describe the experiments defined.

Section 2 specify general information: general objectives, types of experiments, approach, general rules, roles, conditions to be part of experiments, integration with the CCH requirements, reporting and general scheduling.

Next sections of the document detail, for each experiment defined, the following information:

- Detailed objectives
- Success criteria
- Technologies involved
- Experiment main processes and activities
- Main metrics in order to measure objectives and success criteria
- Partners involved and roles

Additionally to this document, a specific and detailed design for each experiment will be available (D3.2 deliverable and also through the Community Portal). This detailed Design for each experiment will contain specific tasks, activities and dataset flows, detailed scheduling and reporting procedures to execute and control the experiments by different partners involved.

2. General information

2.1. High level objectives for experiments

At a high level, the objective is testing the effectiveness of the ACDC end to end model to mitigate and fight against botnets:

- Deploying and integrating solutions (sensors, services or tools) on the ACDC architecture.
- Identifying and analyze botnet elements, infection channels and patterns.
- Launching notification and mitigation actions and services by national support centers (NSCs), CERTs and ISPs.
- Increasing and generating intelligence of the whole model and enhancing solutions within the project, based on a centralized point to share information and technologies.

Specific objectives and success criteria will be defined in detail for the different experiments planned, in sections 3, 4, 5, 6 and 7 of this document.

2.2. Type of experiments

Along the Pilot Project, the ACDC solution is going to be tested through the design, execution and evaluation of, at least, 5 different types of experiments:

- **Spam-botnets** => Detection and mitigation of spam botnets used as infection channels and as a vehicle of a lot of botnet activities.
- **Fast-flux** => Detection and mitigation of domains that implement fast-flux techniques in order to support botnet infrastructures.
- **Websites** => Detection and mitigation of malicious websites used to support main botnet activities like malware distribution and illicitly Internet activity like phishing, and identity theft. Identification of botnets used to attack and compromise websites.
- **DDoS** => Analysis of attacks and mitigation of botnets used to perform DDoS attacks.
- **Mobile bot** => Detection and mitigation of botnets affecting mobile devices.

Experiments will be designed defining a coordinated flow of end to end processes or activities joining the five technical solutions of the project:

- Network Traffic Sensors
- Malicious or Vulnerable Website Analysis
- Centralised Data Clearing House
- Support Centres
- End Customer Tools

2.3. End to end approach

One of the main pillars of ACDC is the end-to-end approach of the solution. Experiments will have this pillar as fundamental, because the final objective is to mitigate the effect of botnets and this cannot be done without an end-to-end approach in mind. This means that different activities will be planned for all the phases related to the problem:

- Detection of valuable data
- Analysis of the data to identify botnet elements and rules
- Aggregation & classification & distribution of information
- Notification to end users
- Mitigation, disinfection & prevention activities

2.4. Legal constraints

All the activities and actions defined under the scope of the experiment must be law compliant. This condition is a responsibility of each partner involved on the experiment.
If some activity cannot be performed because of legal issues, partners must report the problem in order to find a solution by legal teams or to leave the experiment activity.

2.5. General rules to be part of experiments

Based on the end to end approach and the type of experiments, different types of partners with different capacities and solutions will be part of ACDC experiments:

- Partners with technologies that:
  - are able to detect and or analyze different types of malicious activity or botnets elements based on different types of data sources and conditions.
  - want to prove those solutions along the experiments and share data with other organizations through the central ACDC point, the Centralized Data Clearing House (CCH).
- Partners who are owners of large networks or specific infrastructures where this activity can take place, so it is necessary to detect and secure, like ISPs or critical infrastructures owners (like financial institutions).
- Partners with strategic information or data related to the goal of any experiment that can be shared within the project.
- Partners with high expertise and vision related to a specific experiment who wants to contribute to the design and or results analysis, like academia and research facilities, security industry, etc.
- Partners with strategic capacities that are able to coordinate mitigation activities within a specific area, like National CERTs that in most cases supports the National Support Centers (NSCs).
- Law enforcement agencies, local, European or international, in order to effectively fight botnet cybercrime activities.
- End-users who can contribute to the project installing end-user tools and reporting malicious activity.

2.6. Roles

The following table shows the different roles a partner may play (one or more) in the execution of the different experiments:

ROLE	RESPONSIBILITIES
Experiment leader or coordinators	Responsible for the design and planning, coordination and execution of experiments. Their responsibilities

	are: • Design the experiments activities and metrics with partners according to the objectives defined. • Plan the execution and reporting phase. • Assure that partners have the necessary information to integrate their solutions on the experiments and with ACDC central system (CCH). • Coordinate the execution of the experiments (quality control). • Reschedule if necessary. • Analyze intermediate reports and make final report with results.
Tool Owners (a tool could be a solution, a service sharing data, a technology for analysis, etc.)	The responsible for a tool/service involved on the experiment. Responsibilities are: • Participate in the design of experiments. • Ensure that the tool/service works as defined by functional and technical specifications. • Ensure that the tool/service is correctly deployed and integrated with CCH (if applicable). For tools that require deployment outside the "home or scope" of the tool owner, the tool must be provided in an installable format and installation guides must be available to facilitate the operation of the tool. • Ensure with tool operators that the tool is operating during the experiments. • Report possible problems in any phase regarding to own tool. • If apply, analyze experiment results from the point of view of business models and exploitation possibilities of their tools.
Tool Operator (owner or not)	The tool operator is technically responsible for integration, testing and operating the tool during the experiment. Responsibilities are: • Deploy, install and integrate the tool before the experiment. • Test and monitor that the tool runs correctly during the experiment. • Report errors or problems during the integration and operation of the tool. • Report to the experiment coordinator the results based on defined metrics.
CERTs or Network Owners (ISPs or specific companies) (notification & mitigation phase)	Partners who are responsible of launching notification and mitigation activities (depending of specific competencies that could apply to each): • Contribute to the experiments design. • Contribute consuming CCH information to perform analysis & notification activities to affected users if applicable. • Contribute launching notification and/or mitigation activities under its constituency. • Analyze results of experiments to design viability models for long term.
Partners in charge of National Support Centres	Are responsible of: • Disseminate prevention information

	• Provide online anti-botnet services • Disseminate end-user tools to disinfect or secure user devices
Other stakeholders	Those entities involved in the experiments that have none of the above roles. They can: • Contribute to the experiments design • Be end users which deploy end-user tools • Contribute to mitigation in its areas of activity (LEAs) • Contribute, based on CCH information, to perform analysis or research in its areas of activity • Help to disseminate the results of the experiment.

Table 1 - Roles

2.7. Constraints & conditions

Special constraints and conditions that need specific actions to achieve the success criteria must be defined in each experiment detailed design. At least:

- Which incidents reported require an action or several actions to be launched:
  - Analysis
  - Notification
  - Mitigation
  - Collaboration with third parties
  - Etc.
- If these actions are covered by partners on the experiment. Each partner has to define the scope of actions that can be performed (resources, capacity, response times, etc).
- If the action must be triggered on real time or not. In the detailed design of each experiment specific conditions could be specified, for example:
  - Response times from detection to launch notifications or mitigation actions in order to effectively manage the incident (could be different by CERT or country):
    - Per type of botnet element detected
    - Per level of severity of the incident
    - Per type of target affected by the incident

- These actions should be technically detailed.
- These actions should be coordinated and reported.
- If the action is consequence of a false positive botnet detection, revert actions must be defined and notified.

2.8. Integration with CCH

All ACDC experiments have one requirement in common: all datasets shared between partners must use the Centralized Clearing House (CCH) as the global and central system to send, store and distribute or retrieve all the information related to botnet elements.

The following requirements are needed to participate in an experiment:

- Tool owners and/or tool operators must integrate with the CCH in order to share botnet elements detected individually.
- Partners in charge of analysis activities must have access to CCH data of a specific type in order to analyze it and send the results. For example: a partner in charge of malware analysis must have access to suspicious malware samples reported from other partners.
- ISPs, CERTs, NSCs and other partners who are responsible of notification and mitigation activities must retrieve the datasets related to incidents under their constituency or scope, as well as general datasets useful for prevention and mitigation activities (for example blacklists).

In order to accomplish this requirement, partners must access the ACDC Community Portal to find specific procedures about integration with CCH:

- How to securely integrate with the CCH and applying sharing policies:
  - API keys to communicate and authenticate a tool in a secure way with the CCH.
  - How to define, modify and apply sharing policies to data shared.

- How to send datasets to the CCH:
  - Datasets Schemas definition
  - Procedures to modify dataset schemas in the CCH
  - Procedures to send datasets to the CCH

- How to know which datasets are in the CCH:
  - Datasets Schemas repository

- How to retrieve specific datasets from CCH:
  - Procedures to retrieve datasets from the CCH

Additionally, partners sharing datasets through the CCH will use the ACDC Community portal to manage their CCH API-Keys. As detailed in Annex I of D6.2.1, API-Keys enable the interaction among the CCH and its clients, by allowing authenticated and controlled access to CCH functionalities.

2.9. Reporting

Different templates for the intermediate reports of each experiment will be specified in the detailed design for each experiment (D3.2).

These reports will contain the results of each phase, including metrics to analyze success criteria, results, information obtained and possible barriers or disadvantages. For each experiment there will be different intermediate reports, corresponding to the phases:

- Detection and Analysis report.
- Notification report.
- Mitigation report.

Every partner must complete the report according to their role in the experiment and send it to the experiment coordinator with the agreed frequency. The experiments coordinators will

be the responsible of generating the final report summarizing all the information obtained during the experiment, conclusions and lessons learned.

The templates and also the reports will be available for partners on Community Portal website.

2.10. How to join

Any partner who wants to participate in any experiment can formally join through the ACDC Community Portal (CP).

The Community Portal is available at: https://communityportal.acdc-project.eu/home while the application form for joining organizations can be found at https://communityportal.acdc-project.eu/join-us.

When submitting a joining application, the organization can select which of the ACDC Experiments to join, as well as the ACDC Solutions the organization is interested in. This will be then taken into account when the application is processed, to properly associate organizations users to the experiment workspaces within the community portal (see D6.3.1 and D6.2.1 for more details).

2.11. Detailed design of the experiments

The following sections of this document describe the design & planning for the different types of experiments at high level: objectives, success criteria, main processes, technologies and partners involved.

Detailed design for each experiment will be given on the specific design documents deliverables (D.3.2) and will be available on the experiments section of the Community Portal.

As it has been said on the executive summary, the detailed design documents (D3.2) will contain specific tasks, activities and dataset flows, detailed scheduling and reporting procedures to execute and control the experiments by different partners involved.

2.12. Scheduling

General scheduling information:

- Integration of all solutions involved on the experiment with the CCH must be done and tested along September- October 2014[1].
- Preliminary testing of the experiment flow of activities will be tested along October-November 2014.
- Experiment execution phase will start on November (the latest) 2014 until April 2015.

Partners who are developing new tools or external organizations who want to contribute could enter experiment later on.

[1] NOTE: In order to do this the complete API for the CCH must be available on july 2014

3. Experiment: SPAM BOTNETS

3.1. Objectives

General objectives defined in section 2.1 apply to all experiments. Specific and detailed objectives for the Spam experiment are the following:

Detection & analysis:

- Identify and classify active threats involved in spam messages, special focus on botnets sending spam and the components belonging to these botnets:
  - Campaigns.
  - Spambots
  - C&C Servers
  - Malicious contents like associated URLs or attachments.

Notification and mitigation:

- For NSCs involved on the experiment:
  - Through NSC channels, alert end-users about malicious spam campaigns that are detected and affect its constituency.
  - If possible, provide tools or services for end-users to help them identify if their public IP is involved in spambot activities.
  - Provide cleaning tools for bot removal.
- For CERTs involved on the experiment:
  - If a discovered C&C server is located under its constituency, launch notification actions to LEAs (if it is legally feasible) in order to take down and control or sinkhole the server activity.
  - Send to ISPs, not involved in the project, information about spambot IP addresses and bot activity timestamp if ISP belongs to CERT's constituency.
- For ISPs involved on the experiment and if it is legally feasible depending of the country:
  - Based on spambot data obtained, identify end-users affected on its own network, notify them about the infection and give them information about the NSC to disinfect. Alternatively, ISPs could interface their internal SOC/CERT and possibly follow each case through internal processes.

3.2. Success criteria

Success criteria for spam experiment (based on real impact) will be:

- Spam botnet elements are detected by sensors and sent to CCH: at least spambots, campaigns, suspicious files and URLs.
- 75% of suspicious files and URLs in spam are analyzed[2].
- 75% of malicious spam-campaigns detected (related with phishing or malware distribution), affecting end-users of NSCs countries involved on the experiment, are published and accessible through NSCs websites.
- 100% of spambots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).

[2] In the detailed design of the experiment a maximum analysis capacity will be defined.

- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.
- 100% of C&C server discovered are notified to LEAs, in order to start a takedown process, if it is legally feasible depending of the country.

NOTE: Data to which success criteria applies will be only that with a high quality/veracity value. Experimental data will allow contributing to the objectives but not to the success criteria.

3.3. Technologies involved

For this experiment the following solutions and technologies will we used for detection and analysis phase:

SOLUTION NAME	TYPE OF TECHNOLOGY	VALUE DATA FOR THE EXPERIMENT OBJECTIVES
SPAMTRAP	Spamtraps and Honeytokens. Use of a mail server honeypot and several fake email address (honeytokens) spread over internet. All the emails from or to these email addresses are spam emails. Analysis of spam bodies and attachments is also performed (Mediation Server).	Spambot IP addresses. Campaign information. Malicious domain & URLs. Malicious binary sample.
SPAMBOT DETECTOR	Deep analysis traffic (Layer 2 to 7) over filtered SMTP traffic.	Spambot IP addresses.
SPAM ANALYSIS TOOL	Correlation of spam emails into clusters.	Spambot IP addresses (IPs from the same botnet); Malware in spam; Campaigns information (experimental at this moment) Malicious URL.
Operational Intelligence Center	Malware analysis.	Detailed information about the binary analysed.
AHPS	Correlation & analysis functions. SIEM.	
Honeynet	Network of passive sensors	Source IP of connection attempts to port 25 of the sensors. Analysis tools could leverage such information to increase confidence of results.
File Analysis	Static (Signature based) and dynamic	Classification of malware and

Component	(Sandbox / Behaviour Analysis) analysis of malicious binaries and file types	exploits used in Spam Campaign C&C servers, botnet name
URL Analysis Component	Static detection of malicious Websites	Classification of URL involved in Spam Campaign (eg. Phishing / Malware)
HORGA	Honeypot	Source IP of spamming bot

Table 2 - Technologies involved – Spam Botnet

More information about solutions and technologies can be found on the Technology Development Framework document or the technology section of the ACDC Community Portal.

3.4. *Experiment main phases and processes*

The following diagram shows the main phases and processes to be executed in the Spam experiment.

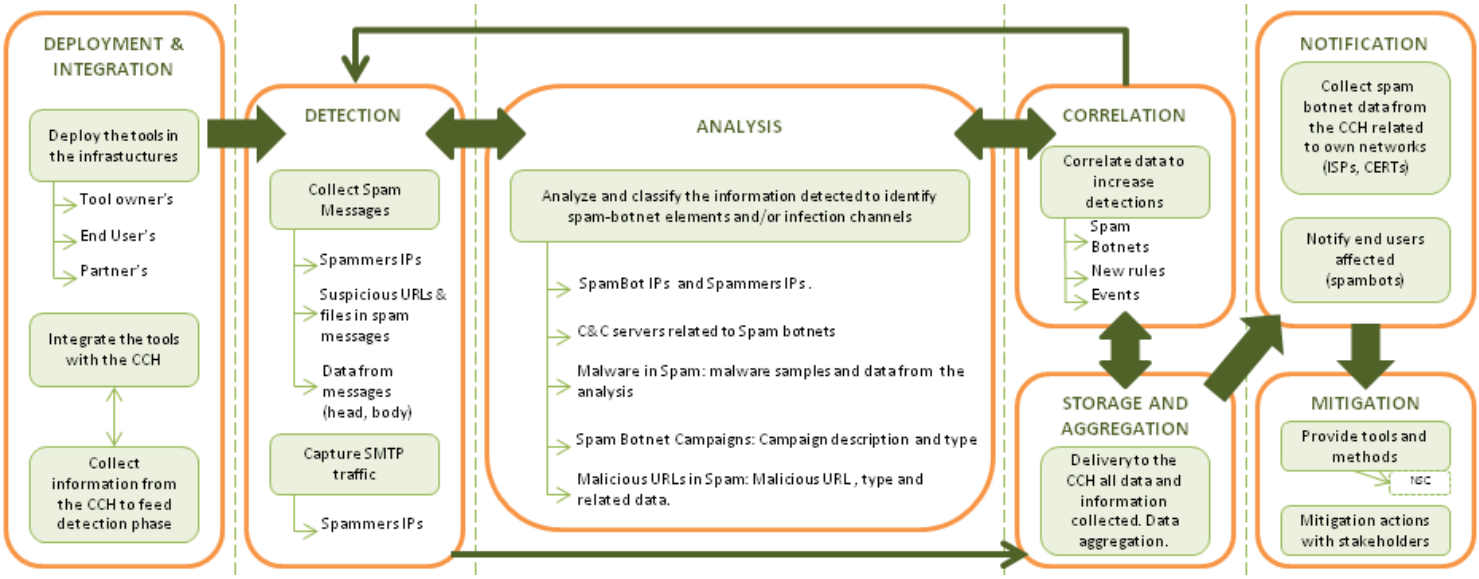

Illustration 1 - Experiment main processes – Spam Botnet

The different phases are conducted in order to achieve the main objectives of the experiment. Within each phase there are several processes defined. Detailed activities and data flows will be specified on the detailed design of each experiment (D3.2 deliverable and also will be available on the Community Portal).

Experiment preparation and preliminary testing phase

Deployment & Integration

During this phase all experiment supplied tools, sensors and/or information services will be deployed over involved partner infrastructure and end user devices, and tested for valid integration with the project central information repository (Central Clearing House).

Experiment execution phase

Detection & analysis

During these phases the following tasks are done:

- Comprising (optionally) the collection of all information useful to feed own detection solutions from the Central Clearing House, including active SPAM campaigns, C&C lists, malware blacklists and malicious URL lists, previously reported by other partners.
- The harvesting of SPAM information through the technologies listed on section 3.3 of this document (spamtrap sensors, SMTP traffic sensors and end user reporting tools).
- The analysis of all data collected to identify spam-botnet elements and/or infection channels: identifying spammers and spambots, C&C servers, malware attachments and malicious URLs in spam, or messages coming from specific SPAM botnet campaigns and or malicious activities.

Storage, aggregation and correlation

At this phase is done the storage and aggregation of the datasets sent individually from the different sensors by partners to make all this information available to all partners and stakeholders that can use the information in three ways (following the sharing policies that apply):

- To correlate and generate new detection rules to increase ACDC intelligence => By correlation systems from partners
- To feed detection phase again, for this or another experiment type => By tool owners partners.
- To activate notification and/or mitigation actions => By ISPs/CERTs and National Support Centers.

Notification

Comprising the collection from Central Clearing House (data aggregated and classified) of all SPAM incidents and relevant data related to specific networks or constituencies by partner, ISPs and CERTs involved in the experiment. With this information, ISPs and CERTs can proceed to notify the SPAM related security incidents to end users affected to raise awareness and motivate them to disinfect their compromised devices.
If any C&C is discovered, CERTs should notify LEAs, if it is legally feasible.

Mitigation

Action by NSCs:

- Distribution of information related to active spam-botnet campaigns
- Provide cleaners to disinfect spambots.

If any C&C is discovered and if notification to LEAs success, actions like sinkholing or at least isolating the server for its analysis should be done by CERTs.

ISPs could launch procedures of spambot blocking or blacklist URL blocking.

3.5. Metrics

METRIC	Description
Partners	Partners contributing to the different phases of the experiment, with tools, infrastructure, knowledge, capacities, etc.
Tools/solutions	Tools and solutions contributing to the experiment.
CCH	Tools & partners integrated with the CCH. Statistical data of usage in the experiment.
Spambots	Spambots identified.
C&C	C&C identified.
Campaigns	Spam campaigns detected.
Malicious content	Messages with malicious content; malware, malicious URLs.
Notification	Notifications sent to end users and processes activated with LEAs.
Mitigation	Mitigation actions and disinfections methods/contents created. Campaigns detected vs published. Usage of mitigation tools or services.

Table 3 - Metrics – Spam Botnet

Detailed metrics will be defined on the specific design document for this experiment. In general, metrics will be given in total and also classified by country, ASNs and TLDs if apply.

3.6. Partners involved – role – availability

3.6.1. Coordination

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
INTECO CARNET	Experiment coordinators	September 2014

Table 4 - Partners – Coordination – Spam Botnet

3.6.2. Detection & analysis

PARTNER	ROLE	Specific solution	AVAILABILITY DATE TO START EXPERIMENT
CARNET	Tool Owner & Operator	SPAMTRAP	September 2014
BGPOST	Tool Operator (CARNET Tool)	SPAMTRAP	September 2014
CERT-RO	Tool Owner & Operator	SPAM ANALYSIS	September 2014
TID	Tool Owner & Operator	SPAMBOT DETECTOR	July 2014 (ISP authorization pending)
ATOS	Tool Owner & Operator	AHPS	September 2014
TI-IT	Tool Owner &	Honeynet	September 2014

	Operator		
G Data	Tool Owner & Operator	File Analysis Component	September 2014
G Data	Tool Owner & Operator	Website Analysis Component	September 2014
Signal Spam	Tool Owner & Operator	Spam reporting centre & analysis component	July 2014
ISCTI/GARR	Tool Owner & Operator	HORGA	September 2014
Cassidian Cybersecurity	Tool Owner & Operator	Operational Intelligence Center	July 2014

Table 5 – Partners - Detection and Analysis – Spam Botnet

3.6.1. Storage & aggregation

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
ECO	Tool Owner & Operator	CCH	September 2014
LSEC	Tool Owner & Operator	STIX	September 2014

Table 6 – Partners - Storage and Aggregation - Spam

3.6.2. Notification & Mitigation

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
ECO	Germany NSC	Available
ISCTI	Italy NSC	July 2014
INTECO	Spain NSC	June 2014
INTECO	CERT (Incorporate ACDC feeds into their notification and mitigation channels)	September 2014
FCCN	Portugal NSC	September 2014
FCCN	CERT (mitigation capacities)	October 2014
CERT-RO	Romania NSC	September 2014
CERT-RO	CERT (mitigation capacities)	September 2014
CARNET	Croatia NSC	Available
CARNET	CERT & ISP (mitigation capacities)	Available
TI-IT	ISP (mitigation capacities, analysis of data related to own ASN and engage its internal CERT, forwarding the ACDC notification)	September 2014

TID	ISP (mitigation capacities, analysis of data related to own ASN and notification)	September 2014
DFCN-CERT	CERT (mitigation capacities) Incorporate ACDC feeds into their notification and mitigation channels	September 2014

Table 7 - Partners - Notification and Mitigation – Spam Botnet

4. Experiment: WEBSITES

4.1. Objectives

General objectives defined in section 2.1 apply to all experiments. Specific and detailed objectives for the Spam experiment are the following:

Detection and analysis:

- Identify and classify malicious websites or URLs focus on techniques of:
  - Drive by download/exploits.
  - Download of malicious code.
  - Phishing.
- Identify vulnerable websites that can be used to launch attacks through them or being compromised.
- Detect bots attacking websites and attack patterns.

Notification and mitigation:

- For CERTs involved on the experiment:
  - If the website is under CERT constituency, notify at least the domain name administrative contact and the hosting ISP in order to alert website owner and mitigate the incident (disinfect, shutdown, etc).
  - If the website is a C&C server and is under its constituency, launch also notification actions to LEAs in order to take down and control or sinkhole the server activity (if it is legally feasible).
- For ISPs involved on the experiment and if it is legally feasible depending of the country:
  - Based on bot data obtained, identify end-users affected on its own network, notify them about the possible infection and give them information about the NSC to disinfect. Alternatively, ISPs could interface their internal SOC/CERT and possibly follow each case through internal processes.
- For NSCs involved on the experiment:
  - Provide information or tools in order to help webmasters to disinfect or protect their websites.
- For partners involved:
  - Implement protection rules on security systems based on blacklists of malicious URLs.

4.2. Success criteria

Success criteria for website experiment (based on real impact) will be:

- Suspicious and malicious websites are detected by sensors and sent to CCH: at least malware distribution.
- Bots attacking websites are discovered and stored in the CCH.
- At least 75% of the suspicious websites stored in the CCH are analyzed[3].
- At least 75% of malware samples obtained from Websites are analyzed[4].

[3] In the detailed design of the experiment a maximum analysis capacity will be defined.

[4] In the detailed design of the experiment a maximum analysis capacity will be defined.

- At least 85% of websites distributing malware are notified (for the ones under scope of partners involved).
- 100% of bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).
- 100% of C&C server discovered are notified to LEAs (if it is legally feasible).
- NSCs publish contents or information related to main type of attacks to websites discovered.

NOTE: Data to which success criteria applies will be only that with a high quality/veracity value. Experimental data will allow contributing to the objectives but not to the success criteria.

4.3. Technologies involved

For this experiment the following solutions and technologies will be used for detection and analysis phase:

SOLUTION NAME	TYPE OF TECHNOLOGY	VALUE DATA FOR THE EXPERIMENT OBJECTIVES
Initiative-S	Scan of the HTML code. Once retrieve the HTML code of a webpage it can be analyze using different techniques like sandboxing, static or dynamic code analysis.	URLs distributing malware. Malware snippet like iframe code and malware links are collected.
Horga	Honeynet. Network of fake servers or computers (honeypots) used to trick bots and any other attackers in order to analyze them and obtain valuable information of attacks for mitigation purposes.	URL distributing malware. Source IP of attacker (suspicious bot). Binary samples.
Skanna	Scan of the HTML code. Once retrieve the HTML code of a webpage it can be analyze using different techniques like sandboxing, static or dynamic code analysis.	URLs distributing malware.
Honeypot Sensor	Honeypot and RFI (Remote file inclusion). Use of a fake web page publishing google "dorks"to trick attackers using google search engine to attack honeypot including remote file	Domain and IP distributing malware. Source IP of attacker compromised server containing remote file-usually exploit). Binary samples.

	from third party server.	
NIRC	Passive internet monitoring tool. Software reads information about already detected compromised web sites in EU member states from several feeds and sends it to CCH. National CERTs in EU could recive information related to their country reading CCH.	C&C servers, IP and domain. List of malicious URLs. Phishing web sites.
SiteVet	Reputational analysis from a database of blacklistings and incidents.	Reputational scores (ASNs, IPs).
WebCheck	Webmaster plugin that protects against and cleans up vulnerabilities and malware from websites.	Malware analysis information (basics such as malware class, filesize, MD5 etc). Attack source information (URL, IP, ASN etc).
SDN HP Sentinel	Detect infected users who generate DNS queries that belong to a proprietary botnet domains blacklist. Bases on Openflow technology.	Bots (IPs) Domains belonging to a botnet.
Honeynet	Honeynet. Use of different honeypots to detect attacks against different services and technologies like SSH, ftp, mysql, etc.	IPs connecting to the honeynet (suspicious to be a bot). URL of the downloaded file.
HoneyNetRO	Honeynet. Use of different honeypots to detect attacks against different services and technologies like SSH, ftp, mysql, etc.	IPs connecting to the honeynet (suspicious to be a bot). URL of the downloaded file. Binaries Redirections (still experimental)
Operational Intelligence Center	Malware analysis.	Detailed information about the binary analysed.
AHPS	Correlation & analysis functions. SIEM.	
File Analysis Component	Static (Signature based) and dynamic (Sandbox / Behaviour Analysis) analysis of malicious binaries and file types	Classification of malware and exploits used on websites. C&C servers, botnet name CVE used for exploit
URL Analysis Component	Static detection of malicious Websites	Classification of URL involved (eg. Phishing / Malware / benign)

Table 8 - Technologies involved Website

More information about solutions and technologies can be found on the Technology Development Framework document or the technology section of the ACDC Community Portal.

4.4. *Experiment main phases and processes*

The following diagram shows the main phases and processes to be executed in the Websites experiment.

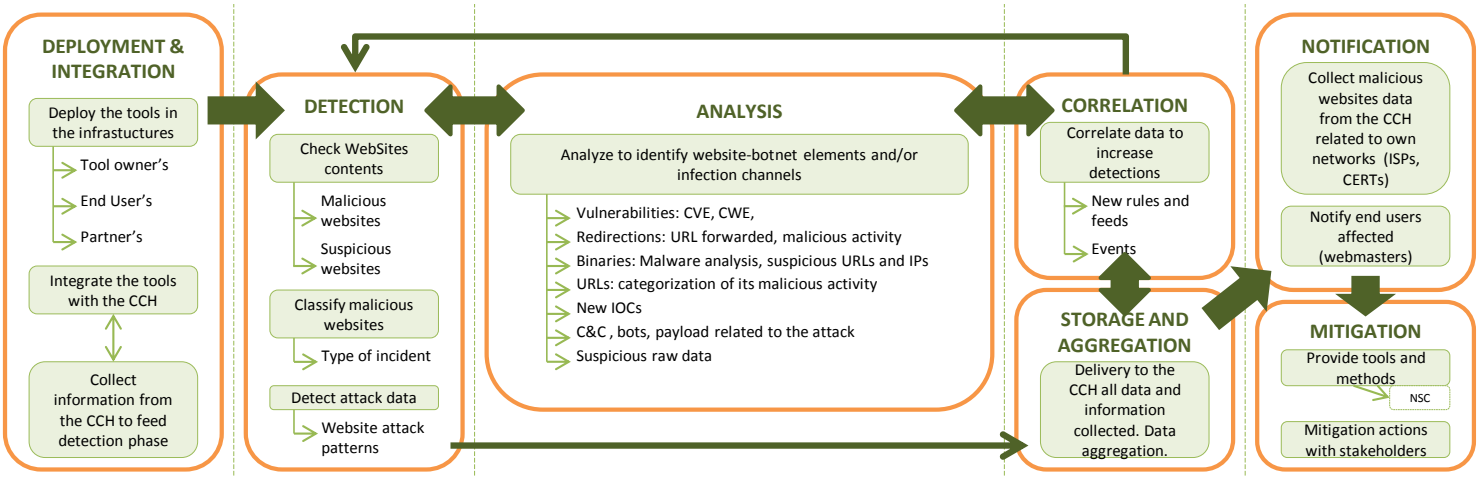

Illustration 2 - Experiment main processes - Websites

The different phases are conducted in order to achieve the main objectives of the experiment. Within each phase there are several processes defined. Detailed activities and data flows will be specified on the detailed design of each experiment (D3.2 deliverable and also will be available on the Community Portal).

Experiment preparation and preliminary testing phase

Deployment & Integration

During this phase all experiment supplied tools, sensors and/or information services will be deployed over involved partner infrastructure and/or end user web servers, and tested for valid integration with the project central information repository (Central Clearing House).

Experiment execution phase

Detection & analysis

During these phases the following tasks are done:

- Comprising (optionally) the collection of all information needed to feed own detection solutions from the Central Clearing House including for instance suspicious URLs, malware hashes and reputation blacklists, known attack patterns and websites infection patterns, etc.
- The detection of ongoing attacks against websites caused by botnets, including for instance attacker IPs, CWE & CVE, shellcodes, malware samples or payloads.

- The analysis of the malicious,infected or suspicious websites discovered including, if possible, the analysis of identified vulnerabilities, redirections, internal URLs and malware binaries, to identify website-botnet elements and/or other infection channels.
- The classification of the malicious or infected website discovered according to the type of incident, based on a specific classification used by ACDC project partners.

Storage, aggregation and correlation

At this phase is done the storage and aggregation of the datasets sent individually from the different sensors by partners to make all this information available to all partners and stakeholders that can use the information in three ways (following the sharing policies that apply):

- To correlate and generate new detection rules and increase ACDC intelligence (By correlation systems from partners)
- To feed detection phase again, for this or another experiment type (By sensors or tool owners partners).
- To activate notification and/or mitigation actions (By ISPs/CERTs and National Support Centers).

Notification

Comprising the collection from Central Clearing House (data aggregated and classified), of all website related incidents and relevant data related to specific networks or constituencies by partner, ISPs and CERTs involved in the experiment, including malicious and vulnerable URLs and bots related to website attacks, downloaded malware, etc. With this information, ISPs and CERTs can proceed to notify the identified malicious/infected website incidents to webmasters or hosting providers, and to infected end users participating in websites attacks, to raise awareness and motivate them to mitigate the threat.
If any C&C is discovered, CERTs should notify LEAs, if it is legally feasible.

Mitigation

NSCs => Dissemination of security alerts informing about current infection vectors used by botnets to compromise websites, tools for website disinfection, etc.

Generate blacklist for malicious domains, URLs, new IOC or rules for IDS systems.

If any C&C is discovered and if notification to LEAs success, actions like sinkholing or at least isolating the server for its analysis should be done.

4.5. Metrics

METRIC	Description
Partners	Partners contributing to the different phases of the experiment, with tools, infrastructure, knowledge, capacities, etc.
Tools/solutions	Tools and solutions contributing to the experiment.
CCH	Tools & partners integrated with the CCH. Statistical data of

	usage in the experiment.
URLs	Malicious and suspicious URLs classified by type of incident.
Exploits	CVE identified.
Bots	Bots identified.
C&C	C&C identified.
Notification	Notifications sent to web masters, or hosting ISPs and processes activated with LEAs.
Mitigation	Mitigation actions and disinfections methods/contents created.

Table 9 – Metrics - Websites

Detailed metrics will be defined on the specific design document for this experiment. In general, metrics will be given in total and also classified by country, ASNs, and TLDs if apply.

4.6. Partners involved – role – availability

4.6.1. Coordination

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
INTECO CERT-RO	Experiment coordinators	September 2014

Table 10 - Partners - Coordination - Websites

4.6.2. Detection & analysis

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
CARNET	Tool Owners& Operator	HONEYPOT SENSOR	September 2014
CARNET	Tool Operator	NIRC	September 2014
BGPOST	Tool Operator (CARNET Tool)	HONEYPOT SENSOR	September 2014
BGPOST	Tool Operator (CERT-RO Tool)	HONEYNET RO	September 2014
CERT-RO	Tool Owner	HONEYNET RO	September 2014
TID	Tool Operator	SND HP SENTINEL	Available (through STIX)
TID	Tool Owner & Operator	HONEYNET	October 2014
TI-IT	Tool Owner & Operator	HONEYNET	September 2014
INTECO	Tool Owner & Operator	SKANNA	July 2014
ISCTI/GARR	Tool Owner & Operator	HORGA	August 2014
ECO	Tool Owner & Operator	INITIATIVE-S	Available

ATOS	Tool Owner & Operator	AHPS	September 2014
G Data	Tool Owner & Operator	Website Analysis Component	September 2014
G Data	Tool Owner & Operator	File Analysis Component	September 2014
FCCN/CERT.PT	Tool Operator	HONEYPOT SENSOR	August 2014
Cassidian Cybersecurity	Tool Owner & Operator	Operational Intelligence Center	July 2014
CYDEF	Tool Owner & Operator	SiteVet	September 2014
CYDEF	Tool Owner & Operator	WebCheck	October 2014

Table 11 - Partners - Detection and Analysis - Websites

4.6.3. Storage and aggregation

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
ECO	CCH Operator	CCH	September 2014
LSEC	STIX Operator	STIX	September 2014

Table 12 - Partners - Storage and Aggregation - Websites

4.6.4. Notification & Mitigation

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
ECO	Germany NSC	Available
ISCTI	Italy NSC	July 2014
INTECO	Spain NSC	June 2014
INTECO	CERT (mitigation capacities)	September 2014
FCCN	Portugal NSC	September 2014
FCCN	CERT (mitigation capacities)	October 2014
CERT-RO	Romania NSC	September 2014
CERT-RO	CERT (mitigation capacities)	September 2014
CARNET	Croatia NSC	Available
CARNET	CERT & ISP (mitigation capacities)	Available
TI-IT	ISP (mitigation capacities, analysis of data related to own ASN and engage its internal CERT, forwarding the ACDC notification)	September 2014
TID	ISP (mitigation capacities, analysis of data related to own ASN and notification)	September 2014

DFCN-CERT	CERT (mitigation capacities) Incorporate ACDC feeds into their notification and mitigation channels	September 2014

Table 13 - Partners - Notification and Mitigation – Websites

5. Experiment: FASTFLUX

5.1. Objectives

General objectives defined in section 2.1 apply to all experiments. Specific and detailed objectives for the FastFlux experiment are the following:

Detection & analysis:

- Identify domains using fast flux techniques and their related components:
  - Domains used by botnets.
  - IPs associated to the domains (bots).
- If it is possible identify the C&C server and classify the botnet.

Notification and mitigation:

- For NSCs involved on the experiment:
  - If possible, provide tools or services for end-users to help them identify if their public IP is involved in fast flux activities.
  - Provide cleaning tools for bot removal.
- For CERTs involved on the experiment:
  - If a discovered C&C server is located under its constituency, launch notification actions to LEAs (if it is legally feasible) in order to take down and control or sinkhole the server activity.
  - Through CERTs channels and within their constituency, alert domain name registrar about incidents and contact with ISP for delivery IPs related with the incident.
  - Send to ISPs, not involved in the project, information about bot activity timestamp if ISP belongs to CERT's constituency.
- For ISPs involved on the experiment and if it is legally feasible depending of the country:
  - Based on bot data obtained, identify end-users affected on its own network, notify them about the malicious activity and give them information about the NSC to disinfect. Alternatively, ISPs could interface their internal SOC/CERT and possibly follow each case through internal processes.

5.2. Success criteria

Success criteria for fastflux experiment (based on real impact) will be:

- Domains using Fast Flux techniques and bots are detected by sensors and sent to CCH.
- At least 85% of the malicious domains detected implementing fastflux are notified to the domain name registrars.
- 100% of fastflux bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).
- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.
- 100% of C&C server discovered are notified to LEAs, in order to start a takedown process, if it is legally feasible depending of the country.

NOTE: Data to which success criteria applies will be only that with a high quality/veracity value. Experimental data will allow contributing to the objectives but not to the success criteria.

5.3. Technologies involved

For this experiment the following solutions and technologies will be used for detection and analysis phase:

SOLUTION NAME	TYPE OF TECHNOLOGY	VALUE DATA FOR THE EXPERIMENT OBJECTIVES
Passive DNS Sensor	Analysis of DNS traffic. Captures and analyzes outgoing DNS queries and responses searching for Fast Flux incidents.	Fast Flux domain name. List of IPs belonging to the domain.
DNS Traffic Sensor and Analysis Tools	Analysis of DNS traffic. Captures and analyzes DNS queries and responses searching for Fast Flux incidents.	Suspicious Fast Flux domain names. List of IPs belonging to the domain.
FFDetection Tool	Spatial analysis of suspicious domains' IP locations	Suspicious Fast Flux domain names. (IP addresses are fetched by the tool)
Flux Detect	Analysis of suspicious domains. Use of periodically queries to resolve the domain name based on the TTL given and through an algorithm discern if the domain is using Fast Flux Techniques	Fast Flux Domain name. List of IPs belonging to the domain.
DNSBot Detector	Extract and analyses DNS queries and responses from access network traffic searching for Fast Flux incidents	Fast Flux domain name and IPs accessing to this domain.
AHPS	Correlation & analysis functions. SIEM.	
File Analysis Component	Static (Signature based) and dynamic (Sandbox / Behaviour Analysis) of malicious binaries.	Classification of malware C&C servers, botnet name
Ransomware Removal	Clean-up Tool for specific malware family	Input source of malware samples and new fast flux domains.

Table 14 - Technologies involved Fast-Flux

More information about solutions and technologies can be found on the Technology Development Framework document or the technology section of the ACDC Community Portal.

5.4. *Experiment main phases and processes*

The following diagram shows the main phases and processes to be executed in the FastFlux experiment.

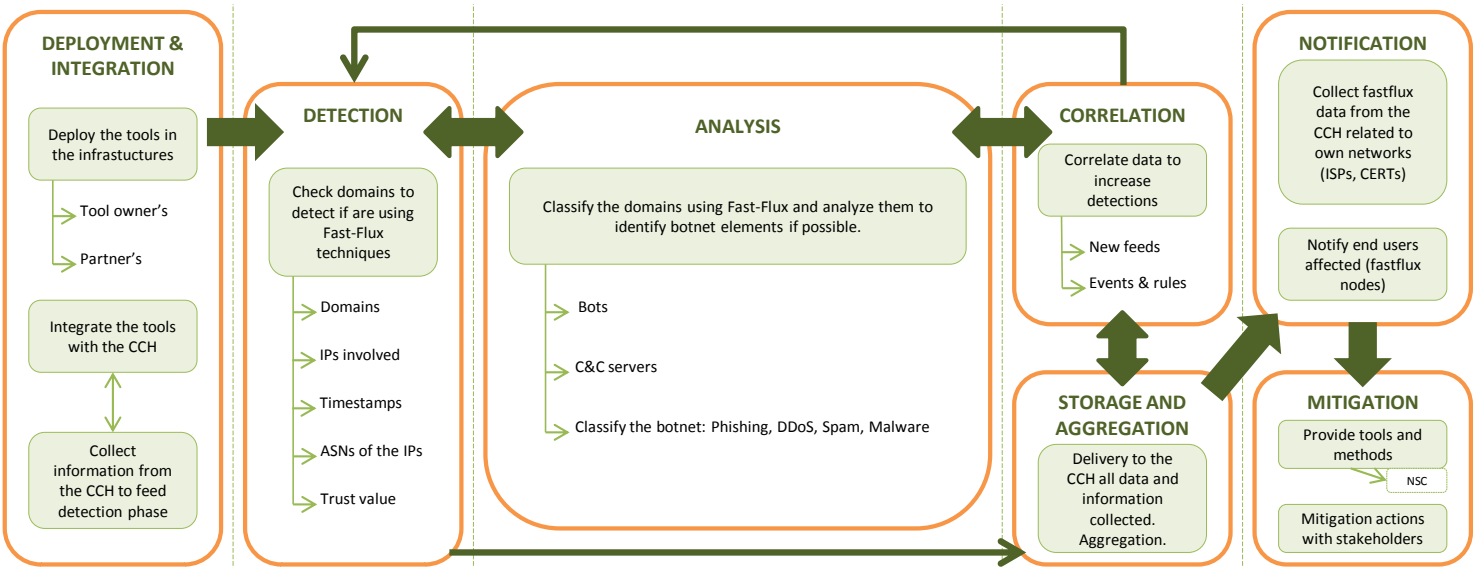

Illustration 3 - Experiment main processes - Fast-Flux

The different phases are conducted in order to achieve the main objectives of the experiment. Within each phase there are several processes defined. Detailed activities and data flows will be specified on the detailed design of each experiment (D3.2 deliverable and also will be available on the Community Portal).

Experiment preparation and preliminary testing phase

Deployment & Integration

During this phase all experiment supplied tools sensors and/or information services will be deployed over involved partner infrastructure and tested for valid integration with the project central information repository (Central Clearing House).

Experiment execution phase

Detection & analysis

During these phases the following tasks are done:

- Comprising (optionally), the collection of all information needed to start detection from the Central Clearing House including for instance blacklist of domains suspicious of being fast-flux.
- Periodic check of all domains collected in order to detect whether the suspicious domain continues using fast-flux techniques and which are the nodes (Bots IPs) involved.
- Analysis and classification of the identified domains belonging to botnets using fast-flux techniques, in order to obtain, if possible, C&C servers and classify

them into, at least, one of those categories: phishing botnet, DDoS botnet, SPAM botnet or malware distribution botnet.

Storage, aggregation and correlation

At this phase is done the storage and aggregation of the datasets sent individually from the different sensors by partners to make all this information available to all partners and stakeholders that can use the information in three ways (following the sharing policies that apply):

- To correlate and generate new detection rules and increase ACDC intelligence (By correlation systems from partners)
- To feed detection phase again, for this or another experiment type (By sensors or tool owners partners).
- To activate notification and/or mitigation actions (By ISPs/CERTs and National Support Centers).

Notification

Comprising the collection from Central Clearing House (data aggregated and classified), of all relevant data related to incidents caused by botnets using fast-flux techniques, including bot IPs under partner ISP ASNs and malicious or suspicious domains and partner CERT constituencies.
With this information, ISPs and CERTs can proceed to notify the identified incidents to affected end users and domain registrars, to raise awareness and motivate them to disinfect their compromised devices.
If any C&C is discovered, CERTs should notify LEAs, if it is legally feasible.

Mitigation

Actions by NSCs:

- Provide online auto-checking services to identify possible fastflux nodes (bots)
- Provide cleaners to disinfect.

If any C&C is discovered and if notification to LEAs success, actions like sinkholing or at least isolating the server for its analysis should be done by CERTs.

ISPs could launch procedures of blacklist fastflux domains blocking.

5.5. Metrics

METRIC	Description
Partners	Partners contributing to the different phases of the experiment, with tools, infrastructure, knowledge, capacities, etc.
Tools/solutions	Tools and solutions contributing to the experiment.
CCH	Tools & partners integrated with the CCH. Statistical data of usage in the experiment.
Domains	Domains using fast-flux and classification: distributing phishing, spam, malware or used for DDoS amplification.
Bots	Fast flux nodes identified.

C&C	C&C servers identified.
Notification	Notifications sent to end users and registrars. Processes activated with LEAs.
Mitigation	% fast flux domains taken down during experiment

Table 15 - Metrics Fast-Flux

Detailed metrics will be defined on the specific design document for this experiment. In general, metrics will be given in total and also classified by country, ASNs, and TLDs if apply.

5.6. Partners involved – role – availability

5.6.1. Coordination

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
INTECO ATOS	Experiment coordinators	September 2014

Table 16 - Partners – Coordination - Fast-Flux

5.6.2. Detection & analysis

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
CARNET	Tool Owner & Operator	PASSIVE DNS SENSOR	September 2014
ATOS	Tool Owner	DNS TRAFFIC SENSOR AND ANALYSIS TOOL	July 2014
BDIGITAL	Tool Operator (ATOS Tool)	DNS TRAFFIC SENSOR AND ANALYSIS TOOL	September 2014
TID	Tool Owner & Operator	DNSBOT DETECTOR	September 2014 (ISP authorization pending)
INTECO	Tool Owner & Operator	FLUX DETECT	Available
ATOS	Tool Owner	AHPS	July 2014
G Data	Tool Owner & Operator	File Analysis Component	September 2014
G Data	Tool Owner & Operator	Ransomware Removal	September 2014
TEC	Tool Owner	FF DETECTION	Available

Table 17 - Partners - Detection and Analysis - Fast-Flux

5.6.3. Storage and aggregation

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
ECO	CCH Operator	CCH	September 2014
LSEC	STIX Operator	STIX	September 2014

Table 18 - Partners - Storage and Aggregation - Fast-Flux

5.6.4. Notification & Mitigation

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
ECO	Germany NSC	Available
ISCTI	Italy NSC	July 2014
INTECO	Spain NSC	June 2014
INTECO	CERT (mitigation capacities)	September 2014
FCCN	Portugal NSC	September 2014
FCCN	CERT (mitigation capacities)	October 2014
CERT-RO	Romania NSC	September 2014
CERT-RO	CERT (mitigation capacities)	September 2014
CARNET	Croatia NSC	Available
CARNET	CERT & ISP (mitigation capacities)	Available
TI-IT	ISP (mitigation capacities, analysis of data related to own ASN and engage its internal CERT, forwarding the ACDC notification)	September 2014
TID	ISP (mitigation capacities, analysis of data related to own ASN and notification)	September 2014
DFCN-CERT	CERT (mitigation capacities) Incorporate ACDC feeds into their notification and mitigation channels	September 2014

Table 19 - Partners - Notification and Mitigation - Fast-Flux

6. Experiment: DDOS

6.1. Objectives

General objectives defined in section in 2.1 apply to all experiments. Specific and detailed objectives for the DDoS experiment are the following:

Detection & analysis:

- Analyze traffic of real DDoS attacks (already detected and stopped) in order to discover bots and C&C (if possible) involved on them.

Notification and mitigation:

- Envision a concept to mitigate DDoS attack traffic by using BGPBlackHole, Darknets, provide blacklist and generate new rules and detection firms. A log file format should be specified in order to inform on past DDoS attacks and improve the detection systems (e.g., bots and C&C).

- For NSCs involved on the experiment:
    - If possible, provide tools or services for end-users to help them identify if their public IP is involved in DDoS activities.

- For CERTs involved on the experiment:
    - If a discovered C&C server is located under its constituency, launch notification actions to LEAs (if it is legally feasible) in order to take down and control or sinkhole the server activity.
    - Send to ISPs, not involved in the project, information about bot activity timestamp if ISP belongs to CERT's constituency.
- For ISPs involved on the experiment and if it is legally feasible depending of the country:
    - Based on data obtained from DDoS traffic analysis, identify end-users affected on its own network, notify them about the infection and give them information about the NSC to disinfect. Alternatively, ISPs could interface their internal SOC/CERT and possibly follow each case through internal processes.

6.2. Success criteria

Success criteria for DDoS experiment (based on real impact) will be:

- The information extracted from DDoS attacks is used to obtain bots.
- At least traffic of 10 DDoS real attacks is analyzed.
- 100% of bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).
- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.
- 100% of C&C server discovered are notified to LEAs, in order to start a takedown process, if it is legally feasible depending of the country.

NOTE: Data to which success criteria applies will be only that with a high quality/veracity value. Experimental data will allow contributing to the objectives but not to the success criteria.

6.3. Technologies involved

For this experiment the following solutions and technologies will be used for detection and analysis phase:

SOLUTION NAME	TYPE OF TECHNOLOGY	VALUE DATA FOR THE EXPERIMENT OBJECTIVES
Black-Holing feature (DE-CIX)	Analysis of DDoS traffic redirected to a blackhole	DDoS bots IPs. DDoS attack analysis & patterns
DDoS Monitoring Tool	Identify DDoS C&C servers via execution DDoS bots in dynamic analysis environment. Monitor impact of recorded DDoS attack commands on targets.	IP address of the C&C server. Domain of the C&C server. Name of DDoS botnet family.
DNS Traffic Sensor and Analysis Tools	Analysis of DNS traffic. Analyzes DNS queries and responses searching for DDoS incidents. Detects attacks of Amplified DDoS.	Suspicious domain or IP participating in an Amplified DDoS incident.
MMT	Network behaviour analysis. Normal or abnormal behaviour can be specified and used by the DPI and analysis modules to identify attacks and extract packet or flow related data and metadata	The source and destination IPs and ports are obtained from the events that triggered the abnormal behaviour or attacks. The source IP identifies the computers that participate in the attacks. These can be either attacker or infected machines.
Honeynet-Statistics	Statistical aggregation of captured data in order to detect suspicious DOS attacks	Source IP, destination Port of suspicious attack flow
AHPS	Correlation & analysis functions. SIEM.	
File Analysis Component	Static (Signature based) and dynamic (Sandbox / Behaviour Analysis) of malicious binaries.	Classification of malware involved in DDOS attack C&C servers, botnet name

Table 20 - Technologies involved - DDoS

More information about solutions and technologies can be found on the Technology Development Framework document or the technology section of the ACDC Community Portal.

6.4. *Experiment main phases and processes*

The following diagram shows the main phases and processes to be executed in the DDoS experiment.

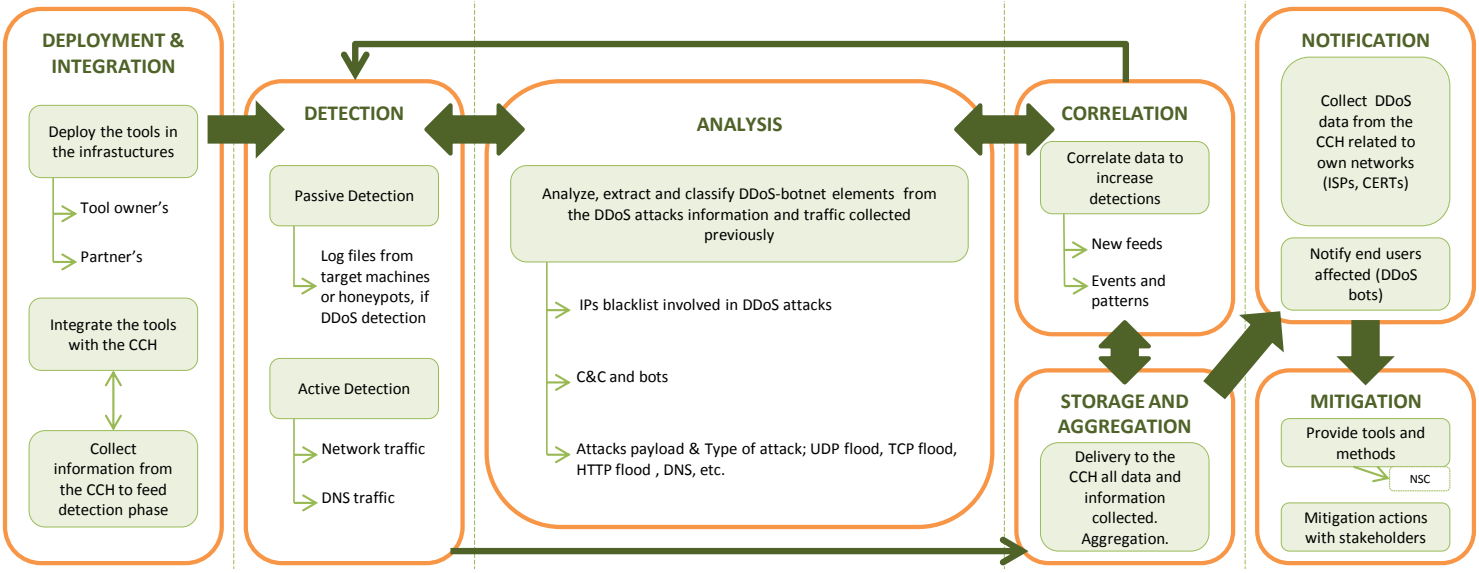

Illustration 4 - Experiment main processes - DDoS

The different phases are conducted in order to achieve the main objectives of the experiment. Within each phase there are several processes defined. Detailed activities and data flows will be specified on the detailed design of each experiment (D3.2 deliverable and also will be available on the Community Portal).

Experiment preparation and preliminary testing phase

Deployment & Integration

During this phase, all experiment supplied tools, sensors and/or information services will be deployed over involved partner infrastructures and tested for valid integration with the project central information repository (Central Clearing House).

Experiment execution phase

Detection & analysis

During these phases the following tasks are done:

- Passive detection of DDoS botnets by analysis of network traffic in general, DNS traffic, log files to obtain attacker IPs and attack payloads.

- Analysis of all data collected in order to identify botnets responsible for the attacks, its components including C&C and bots, and/or DDoS botnet infection channels.

Storage, aggregation and correlation

In this phase the storage and aggregation of the datasets sent by the different sensors will allow all the partners and stakeholders to use the information collected in the following ways (depending on the sharing policies defined):

- To correlate and generate new detection rules and increase ACDC intelligence, validate results and eliminate false positives (using correlation tools from partners)
- To again serve as input to the detection phase, for this or other types of experiments (using sensors or tools from partners).
- To activate notification and/or mitigation actions (by ISPs/CERTs and National Support Centers and/or using tools from partners).

Notification

This comprises the aggregation and classification of the data stored in theCentral Clearing House, of all relevant information related to DDoS botnet incidents, including bots and C&C IPs, under partner ISP ASNs, and partner CERT constituencies.

With this information, ISPs and CERTs can then proceed to notify the affected end users on the DDoS botnet related incidents. In this way it is to raise awareness and motivate them to disinfect their compromised devices. This can be done through human intervention, with or without tool support to automate or semi-automate the notification process.

If any C&C are discovered, the CERTs should notify the LEAs, if it is legally feasible.

Mitigation

Actions by Network Operators:

- Implementation of blackholing techniques.

Actions by NSCs:

- Provide online auto-checking services to identify possible DDoS bots
- Provide cleaners to disinfect.
- Publish preventive information about DDoS attacks types.

If any C&C is discovered and if notification to LEAs success, actions like sinkholing or at least isolating the server for its analysis should be done by CERTs.

6.5. Metrics

METRIC	Description
Partners	Partners contributing to the different phases of the experiment, with tools, infrastructure, knowledge, capacities, etc.

Tools/solutions	Tools and solutions contributing to the experiment.
CCH	Tools & partners integrated with the CCH. Statistical data of usage in the experiment.
Attacks	Attacks info and analysis documentation. Patterns
Bots	Bots detected.
C&C	C&C detected.
Notification	Notifications sent to end users and processes activated with LEAs.
Mitigation	Blackholing metrics. Information published on NSCs.

Table 21 – Metrics - DDoS

Detailed metrics will be defined on the specific design document for this experiment. In general, metrics will be given in total and also classified by country, ASNs, and TLDs whenever applicable.

6.6. Partners involved – role – availability

6.6.1. Coordination

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
INTECO DE-CIX	Experiment coordinators	September 2014

Table 22 - Partners Coordination - DDoS

6.6.2. Detection & analysis

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
DE-CIX	Tool Owner & Operator	Black-Hole Feature	Already operational (Legal issues must be clarified in order to provide data to the CCH)
IF-IS	Tool Owner & Operator	DDoS Monitoring Tool	July 2014
MONTIMAGE	Tool Owner & Operator	MMT	June 2014
BGPOST	Tool Operator (Montimage Tool)	MMT	July 2014
ATOS	Tool Owner & Operator	DNS TRAFFIC SENSOR AND ANALYSIS TOOL	July 2014
TID	Tool Owner & Operator	HONEYNET	October 2014
TI-IT	Tool Owner & Operator	HONEYNET-Statistics	September 2014
ATOS	Tool Owner & Operator	AHPS	September 2014

G Data	Tool Owner & Operator	File Analysis Component	September 2014

Table 23 - Partners - Detection and Analysis - DDoS

6.6.3. Storage and aggregation

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
ECO	CCH Operator	CCH	September 2014
LSEC	STIX Operator	STIX	September 2014

Table 24 – Partners - Storage and Aggregation - DDoS

6.6.4. Notification & Mitigation

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
DE-CIX	ISP (mitigation capacities)	
ECO	Germany NSC	Available
ISCTI	Italy NSC	July 2014
INTECO	Spain NSC	June 2014
INTECO	CERT (mitigation capacities)	September 2014
FCCN	Portugal NSC	September 2014
FCCN	CERT (mitigation capacities)	October 2014
CERT-RO	Romania NSC	September 2014
CERT-RO	CERT (mitigation capacities)	September 2014
CARNET	Croatia NSC	Available
CARNET	CERT & ISP (mitigation capacities)	Available
TI-IT	ISP (mitigation capacities, analysis of data related to own ASN and engage its internal CERT, forwarding the ACDC notification)	September 2014
TID	ISP (mitigation capacities, analysis of data related to own ASN and notification)	September 2014
DFCN-CERT	CERT (mitigation capacities) Incorporate ACDC feeds into their notification and mitigation channels	September 2014

Table 25 – Partners - Notification and Mitigation - DDoS

7. Experiment: MOBILE BOT

7.1. Objectives

General objectives defined in section 2.1 apply to all experiments. Specific and detailed objectives for the Mobile bot experiment are the following:

Detection & analysis:

- Detect and analyze attacks generated from mobile networks (tagging incidents as originated from mobile network).
- Analyze mobile devices through apps and services, detecting the malicious and suspicious APKs or activities and alert the end user.

Notification and mitigation:

- For NSCs involved on the experiment:
  - Through NSC channels, alert end-users about malicious APKs in public markets
  - Provide information about security apps and tools for mobile devices.
- For CERTs involved on the experiment:
  - If as a result of an APK analysis, a C&C server is discovered and located under its constituency, launch notification actions to LEAs (if it is legally feasible) in order to take down and control or sinkhole the server activity.
  - Send to ISPs, not involved in the project, information about mobile bot activity timestamp if ISP belongs to CERT's constituency
- For ISPs involved on the experiment and if it is legally feasible depending of the country:
  - Based on bot data obtained from CCH (from any type of incident), identify end-users affected on its own mobile network, notify them about the infection and give them information about the NSC to disinfect. Alternatively, ISPs could interface their internal SOC/CERT and possibly follow each case through internal processes.

7.2. Success criteria

Success criteria for mobile bot experiment (based on real impact) will be:

- End-user tools are accessible for users in ACDC countries.
- Attacks from mobile devices are detected by sensors and tools and sent to CCH.
- At least 50% of malicious contents (APKs or others) discovered are analysed[5].
- At least 50% attacks to mobile networks are analyzed[6].
- 100% of C&C server discovered are notified to LEAs, in order to start a takedown process, if it is legally feasible depending of the country.
- NSCs alert end-users about 75% of malicious APKs discovered (if the APK is available on the country's market)

NOTE: Data to which success criteria applies will be only that with a high quality/veracity value. Experimental data will allow contributing to the objectives but not to the success criteria.

[5] In the detailed design of the experiment a maximum analysis capacity will be defined.

[6] In the detailed design of the experiment a maximum analysis capacity will be defined.

7.3. Technologies involved

For this experiment the following solutions and technologies will be used for detection and analysis phase:

SOLUTION NAME	TYPE OF TECHNOLOGY	VALUE DATA FOR THE EXPERIMENT OBJECTIVES
Device Monitor and GCMServer	Analysis of the mobile device. Check different components, behaviour and apps installed in the mobile devices to discover anything malicious in the device.	Event id, rule id, timestamp, device id, event details: protocol, remote ip, remote port, state, type of the event, local ip, local port
Suricata IDS	IDS. System able of discover malicious traffic from mobile devices passing through it. Usually works with firms, rules and sometimes with deep packet inspection.	Source IP, source port, destination IP, destination port, protocol, timestamp, event details.
EventCorrelator (Analyser)	Correlates malicious events within a mobile network and identifies malicious connections between the nodes in the network in an attempt to locate instances that are parts of a botnet.	IPs of devices taking part in the event: source IP, source port, destination IP, destination port, Timestamp, event details.
Conan Mobile	Analysis of the device. Check different components, behaviour, connections and apps installed in the mobile devices to discover anything malicious in the device.	Statistics data related to the mobile devices monitored and the ASN and countries they belong to.
Honeynet-Statistics	Statistical aggregation of captured data in order to detect suspicious behaviours	Source IP, destination Port of suspicious attack flow
DNSBot Detector	Extract and analyses DNS queries and responses from mobile access network traffic searching for botnets	Mobile IPs accessing to botnets domains.

File Analysis Component	Static (Signature based) and dynamic (Sandbox / Behaviour Analysis) analysis of malicious binaries (including APKs).	Classification of mobile malware families botnet name
AHPS	Correlation & analysis functions. SIEM.	

Table 26 – Technologies involved - Mobile

More information about solutions and technologies can be found on the Technology Development Framework document or the technology section of the ACDC Community Portal.

7.4. Experiment main phases and processes

The following diagram shows the main phases and processes to be executed in the Mobile experiment.

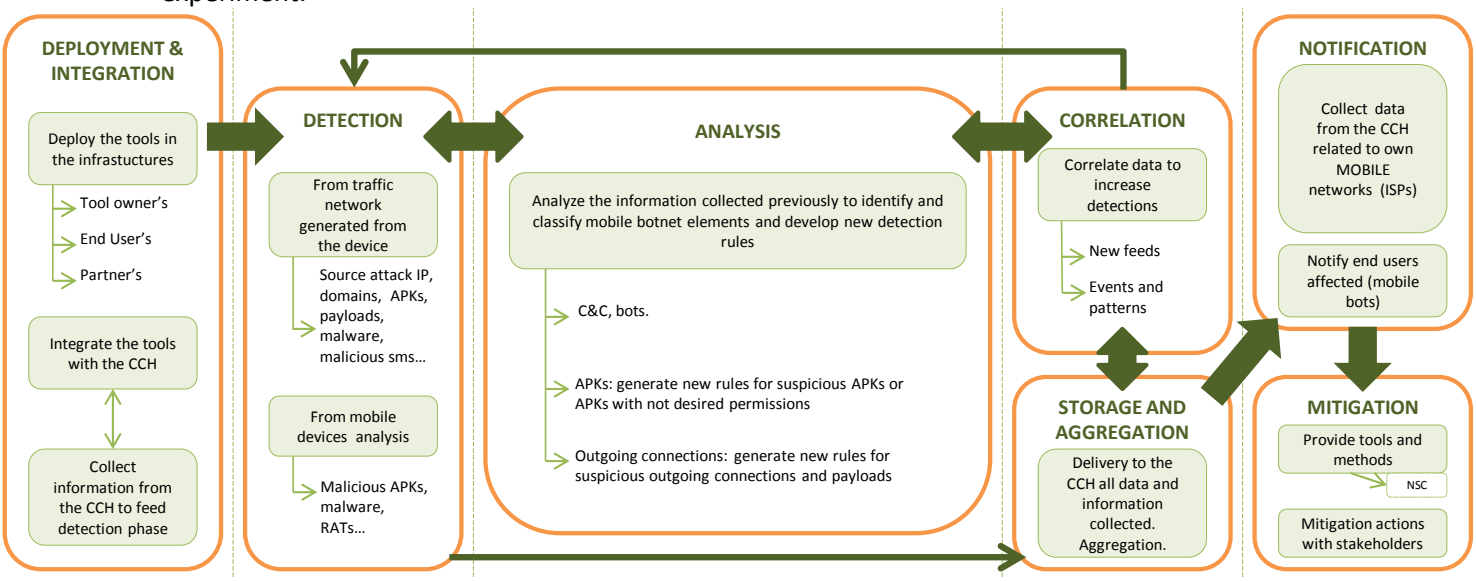

Illustration 5 - Experiment main processes - Mobile

The different phases are conducted in order to achieve the main objectives of the experiment. Within each phase there are several processes defined. Detailed activities and data flows will be specified on the detailed design of each experiment (D3.2 deliverable and also will be available on the Community Portal).

Experiment preparation and preliminary testing phase

Deployment & Integration

During this phase all experiment supplied tools sensors and/or information services will be deployed over involved partner infrastructure and tested for valid integration with the project central information repository (Central Clearing House).

Experiment execution phase

Detection & analysis

During these phases the following tasks are done:

- Comprising (optionally) the collection of all information needed to start detection from the Central Clearing House, including IP, domain, malware and APK blacklists, and predefined detection rules previously reported by other partners.
- Detection of mobile security incidents by means of checking end user mobile devices (with the user consent) and the network traffic generated by them, to identify attack sources (IPs), malicious outgoing connections, payloads, malware, malicious APK's, Remote Access Tools (RATs), malicious SMS, and apps with not desired permissions.
- Detection of mobile security incidents by means of deploying honeypots on mobile networks.
- Analysis of all data collected during the detection phase to identify mobile botnet elements like C&C and bots and/or infection channels.

Storage, aggregation and correlation

At this phase is done the storage and aggregation of the datasets sent individually from the different sensors by partners to make all this information available to all partners and stakeholders that can use the information in three ways (following the sharing policies that apply):

- To correlate and generate new detection rules and increase ACDC intelligence (By correlation systems from partners)
- To feed detection phase again, for this or another experiment type (By sensors or tool owners partners).
- To activate notification and/or mitigation actions (By ISPs/CERTs and National Support Centers).

Notification

Comprising the collection from Central Clearing House (data aggregated and classified), by ISPs, of all incidents (**any type**) under **mobile** network ASNs. With this information, ISPs can proceed to notify the identified Mobile botnet incidents to affected end users, to raise awareness and motivate them to mitigate the threat.
If any C&C is discovered, CERTs should notify LEAs, if it is legally feasible.

Mitigation

Actions by NSCs:

- Alert end-users about malicious apks in public markets.
- Provide information about security apps and tools for mobile devices.

If any C&C is discovered and if notification to LEAs success, actions like sinkholing or at least isolating the server for its analysis should be done by CERTs.

7.5. Metrics

METRIC	Description
Partners	Partners contributing to the different phases of the experiment, with tools, infrastructure, knowledge, capacities, etc.
Tools/solutions	Tools and solutions contributing to the experiment.
CCH	Tools & partners integrated with the CCH. Statistical data of usage in the experiment.
Devices	Mobile devices vulnerable, infected.
Malware, APKs	Mobile malware information.
Attacks	Mobile attacks information.
Bots	Mobile bots detected and bots attacking mobile devices.
C&C	C&C identified.
Notification	Notifications sent to end users and processes activated with LEAs.
Mitigation	Alerts and contents published.

Table 27 - Metrics - Mobile

Detailed metrics will be defined on the specific design document for this experiment. In general, metrics will be given in total and also classified by country, ASNs, and TLDs if apply.

7.6. Partners involved – role – availability

7.6.1. Coordination

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
INTECO TID TI-IT XLAB	Experiment coordinators	September 2014

Table 28 - Partners – Coordination - Mobile

7.6.2. Detection & analysis

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
XLAB	Tool Owner & Operator	DEVICE MONITOR AND GCMSERVER	October 2014
XLAB	Tool Owner & Operator	SURICATA IDS	October 2014
XLAB	Tool Owner & Operator	EVENT CORRELATOR (ANALYSER)	October 2014
INTECO	Tool Owner & Operator	CONAN MOBILE	September 2014
TI-IT	Tool Owner & Operator	honeynet	October 2014
BDIGITAL	Analysis	(APKs analysis &	

	capacities	expertise)	
ATOS	Tool Owner & Operator	AHPS	September 2014
G Data	Tool Owner & Operator	File Analysis Component	September 2014
Cassidian Cybersecurity	Tool Owner & Operator	Operational Intelligence Center	July 2014

Table 29 – Partners - Detection and Analysis - Mobile

7.6.3. Storage and aggregation

PARTNER	ROLE	Specific solutions	AVAILABILITY DATE TO START EXPERIMENT
ECO	CCH Operator	CCH	September 2014
LSEC	STIX Operator	STIX	September 2014

Table 30 – Partners - Storage and Aggregation - Mobile

7.6.4. Notification & Mitigation

PARTNER	ROLE	AVAILABILITY DATE TO START EXPERIMENT
ECO	Germany NSC	Available
ISCTI	Italy NSC	July 2014
INTECO	Spain NSC	June 2014
INTECO	CERT (mitigation capacities)	September 2014
FCCN	Portugal NSC	September 2014
FCCN	CERT (mitigation capacities)	October 2014
CERT-RO	Romania NSC	September 2014
CERT-RO	CERT (mitigation capacities)	September 2014
CARNET	Croatia NSC	Available
TI-IT	ISP (mitigation capacities, analysis of data related to own Mobile Network and engage its internal CERT, forwarding the ACDC notification)	September 2014
TID	ISP (mitigation capacities, analysis of data related to own Mobile network and notification)	September 2014
DFCN-CERT	CERT (mitigation capacities) Incorporate ACDC feeds into their notification and mitigation channels	September 2014

Table 31 - Partners - Notification and Mitigation - Mobile