ACDC
the Advanced Cyber Defence Centre

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

Deliverable	**D1.3.2 Specification of Tool Group "Support Centre"**
Work package Due date Submission date Revision Status of revision	WP1 Requirements & Specifications M30 31.07.2015 1.0 Review
Responsible Partner	ECO
Contributors	Peter Meyer (ECO), Christian Giebe (ECO), Thomas Berchem (ECO) Michael Weirich (ECO) Andreas Fobian (GDATA), Darko Perhoc (CARnet) Angela Garcia (INCIBE), Tiziano Inzerilli (ISCTI), Kurt Liessens (LSEC), Jorge de Carvalho (FCT/FCCN), Catalin Patrascu (CERT.ro), Thomas Fontvielle (SignalSpam)
Reviewer	Elsa Prieto (ATOS)
Project Number Project Acronym Project Title Start Date of Project	CIP-ICT PSP-2012-6 / 325188 ACDC Advanced Cyber Defence Centre 01/02/2013

Dissemination Level	
PU: Public	X
PP: Restricted to other programme participants (including the Commission)	
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	Notes
Vers.0.1	04/20/2015	Peter Meyer (ECO) / Christian Giebe (ECO)	Initial structure of the document / table of content
Vers.0.2	04/27/2015	Peter Meyer (ECO) / Christian Giebe (ECO)	First draft on standard requirements, recommendations and description for the German NSC
Vers.02.5	06/09/2015	Peter Meyer (ECO) / Andreas Fobian (GDATA)	Updated specifications for EU-Cleaners
Vers.0.3	06/11/2015	Darko Perhoc (CARNET)	Contributions Croatian NSC
Vers.0.4	06/22/2015	Angela Garcia (INCIBE)	Contributions Spanish NSC
Vers.0.5	06/29/2015	Tiziano Inzerilli (ISCTI) Kurt Liessens (LSEC)	Contributions Italian NSC Contributions Belgian NSC
Vers.0.6	07/01/2015	Jorge de Carvalho(FCT)	Contributions Portuguese NSC
Vers.0.7	07/07/2015	Catalin Patrascu (CERT.ro)	Contributions Romanian NSC
Vers.0.8	07/15/2015	Thomas Fontvielle (SignalSpam)	Contributions French NSC
Vers.0.9	07/16/2015	Thomas Berchem (ECO) / Christian Giebe (ECO)	Editing and Review
Vers0.95	07/20/2015	Elsa Prieto (Atos)	Peer Review
Vers1.0	07/23/2015	Peter Meyer (ECO) / Georg Roßrucker (ECO)	Finalisation

Glossary

ABBZ	German Anti Botnet Advisory Centre
ACDC	Advanced Cyber Defence Centre
ASN	Autonomous System
AV	Anti-Virus
CCH	Centralized data Clearing House
EABSCA	European Anti-Botnet Support Centre Alliance
ECO	Association of the German Internet Industry
FAQ	Frequently Asked Questions
ISP	Internet Service Provider
LEA	Law Enforcement Agency
NGN	Next Generation Network
NSC	National Support Centre
OTRS	Customer Support System
PC	Personal Computer
SME	Small-and Medium Enterprises
URL	Uniform Resource Locator
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
XMPP	Extensible Messaging and Presence Protocol

TABLE OF CONTENT

Index of Figures and Images

Tables

1 Introduction

The ACDC-Project has the aim to provide end-to-end protection and a set of services to all stakeholder groups identified in deliverable *D6.1.1: User profiles and categorization*. One of the project goals is the provision of eight National Anti-Botnet Support Centres (NSC) across Europe offering dedicated support services to End Users or Small and Medium Enterprises (SMEs).

A national Anti-Botnet Support Centre in Germany was already operational before the project launch and their concept and experience was used to carry out this concept to other European member states. The collaboration has been driven through a specific task force, whose goals were oriented towards the identification of common standards, specifications and recommendations for the operation of an exemplary National Anti-Botnet Support Centre that could be easily set-up by any interested organization/Member State.

2 Executive Summary

The set-up of National Anti-Botnet Support Centres across Europe is one of the main columns of the ACDC-Project in offering an end-to-end approach to fight and mitigate botnet infections.

In this model, the NSCs inherit the role of the first-level contact point for infected end-users at a national level.

The German ABBZ is operating since 2010 and during the ACDC project duration, it has been proven that the model of National Anti-Botnet Support Centres can be carried out successfully to other European member states as well.

As part of the ACDC project, new NSCs have been established in Spain, Italy, Belgium, Portugal, France, Romania and Croatia. Additionally, the concept has convinced organisations from Luxembourg and Bulgaria to follow the ACDC approach and to establish NSCs in their countries, too. The concept has been presented to other countries as well and organisations from Ireland, Slovenia or The Netherlands stated an interest to adapt the concept of NSCs under the ACDC umbrella in the near future. A bilateral consultancy with similar initiatives in Japan (ACTIVE-Project) and Australia (ACMA-Service) has been established during the project. These organisations have similar goals and services as the NSCs of ACDC.

Driven by the NSC task force during the project duration, a fruitful and regular exchange between the different partner organisations was established. The task group agreed on applying common standards and introduced an ongoing exchange of information, resources and expertise. The Spanish NSC, operated by partner INCIBE (INTECO), has also exemplary participated in the experiments of ACDC within WP3 as a proof of concept on the detection to mitigation approach as defined in the project goals.

The ACDC project with its NSCs however missed one of its goals during the project span - the direct involvement into a botnet takedown driven by law enforcement agencies.

However, several NSC’s support centres were involved into takedowns like on CryptoLocker or GameOver.Zeus during the project span, but these have been tackled at a national level only, without internal coordination or involvement of ACDC.

The main reasons for the non-involvement of the ACDC NSCs are the strict confidentiality levels of such police operations, the restrictions of information disclosure to third parties and the missing availability of a supervising legal entity for the National Support Centres.

As a consequence of this, the operators of the NSCs intend to establish an alliance for National Anti-Botnet Support Centres in the European Union after the end of the project. This future European Anti-Botnet Support Centre Alliance (EABSCA) will act as a coordinating and supporting organisation for the NSCs, with the goal to drive the exchange and collaboration among each other, but also with European organisations like Europol, CERTs, ENISA or the European Commission on botnet takedowns or campaigns like the Internet Safety Day. All national support centres prefer being independent entities, responsible for their service, funding and equipment in the future.

3 Task Force National Support Centre

The task force “National Support Centres” was introduced as defined in the deliverable *D2.2 Establishment of Component Task Forces* and reflects the Component Task Force 3: End Customer Tools and Support Centres that is described on page 8 in that deliverable.
An early decision of the initial task group divided the initial task group into two working groups. The component Support Centres has been led by ECO, the component End Customer Tools by LSEC. Members were the operators of the National Support Centres, but other project partners like ATOS (for the sustainability planning) or GData (as a tool provider with their EU-Ransomware cleaner) were regularly participating at these task group meetings as well. The task force leaders were also leading the reach-out and follow-ups with external partners that stated interest in building own NSCs, like the Bulgarian CERT. Task force leader ECO also forced the international collaboration with organisation from Japan, Australia or South Korea.

The task force agreed on a meeting schedule once a quarter, either by phone or during internal ACDC summits. The topics of the support centre task force meetings covered status updates to the progress of setting up the national centres, the collaboration at a European Level, Updates from operating National Centres, the exchange of lessons learned, general feedback, same as surveys and their outcome. As a part of the internal discussion towards the long-term sustainability of the NSC, it is planned to continue the collaboration under the umbrella of the future European Anti-Botnet Support Centre Alliance (EABSCA)

	Date	Type/Event	Note
1	21.02.13	Meeting	ACDC Kick-Off
2	13.06.13	Telco	General sync-up
3	25.09.13	Meeting	General Assembly 2013
4	04.12.13	Meeting	WP1/2 Workshop, Nantes
5	28.05.14	Meeting	ACDC Workshop, Frankfurt
6	02.09.14	Telco	Preparation call GA
7	25.09.14	Meeting	General Assembly 2014
8	25.02.14	Telco	Status Updates, Results Survey
9	01.04.15	Telco	Status Call, launch of all NSCs
10	12.05.15	Meeting	General Assembly 2015

Table 1: List of NSC Task Force Meetings

4 Standards requirements for a National Support Centres

The primary purpose of a national support centre is to reduce the number of botnet-infected computers in the operating country, educate users on the subject of Internet security, and provide assistance removing malicious botnet software from an infected end-device.

The target group of a NSC are end-users, same as small-and medium sized enterprises. Practical experience and knowledge of the operation of the NSC in Germany, but also common know-how on Customer Services especially on IT-Security clearly underline that a service of a National Anti-Botnet support centre needs to be free of charge. Charging users for the intended services would clearly miss the objectives like reducing the number of botnet infections at a national level. The majority of end-users are simply not willed to pay for such type of services.

National support centres participating in the ACDC-Project are fully independent entities. Each operator can decide based on his available budget and funding, which service level his NSC can provide. Due to different budgets, own demands, national peculiarities or industry partners, the definition of these basic requirements enables a minimum standard for a national support centre. The ACDC Support Centre Task Group has defined and agreed on these minimal requirements that a provider needs to fulfil to comply as a national anti-botnet support centre under the ACDC brand.

4.1 Operator

The operator of a National Support Centre does not need to be a consortium member of the ACDC project, but it needs to an entity based in the country that the NSC is dedicated to. This requirement is necessary to ensure a high level of trust by a national operator among its citizens, the industry partners like the ISPs and finally the government or CERT community. Additionally, legal barriers like the domain registration guidelines prevent organisation abroad to register specific Country code top-level domains as well. As an example, a German organisation would not be entitled to run a National Support Centre in Austria.

4.2 Languages

The website of a National Support Centre should be available in at least one official language spoken in the hosting country. An additional English version is not mandatory, but recommended to enable support to foreigners in the particular country, too.

4.3 Service level

The minimal requirement for the service of a National Support Centre is a static website.

Each National Support Centre must provide an option to contact the operating organisation and the responses need to be handled in a timely manner.

Additional levels of technical support[1] provided by a NSC are not compulsory, each organisation must decide which services it can provide based on its available budget and funding.

Further, activities in social media, the availability of a support forum, a blog and activities beyond are appreciated, but not compulsory. It is recommended that NSCs use the synergies of other National Support Centres, e.g. by linking to available international support forums, blogs or social media accounts.

[1] http://en.wikipedia.org/wiki/Technical_support

4.4 Branding

A National Support Centre related to ACDC has to display the ACDC Logo and a link to the project website on its main website. Displaying the logo and the link on other subpages is appreciated, but not mandatory. Besides that, each National Support Centre has the right to implement its own web design and layout. ECO has granted interested project partners the cost-free usage of their web page template.

It is recommended to host the NSC on its own domain and the national top-level domain. The domain name of the national support centre is not compulsory, but it is recommended following the naming convention of ***.botfree.***, ***.antibot.*** or localised variations.

4.5 Content

A NSC should apply a terminology, wording and language that is understandable by its target customer/visitor group. Information displayed on a NSC should include general information about botnets and should ideally also address other common and related IT-security threats like Phishing. The website of a NSC should also include basic advice how to protect a computer device and how to "stay safe" on the Internet. This particularly includes the advice of the regular installation of updates and patches to tools, browser, plugins, apps or the operating system, the usage of security tools like an Anti-Virus product and a firewall.

The website of a NSC must provide guidance, help and assisting information that a user needs to take in case of an infection with Malware, Trojan or other security threats. This can include their own support services; own cleaning or removal tools, reference to other National Support Centres or links to external services that provide helpful information, services or tools. The content of a NSC should also be regularly maintained and updated by the operator.

4.6 Tools

All provided dissemination tools that are displayed, hosted or linked on the website of a NSC need to be free of charge. This is necessary, as a NSC acts as a national service to its citizens and follows the approach to reduce the number of infected computers in the country. A fee for this service would detain a lot of users from using this type of service.

Organisations are entitled to promote commercial tools along with upselling possibilities, but these need to be labelled accordingly and separated from the free of charge tools.

4.6.1 Specifications for EU-Cleaners

An EU cleaner should meet the following specifications:

- An EU-Cleaner needs to be a transparent tool with step-by-step instructions, allowing a simple and uncomplicated installation and usage by inexperienced PC users.
- An EU-Cleaner needs to be free of any charges; its licence should not expire.
- An EU-Cleaner needs to be a self-extracting file, creating its own folder(s), adding an icon to the desktop and it has to launch automatically after the installation. Alternatively, an EU-cleaner can be provided to run on a boot CD or boot USB stick.
- An EU-Cleaner shall not add any perpetual changes to the computer registry as part of its installation.
- An EU-Cleaner needs to be a standalone-tool and it shall not include additional components, tools or apps. It shall not be part of bundle installation either.
- An EU-Cleaner needs to run on all common Microsoft Windows versions.
- An EU-Cleaner needs to include the latest AV signatures or Heuristics, as certain Malware infections could deny access to the Internet.
- An EU-Cleaner needs to include the ACDC logo.
- An EU-Cleaner needs to support the start and stop of scan process and display the progress of the scan process.
- Possible EU-Cleaner detections should be displayed during the scan process.

- An EU-Cleaner should not impact the usage of previously installed Anti-Virus Products.
- An EU-Cleaner should remove all malware it is capable to detect.
- An EU-Cleaner should scan all system files, the computer registry and all other files on the PC.
- An EU-Cleaner should provide detailed statistics about its scan results, including the name and location of all detections made. These details need to be exportable into a text/log file.
- An EU-Cleaner needs to notify the user if a threat couldn't be removed.
- An EU-Cleaner needs to inform the user about additional security measurements.
- An undo-button needs to allow the users to recover the system installation prior to scan or malware removal, files moved into a quarantine folder need to be restorable.
- An EU-Cleaner should not require a full system back up prior to its scan process.

4.7 External Links

A national support centre should provide a strong and comprehensive directory of security websites, covering all areas of Internet security, privacy etc. The links may be marked with affiliate programs to additional funding of the NSC; the same option applies to sponsored ads. Any placed Ads on botfree.eu needs to be related to the aims of the ACDC-project with a clear focus on security related advertisement, brands and products. This section needs to be separated from free-tools and the EU cleaners.

4.8 Data Protection, Privacy & Terms of Use

A National Support Centre must to comply with data privacy standards based on National and EU directives. A data privacy statement and the terms of use must be displayed on the website of each NSC. The website of a National Support Centre also needs to display an imprint as well. Recommended, provided, promoted or linked tools need to be compliant with common data standards. A contact address needs to be provided.

4.9 Security

A National Support Centre needs to apply the highest security standards to its services. This includes the security of the website itself, same as all associated services, tools or plugins.
Unrestricted access to personal data by a third party must be safeguarded at any time. A penetration test or security audit/certification is recommended, but not mandatory.

5 Recommendations for the operation of a NSC

5.1 Support & Service of a National Support Centre

Each national support centre will be able to decide based on its funding how to setup their service level for a national support centre. The options below are a recommendation how to extend the service beyond the availability of the website.

5.1.1 Email Support

Support by email should be handled through a central help desk system. Privacy needs to be in line with national regulations. Responses should be made in a timely manner, staffing adapted to the service volume. Staff of a NSC needs to have the appropriate technical skills and the ability to explain issues at the experience level of the basic end-users.
User should always receive a confirmation for their support request, providing ticket numbers to customers is recommended. The usage of standard templates for common requests is helpful.

5.1.2 Telephone Support

The costs of a phone call should not exceed the costs of a local call, ideally toll-free numbers should be made available.
A service during regular business hours/days mainly addresses small-and medium size enterprise customers, whereby end-users tend to address possible Malware removals after work or at the weekends. Each NSC should properly weigh in his operational telephone support time based on his target group and available budget, as especially support services outside the regular business or weekends correlate with additional costs.

5.1.3 Support-Forum / WIKI / FAQ

The operation of a support forum, a sophisticated wiki-system or other knowledge repository and a list of the Frequently Asked Questions will help keeping the efforts and costs for phone and email support at an adequate level.
A support forum needs to be living forum, so it is recommended to work with volunteers like ICT students or other Internet security enthusiasts that actively contribute to the forum as well.

5.1.4 Support through Social Media

Support through social media should be taken into consideration, too, but the recommendation is to use these social channels for the first contact. Advanced support should be provided by regular channels as phone, forum or email only.

5.2 Tools and Services

It is recommended that all promoted or provided tools should be presented along with a detailed tutorial and screenshots on the website.
The portfolio of tools should include specific threat-related removal tools, tools for general detection and analysis, same as additional tools for maintenance, such as backups.
Based on the current threat landscape, the NSC should set their focus on the Microsoft Windows[2] for desktops and Android[3] for the mobile sector. Support to other operating system should not be kept aside, but can play a minor role.

[2] http://en.wikipedia.org/wiki/Microsoft_Windows

[3] http://en.wikipedia.org/wiki/Android_%28operating_system%29

5.3 Dissemination

5.3.1 Collaboration

A National Support Centre is encouraged to collaborate with national ISPs, CERTs, government, industry, media and other stakeholders to receive high visibility. A proactive outreach is recommended, and regular joint campaigns and initiatives desired. Dissemination towards the stakeholder groups like presentation at conferences should give additional and broad visibility, too.

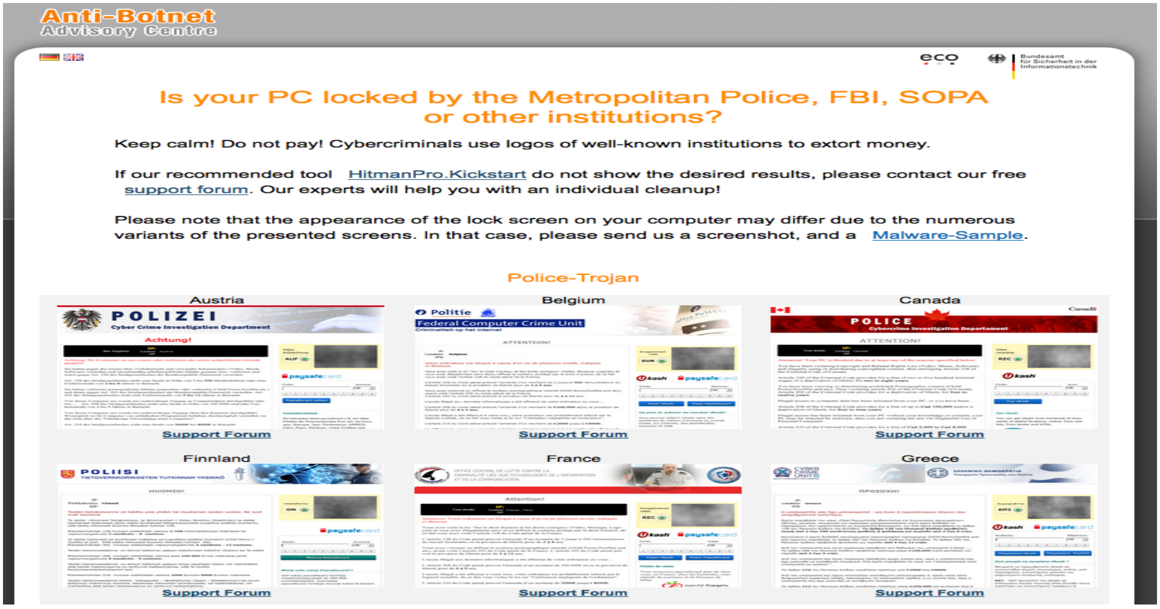
5.3.2 Blogs & Social Media

It is recommended to provide a blog with recent activities of the National Support Centre, updates on IT-Security topics like urgent threat alerts, tool reviews and general information how to stay safe on the internet. This service should be included into the support centre website and content regularly maintained.

It is also helpful to be actively present on common social media platforms like Facebook, Twitter or YouTube. Activities can be either linked to the blog directly or maintained independently with additional content. A combination of blog and social media channels ensure a high visibility towards end-users.

5.3.3 Special Landing Pages

In case of a campaign related to a specific Malware, Ransomware[4] or Trojans with a high visibility in press or media, it might be useful to provide a dedicated landing page, addressing that specific topic. One example is http://www.police-trojan.com from the German National Support Centre, a website dedicated to Ransomware infections (a.k.a. Police-Trojans). This service comes along with common screenshots of the different browser notifications and the appropriate links to the ABBZ Forum.



Is your PC locked by the Metropolitan Police, FBI, SOPA or other institutions?

Keep calm! Do not pay! Cybercriminals use logos of well-known institutions to extort money.

If our recommended tool HitmanPro.Kickstart do not show the desired results, please contact our free support forum. Our experts will help you with an individual cleanup!

Please note that the appearance of the lock screen on your computer may differ due to the numerous variants of the presented screens. In that case, please send us a screenshot, and a Malware-Sample.

Figure 1: Example Special Landing Page

5.4 Accessibility

With the increasing number of mobile and tablet users, the service of a National Support Centre should also provide service to mobile users and not to desktop PCs only. Therefore, the website should be customized for mobile access.

The website of a NSC should also be optimized for the most popular search engines to achieve a high ranking in searches related to IT Security, Botnets and other relevant issues

[4] http://en.wikipedia.org/wiki/Ransomware

6 National Support Centres

The following chapter describes the different national support centres and their services.

6.1 Germany

The German national support centre ABBZ (Anti Botnet Advisory Centre) is an initiative by eco e.V., its member from the Internet Industry and supported by the Federal Office for Information Security (BSI). The service addresses private end-users, same as small-and medium enterprises. The service is completely free of charge.
The goal of this initiative is to reduce the number of botnet infected computer clients in Germany. It aims to inform about botnets, to clean infected computers and to prevent future infections. The participating industry partners provide their own Spamtraps and Honeypots and use the ABBZ and now ACDC with its Centralized Clearing House as a relay to share information about infected users.
The Anti Botnet Advisory Centre (*Anti-Botnet-Beratungs-Zentrum*) provides a website, a help desk and telephone support. Additional customer services are a blog, a forum and social media activities.

6.1.1 Workflows

An infected computer sends out Spam received by a spamtrap or tries to infect a honeypot with Malware. The sensor reports the infection back to the Internet Service Provider (ISP). The ISP identifies the customer based on his IP and notifies him by email about an infection of his Internet account.
This email to the customer contains the following information:

- Customer & Contract number
- Name/Type of the (Virus)-Detection
- Timestamp of detected infection
- Link to botfrei.de
- Telephone-Number of the help-desk at botfrei.de
- A unique ticket (voucher) number
- Additional Security information and advice

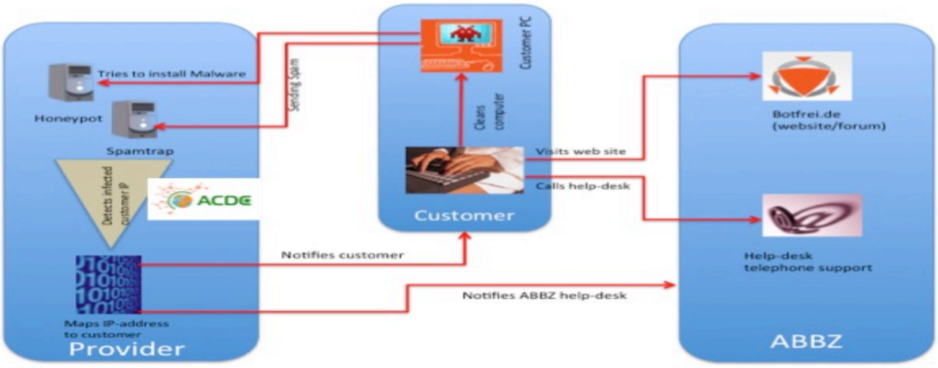


Figure 2: Workflow ABBZ Germany

The customer now has the chance to remove the Malware with the information and the tools available on the botfrei.de website or through the help of botfrei.de – Forum.
Additionally, the customer has the possibility to contact the ABBZ help desk team by telephone, referring to his voucher number.

Therefore, the ISP automatically submits a second email to the ABBZ. This email does not contain any personal information of the customer; only the ticket (voucher) number and the type of infection are included in this second email.
Besides the workflow under involvement of the ISPs, the service of the ABBZ also supports regular contact and support requests by email. This email-address is available on the website.

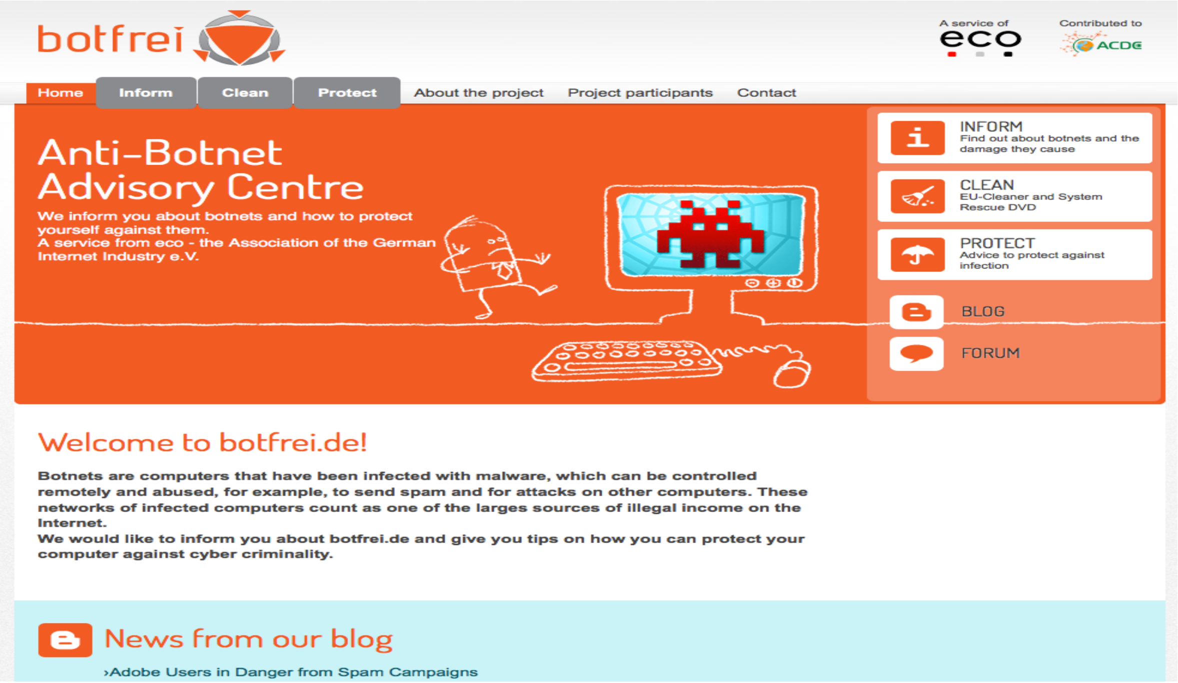
6.1.2 Staff

The ABBZ help desk team is a professional team of IT-experts. All staff member have an experience in providing 1st and 2nd level support along with dedicated knowledge in IT-Security.
Besides the full-time employees, several volunteers provide additional support through the forum. The regular employees and the volunteers regularly exchange their knowledge through regular meetings, conference calls or instant messaging services.
An internal and external knowledge database is maintained, same as several guidelines and process documents. All are living documents and available on a central repository. The official language for communication and documentation is German.

6.1.3 Service Level

The ABBZ has moved their services to a 2nd level support only. This includes support by phone, email and through a web forum. Operating hours of the ABBZ are regular business days, phone support is provided during a period of 09:00-18:00. Volunteers are even available on the forum outside the regular business hours, partly even at the weekend or at night.

6.1.3.1 Website



Anti-Botnet Advisory Centre

We inform you about botnets and how to protect yourself against them.
A service from eco - the Association of the German Internet Industry e.V.

INFORM Find out about botnets and the damage they cause

CLEAN EU-Cleaner and System Rescue DVD

PROTECT Advice to protect against infection

Welcome to botfrei.de!

Botnets are computers that have been infected with malware, which can be controlled remotely and abused, for example, to send spam and for attacks on other computers. These networks of infected computers count as one of the larges sources of illegal income on the Internet.
We would like to inform you about botfrei.de and give you tips on how you can protect your computer against cyber criminality.

News from our blog

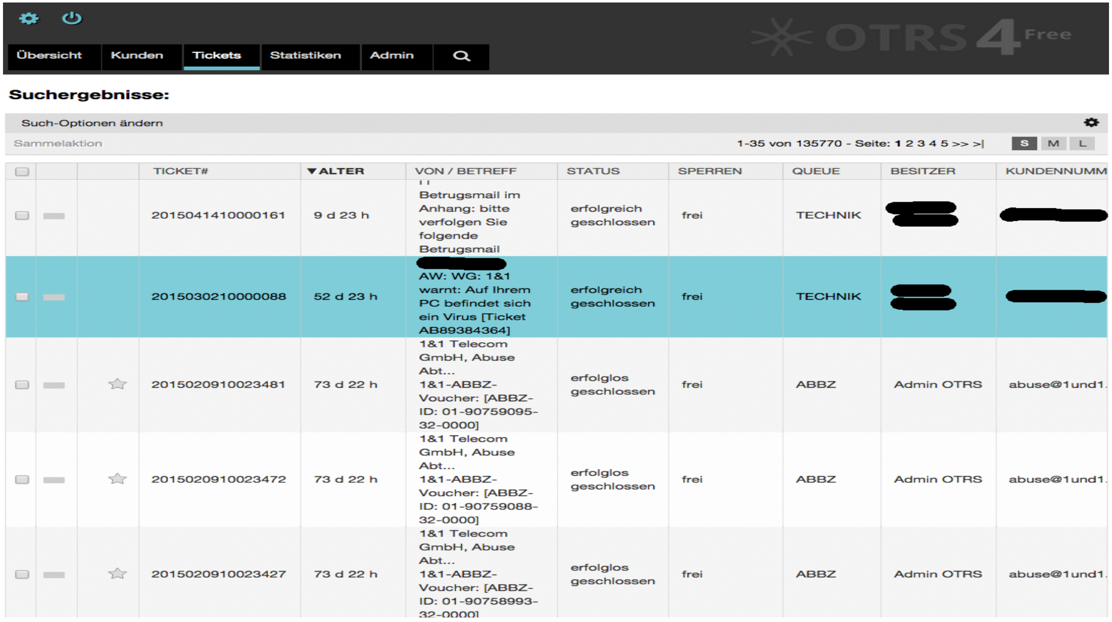
›Adobe Users in Danger from Spam Campaigns

Figure 3: Screenshot botfrei.de

The barrier-free botfrei.de website is available in German and English language. An existing partnership with a Japanese anti-botnet initiative has been renewed during the project. A link to the ACTIVE Project, operated by Japan's Ministry of Internal Affairs and Communications, refers Japanese users to their national anti-botnet support initiative. (http://www.active.go.jp)
A re-launch of the website with a new design and additional features was published in April 2014. The website is based on three columns Inform, Clean, Protect. The forum and blog are featured on subpages, an extended software catalogue and FAQ list are available, too.

6.1.3.2 *Email-Support*

All ABBZ email-support is processed through a ticketing system. As described in the process above, tickets are considered as automatic notifications made by the Internet Service Providers and manual email-requests submitted through the available contact address on the website. Tickets opened by the ISPs without any customer follow-up are automatically closed after ten weeks. The ticket-queues are split into various subtopics like technical issues, specific infections, or languages. These are applied by sophisticated filter-rules.



Suchergebnisse:

Such-Optionen ändern

Sammelaktion

1-35 von 135770 - Seite: 1 2 3 4 5 >> >|

□			TICKET#	▼ALTER	VON / BETREFF	STATUS	SPERREN	QUEUE	BESITZER	KUNDENNUMM
□	▬		2015041410000161	9 d 23 h	' ' Betrugsmail im Anhang: bitte verfolgen Sie folgende Betrugsmail	erfolgreich geschlossen	frei	TECHNIK	[redacted]	[redacted]
□	▬		2015030210000088	52 d 23 h	[redacted] AW: WG: 1&1 warnt: Auf Ihrem PC befindet sich ein Virus [Ticket AB89384364]	erfolgreich geschlossen	frei	TECHNIK	[redacted]	[redacted]
□	▬	☆	2015020910023481	73 d 22 h	1&1 Telecom GmbH, Abuse Abt... 1&1-ABBZ-Voucher: [ABBZ-ID: 01-90759095-32-0000]	erfolglos geschlossen	frei	ABBZ	Admin OTRS	abuse@1und1.
□	▬	☆	2015020910023472	73 d 22 h	1&1 Telecom GmbH, Abuse Abt... 1&1-ABBZ-Voucher: [ABBZ-ID: 01-90759088-32-0000]	erfolglos geschlossen	frei	ABBZ	Admin OTRS	abuse@1und1.
□	▬	☆	2015020910023427	73 d 22 h	1&1 Telecom GmbH, Abuse Abt... 1&1-ABBZ-Voucher: [ABBZ-ID: 01-90758993-32-0000]	erfolglos geschlossen	frei	ABBZ	Admin OTRS	abuse@1und1.

Figure 4: German Ticketing System

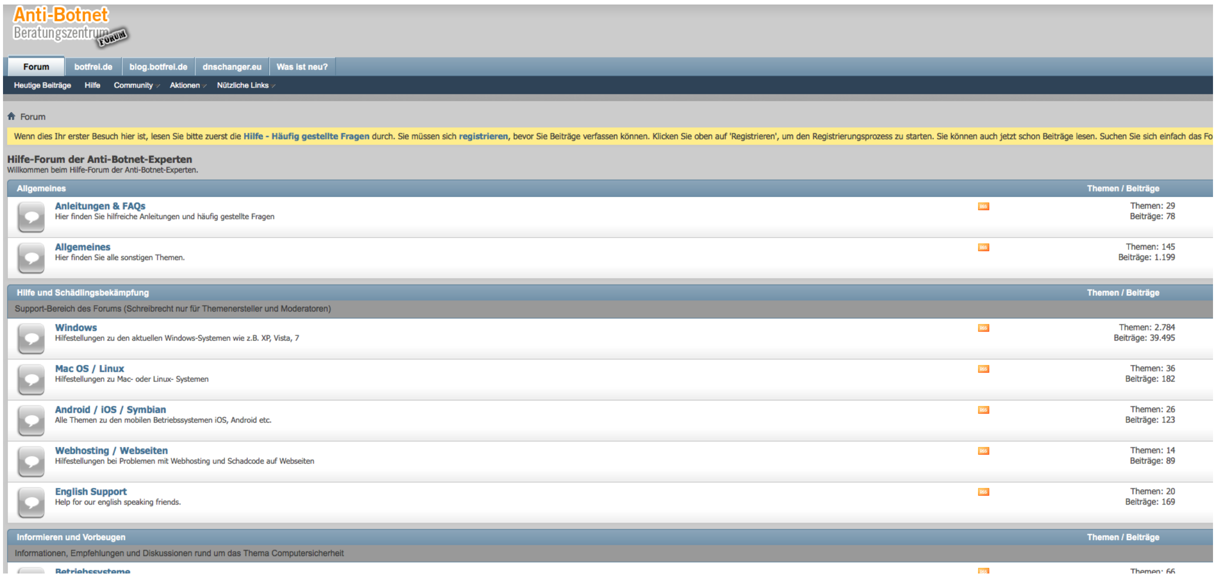
6.1.3.3 *Telephone Support*

The ABBZ help desk is an inbound help desk only. The telephone number is not available publically, only customer that received an official email notification from their ISP can contact the help desk by phone. Telephone support by the ABBZ help desk team is provided on business days from Mondays through Fridays from 09:00 to 18:00. Service calls are billed as a local call without any additional charges.

6.1.3.4 *Forum*

The support team of the ABBZ manages the Botfrei-Forum. Several volunteers support the regular ABBZ team in the moderation and maintenance of the forum. The forum has mainly German threads, but a special section covers topics in English. The support team and the volunteers continuously foster the growth of the FAQ-section and the knowledge database.

With almost 12.000 threads, over 120.000 posts and nearly 23.000 registered users since its launch in 2010, the botfrei.de - forum is recognized as one of the primary resources on the German Internet in regards of malware support.



Wenn dies Ihr erster Besuch hier ist, lesen Sie bitte zuerst die **Hilfe - Häufig gestellte Fragen** durch. Sie müssen sich **registrieren**, bevor Sie Beiträge verfassen können. Klicken Sie oben auf 'Registrieren', um den Registrierungsprozess zu starten. Sie können auch jetzt schon Beiträge lesen. Suchen Sie sich einfach das Fo

Hilfe-Forum der Anti-Botnet-Experten
Willkommen beim Hilfe-Forum der Anti-Botnet-Experten.

Allgemeines	Themen / Beiträge
Anleitungen & FAQs Hier finden Sie hilfreiche Anleitungen und häufig gestellte Fragen	Themen: 29 Beiträge: 78
Allgemeines Hier finden Sie alle sonstigen Themen.	Themen: 145 Beiträge: 1.199

Hilfe und Schädlingsbekämpfung Support-Bereich des Forums (Schreibrecht nur für Themenersteller und Moderatoren)	Themen / Beiträge
Windows Hilfestellungen zu den aktuellen Windows-Systemen wie z.B. XP, Vista, 7	Themen: 2.784 Beiträge: 39.495
Mac OS / Linux Hilfestellungen zu Mac- oder Linux- Systemen	Themen: 36 Beiträge: 182
Android / iOS / Symbian Alle Themen zu den mobilen Betriebssystemen iOS, Android etc.	Themen: 26 Beiträge: 123
Webhosting / Webseiten Hilfestellungen bei Problemen mit Webhosting und Schadcode auf Webseiten	Themen: 14 Beiträge: 89
English Support Help for our english speaking friends.	Themen: 20 Beiträge: 169

Informieren und Vorbeugen Informationen, Empfehlungen und Diskussionen rund um das Thema Computersicherheit	Themen / Beiträge
Betriebssysteme	Themen: 66

Figure 5: Botfrei Forum

6.1.3.5 Blog & Social Media

The ABBZ is running its own blog at blog.botfrei.de. Usually, one blog article per day is published. The topics range from software reviews, threat and scam alerts and new available software updates up to general IT-Security news. Blog post are mostly German, relevant articles are translated into English.
Botfrei.de social media presence is focussed on Facebook and has almost 10.000 Followers. Additionally, the service is also available on Twitter and Google Plus.
The ABBZ team makes a post on daily basis. All social media activity is made in German only.

- Blog: http://blog.botfrei.de
- Facebook: https://www.facebook.com/botfrei
- Twitter: https://twitter.com/botfrei
- Google Plus: https://plus.google.com/108464595091505390471

6.1.4 Infrastructure

The infrastructure of the ABBZ includes multiple layers; most of the used services and tools are freeware.

6.1.4.1 Ticketing System

The ticketing system of the ABBZ is an OTRS[5] application.

6.1.4.2 Phone System

The telephone system is VoIP-based. Support agents can process multiple calls simultaneously. The phone number is local phone number without any additional costs for the calling users.

6.1.4.3 Forum-System

The ABBZ-forum is based on a VBulletin[6] installation with a customized template.

6.1.4.4 Test Lab

The ABBZ operates an internal test-lab to enhance their 2nd-level support service capabilities. This test-lab system is operating in its own network with an independent Internet connection. The lab consists out of six differently configured Windows-PC systems. These systems are e.g. intended to replicate certain infections at the customer side and to verify the effectiveness of recommended tools like the EU-Cleaners.

[5] http://www.otrs.com

[6] http://www.vbulletin.com

6.1.5 Customer Tools

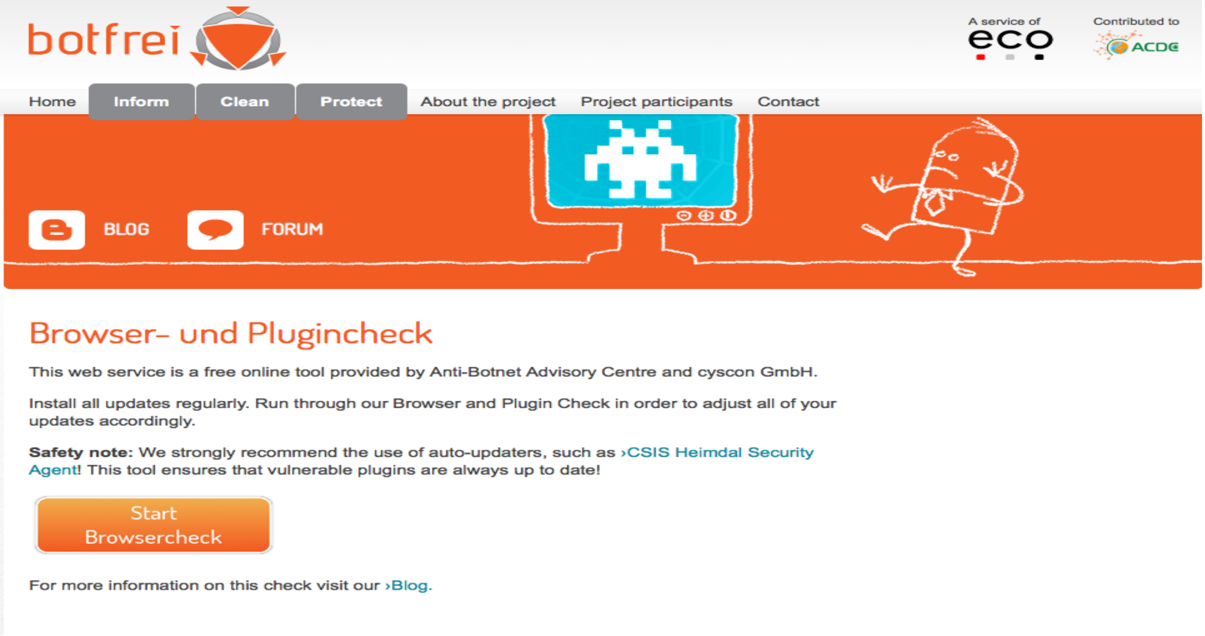
The ABBZ recommends a set of tools and services on their website. These tools are related to IT-Security, but also include common tools for IT-Maintenance like back up or analysis tools.

6.1.5.1 EU-Cleaners

Three EU-Cleaners have been made available to the German ABBZ and to the other National Support Centers. These cleaners are no full Anti-Virus Products; these cleaners are just dedicated to remove Malware from customer PCs. All tools are free of charge.
The EU-Cleaners have been made available with friendly support from the partners **Avira**[7]**, SurfRight**[8] and **GData.** Advanced tutorials for all tools are available on the website.

6.1.5.2 Online-Scanner

Together with the ABBZ partner cyscon GmbH[9], the ABBZ is providing a browser-and plugin-in check. This service allows users to verify if the current version of their browser and the installed browser-plugins are up-to-date.



Browser- und Pluginсheck

This web service is a free online tool provided by Anti-Botnet Advisory Centre and cyscon GmbH.

Install all updates regularly. Run through our Browser and Plugin Check in order to adjust all of your updates accordingly.

Safety note: We strongly recommend the use of auto-updaters, such as ›CSIS Heimdal Security Agent! This tool ensures that vulnerable plugins are always up to date!

For more information on this check visit our ›Blog.

Figure 6: Browser and Plugin-Check

6.1.5.3 Link directory

The link / tool list of botfrei.de is split into a consumer (https://www.botfrei.de/en/privat.html) and business section (https://www.botfrei.de/en/unternehmen.html). The business section lists only commercial anti-virus products; the extended consumer directory distinguishes between seven sub-categories. These are:

- Security Solutions from ISPs
- Freeware Virus Scanners
- Payware Virus Scanner
- Security products for Mac Users
- Browser Plugins
- Further useful tools
- Protection for Mobile Devices

[7] http://www.avira.com
[8] http://www.surfright.nl
[9] http://www.cyscon.de

6.1.6 Statistics / Metrics

Since its launch in November 2010, the German ABBZ has processed over 250.000 Customer tickets and almost 10.000 support calls. The Forum has nearly 12.000 threads with 125.000 posts. These have been made by almost 30.000 registered users. The Botfrei.de website including the Forum, the blog and the special landing pages bka-trojaner.de and dnschanger.eu, gets over 3.900.000 pages visits each year. The different EU-cleaners have been downloaded over 2.500.000 times since the launch of the service.

6.1.7 Privacy, Data Protection and Security

The ABBZ strictly upholds the rules of the national data protection laws. The terms of use and the data privacy statements are displayed on the website at www.botfrei.de/en/datenschutz.html (data privacy) and at www.botfrei.de/en/nutzungsbedingungen.html (terms of use).

All internal processes have been evaluated and analysed to ensure the high data privacy and security standards. The compliance to these standards is regularly tested.

The ABBZ does not store, trace or receive any personal data from an infected user or from his computer and only attacks from infected PCs are evaluated. An evaluation of the Internet traffic through deep packet inspection or similar methods is strictly permitted, user behaviour is not recorded or evaluated.

Access to the entire ABBZ infrastructure is limited to a restricted group of users, based on the internal security policies and standards.

6.1.8 Contributions / interaction with ACDC

ISP that have been working with eco e.V. on the national German Support Centre in the past are now receiving additional abuse information directly from the ACDC Centralised Clearing House. ECO has been also active in press and social media promoting the ACDC project.

6.1.9 Dissemination

The German NSC Botfrei.de has a big visibility in Germany. Besides the collaboration with the ISPs, there has been an ongoing reference and coverage on major websites like the SPIEGEL Online, STERN.de or FOCUS Online. The website is also linked by the BSI (a national CERT), several Law Enforcement agencies and several security websites.

6.1.10 Sustainability

The German NSC Botfrei.de is operated by ECO since 2010. There is no intent to stop providing this service. ECO is even in negotiations to extend the service level during the next year. ECO is also willed to continue with Botfrei.de within the European Anti-Botnet Support Centre Alliance (EABSCA)

6.2 Croatia

Croatian Academic and Research Network – CARNet is a government agency founded in 1995 and operating as an independent part of the Croatian Ministry of Science, Education and Sports. Following a mission to develop advanced ICT infrastructure for the educational and scientific community including a fast and secure network infrastructure, diverse content and services, CARNet's activities are divided into four primary areas: providing ICT infrastructure and connectivity to the Croatian academic, scientific and other educational institutions, fostering the development of information society, supporting the development of a modern education system and running national services – National CERT and .hr Domain Registry.

Croatian National CERT was established in accordance with the Information security law and its main task is processing of incidents on the Internet, i.e., preservation of the information security in Croatia. Its constituency are all Internet users in Croatia. National CERT is hosted by CARNet and organized as a department. All services provided by the National CERT are free of charge as this is a government-funded organisation. National CERT cooperates with different commercial entities: hosting providers, ISPs, banks, etc. Activities of National CERT include receiving and disseminating information on incidents from and to its constituency, being Croatian national point of contact for incident reporting.

The fact is that National CERT disseminated information about bots to ISPs also before ACDC project start. These information was collected mostly by passive Internet monitoring (receiving bot information from various feeds like shadowserver, clean-mx.de etc.). In this way National CERT intents to integrate ACDC results received from ACDC CCH into daily CERT operation.

6.2.1 Workflows

The following picture shows daily National CERT operations where incident indicators or observables are received from various sources and additionally from ACDC project (1). If the information is related to dynamically received IP addresses assigned to bots it is disseminated to corresponding ISP automatically (2) and if the information is related to static IP address like information about malicious web server, this information is analysed by CERT engineers (3) and entered into CERT ticketing system (RTIR) (4). In this way the information received from ACDC project is processed by software just in the same way as the other information received by CERT thus integrating results received from ACDC project in daily operations of National CERT.

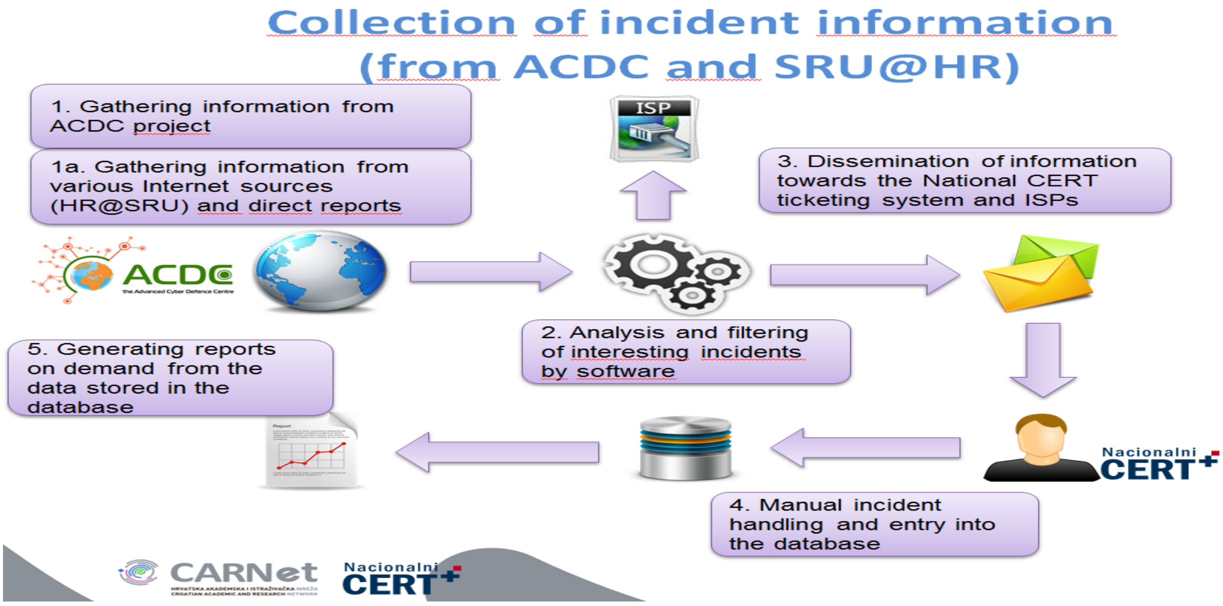

Collection of incident information
(from ACDC and SRU@HR)
1. Gathering information from ACDC project
1a. Gathering information from various Internet sources (HR@SRU) and direct reports
ISP
3. Dissemination of information towards the National CERT ticketing system and ISPs
ACDC
the Advanced Cyber Defence Centre
2. Analysis and filtering of interesting incidents by software
5. Generating reports on demand from the data stored in the database
Report
Nacionalni CERT
4. Manual incident handling and entry into the database
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK
Nacionalni CERT

Figure 7: Processes Croatian NSC

From technical point of view, data received from CCH is related mostly to bots and their activities and to malicious or phishing URLs. The information is read using XMPP protocol and stored to incident database. The content of incident database is processed by software in the way that the bot information is sent to ISP and information about web servers is sent to National CERT by e-mail to be manually processed by National CERT what is also in accordance with the above picture.

Some larger Croatian ISPs usually forward received bot information to the infected end users together with the guidance and link to NSC portal as it is shown in the picture below. The user can access antibot.hr portal to fetch some tools or contact ACDC NSC in case of further clarification or support by mail.

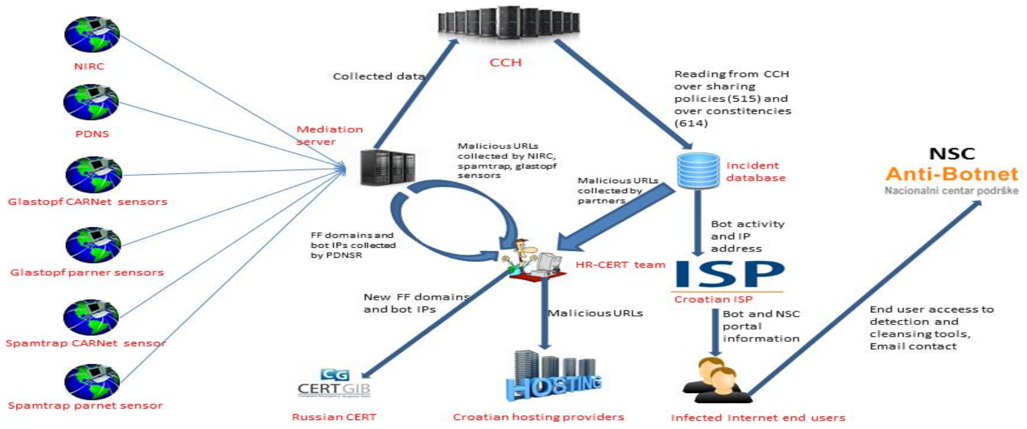

NIRC
PDNS
Glastopf CARNet sensors
Glastopf parner sensors
Spamtrap CARNet sensor
Spamtrap parnet sensor
Mediation server
Collected data
CCH
Reading from CCH over sharing policies (515) and over constitencies (614)
Malicious URLs collected by NIRC, spamtrap, glastopf sensors
FF domains and bot IPs collected by PDNSR
Malicious URLs collected by partners
Incident database
HR-CERT team
Bot activity and IP address
ISP
Croatian ISP
New FF domains and bot IPs
Malicious URLs
Bot and NSC portal information
CERT GIB
Russian CERT
HOSTING
Croatian hosting providers
Infected Internet end users
NSC
Anti-Botnet
Nacionalni centar podrške
End user access to detection and cleansing tools, Email contact

Figure 8: Workflow Croatian NSC

6.2.2 Staff

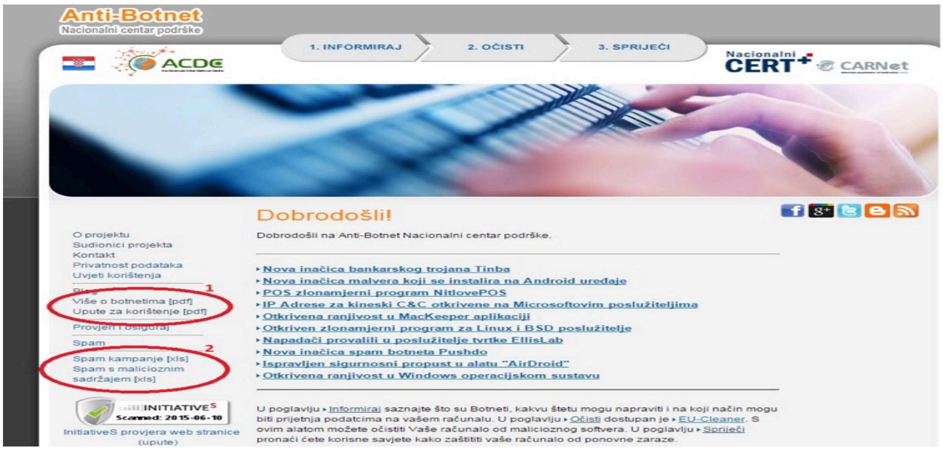
National CERT performs all activities regarding Croatian National Support Centre (NSC), since reports received from ACDC project perfectly fit to already established procedures of National CERT as well as to its responsibilities given by Information Security Act. National CERT has 9 employees, which could be allocated as needed to activities of National Support Centre.

6.2.3 Service Level

National support centre is giving support to Internet users mostly by email. The operating hours of the NSC are regular business days with mail support provided during a period of 08:00-17:00.

6.2.3.1 Website

The following picture shows index page of NSC portal which gives general information about botnets and also points to two published white papers, one explaining what botnets are and second as a simple portal guide for ordinary internet users (1). The website is implemented in Croatian language containing very similar content and services as German www.botfrei.de portal. Compared with German portal, there are two additionally published XLS files containing information about malicious spam carrying malicious URL or attachment (2) as well as information about current spam campaigns. The lists are updated automatically every day with the new information received from spamtrap sensors.



Anti-Botnet
Nacionalni centar podrške

1. INFORMIRAJ
2. OČISTI
3. SPRIJEČI

Nacionalni CERT
CARNet

O projektu
Sudionici projekta
Kontakt
Privatnost podataka
Uvjeti korištenja
Blog
Više o botnetima [pdf]
Upute za korištenje [pdf]
Provjeri i osiguraj
Spam
Spam kampanje [xls]
Spam s malicioznim sadržajem [xls]

INITIATIVES
Scanned: 2015-06-10
InitiativeS provjera web stranice (upute)

Dobrodošli!

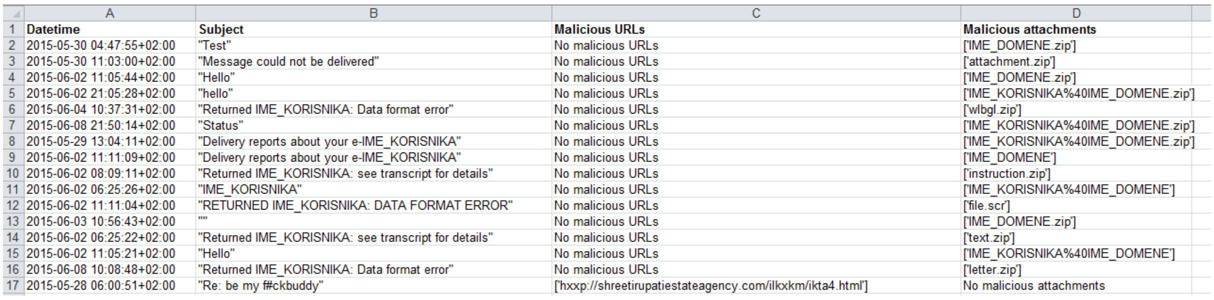
Dobrodošli na Anti-Botnet Nacionalni centar podrške.

- Nova inačica bankarskog trojana Tinba
- Nova inačica malvera koji se instalira na Android uređaje
- POS zlonamjerni program NitlovePOS
- IP Adrese za kineski C&C otkrivene na Microsoftovim poslužiteljima
- Otkrivena ranjivost u MacKeeper aplikaciji
- Otkriven zlonamjerni program za Linux i BSD poslužitelje
- Napadači provalili u poslužitelje tvrtke EllisLab
- Nova inačica spam botneta Pushdo
- Ispravljen sigurnosni propust u alatu "AirDroid"
- Otkrivena ranjivost u Windows operacijskom sustavu

U poglavlju Informiraj saznajte što su Botneti, kakvu štetu mogu napraviti i na koji način mogu biti prijetnja podatcima na vašem računalu. U poglavlju Očisti dostupan je EU-Cleaner. S ovim alatom možete očistiti Vaše računalo od malicioznog softvera. U poglavlju Spriječi pronaći ćete korisne savjete kako zaštititi vaše računalo od ponovne zaraze.

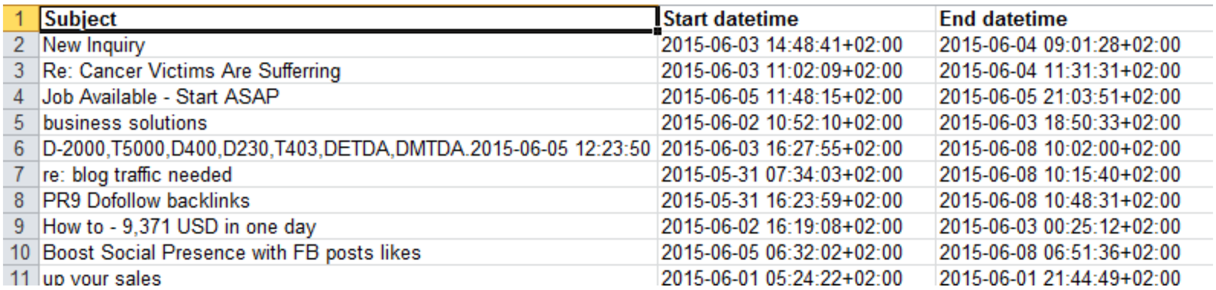
Figure 9: Screenshot antibot.hr

Published lists of malicious spam contain timestamp, subject, malicious attachment filename and/or malicious URL contained in mail body. In this way, the users of Internet could find malicious spam sent to Croatian Internet space and protect themselves from not targeted phishing campaigns where malware is used.
Published lists of malicious spam and spam campaigns are shown on the following picture



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

Figure 10: Report Malicious Spam Campaigns Croatia



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

Figure 11: Screenshot Spam Campaigns Croatian NSC

6.2.3.2 *Blog & Social Media*

Croatian NSC is running its own blog at http://www.antibot.hr/blog/ informing users mostly about threats and alerts, tools and other IT-Security news. Blog posts are in Croatian language and the list of blogs posts is displayed also on antibot.hr index page. The content is updated by National CERT staff. Social media URLs are published at antibot.hr portal point to common project URLs:

- https://twitter.com/AntiBotHR
- https://www.facebook.com/botfree.eu
- https://plus.google.com/u/0/118250901031237479359/posts

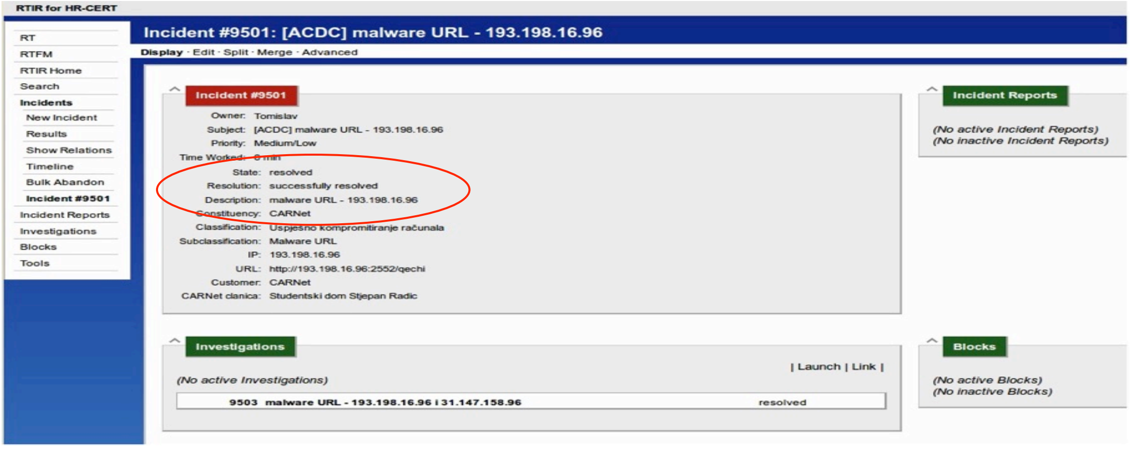
6.2.4 Infrastructure

The National Support Centre operates on fully redundant information systems. The systems are replicated in real time so it is possible to switch manually to redundant site in a couple of minutes just by changing addresses in DNS records. National CERT is also administering the antibot.hr domain and this change is under its control. Replicated are web portals and also previously established RTIR ticketing systems. All systems are based on Linux operating system and other open source solutions.

6.2.4.1 Ticketing System

National Support Centre is using the same ticketing system as National CERT – open source RTIR as National CERT does not make a difference between incident information received from ACDC CCH and other sources, so in this way, the incident handling procedure is the same.

The entry in RTIR ticketing software showing the information received from ACDC CCH about compromised server in Croatian address space is presented in the picture below.



Incident #9501: [ACDC] malware URL - 193.198.16.96

Incident #9501

Owner: Tomislav
Subject: [ACDC] malware URL - 193.198.16.96
Priority: Medium/Low
Time Worked: 0 min
State: resolved
Resolution: successfully resolved
Description: malware URL - 193.198.16.96
Constituency: CARNet
Classification: Uspješno kompromitiranje računala
Subclassification: Malware URL
IP: 193.198.16.96
URL: http://193.198.16.96:2552/qechi
Customer: CARNet
CARNet clanica: Studentski dom Stjepan Radic

Incident Reports

(No active Incident Reports)
(No inactive Incident Reports)

Investigations

(No active Investigations)

9503 malware URL - 193.198.16.96 i 31.147.158.96 resolved

Blocks

(No active Blocks)
(No inactive Blocks)

Figure 12: Ticketing System Antibot.hr

6.2.4.2 Test Lab

National CERT also operates an internal test-lab that can be used for testing the effectiveness of particular tools published on the antibot.hr portal.

6.2.5 Customer Tools

Antibot.hr portal recommends a set of tools and services on its pages. These tools are related to IT-Security, but also include common tools for IT-Maintenance like back up or analysis tools. Recommended are also two online scanners one for detection of open ports and another for detection of vulnerable, not updated browser plugins used by end user.

6.2.5.1 End user tools

Two EU-Cleaners have been made available to the antibot.hr portal. These cleaners are no full Anti-Virus Products; these cleaners are just dedicated to remove Malware from customer PCs. Both tools are free of charge. The EU-Cleaners have been made available with friendly support from the partners **Avira**[10],**SurfRight**[11] **and G Data**[12].

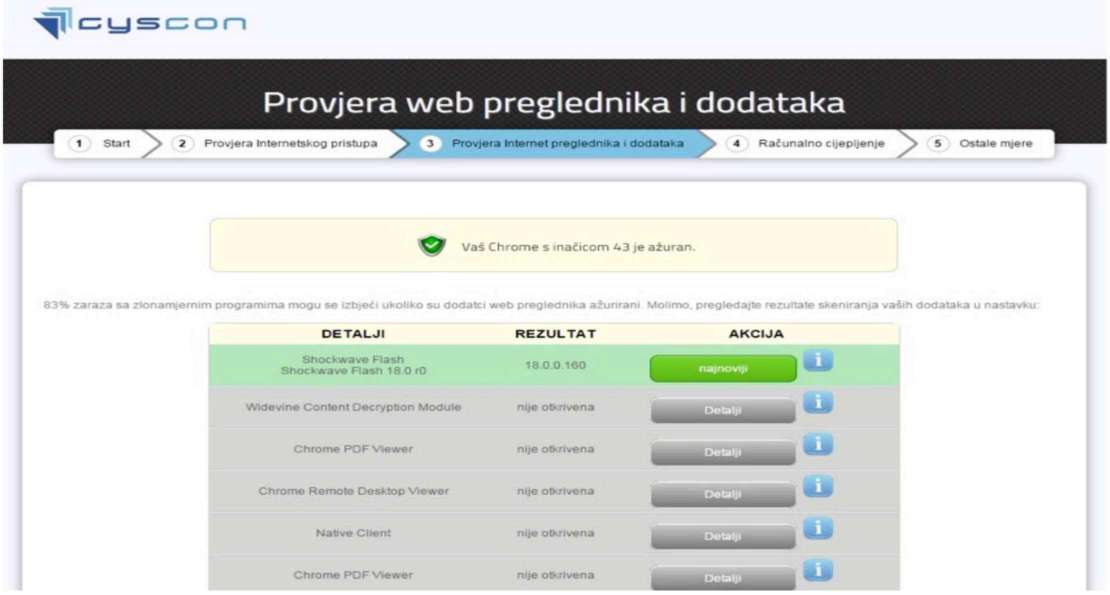
[10] http://www.avira.com

[11]http://www.surfright.nl

[12] http://www.gdata.de

6.2.5.2 *Online-Scanner*

Together with the associated project partner cyscon GmbH[13], the antibot.hr is providing a browser- and plugin-in check at https://www.check-and-secure.com/browsercheck/_hr/ . This service allows users to verify if the current version of their browser and the installed browser-plugins is up-to-date. The scanner server was also customized due to translation of all pages into Croatian languages it is shown in the picture below.



Provjera web preglednika i dodataka

1 Start 2 Provjera Internetskog pristupa 3 Provjera Internet preglednika i dodataka 4 Računalno cijepljenje 5 Ostale mjere

Vaš Chrome s inačicom 43 je ažuran.

83% zaraza sa zlonamjernim programima mogu se izbjeći ukoliko su dodatci web preglednika ažurirani. Molimo, pregledajte rezultate skeniranja vaših dodataka u nastavku:

DETALJI	REZULTAT	AKCIJA
Shockwave Flash Shockwave Flash 18.0 r0	18.0.0.160	najnoviji
Widevine Content Decryption Module	nije otkrivena	Detalji
Chrome PDF Viewer	nije otkrivena	Detalji
Chrome Remote Desktop Viewer	nije otkrivena	Detalji
Native Client	nije otkrivena	Detalji
Chrome PDF Viewer	nije otkrivena	Detalji

Figure 13: Online Plugin-Check

6.2.5.3 *Link directory*

The link / tool list of botfrei.de is split into a consumer (http://antibot.hr/popisalata) and business section (http://antibot.hr/pravneosobe). Also, the extended consumer directory distinguishes between seven sub-categories. These are:

- Security Solutions from ISPs
- Freeware Virus Scanners
- Payware Virus Scanner
- Security products for Mac Users
- Browser Plugins
- Further useful tools
- Protection for Mobile Devices

[13] http://www.cyscon.de

6.2.6 Statistics / Metrics

Antibot.hr portal started its work in April 2014 with a solid number of visits shown in the picture below.

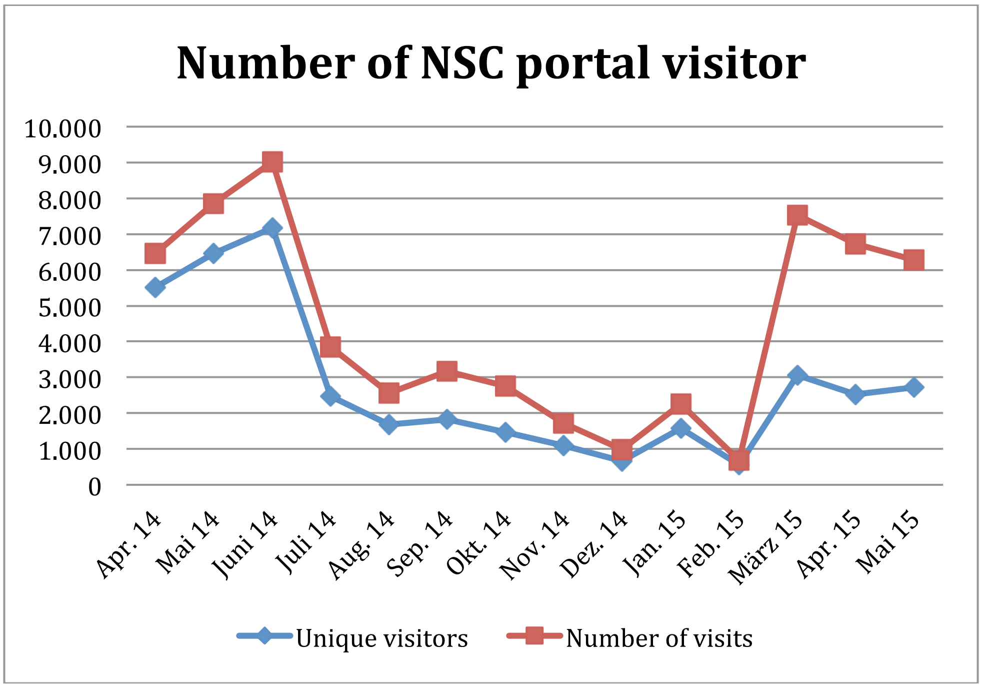


Figure 14: Visitor Statistics Croatia

6.2.7 Privacy, Data Protection and Security

The Croatian National Support Centre does not store, trace or receive any personal data from an infected user on the systems publicly accessible from Internet. Any information, correspondence or information of victims and their information systems is kept on internal systems reachable only from internal CERT networks and is classified as information of internal use only.

In order to harden security of NSC portal, antibot.hr web site was also scanned with commercial and open source vulnerability scanners and protected by NGN Firewall using several security features.

6.2.8 Dissemination

The Croatian NSC portal antibot.hr was advertised and it has good visibility in Croatia. National CERT portal www.cert.hr and also other portals are pointing to antibot.hr portal informing their users to use antibot.hr portal services for prevention and detection/malware cleansing reasons.

Also, the information about antibot.hr portal was disseminated on many conferences in presentations delivered by National CERT, newspaper articles and TV broadcasts of Croatian National TV (HTV).

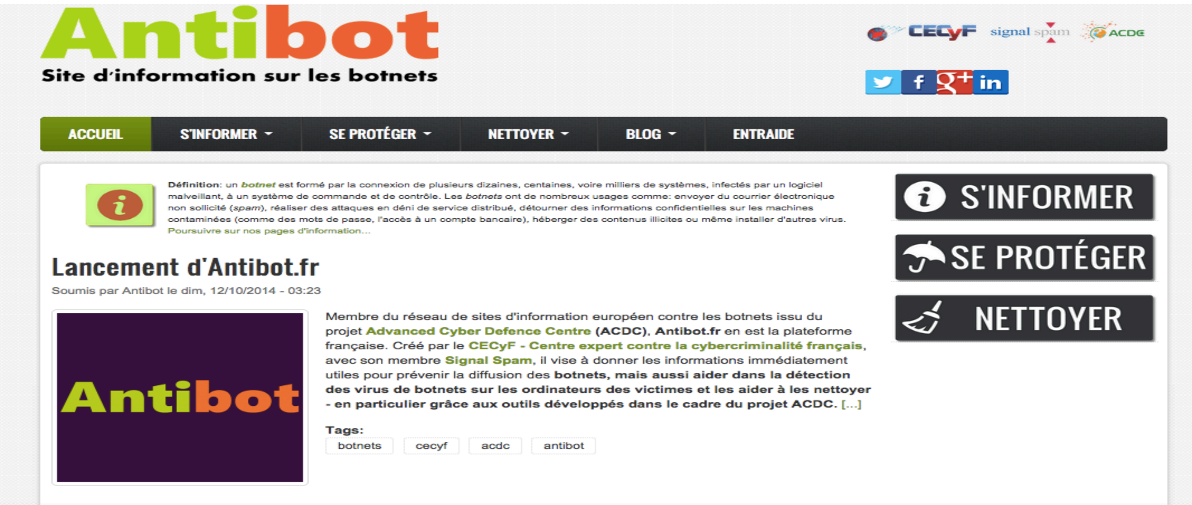
6.2.9 Sustainability

There is no intent to stop providing NSC with antibot.hr service but possibly extend the cooperation with other partners NSCs.

6.3 France

The French national support centre - antibot.fr - is an initiative by the CECyF[14] (French Expert Centre against Cybercrime) and Signal Spam (partner in ACDC), with the support of their respective members.

The Internet website antibot.fr offers information and tools to end users to learn about botnet, find out if their devices are infected, and clean the terminals. Infection analysis tools and cleaning tools available are listed on the website, included solutions developed within ACDC. Antibot.fr is mainly an information page for end users, providing links towards tools developed by ACDC and French ISPs who need to be identified as the main source of support for their customers.



Définition: un *botnet* est formé par la connexion de plusieurs dizaines, centaines, voire milliers de systèmes, infectés par un logiciel malveillant, à un système de commande et de contrôle. Les *botnets* ont de nombreux usages comme: envoyer du courrier électronique non sollicité (*spam*), réaliser des attaques en déni de service distribué, détourner des informations confidentielles sur les machines contaminées (comme des mots de passe, l'accès à un compte bancaire), héberger des contenus illicites ou même installer d'autres virus. Poursuivre sur nos pages d'information…

Lancement d'Antibot.fr

Soumis par Antibot le dim, 12/10/2014 - 03:23

Membre du réseau de sites d'information européen contre les botnets issu du projet **Advanced Cyber Defence Centre (ACDC)**, **Antibot.fr** en est la plateforme française. Créé par le **CECyF - Centre expert contre la cybercriminalité français**, avec son membre **Signal Spam**, il vise à donner les informations immédiatement utiles pour prévenir la diffusion des **botnets, mais aussi aider dans la détection des virus de botnets sur les ordinateurs des victimes et les aider à les nettoyer - en particulier grâce aux outils développés dans le cadre du projet ACDC.** [...]

Tags:
botnets cecyf acdc antibot

Figure 15: Screenshot Antibot.fr

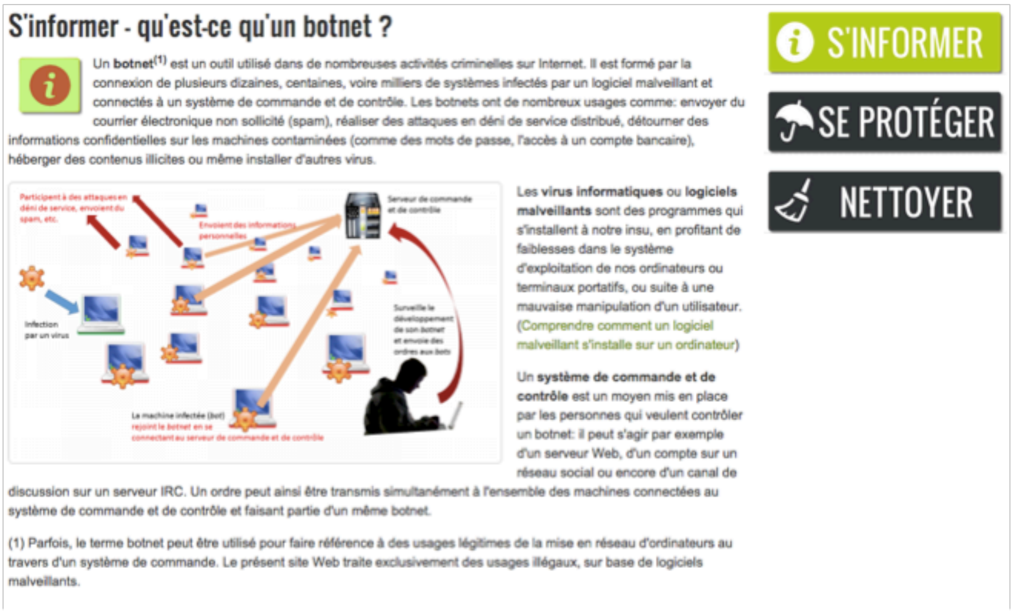
6.3.1 Website

Antibot.fr was launch in October 2014. The website is based on three primary actions: inform, prevent and clean, with the possibility to consult external blogs and repositories linked on the website. No support is offered; therefore no regular staff is required. The website is operated by Signal Spam and the CECyF.

6.3.2 Information and Protection

Antibot.fr is before everything else an information portal where end users can access comprehensive explanations about botnets and the threats they pose, and general advises on how to protect oneself against infections.

[14] *https://www.cecyf.fr/*



S'INFORMER
SE PROTÉGER
NETTOYER
Participent à des attaques en déni de service, envoient du spam, etc.
Envoient des informations personnelles
Serveur de commande et de contrôle
Infection par un virus
Surveille le développement de son botnet et envoie des ordres aux bots
La machine infectée (bot) rejoint le botnet en se connectant au serveur de commande et de contrôle

S'informer - qu'est-ce qu'un botnet ?

Un **botnet**(1) est un outil utilisé dans de nombreuses activités criminelles sur Internet. Il est formé par la connexion de plusieurs dizaines, centaines, voire milliers de systèmes infectés par un logiciel malveillant et connectés à un système de commande et de contrôle. Les botnets ont de nombreux usages comme: envoyer du courrier électronique non sollicité (spam), réaliser des attaques en déni de service distribué, détourner des informations confidentielles sur les machines contaminées (comme des mots de passe, l'accès à un compte bancaire), héberger des contenus illicites ou même installer d'autres virus.

Les **virus informatiques** ou **logiciels malveillants** sont des programmes qui s'installent à notre insu, en profitant de faiblesses dans le système d'exploitation de nos ordinateurs ou terminaux portatifs, ou suite à une mauvaise manipulation d'un utilisateur. (Comprendre comment un logiciel malveillant s'installe sur un ordinateur)

Un **système de commande et de contrôle** est un moyen mis en place par les personnes qui veulent contrôler un botnet: il peut s'agir par exemple d'un serveur Web, d'un compte sur un réseau social ou encore d'un canal de discussion sur un serveur IRC. Un ordre peut ainsi être transmis simultanément à l'ensemble des machines connectées au système de commande et de contrôle et faisant partie d'un même botnet.

(1) Parfois, le terme botnet peut être utilisé pour faire référence à des usages légitimes de la mise en réseau d'ordinateurs au travers d'un système de commande. Le présent site Web traite exclusivement des usages illégaux, sur base de logiciels malveillants.

Figure 16: Botnet Explanation France

6.3.3 Social Media

End users can follow antibot.fr on:

- Twitter (https://twitter.com/antibotfr)
- Facebook (https://www.facebook.com/antibotfr)
- Google + (https://plus.google.com/116037450239462514219)
- LinkedIn (https://www.linkedin.com/grp/home?gid=8188970)

6.3.4 Support

Antibot.fr does not provide support (e-mail or hotline): French ISPs regard it as their mission to provide support in such matter to their customers. Therefore antibot.fr only references abuse contacts at ISPs and refers to ACDC (Check & Secure, EU-cleaner), ISPs, and Security Vendors scan and cleaning tools, with in-depth explanations.

6.3.4.1 EU-Cleaners

Two EU-Cleaners have been made available to the German ABBZ and to the other National Support Centres. These cleaners are no full Anti-Virus Products; these cleaners are just dedicated to remove Malware from customer PCs. Both tools are free of charge.
The EU-Cleaners have been made available with friendly support from the partners **Avira** and **SurfRight**, and are referenced here: http://www.antibot.fr/nettoyer/eu-cleaner

6.3.5 Privacy, Data Protection and Security

Antibot.fr strictly upholds the rules of the national data protection laws. The terms of use and the data privacy statements are displayed on the website at http://www.antibot.fr/mentions-legales (terms of use).
All internal processes have been evaluated and analysed to ensure the high data privacy and security standards. The compliance to these standards is regularly tested.
Antibot.fr does not store, trace or receive any personal data from an infected user or from his computer and only attacks from infected PCs are evaluated. An evaluation of the Internet traffic through deep packet inspection or similar methods is strictly permitted, user behaviour is not recorded or evaluated.
Access to the entire antibot.fr infrastructure is limited to a restricted group of users, based on the internal security policies and standards.

6.3.6 Contributions / interaction with ACDC

Antibot.fr provides guidelines and tools built by ACDC and its members. Signal Spam (part of the national support centre as the national spam reporting centre) feeds the CCH with spam reports.

6.3.7 Dissemination

The CECyF and Signal Spam (with the support of their members) give antibot.fr all the visibility they can.

6.3.8 Sustainability

Antibot.fr requires no staff, as no support is in place. Signal Spam is responsible for the costs of hosting the antibot.fr website.

6.3.9 Signal Spam reporting workflow

Signal Spam completes the frame of the support centre by providing the national spam reporting centre solution, and feeding ACDC's Centralized Clearing House with spam reports. End Users report everything they consider to be a spam. The reports are analysed, processed, and sent in data feeds to relevant partners. Spambot analysis is a string focus and reports are notably sent to the CCH.

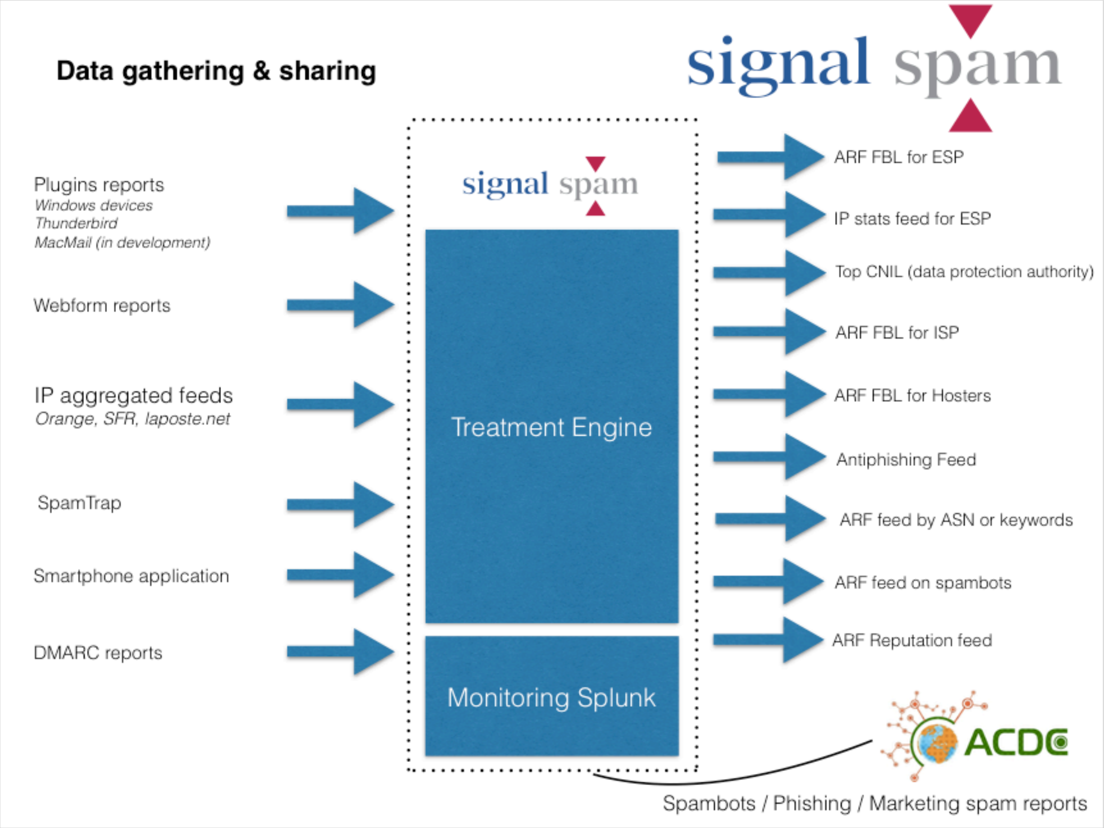


Figure 17: Processes Antibot.fr

6.4 Belgium

Botvrij.be is an initiative by LSEC - Leaders In Security as a part of the support centres of the European Advanced Cyber Defence Centre (ACDC-project) on the basis of the Anti-Botnet activities of the German ISP's association ECO.
The service addresses private end-users, same as small-and medium enterprises. The service is completely free of charge.
The goal of this initiative is to reduce the number of botnet infected computer clients in Belgium. It aims are to inform about botnets, to clean infected computers and to prevent future infections.
The Belgian national support centre provides a website. A help desk and telephone support are planned for the near future. Additional customer services are a blog, a forum and social media activities.
The Belgian national support center provides a centralized point of help/support for end-users. Support activities include a user forum. The website is focused on Information, Dissemination & Prevention.

The Belgian national support center aims to be a sustainable support center, and a broad security platform for end users (civilians). The Belgian Support Center will:

- Create awareness on it- and cyber security
- Provide information about relevant risks, threats and infections, and how to
- Provide access to tools, videos, documentation etc., all to support end users

The Support Center will build relationships with 3rd parties, government, experts from the security-industry and other organizations that are willing to support the solution by means of added value content and functionality, visibility and eventually (leading to) financial contributions in order to create and maintain a sustainable platform that helps end users to protect their systems and information.

6.4.1 Workflows

No workflow present. Only a website is available.

6.4.2 Staff

The website of the Belgian national support centre uses the base of www.botfrei.de. The Belgian national support centre's website www.botvrij.be is customized by professionals of LSEC.
Currently, there is no 1st and 2nd level support.
The official languages for communication and documentation are Dutch, French and English.

6.4.3 Service Level

Currently there are no service levels.
The goal is to make volunteers available to treat the forum.

6.4.3.1 Website

The website is available in 3 languages: Dutch, French, and English

The following is a graphical representation of the most current attacks taking place in the world and is available on the home site of www.botvrij.be.

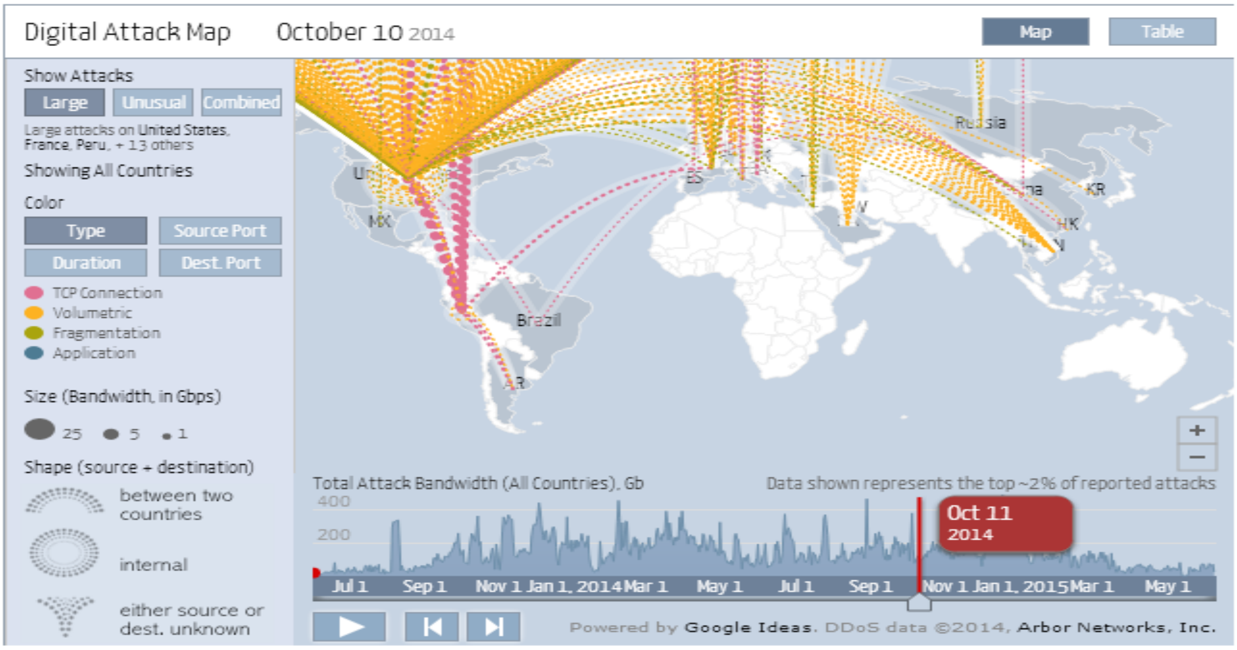


Figure 18: Digital Attack Map botvrij.be

The website was published in April 2014. The website is based on three columns "Inform", "Clean", "Protect". The forum and blog are featured on subpages; an extended software catalogue and FAQ list are available, too.

6.4.3.2 *Email-Support*

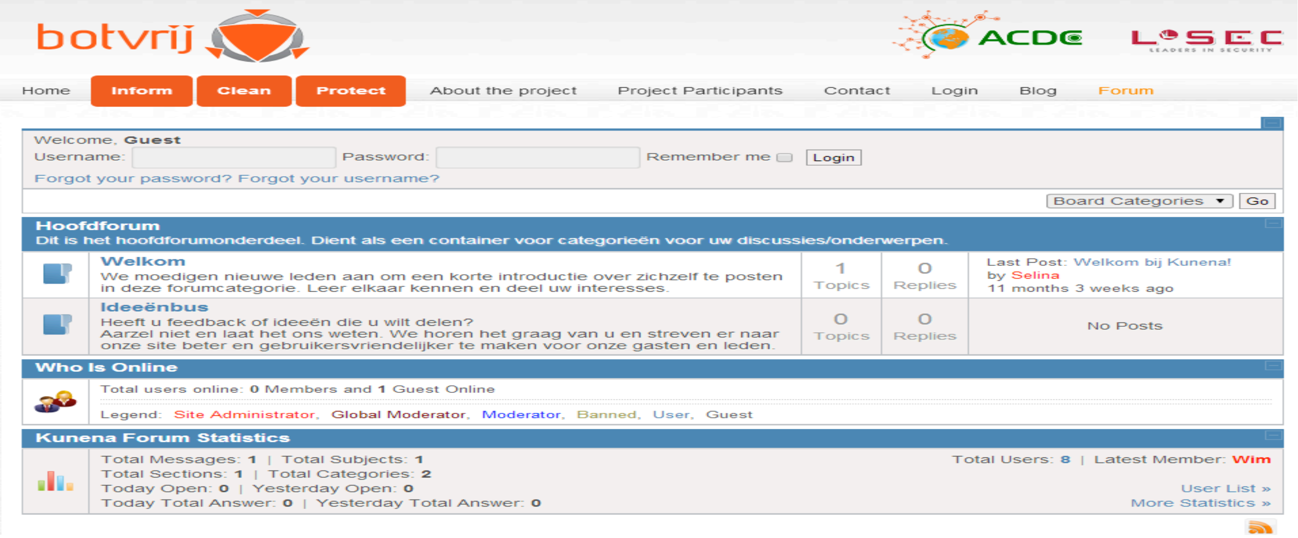
There is no email-support available.

6.4.3.3 *Telephone Support*

There is no telephone support available.

6.4.3.4 *Forum*

LSEC is currently supporting the forum. In a later stage volunteers can treat the forum.



Welcome, **Guest**

Username: Password: Remember me □

Forgot your password? Forgot your username?

Hoofdforum

Dit is het hoofdforumonderdeel. Dient als een container voor categorieën voor uw discussies/onderwerpen.

Welkom We moedigen nieuwe leden aan om een korte introductie over zichzelf te posten in deze forumcategorie. Leer elkaar kennen en deel uw interesses.	1 Topics	0 Replies	Last Post: Welkom bij Kunena! by Selina 11 months 3 weeks ago
Ideeënbus Heeft u feedback of ideeën die u wilt delen? Aarzel niet en laat het ons weten. We horen het graag van u en streven er naar onze site beter en gebruikersvriendelijker te maken voor onze gasten en leden.	0 Topics	0 Replies	No Posts

Who Is Online

Total users online: **0** Members and **1** Guest Online

Legend: Site Administrator, Global Moderator, Moderator, Banned, User, Guest

Kunena Forum Statistics

Total Messages: **1** | Total Subjects: **1**
Total Sections: **1** | Total Categories: **2**
Today Open: **0** | Yesterday Open: **0**
Today Total Answer: **0** | Yesterday Total Answer: **0**

Total Users: **8** | Latest Member: **Wim**

User List »
More Statistics »

Figure 19: Botvrij Forum

6.4.3.5 Blog & Social Media

LSEC is running its own blog at http://www.botvrij.be/index.php/en/blog-en.
Social media:

- Blog: http://www.botvrij.be/index.php/en/blog-en
- Facebook: https://www.facebook.com/botfree.eu
- Twitter: https://twitter.com/AntiBotnet
- Google Plus: https://plus.google.com/u/0/118250901031237479359/posts

6.4.4 Infrastructure

The website is based on Joomla[15]. Most of the used services and tools are freeware.

6.4.4.1 Ticketing System

There is no ticketing system available.

6.4.4.2 Phone System

There is no phone system available.

6.4.4.3 Forum-System

The forum is based on Kunena[16].

6.4.5 Customer Tools

The Belgian national support centre recommends a set of tools and services on their website. These tools are related to IT-Security, but also include common tools for IT-Maintenance like back up or analysis tools.

6.4.5.1 EU-Cleaners

Two EU-Cleaners have been made available to the Belgian national support centre and to the other National Support Centers. These cleaners are no full Anti-Virus Products; these cleaners are just dedicated to remove Malware from customer PCs. Both tools are free of charge.
The EU-Cleaners have been made available with friendly support from the partners **Avira**[17] and **SurfRight**[18].

6.4.5.2 Online-Scanner

Together with the ABBZ partner cyscon GmbH, the Belgian national support centre is providing a browser-and plugin-in check at http://www.check-and-secure.com/browsercheck/_en/. This service allows users to verify if the current version of their browser and the installed browser-plugins is up-to-date. There are also links to additional online scanners available on the website from:

- Bitdefender
- F-Secure
- Panda security
- Emsisoft
- Trend Micro

[15] http://www.joomla.org/
[16] http://www.kunena.org/
[17] http://www.avira.com
[18] http://www.surfright.nl

6.4.5.3 Link directory

The link / tool list of botvrij.be is split into a consumer and business section.
The business section lists only commercial anti-virus products; the extended consumer directory distinguishes between seven sub-categories. These are:

- Security Solutions from ISPs
- Freeware Virus Scanners
- Payware Virus Scanner
- Security products for Mac Users
- Browser Plugins
- Further useful tools
- Protection for Mobile Devices

6.4.6 Privacy, Data Protection and Security

The Belgian national support centre strictly upholds the rules of the national data protection laws. The terms of use and the data privacy statements are displayed on the website at http://www.botvrij.be/index.php/en/enterprise-sector-products/11-uncategorized/101-data-privacy (data privacy) and at http://www.botvrij.be/index.php/en/enterprise-sector-products/11-uncategorized/99-terms-of-use

All internal processes have been evaluated and analysed to ensure the high data privacy and security standards. The compliance to these standards is regularly tested.
The Belgian national support centre does not store, trace or receive any personal data from an infected user or from his computer and only attacks from infected PCs are evaluated. An evaluation of the Internet traffic through deep packet inspection or similar methods is strictly permitted, user behaviour is not recorded or evaluated.
Access to the entire Belgian national support centre infrastructure is limited to a restricted group of users, based on the internal security policies and standards.

6.4.7 Contributions / interaction with ACDC

LSEC has organized meetings with Belgian ISPs and upon request the ISP can get information from the ACDC Centralised Clearing House. LSEC has been also active in press and social media promoting the Belgian national support centre.

6.4.8 Dissemination

The Belgian national support centre botvrij.be has some visibility in Belgium. Besides the collaboration with the ISPs, there has been an ongoing reference and coverage on major websites.

6.4.9 Sustainability

The website botvrij.be is in an operational state since 2014. There is no intent to stop providing this service. LSEC is willed to continue with botvrij.be within a possible plan network of European Anti-Botnet Support Centres.

6.5 Italy

The Italian National Support Centre was realized within the ACDC project hosted and run by ISCTI. Services are accessible through the dedicated website (www.antibot.it) published in September 2012 and hosted in ISCTI site in Rome at the Italian Ministry of Economic Development.

This initiative is focused mainly on three dimensions of fight against botnets:

- *Prevention policies* – the initiative aims at informing and raising awareness of Internet users on botnet threats the website provides useful information on botnets and guidelines for self-check, scan and avoid infections by botnets.
- *Mitigation policies* – online free resources for checking one's computer is infected and for removing infections are provided. Enlisted tools are provided by partners of ACDC consortium.
- *Notification of incidents* – reports from the ACDC CCH are regularly collected, stored, processed and used to generate automatic notifications towards Italian ISPs involved in botnet incidents.

This initiative also addresses the institutional activity of ISCTI for network and electronic communication protection realized through the Italian National CERT (under Art. 14 of the 2013 Prime Minister's Decree 158) whose ISCTI has been entrusted.

6.5.1 Staff

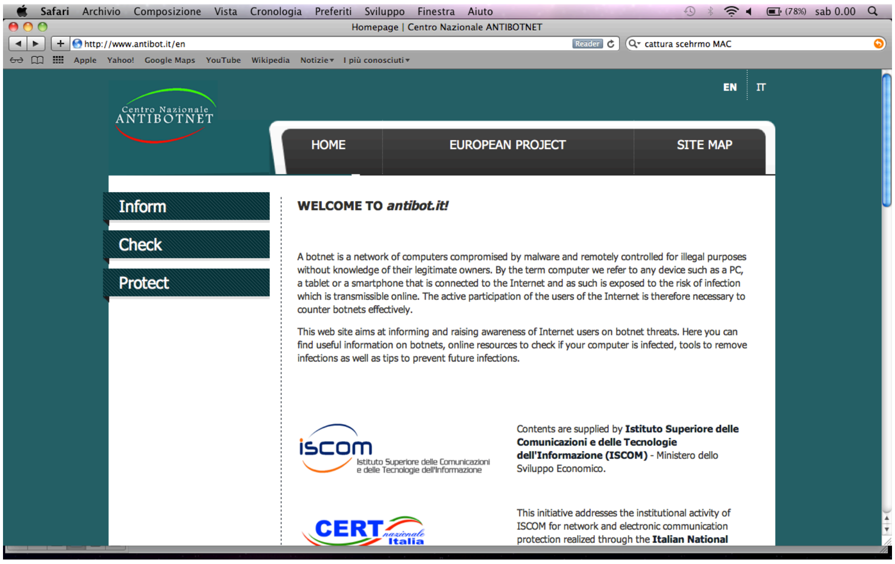
The activity of the Anti-Botnet National Support Centre is assured by permanent staff appointed also to the Italian National CERT.

6.5.2 Fronted System – the Website

The Anti-Botnet NSC website is a result of collaboration between ISCTI and EII, which is realized through Drupal CMS. EII provided a basic template for the site and programmed some graphical and structural adjustments, while ISCTI provided all the contents and implemented partial changes though Drupal CMS. Though it is primarily thought for Italian citizens, it is totally bilingual in Italian and English.

The website is the instrument for implementation of prevention and mitigations policies. It is organized in three sections:

- Information pages
- Guidelines and tools for disinfection and for prevention of infections
- Legal aspects, privacy policy and accessibility



WELCOME TO *antibot.it!*

A botnet is a network of computers compromised by malware and remotely controlled for illegal purposes without knowledge of their legitimate owners. By the term computer we refer to any device such as a PC, a tablet or a smartphone that is connected to the Internet and as such is exposed to the risk of infection which is transmissible online. The active participation of the users of the Internet is therefore necessary to counter botnets effectively.

This web site aims at informing and raising awareness of Internet users on botnet threats. Here you can find useful information on botnets, online resources to check if your computer is infected, tools to remove infections as well as tips to prevent future infections.

Contents are supplied by **Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)** - Ministero dello Sviluppo Economico.

This initiative addresses the institutional activity of ISCOM for network and electronic communication protection realized through the **Italian National**

Figure 20: Screenshot Antibot.it

6.5.2.1 Information pages

The top menu of the site provides basic information on the site including:

- The homepage presenting the objective of the site
- A dedicated page for the ACDC project from which the site takes its origin
- The map of the site showing its structure

The page dedicated to the ACDC project emphasize the role of the National Support Centre in Europe and highlights that the ACDC project is cited in the Italian National Plan for Cyberspace Security.

6.5.2.2 Guidelines and tools for disinfection and for prevention of infections

The left menu provides links to detailed content on botnets and tools for scanning and disinfecting one's computer. Namely, it includes:

- An information page on botnets and links to articles
- A list of scanning and disinfection tools as provided by the ACDC consortium, which are:
    - Check&Secure - a free online security self-check service managed by the associated ACDC Partner cyscon GmbH.
    - EU-Cleaner - a downloadable tool available at the German Support Centre.
    - Initiative-S - an initiative by eco – Association of the German Internet Industry (eco - Verband der deutschen Internetwirtschaft e.V.) - providing information and tools.
    - Servicio AntiBotnet - an online self-check services to verify if your computer is part of a botnet by the Spanish Support Centre (website in Spanish).
    - Device Monitor - a network data traffic analyser for security threats of both personal computers and mobile devices. Version for Android mobile devices available from Google Play. The tool is realized by XLAB, partner of ACDC.
    - CONAN mobile - a scanner and data traffic analyser for security threats of mobile devices. Version for Android mobile devices available from Google Play. The tool is realized by INCIBE, partner of ACDC (website in Spanish).
- A page providing basic recommendation so as not to get infected.

6.5.2.3 Legal aspects, privacy policy and accessibility

The bottom menu of the site provides links to

- Contact info for the owner of the site, i.e. ISCTI
- The privacy policy of the site
- Accessibility requirements for the sites, which are satisfied to assure utilization by people with disabilities, which are mandatory for all public administration sites in Italy.

6.5.3 The Backend System - Storage and processing of incident reports

If the website www.antibot.it represents the frontend function of the Italian NSC addressing the Internet users, a backend part was developed to store a process incident reports for analysis and notifications to Italian ISPs.

Namely, an XMPP client regularly retrieves from the CCH incident reports pertaining Italian ASNs. Data are stored, classified by ASN and used to generate automatic notification emails which are sent on a regular basis to Italian ISPs whenever one of their ASN is interested in a botnet incidents.

6.5.4 Privacy, Data Protection and Security

Currently the Italian National Support Centre website does not exhibit any particular privacy or data protection since interactive services for users are not yet provided. Data privacy issues linked to the browsing of the website are discussed in the page http://www.antibot.it/en/content/privacy-policy, which is dedicated to these issues.

As for the backend-part incident reports which are stored do not contain any sensitive data and are dealt with to implement the institutional function of the Italian National CERT of protection of electronic communication.

6.5.5 Sustainability and development plan

The Italian National Support Centre run by ISCTI, as part of the ACDC project, will be part of the network of support centre in order to share information and strategies at European level to fight against botnets. In turn, ISCTI, at national level, as Italian National CERTs chairs a Technical Board, in which the biggest Italian ISPs are involved. Within the Board it is possible to discuss botnet strategies at national level.

The activity of the Anti-Botnet National Support Centre is assured by permanent staff appointed also to the Italian National CERT along with the other necessary resources for development and maintenance of the National CERT Network.

Development plan of the Anti-Botnet National Support Centre include the deployment of support services, via email or phone, for Internet users is under discussion in both the network of European Support Centres and in the National Technical Board with Italian ISPs. Namely, a support centre in the English language can be realized easily by the network of NSCs while synergies from Italian ISPs are required for the activation of a service in Italian.

6.6 Portugal

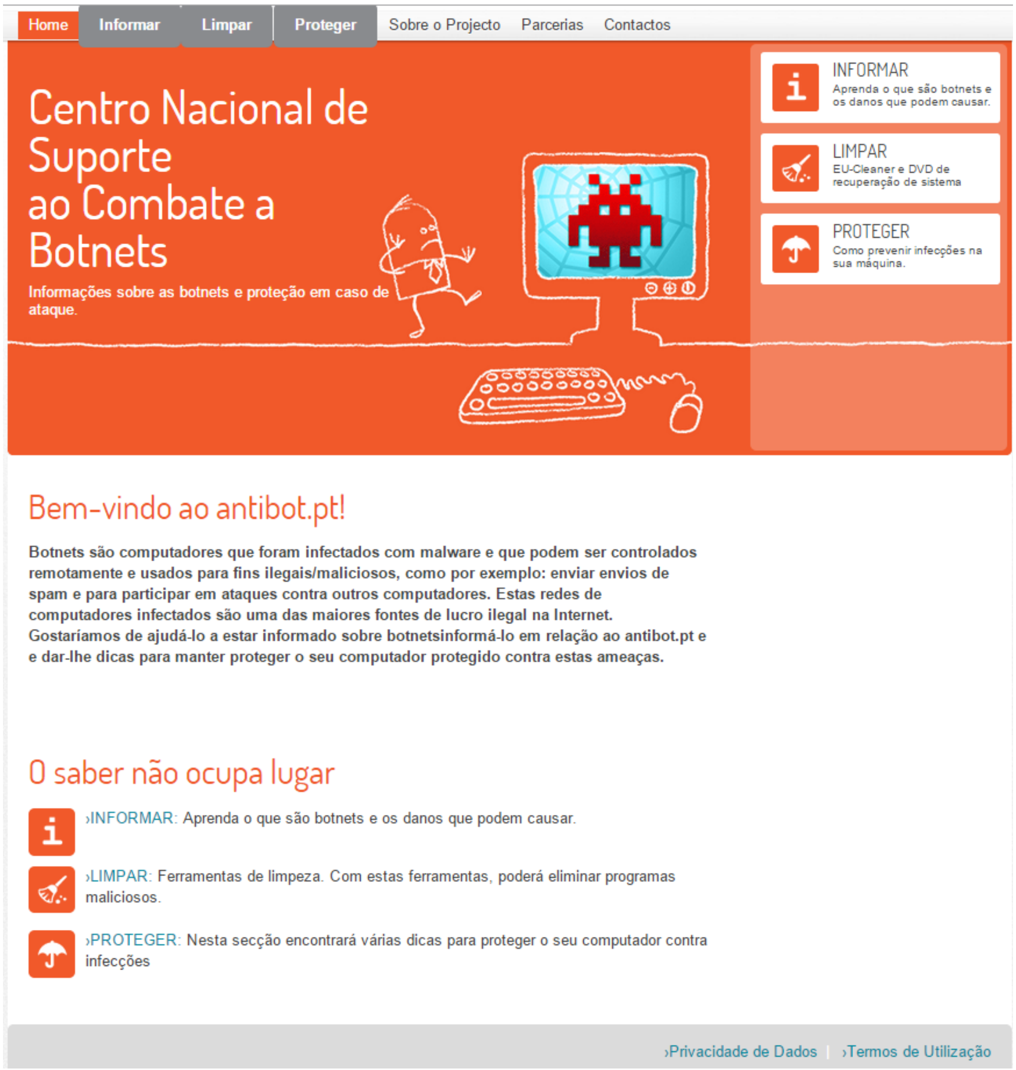
The Portuguese National Support Center, antibot.pt, is a initiative from FCT|FCCN – Fundação para a Ciencia e Tecnologia – Computação Cientifica National. Its scope is guided to the end user, especially those that are part of RCTS community, the Portuguese academic network.
As the other NSCs from ACDC Project, its purpose is the dissemination of information on botnets and help the end user in the cleaning of his device (computer, tablet or mobile phone).

6.6.1 Staff and Contact

Due to significant reduction in the number of elements of the RCTS CERT team, which is responsible for the implementation, management and operation of the Portuguese NSC, it was only possible in this project pilot represent the NSC through the website www.antibot.pt and email address: ajuda@antibot.pt.

6.6.2 Website

The website www.antibot.pt is available in Portuguese and English language, it was based on the German structure and uses its layout as a template.



Centro Nacional de Suporte ao Combate a Botnets

Informações sobre as botnets e proteção em caso de ataque.

INFORMAR
Aprenda o que são botnets e os danos que podem causar.

LIMPAR
EU-Cleaner e DVD de recuperação de sistema

PROTEGER
Como prevenir infecções na sua máquina.

Bem-vindo ao antibot.pt!

Botnets são computadores que foram infectados com malware e que podem ser controlados remotamente e usados para fins ilegais/maliciosos, como por exemplo: enviar envios de spam e para participar em ataques contra outros computadores. Estas redes de computadores infectados são uma das maiores fontes de lucro ilegal na Internet. Gostaríamos de ajudá-lo a estar informado sobre botnetsinformá-lo em relação ao antibot.pt e e dar-lhe dicas para manter proteger o seu computador protegido contra estas ameaças.

O saber não ocupa lugar

›INFORMAR: Aprenda o que são botnets e os danos que podem causar.

›LIMPAR: Ferramentas de limpeza. Com estas ferramentas, poderá eliminar programas maliciosos.

›PROTEGER: Nesta secção encontrará várias dicas para proteger o seu computador contra infecções

›Privacidade de Dados | ›Termos de Utilização

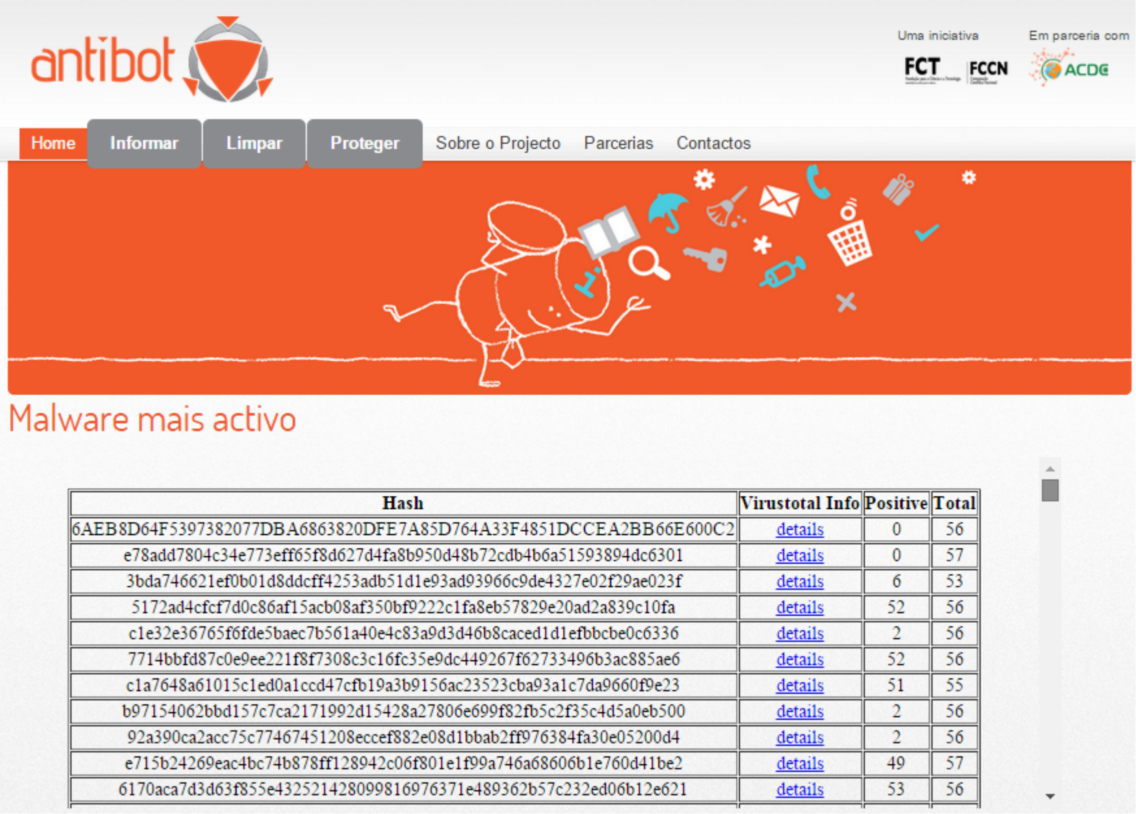
Figure 21: Antibot.pt Screenshot

6.6.3 Forum and Blog

Although the Portuguese NSC website does not have its own forum and blog, it presents the link to the English version of the German forum and blog.

6.6.3.1 Tools and Services

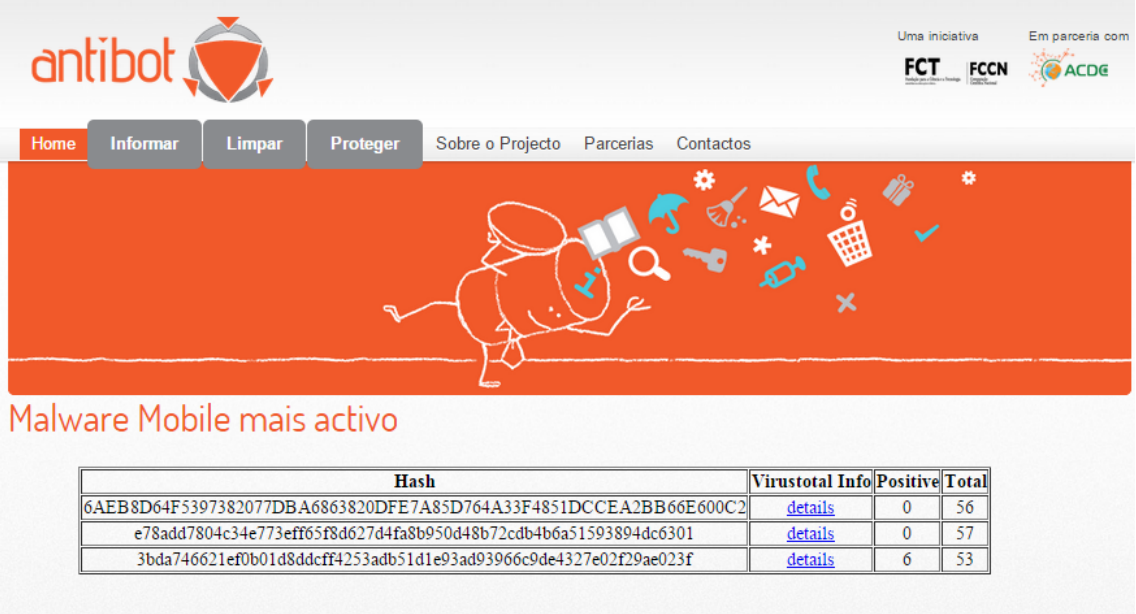
In order to add more value to the website and to take advantage from data collected by CCH, in a daily base is presented, for both Windows and mobile devices, the most active malware. For each row is added a link to *Virustotal* website, to have more detail about the malware. The first idea was to collect these details from *Virustotal* and put them in the NSC website, but the free API *Virustotal* version does not allow the gathering of all the required data.



Malware mais activo

Hash	Virustotal Info	Positive	Total
6AEB8D64F5397382077DBA6863820DFE7A85D764A33F4851DCCEA2BB66E600C2	details	0	56
e78add7804c34e773eff65f8d627d4fa8b950d48b72cdb4b6a51593894dc6301	details	0	57
3bda746621ef0b01d8ddcff4253adb51d1e93ad93966c9de4327e02f29ae023f	details	6	53
5172ad4cfcf7d0c86af15acb08af350bf9222c1fa8eb57829e20ad2a839c10fa	details	52	56
c1e32e36765f6fde5baec7b561a40e4c83a9d3d46b8caced1d1efbbcbe0c6336	details	2	56
7714bbfd87c0e9ee221f8f7308c3c16fc35e9dc449267f62733496b3ac885ae6	details	52	56
c1a7648a61015c1ed0a1ccd47cfb19a3b9156ac23523cba93a1c7da9660f9e23	details	51	55
b97154062bbd157c7ca2171992d15428a27806e699f82fb5c2f35c4d5a0eb500	details	2	56
92a390ca2acc75c77467451208eccef882e08d1bbab2ff976384fa30e05200d4	details	2	56
e715b24269eac4bc74b878ff128942c06f801e1f99a746a68606b1e760d41be2	details	49	57
6170aca7d3d63f855e43252142809981697637 1e489362b57c232ed06b12e621	details	53	56

Figure 22: Virustotal Integration Malware



Malware Mobile mais activo

Hash	Virustotal Info	Positive	Total
6AEB8D64F5397382077DBA6863820DFE7A85D764A33F4851DCCEA2BB66E600C2	details	0	56
e78add7804c34e773eff65f8d627d4fa8b950d48b72cdb4b6a51593894dc6301	details	0	57
3bda746621ef0b01d8ddcff4253adb51d1e93ad93966c9de4327e02f29ae023f	details	6	53

Figure 23: Virustotal - Mobile Threats Integration

6.6.4 Outlook and Sustainability

Due to the restrictions identified at the beginning of this document, it will be not possible to FCT|FCCN, in particular the RCTS CERT continuing to provide this service after the end of the project.

6.7 Spain

The Spanish National CyberSecurity Institute (INCIBE) is a state owned company attached to the Spanish Ministry of Industry, Energy and Tourism through the State Secretariat for Telecommunications and for the Information Society.

INCIBE is the responsible, through its CERT, to managing the defence of the cyberspace and serve as preventive and reactive security support to Spanish entities and users. INCIBE has the ability to act in response to security incidents ranging from the citizen to the business sector, especially strategic and critical infrastructure sectors, and the specific area of academic network.

At present, the government of Spain has several agents working from different perspectives in order to achieve a secure cyberspace. INCIBE is a leading figure in the panorama of national CyberSecurity, both from the point of view of providing services to different target audiences, and in the exercise of awareness and communication needs and current challenges of CyberSecurity.

Spanish National Support Centre, known as OSI https://www.osi.es/ (Security Office of the Internet Users) is working since 2008. In the scope of ACDC a new version of the website was launched in 2014, with a new look and feel, contents and services. Its mission is to generate cyber-confidence through cybersecurity education, encouraging users' confidence in a digital environment and foment its use to carry out their everyday tasks in a safe way.

OSI objectives for users are to:

- Understand, assimilate and adopt a minimum of good practices when using Internet.
- Be aware of their responsibility in security matters, becoming an active and proactive element in the security of their information and devices.
- Reduce the quantity and critical nature of threats or incidents that they are exposed to when using Internet.

The operation of the Spanish NSC is based in three different groups:

- **Awareness and Education Services** focuses on improving the cybersecurity knowledge of users as well as informing them about the latest novelties, news and incidents related to security in Internet.
  These services are provided with the content and documentation of the sections: blog, security alerts, real stories, video tutorials, "how much do you know?" and "what should I know?".
- **Tools and Services** in order to facilitate the tools that users need to use Internet safely and confidently.
  The services offered are free tools, Conan Mobile and the Anti-Botnet Service.
- **Support Services** offers users direct contact with the OSI to solve doubts and get help in cybersecurity matters, through a telephone number, email contact, forum and the different social networks.

All services offered are free of charge for the users.

6.7.1 Workflows

The different services of OSI are operating by different teams such as incident management (levels 1 and 2) and contents development. In order to generate the different alerts, advisors, posts etc. OSI team is permanently investigating and analyzing the latest news and incidents related to cybersecurity, offering the results to the users through the different services, and always in an easy way to understand them for people who do not have specialized IT knowledge.

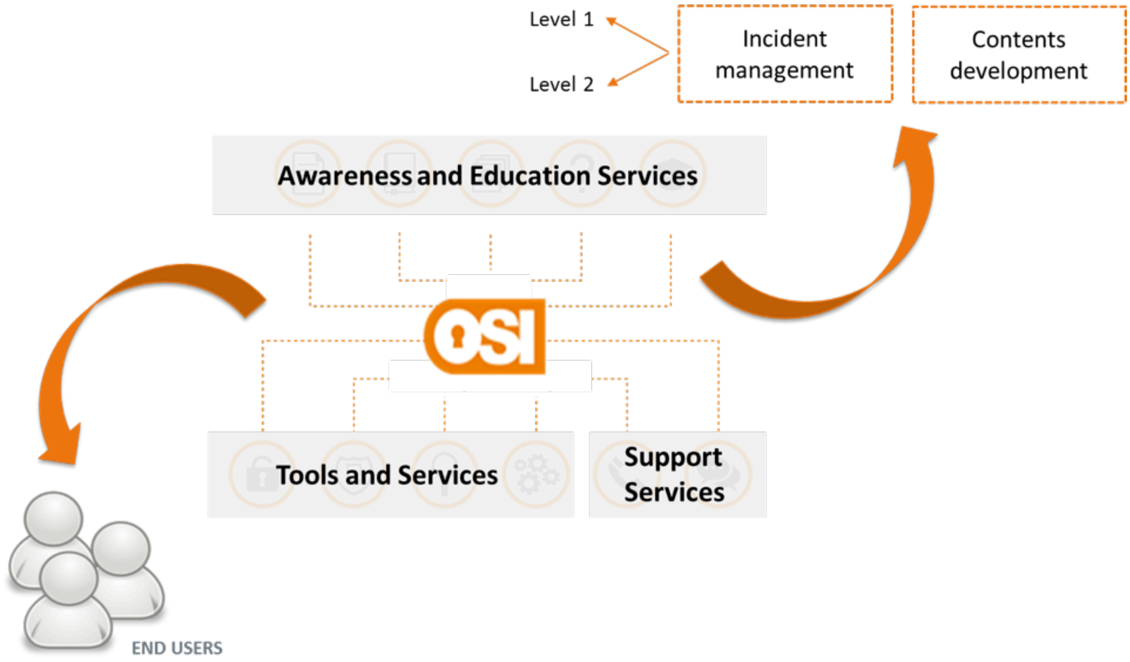


Figure 24: Concept Spanish NSC

One of these services is the Anti-Botnet Service, developed on the scope of ACDC. It has as objective the mitigation of botnets, offering to the users the possibility to identify if from its internet connection has been detected some incident related botnet, contributing to a more secure Internet for everyone. The concrete workflow of this service is the following:

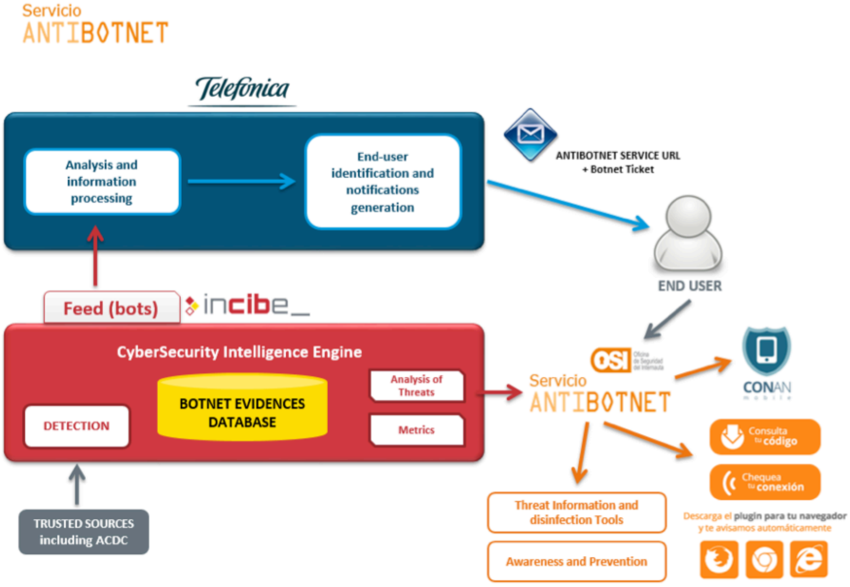

Servicio ANTIBOTNET
Telefónica
Analysis and information processing
End-user identification and notifications generation
ANTIBOTNET SERVICE URL + Botnet Ticket
END USER
Feed (bots)
incibe_
CyberSecurity Intelligence Engine
DETECTION
BOTNET EVIDENCES DATABASE
Analysis of Threats
Metrics
TRUSTED SOURCES including ACDC
OSI
Servicio ANTIBOTNET
CONAN mobile
Consulta tu código
Chequea tu conexión
Descarga el plugin para tu navegador y te avisamos automáticamente
Threat Information and disinfection Tools
Awareness and Prevention

Figure 25: Processes Spanish NSC

The Anti-Botnet Service database provides in real time information about public IP addresses that are associated with incidents related botnets. INCIBE obtains those evidences from different internal and external trusted sources; one of them is the data collected from the CCH of the ACDC project.
All evidences are automatically processed and the evidence enters it the notification workflow.
The Anti-Botnet Service team documents the botnet in the backend of the service (if it is not already documented), with relevant information that must be shown to the user in the NSC when he will consult the incident. In addition, each botnet has associated a code. The code or ticket associates the bot evidences with its information for the notification service.
INCIBE generates daily a feed with all the bots evidences that correspond to each Spanish ISP. This notification is made in order to improve the networks security in a public-private partnership, under the mandates of the Action 5 of the Digital Trust Plan and in compliance with the ninth additional provision of the Law 347202, of July 11, 2014.

Thanks to this collaboration, the Spanish ISP Telefónica, gets its own feed each day and process it in order to generate the user notification. With the IP and the timestamp, they can identify the internet line affected and contact by email with the user.
With all the information an email is sent by Telefónica abuse team (Némesys) to the affected user informing about the incident, and providing the code, which the user can access the NSC to get more information about the botnet and how disinfect its device.
All users can check their public IPs through the online service or the plugins. If the network of the user is affected, he will be informed about the incident detected by the service.
More information about the service is given in the section Anti-Botnet Service of this document.Anti-Botnet Service

6.7.2 Staff

All the staff of the Spanish NSC has a big trajectory and experience in IT and cybersecurity projects and count with technical studies and different official certifications related IT.
The team involved and number of staff is the following:

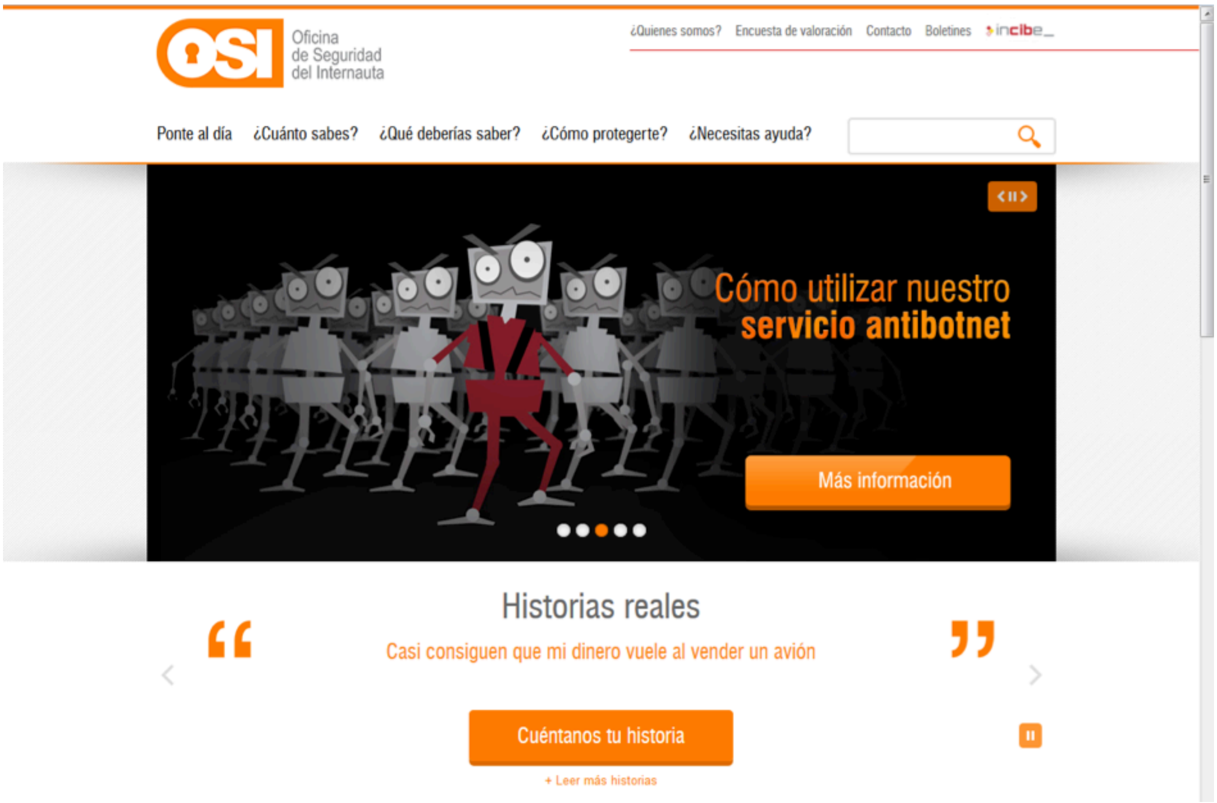
- Product Owner (the responsible of the portal operation and services): 1
- Content team: 3.
- Threat Analysis team: 1
- Support team – level I (email and CAU): 2 (partially)
- Support team – level II: 2 (partially, on demand)
- IT support team: 1 (partially, on demand)
- Software Development team: 2
- Software Maintenance team: 1 (partially, on demand)
- Community manager: 1

6.7.3 Service Level

Spanish NSC offers 1st and 2nd level of technical support to end-users. The objective is to solve doubts and provide personalized help and direct contact for Internet users that need assistance in cybersecurity matters. Users have different channels to contact in an easy and simply way, such as email, phone, forum or through the different social networks.

6.7.3.1 Website

Spanish NSC website https://www.osi.es/ has the objective to educate users and offers them the necessary information and advices to improve their cybersecurity education through its different sections.



Cómo utilizar nuestro servicio antibotnet

Historias reales

Casi consiguen que mi dinero vuele al vender un avión

Figure 26: Botnet Information Page Spain

6.7.3.1.1.1 Awareness and Education Services

The services that integrate the "awareness and education services" group are geared towards offering practical advice and cybersecurity education. Its aim is to offer users news and novelties regarding Internet Security. Through these services, users can adopt a proactive habit of updating and expanding their security knowledge, as a preventive measure to use new technologies with confidence.

6.7.3.1.1.2 Blog

The blog has been created to incite curiosity about Internet news. It is updated almost daily with news about security, not only related to Internet but any topic related to ICTs that can affect users. All contents are written with a familiar and simple vocabulary for users who find it hard to read texts with a more technical vocabulary that are aimed at a more professional public. The focus of the articles is mainly practical although it is talked too about theoretical concepts that must be known and understood.
In conclusion, it is explained to users what they must do to improve their security and use new technologies confidently.

6.7.3.1.1.3 Security Alerts

Latest news about errors, alerts and threats that affect the security of users on Internet are described and explained in an easy way for users who do not have specialized IT knowledge.
It helps citizens to be updated about the latest alerts, and learn how to protect themselves.

6.7.3.1.1.4 Real stories

This section shows real cases of online frauds. There are cases where the user has been the victim of a fraud. In other cases, users have been able to identify the fraud and have been able to avoid it and protect themselves adequately. In both cases, the objective is to share their case in order to prevent others from being victims of these frauds.

The objective of publishing these real cases is to encourage the users' interest in cybersecurity as the section points out problems that could affect them and therefore they can get interested in what they have to do and how they have to react to those cases.

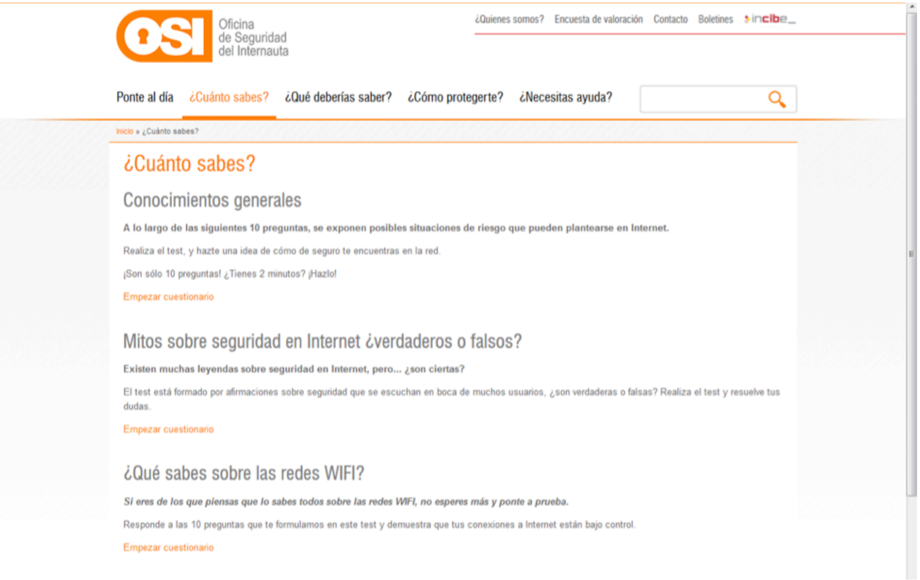
Therefore, this section is another way to alert users, allowing them to identify possible fraud attempts and know how to protect themselves and to report if they have been victims. Every real story includes practical advice and useful information about defense, protection and report mechanisms.

6.7.3.1.1.5 Video tutorials

OSI YouTube channel offers users practical videos with advice about how to improve the protection of information and devices. This is the ideal educational resource for explaining certain practical concepts that could be vague or ambiguous in text form. All video tutorials include subtitles that can be activated to make it easier to follow the explanation https://www.youtube.com/user/OSIseguridad/

6.7.3.1.1.6 How much do you know?

The purpose of this section is to test the users' knowledge about security and Internet in a quick and fun way, while also expanding and updating their knowledge at the same time. Tests are made up of 10 questions based on possible risk situations that users could be exposed to. Users are offered multiple choices from which they have to select the correct one. Once the test is finished, users can find out the percentage of correct answers, and which are the correct answers to the questions they got wrong.



¿Cuánto sabes?

Conocimientos generales

A lo largo de las siguientes 10 preguntas, se exponen posibles situaciones de riesgo que pueden plantearse en Internet.

Realiza el test, y hazte una idea de cómo de seguro te encuentras en la red.

¡Son sólo 10 preguntas! ¿Tienes 2 minutos? ¡Hazlo!

Empezar cuestionario

Mitos sobre seguridad en Internet ¿verdaderos o falsos?

Existen muchas leyendas sobre seguridad en Internet, pero... ¿son ciertas?

El test está formado por afirmaciones sobre seguridad que se escuchan en boca de muchos usuarios, ¿son verdaderas o falsas? Realiza el test y resuelve tus dudas.

Empezar cuestionario

¿Qué sabes sobre las redes WIFI?

Si eres de los que piensas que lo sabes todos sobre las redes WIFI, no esperes más y ponte a prueba.

Responde a las 10 preguntas que te formulamos en este test y demuestra que tus conexiones a Internet están bajo control.

Empezar cuestionario

Figure 27: Security Quiz Spain

6.7.3.1.1.7 What I should know?

This section comprises22 monographs on topics related to Internet and new technologies from a cybersecurity point of view. Each monograph addresses one topic of high interest for users: security in social networks, protection and safe use of WiFi, online banking…

At the same time, each addressed topic is underpinned by other related publications that develop the content. These publications can be presented in diverse formats: graphics, posts, video blogs, etc.

6.7.3.1.2 Tools and Services

The Spanish NSC provides its users with different free useful tools and solutions to protect and improve the security level of their information, devices and actions. By using these services, users can use new technologies and Internet with the knowledge that they are better protected.

6.7.3.1.2.1 Free tools

The Spanish NSC offers users a variety of free tools for main platforms, classified by type and utility, which can be downloaded and used depending on the users' needs.

The user firstly selects the operating system the device that he is going to install the application on has. Then, the user selects the type of tool that he is searching from the 15 available types in the section, and from these search options, the user obtains a list of possible applications that he can download and install in his devices to improve their security level, accompanied by support documentation to make the most of the tool.

6.7.3.1.2.2 CONAN Mobile

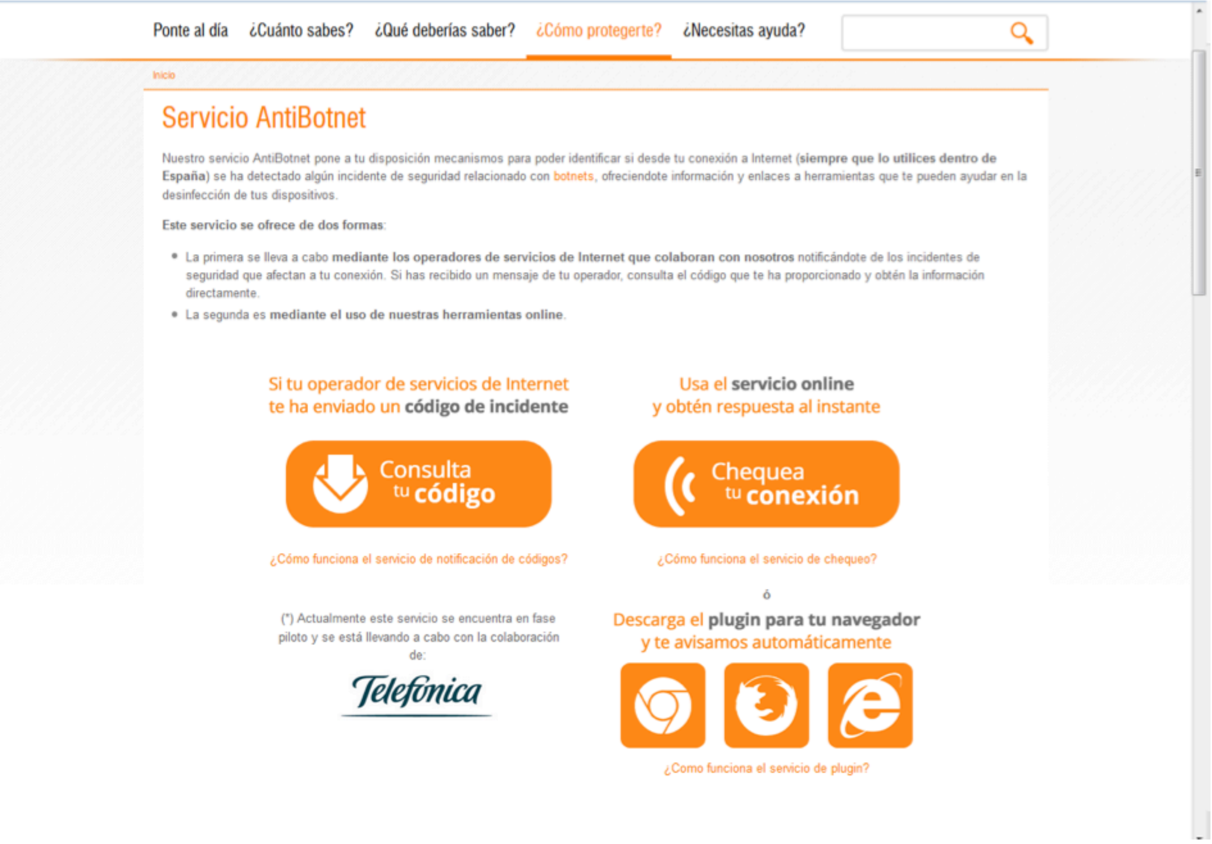
This tool is provided in the scope of the ACDC project. This is a free application for Android mobile devices, available on the European Google market. This tool alerts the user about the security level of his device, offering possible solutions to improve their security.

- http://www.osi.es/es/conan-mobile
- https://play.google.com/store/apps/details?id=es.inteco.conanmobile&hl=es

6.7.3.1.2.3 Anti-Botnet Service

In the scope of ACDC, the Spanish NSC launched its Anti-Botnet Service in June 2014 and in November 2014 was launched a second version incorporating to the initiative the collaboration of Telefónica, the main ISP in Spain, with the notification to end-users.

The Anti-Botnet Service has as objective the mitigation of botnets. It offers to the users the possibility to identify if from its internet connection has been detected some incident related botnet, offering information and tools links for the disinfection.



Servicio AntiBotnet

Nuestro servicio AntiBotnet pone a tu disposición mecanismos para poder identificar si desde tu conexión a Internet (**siempre que lo utilices dentro de España**) se ha detectado algún incidente de seguridad relacionado con botnets, ofreciendote información y enlaces a herramientas que te pueden ayudar en la desinfección de tus dispositivos.

Este servicio se ofrece de dos formas:

- La primera se lleva a cabo **mediante los operadores de servicios de Internet que colaboran con nosotros** notificándote de los incidentes de seguridad que afectan a tu conexión. Si has recibido un mensaje de tu operador, consulta el código que te ha proporcionado y obtén la información directamente.
- La segunda es **mediante el uso de nuestras herramientas online**.

Si tu operador de servicios de Internet te ha enviado un **código de incidente**

¿Cómo funciona el servicio de notificación de códigos?

(*) Actualmente este servicio se encuentra en fase piloto y se está llevando a cabo con la colaboración de:

Telefónica

Usa el **servicio online** y obtén respuesta al instante

¿Cómo funciona el servicio de chequeo?

ó

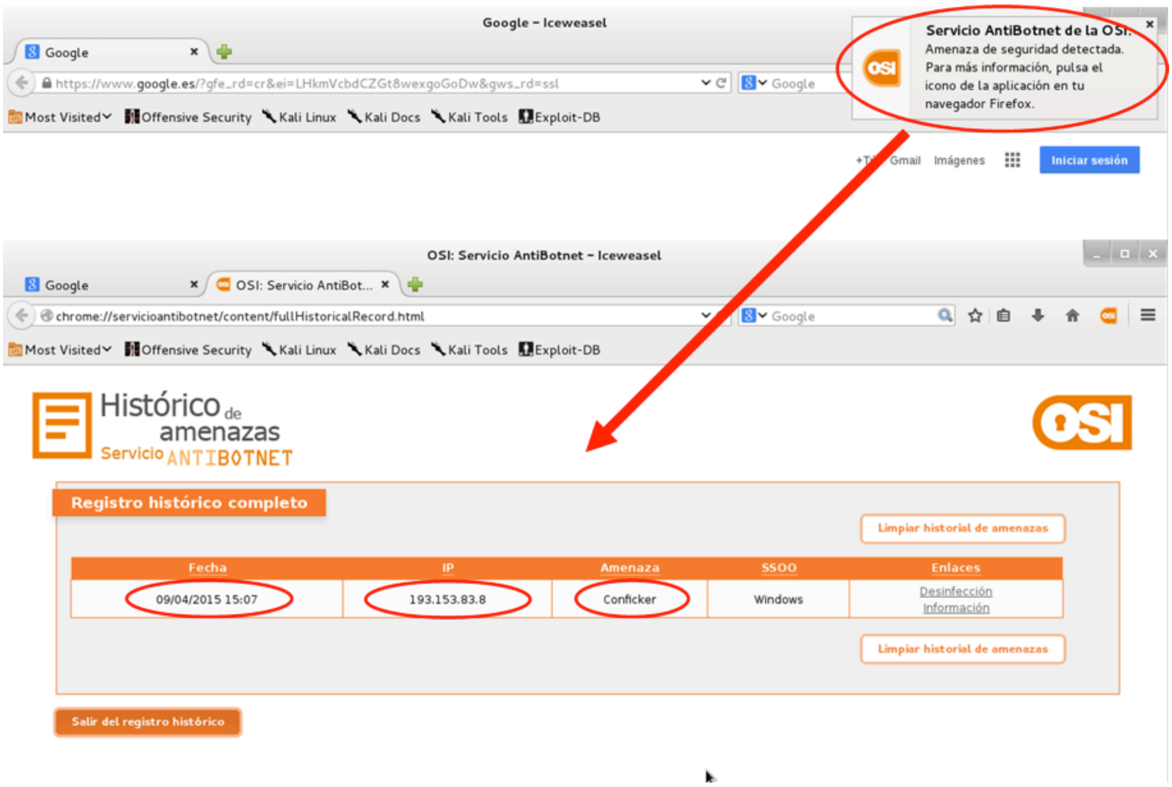
Descarga el **plugin para tu navegador** y te avisamos automáticamente

¿Como funciona el servicio de plugin?

Figure 28: Anti-Botnet Services

The Anti-Botnet Service is offered to end-users through five different ways:

- **Online Service**: End-users can check online if their public IP is involved in botnet activities (service practically in real time because of the dynamic IPs). For that, the IP public of the user is checked with the database of the Anti-Botnet Service.
- **Plugin Service**: Plugin available for Google Chrome, Firefox and Internet Explorer. Once it is installed as a complement of the browser, it is executed periodically and automatically. In the same way of the online service, the plugin alerts regularly about threats or cybersecurity incidents related with botnets, so that users do not need to check their IP manually with the online service.
- **CONAN Mobile**: application for Android devices, which helps to check the level of security of the configuration and applications installed on it. This ACDC tool integrates the functionality of the Anti-Botnet Service, which allows identifying security threats related to botnets in the current WiFi connection.
- **ISP Notification**: The Spanish ISP Telefónica notifies end-users by email about botnet- related incidents that affect their internet connections. INCIBE provides Telefónica every day with a feed containing bot evidences related to their ASNs. With this information, Telefónica identifies their affected end-users and send those notifications. In the notification it is indicated the IP affected, the timestamp of the detection, the URL of the Spanish NSC and a ticket or code related to the detected incident. With this code the end-user can access detailed information about the botnet and suitable disinfection tools.
- **API for companies:** API that allows IT personal to integrate the service in their network monitoring systems. This service is oriented to companies.



Google – Iceweasel
Google
https://www.google.es/?gfe_rd=cr&ei=LHkmVcbdCZGt8wexgoGoDw&gws_rd=ssl
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Gmail
Imágenes
Iniciar sesión
OSI: Servicio AntiBotnet – Iceweasel
OSI: Servicio AntiBot...
chrome://servicioantibotnet/content/fullHistoricalRecord.html

Servicio AntiBotnet de la OSI.
Amenaza de seguridad detectada.
Para más información, pulsa el icono de la aplicación en tu navegador Firefox.

Histórico de amenazas
Servicio ANTIBOTNET

Registro histórico completo

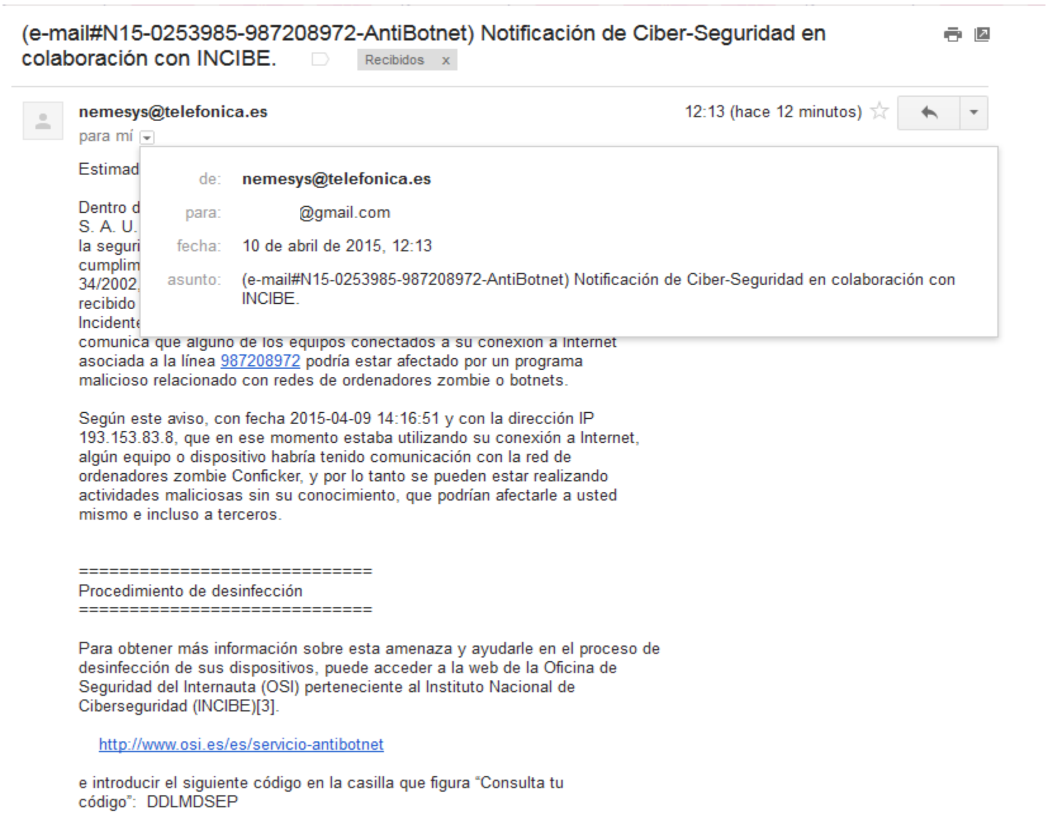
Limpiar historial de amenazas

Fecha	IP	Amenaza	SSOO	Enlaces
09/04/2015 15:07	193.153.83.8	Conficker	Windows	Desinfección Información

Limpiar historial de amenazas

Salir del registro histórico

Figure 29: Ticketing System Spain



(e-mail#N15-0253985-987208972-AntiBotnet) Notificación de Ciber-Seguridad en colaboración con INCIBE.

nemesys@telefonica.es
para mí

12:13 (hace 12 minutos)

de: nemesys@telefonica.es
para: @gmail.com
fecha: 10 de abril de 2015, 12:13
asunto: (e-mail#N15-0253985-987208972-AntiBotnet) Notificación de Ciber-Seguridad en colaboración con INCIBE.

Estimad

Dentro d
S. A. U.
la seguri
cumplim
34/2002
recibido
Incident
comunica que alguno de los equipos conectados a su conexión a Internet asociada a la línea 987208972 podría estar afectado por un programa malicioso relacionado con redes de ordenadores zombie o botnets.

Según este aviso, con fecha 2015-04-09 14:16:51 y con la dirección IP 193.153.83.8, que en ese momento estaba utilizando su conexión a Internet, algún equipo o dispositivo habría tenido comunicación con la red de ordenadores zombie Conficker, y por lo tanto se pueden estar realizando actividades maliciosas sin su conocimiento, que podrían afectarle a usted mismo e incluso a terceros.

=============================
Procedimiento de desinfección
=============================

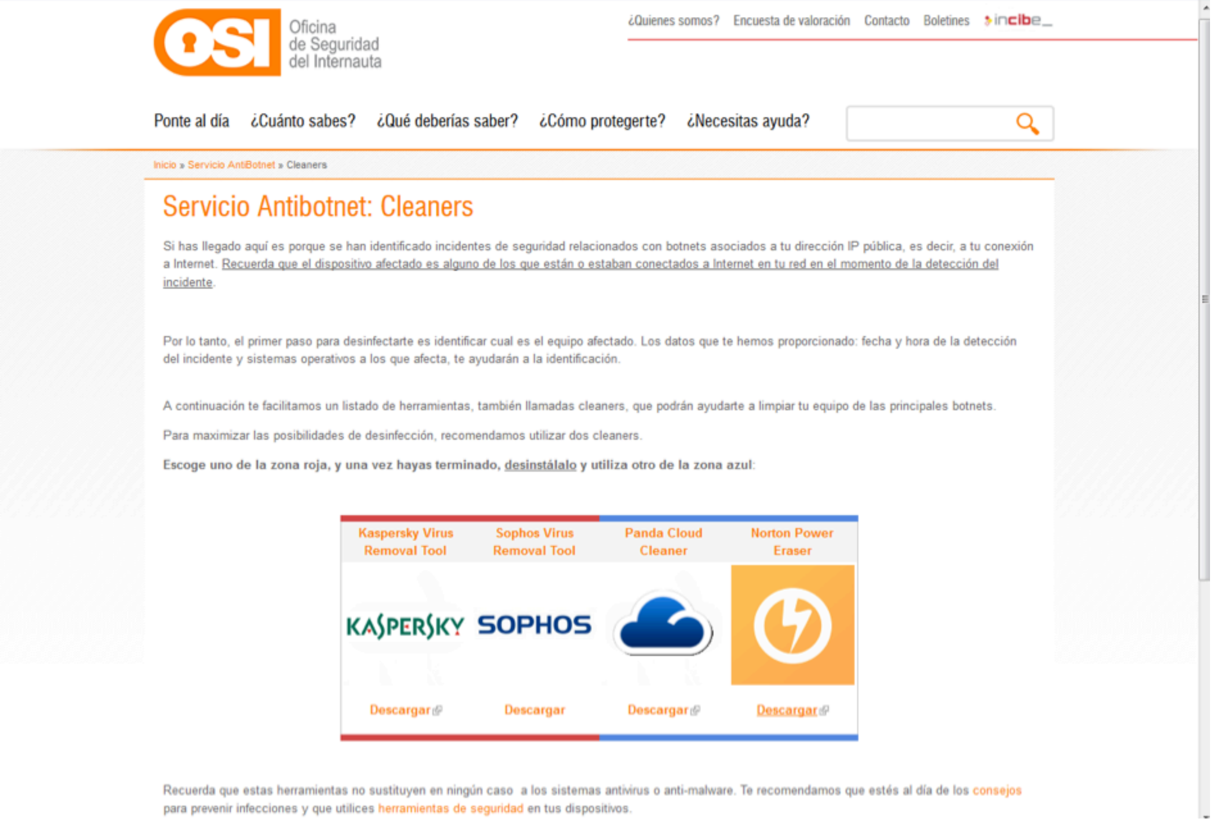
Para obtener más información sobre esta amenaza y ayudarle en el proceso de desinfección de sus dispositivos, puede acceder a la web de la Oficina de Seguridad del Internauta (OSI) perteneciente al Instituto Nacional de Ciberseguridad (INCIBE)[3].

http://www.osi.es/es/servicio-antibotnet

e introducir el siguiente código en la casilla que figura "Consulta tu código": DDLMDSEP

Figure 30: Customer Notification

The Anti-Botnet Service offers information to infected users about the botnet and links to free cleaners in order to help them with the disinfection of their devices.



Servicio Antibotnet: Cleaners

Si has llegado aquí es porque se han identificado incidentes de seguridad relacionados con botnets asociados a tu dirección IP pública, es decir, a tu conexión a Internet. Recuerda que el dispositivo afectado es alguno de los que están o estaban conectados a Internet en tu red en el momento de la detección del incidente.

Por lo tanto, el primer paso para desinfectarte es identificar cual es el equipo afectado. Los datos que te hemos proporcionado: fecha y hora de la detección del incidente y sistemas operativos a los que afecta, te ayudarán a la identificación.

A continuación te facilitamos un listado de herramientas, también llamadas cleaners, que podrán ayudarte a limpiar tu equipo de las principales botnets.

Para maximizar las posibilidades de desinfección, recomendamos utilizar dos cleaners.

Escoge uno de la zona roja, y una vez hayas terminado, desinstálalo y utiliza otro de la zona azul:

Kaspersky Virus Removal Tool	Sophos Virus Removal Tool	Panda Cloud Cleaner	Norton Power Eraser
KASPERSKY	SOPHOS		
Descargar	Descargar	Descargar	Descargar

Recuerda que estas herramientas no sustituyen en ningún caso a los sistemas antivirus o anti-malware. Te recomendamos que estés al día de los consejos para prevenir infecciones y que utilices herramientas de seguridad en tus dispositivos.

Figure 31: Mitigation Tools Spain

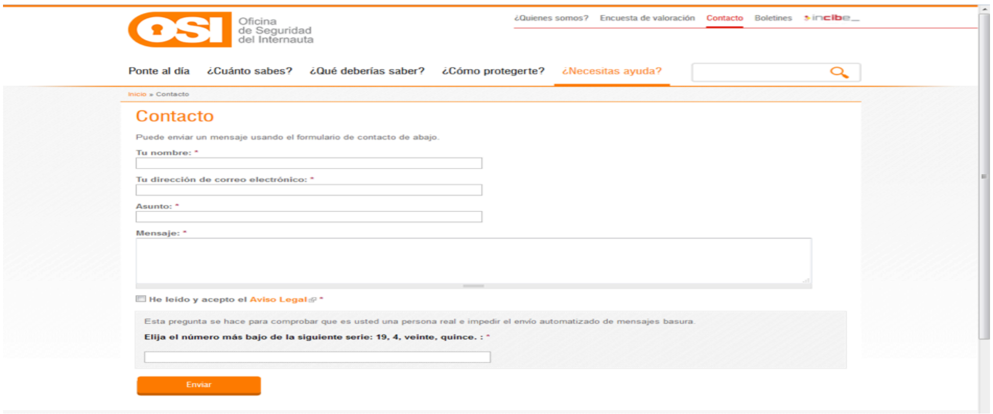
The Anti-Botnet Service has at this moment more than 40 botnets documented. There are evidences of infection of all of them, and all are being notified to affected end-users.

6.7.3.1.3 Support Services

The support service provides personalized help for Internet users in cybersecurity matters.

6.7.3.1.3.1 Email-Support

Users can contact the NSC through email using a form available on the web. Email support is available from Monday to Friday on business hours, offering users required and tailored help to solve their doubts. 90% of received emails are addressed within 1-2 business days; 100% of questions are answered in 7 business days, except on specific year periods (e.g. Christmas).



Contacto

Puede enviar un mensaje usando el formulario de contacto de abajo.

Tu nombre: *

Tu dirección de correo electrónico: *

Asunto: *

Mensaje: *

□ He leído y acepto el Aviso Legal *

Esta pregunta se hace para comprobar que es usted una persona real e impedir el envío automatizado de mensajes basura.

Elija el número más bajo de la siguiente serie: 19, 4, veinte, quince. : *

Enviar

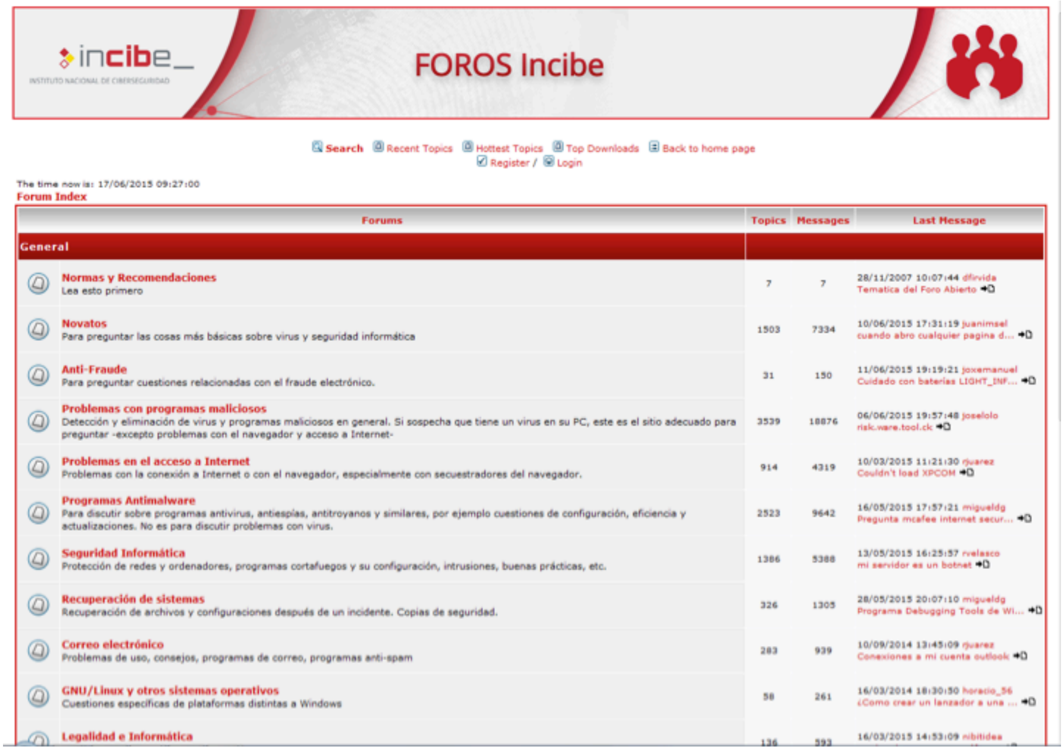
Figure 32: Contact Form on Website

6.7.3.1.3.2 Telephone Support

Users have a constant and direct contact to the Spanish NSC through the call centre service. It is a telephone number to report any security problems or put across doubts that are affecting users, which offering help and assistance with any necessary technical support. The contact telephone is available during working hours from Monday to Friday. It has two level of attention.

6.7.3.1.3.3 Forum

A forum is available for users to interact along its 14 different topics about cybersecurity. Almost 18.000 threats have been created and more than 73.000 messages have been posted. The forum counts with more than 16.100 users registered.



The time now is: 17/06/2015 09:27:00

Forum Index

Forums	Topics	Messages	Last Message
General			
Normas y Recomendaciones Lea esto primero	7	7	28/11/2007 10:07:44 dfirvida Tematica del Foro Abierto
Novatos Para preguntar las cosas más básicas sobre virus y seguridad informática	1503	7334	10/06/2015 17:31:19 juanimsel cuando abro cualquier pagina d...
Anti-Fraude Para preguntar cuestiones relacionadas con el fraude electrónico.	31	150	11/06/2015 19:19:21 joxemanuel Cuidado con baterias LIGHT_INF...
Problemas con programas maliciosos Detección y eliminación de virus y programas maliciosos en general. Si sospecha que tiene un virus en su PC, este es el sitio adecuado para preguntar -excepto problemas con el navegador y acceso a Internet-	3539	18876	06/06/2015 19:57:48 joselolo risk.ware.tool.ck
Problemas en el acceso a Internet Problemas con la conexión a Internet o con el navegador, especialmente con secuestradores del navegador.	914	4319	10/03/2015 11:21:30 rjuarez Couldn't load XPCOM
Programas Antimalware Para discutir sobre programas antivirus, antiespías, antitroyanos y similares, por ejemplo cuestiones de configuración, eficiencia y actualizaciones. No es para discutir problemas con virus.	2523	9642	16/05/2015 17:57:21 migueldg Pregunta mcafee internet secur...
Seguridad Informática Protección de redes y ordenadores, programas cortafuegos y su configuración, intrusiones, buenas prácticas, etc.	1386	5388	13/05/2015 16:25:57 rvelasco mi servidor es un botnet
Recuperación de sistemas Recuperación de archivos y configuraciones después de un incidente. Copias de seguridad.	326	1305	28/05/2015 20:07:10 migueldg Programa Debugging Tools de Wi...
Correo electrónico Problemas de uso, consejos, programas de correo, programas anti-spam	283	939	10/09/2014 13:45:09 rjuarez Conexiones a mi cuenta outlook
GNU/Linux y otros sistemas operativos Cuestiones específicas de plataformas distintas a Windows	58	261	16/03/2014 18:30:50 horacio_56 ¿Como crear un lanzador a una ...
Legalidad e Informática	136	593	16/03/2015 14:53:09 nibitidea

Figure 33: INCIBE Support Forum

6.7.3.1.3.4 Social Media

Users can interact with the Spanish NSC, sharing their experiences and follow OSI on the main social networks.

- Facebook -> https://www.facebook.com/osiseguridad
- Twitter -> https://twitter.com/osiseguridad
- Youtube -> https://www.youtube.com/user/OSIseguridad
- Google + -> https://plus.google.com/100714825184222636522/posts
- Tuenti -> http://www.tuenti.com/piensoluegoclico

6.7.4 Infrastructure

Spanish NSC is based on Drupal technology. The Anti-Botnet Service has been developed under the following technologies:

- Frontend/Backend: HTML, CSS, Javascript, PHP
- Webservices: Java, Python
- Data base: MongoDB

A subcontract company, always under continuous support by INCIBE staff, attends the support call centre.

6.7.5 Statistics / Metrics

Some general statistics about the Spanish NSC referring visitor to the website, to the blog, and number of publications are shown in the following graphs.

The evolution of the number of page views, visits and visitors of the Spanish NSC since the launch of the Anti-Botnet Service is the following:

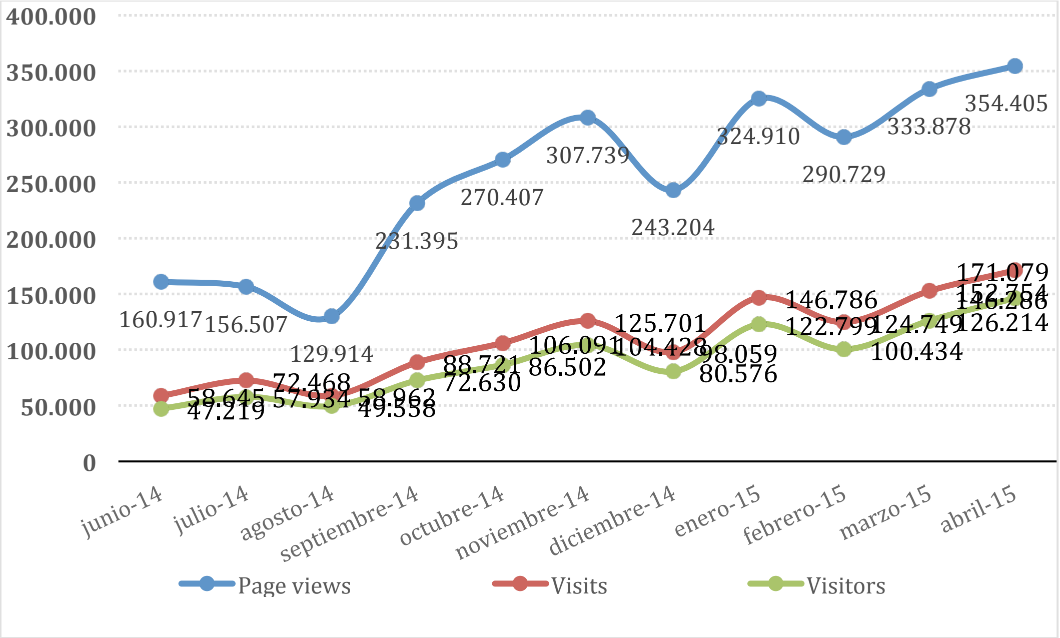


Figure 34: Visits and visitors Spanish NSC

The evolution of the visits to the blog of the Spanish NSC since the launch of the Anti-Botnet Service is the following:

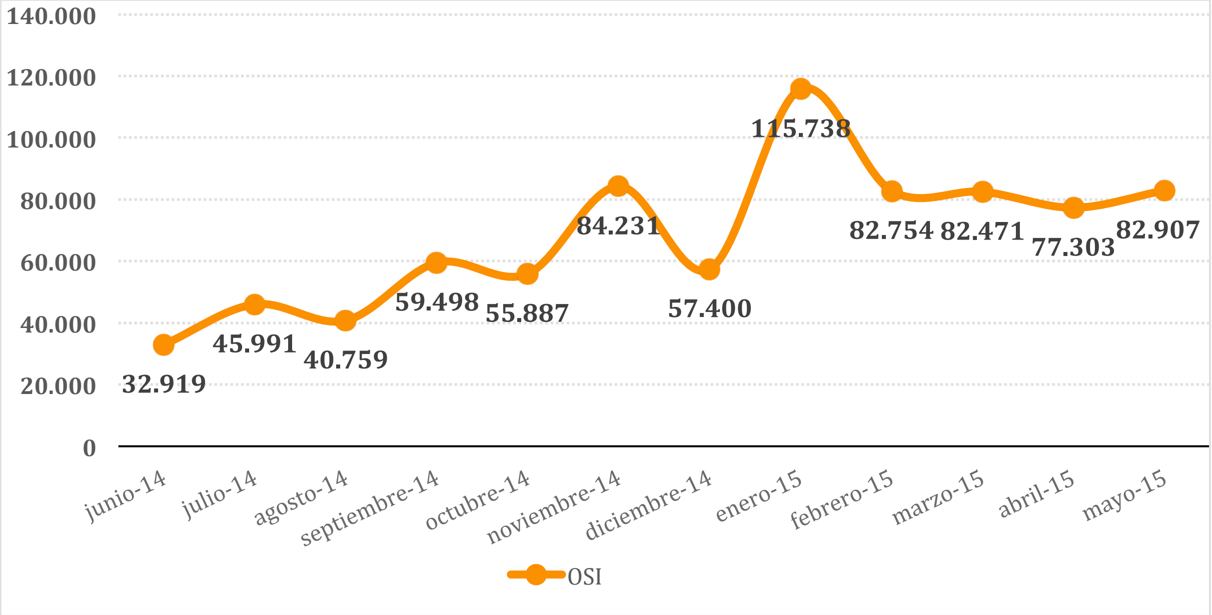


Figure 35: Visitors of the blog

Following it is shown the statistics about publications by type and years on the Spanish NSC.

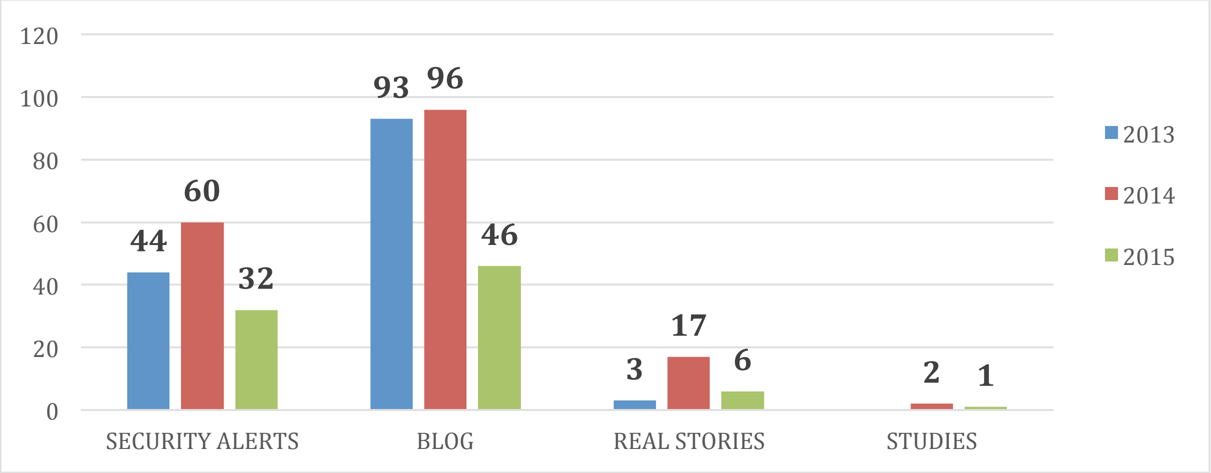


Figure 36: Publications by the Spanish NSC

About specific statistics of the Anti-Botnet Service, the main numbers are the following:

- The Spanish NSC has more than **5.000.000 reliable evidences** per day that affect more than **350.000 unique IP addresses** per day in Spain.
- Since the beginning of the Anti-Botnet Service in June 2014, the service has received more than **100.000 visits**. The service has been executed more than **50.000 times** through the online service, and more than **7.300 plugins** have been installed.
- Since the beginning of the pilot with the collaboration of Telefónica, middle of November, INCIBE has notified to Telefónica **957.470 unique IPs**. Telefónica has sent **82.400 notifications** to **16.627 different end-users**. An average of **6 notifications** have been sent to recurring clients, and each month 1**.450 new customers** are notified. More than **10.000 tickets** has been consulted on the website. Finally it has been determined that **44% of notified end-users would have been disinfected.**

The top 10 botnets detected by the Anti-Botnet Service are the following:

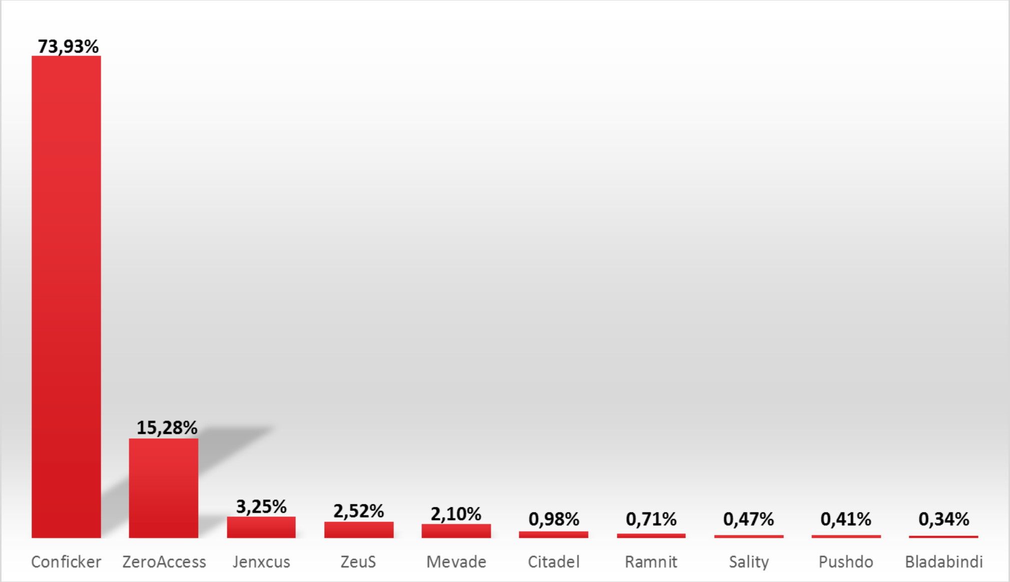


Figure 37: Botnets Statistics Spain

6.7.6 Privacy, Data Protection and Security

The terms of use of the Spanish NSC can be consulted on the website https://www.incibe.es/aviso_legal.

The terms of use and privacy of the Anti-Botnet Service must be accepted by the user before using it. The Service uses the public IP always with the explicit consent of the user in order to check it with the database of the service to be able to show the result. The public IP is not associated with any particular user and it is only stored for statistics purpose of the service.
INCIBE IT area is certified on Information Security Management System (ISMS) according to the UNE - ISO / IEC 27001: 2007. Therefore the Spanish NSC is compliant with all the security procedures and technical measures under the ISMS. The security is ensured by:

- Performing the process of risks analysis and management within our ISMS. Our strategic development process for cybersecurity technologies, including in the scope of the ISMS, is assessed annually at the stage of AGR under the MAGERIT methodology (using PILAR software), being evaluated the processes / services and systems that support them on the three dimensions of security.
- Conducting technical security audits of applications depending of the level of criticality, previously evaluated. The Spanish NSC has been audited.
- Compliance with safety requirements established under the procedure of developing and maintaining software applications, among which include: source code security requirements, secure development OWASP, internal processing control, security among controlled environments promotion processes, software quality, etc.

INCIBE has appointed a member of the Company Management Team as Head of Internal Security Management (RGI) who oversees it, ultimately, both corporate management for the protection of personal data as the maintenance and improvement of the Information Security Management System (ISMS) that has implemented and certified according to the UNE - ISO / IEC 27001: 2007. This role (the RGI) assumes among its main functions: a) contact with the national bodies for the protection of personal data (AEPD), b) proper maintenance and updating of the Security Document, c) the registration of files in the RGPD (Data Protection General Register), d) the supervision of the audit processes both in the field of personal data protection management as part of information security management, e) the supervision of the processes of risks analysis and risks management, f) the implementation and supervision of action plans or risk treatment, etc.

6.7.7 Contributions / interaction with ACDC

Both, Conan Mobile and the Anti-Botnet Service are services provided within the scope of ACDC project. One of the sources of the Anti-Botnet Service is the data provided to ACDC by other project partners. All bots received from ACDC are validated and then incorporated to the process of notification.

6.7.8 Dissemination

The Spanish NSC has made different campaigns of disseminations of its services CONAN Mobile, Anti-Botnet Service and ACDC, through different activities such posts in blogs, tweets, press release, articles in newspapers and promotional videos.

- Anti-Botnet Service promotional video: https://www.youtube.com/watch?v=C-rtCZamKH0
- CONAN Mobile promotional video: https://www.youtube.com/watch?v=6LxLb1tWW_o

As it was launched as a pilot, it is planned to design and execute a bigger diffusion of the Anti-Botnet Service.

6.7.9 Sustainability

The Spanish NSC will continue providing its services to end users in the same line the following years, working to reinforce confidence in the digital ecosystem under the Spanish Digital Agenda 2014-2015, but also in line with the goals of the Digital Agenda for Europe 2015-2020. After 2015, the Spanish government must detail the roadmap for the INCIBE's public services under the National Cybersecurity Strategy 2015-2017 and in line with the Agenda for Europe 2015-2020.

About the Anti-Botnet Service, it is planned to extend the collaboration and the incorporation to the notification process of other Spanish ISPs.

6.8 Romania

The Romanian National Support Centre is hosted and operated by the Romanian National Computer Security Incident Response Team – CERT-RO. The services of the Romanian NSC are offered through the website http://www.botfree.ro.

6.8.1 Workflow

All the data generated by the sensors within HoneyNetRo and the data collected via CCH are stored in a local database for further correlation and analysis. Further, all the reports are notified to the ISP's, which are instructed to notify the end users.

The notification is done through CERT-RO's ticketing system and contains information about the ACDC project and how the NSC and CERT-RO could be reached for further assistance.

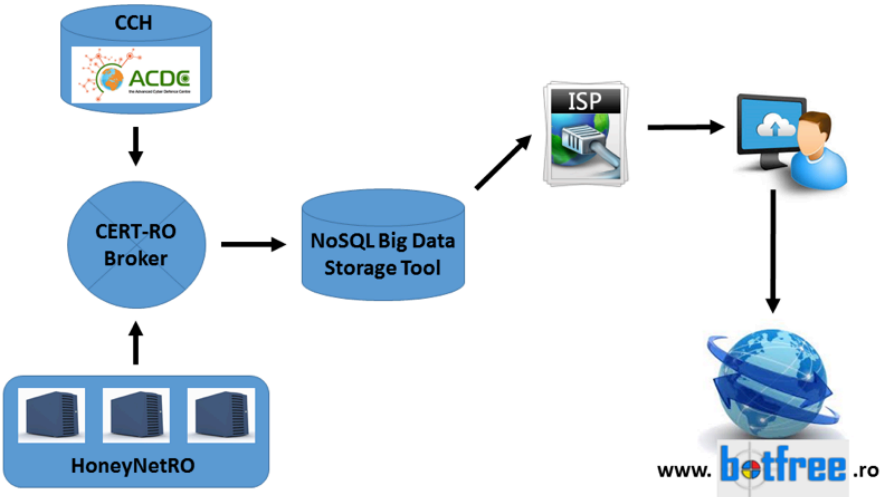


Figure 38: Workflow botfree.ro

6.8.2 Staff

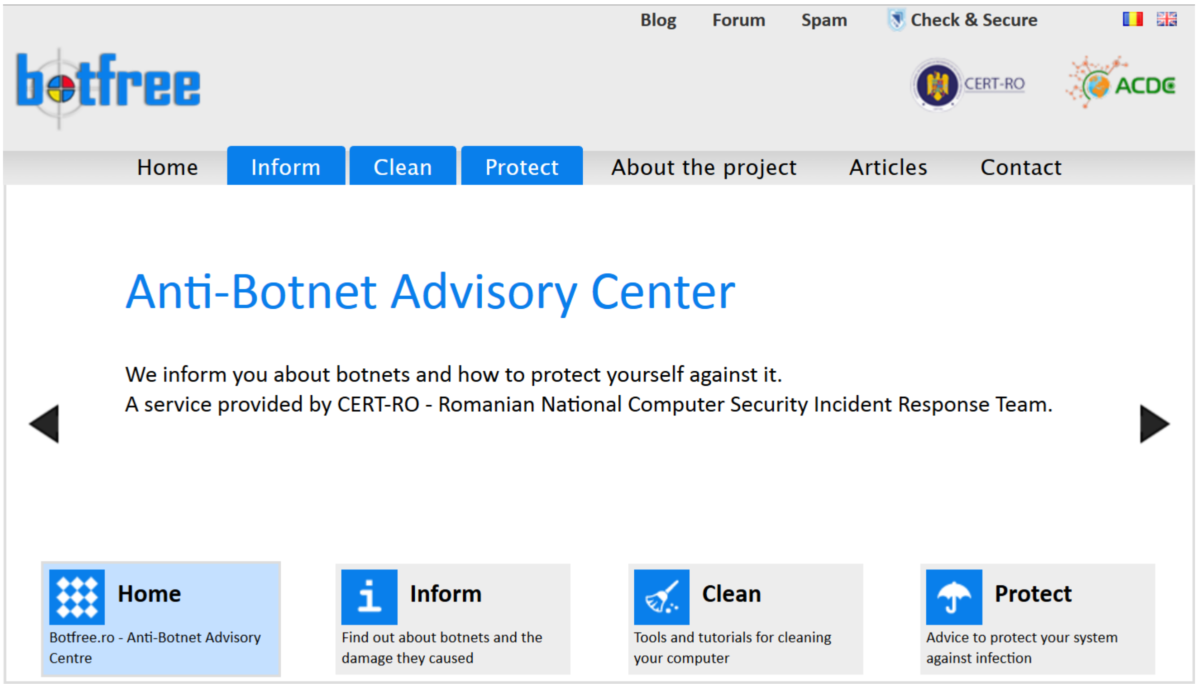
The Romanian NSC is operated by the CERT-RO's incident handling department formed by professional cyber security experts and incident response operators.

All the reports received through the Romanian NSC are managed accordingly to the already in-place incident response procedures used by CERT-RO.

6.8.3 Service Level

The services of the Romanian NSC are offered through a 2nd level support. This includes support via email and phone within normal business hours (08:00 – 17:00).

6.8.4 Website



Anti-Botnet Advisory Center

We inform you about botnets and how to protect yourself against it.
A service provided by CERT-RO - Romanian National Computer Security Incident Response Team.

Home Botfree.ro - Anti-Botnet Advisory Centre

Inform Find out about botnets and the damage they caused

Clean Tools and tutorials for cleaning your computer

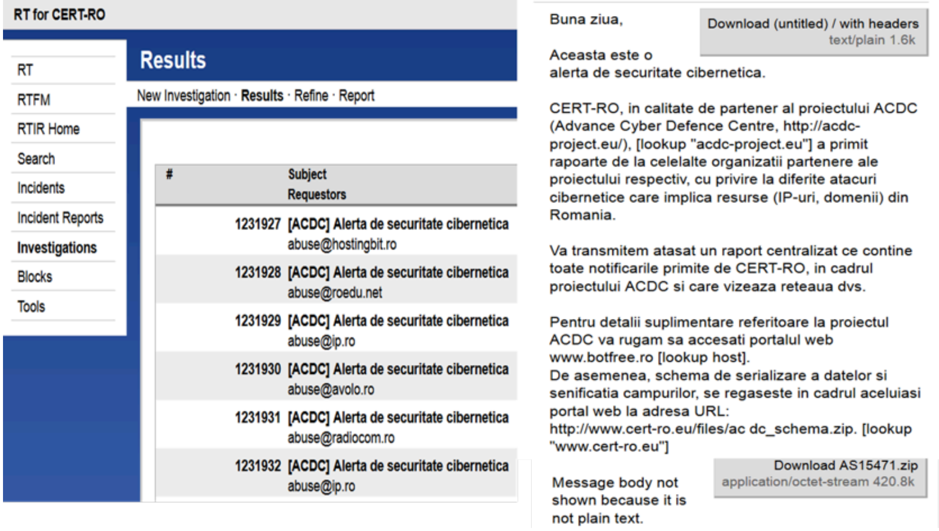
Protect Advice to protect your system against infection

Figure 39: Screenshot Botfree.ro

The website is available both in English and Romanian language.
The services are offered free of charge and they are organized in the main three sections of the web portal: Inform, Clean, Protect.
It also contains a section called “About the project” where visitors can find out more information about the ACDC project.

6.8.5 Contact and ticketing system

The contact section contains detailed information that can be used to contact the NSC staff, including email address, phone number and fax number.
All the reports collected from CCH and from HoneyNetRO sensors are sent to ISP’s through the ticketing system. Also, all the notifications sent by the NSC visitors are automatically imported to the ticketing system and are included in the normal incident response workflow.



#	Subject Requestors
1231927	[ACDC] Alerta de securitate cibernetica abuse@hostingbit.ro
1231928	[ACDC] Alerta de securitate cibernetica abuse@roedu.net
1231929	[ACDC] Alerta de securitate cibernetica abuse@ip.ro
1231930	[ACDC] Alerta de securitate cibernetica abuse@avolo.ro
1231931	[ACDC] Alerta de securitate cibernetica abuse@radiocom.ro
1231932	[ACDC] Alerta de securitate cibernetica abuse@ip.ro

Download (untitled) / with headers
text/plain 1.6k

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/), [lookup "acdc-project.eu"] a primit rapoarte de la celelalte organizatii partenere ale proiectului respectiv, cu privire la diferite atacuri cibernetice care implica resurse (IP-uri, domenii) din Romania.

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 [lookup host].
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/ac dc_schema.zip. [lookup "www.cert-ro.eu"]

Message body not shown because it is not plain text.

Download AS15471.zip
application/octet-stream 420.8k

Figure 40: Ticketing System Romania

6.8.6 Mitigation Services

Two EU-Cleaners have been made available to the Romanian NSC with friendly support from the partners Avira and SurfRight. These cleaners are no full Anti-Virus Products as they are just dedicated to remove Malware from customer PCs. Both tools are free of charge and can be obtained from:

- http://botfree.ro/download/avira-eu-cleaner.exe
- http://botfree.ro/download/hitmanpro_x64.exe.

6.8.7 Online scanners

The Check-and-Secure service is a free online tool provided by cyscon GmbH and Vodafone. Based on the results of the scan the end user is conducted through a variety of checks step by step.

Figure 41: Romanian Online-Services

Additionally, a selection of three online scanners that are free of charge are recommended:

- Bitdefender Online Scanner - http://www.bitdefender.ro/scanner/online/free.html
- F-Secure Online Scanner - http://www.f-secure.com/en/web/home_global/online-scanner
- Panda Online Scanner - http://www.pandasecurity.com/activescan/index/

6.8.8 Privacy, Data Protection and Security

CERT-RO does not store any personal data related to the infected end users, while information related to the users affected systems and correspondence is stored on a storage capability, which is only accessible from internal network.

The NSC portal is protected by a hardware web application firewall (WAF) and is constantly scanned with CERT-RO's commercial and open source vulnerability scanners.

6.8.9 Dissemination

The Romanian National Support Centre is constantly advertised through different means, including social networks, national and international conferences and a visible link on the CERT-RO's website.

6.8.10 Sustainability

CERT-RO plans to further support and develop the Romanian National Support Centre which is already a part of the CERT-RO's services offered to the national constituency.

6.9 Additional ACDC Support Centers

The following support centres have been established outside of ACDC and are not directly associated to the ACDC project. No funding or resources out of the ACDC project budget have been allocated into the setup of these support centres.

6.9.1 Luxembourg

The National Anti-Botnet Support Centre in Luxembourg is located at Botfree.lu and available in English language. The initiative is hosted by the Computer Incident Response Center Luxembourg (CIRCL) and is operated in collaboration with BEE SECURE (https://www.bee-secure.lu) and SMILE (https://securitymadein.lu). Both websites have similar goals as the ACDC project, but at a national level.

The Botfree.lu website provides minimal services on the website itself, as the two associated partner organisation already provide a large set of similar services like for example the German or Spanish National Support Centre. The contribution of Luxembourg to the ACDC support centre network has been setup without any financial contributions out of the ACDC funding.

Laudable in this context is the dedication from project partner University of Luxembourg to establish the liaison with these organisations and the provisions of this additional NSC.

Botfree.lu - Luxembourg anti-botnet support - ACDC Luxembourg support center

Botfree.lu - Luxembourg anti-botnet support - ACDC Luxembourg support center

Infected systems are often part of a botnet which can be controlled remotely by attackers to perform criminal activities like attacking other computers, sending malicious emails or performing denial-of-service attack.

Botfree.lu - Luxembourg anti-botnet support - ACDC Luxembourg support center

Botfree.lu - Luxembourg anti-botnet support - ACDC Luxembourg support center

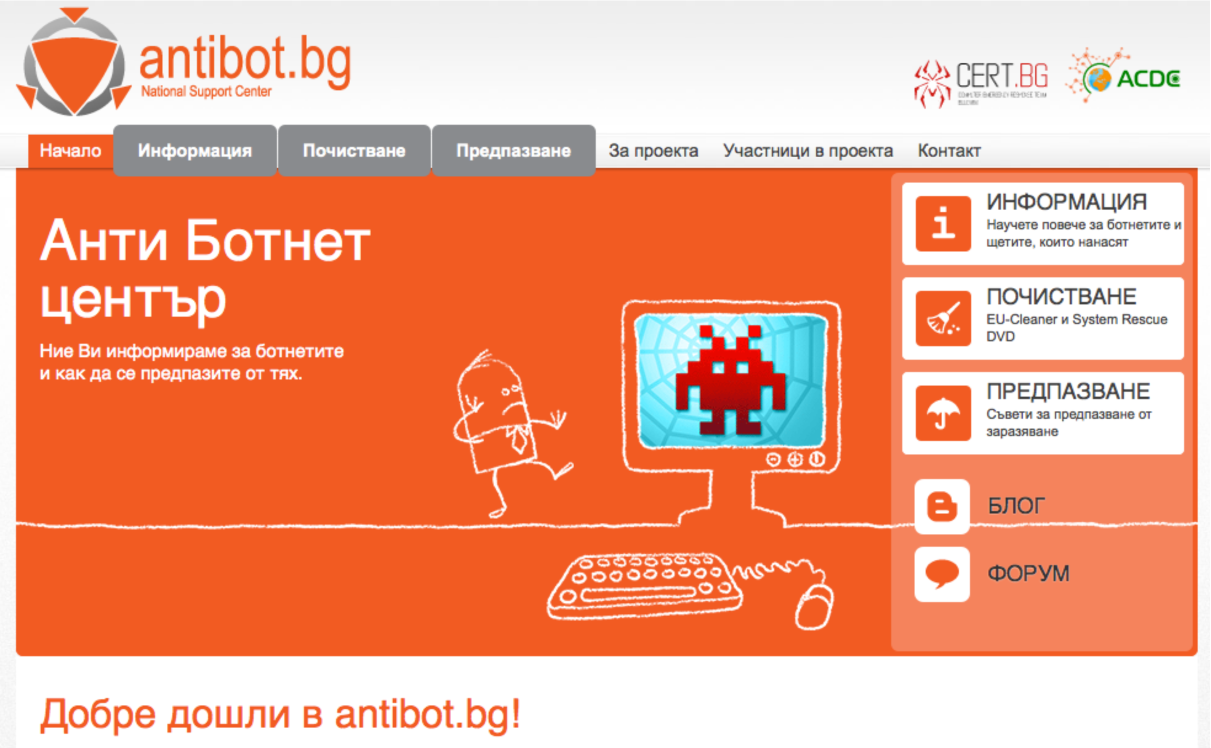
Figure 42: Botfree.lu

6.9.2 Bulgaria

The National Anti-Botnet Support Centre in Bulgaria is located at Antibot.bg and currently available in Bulgarian only. The initiative is hosted and operated by the Bulgarian CERT (cert.bg). The website is a translation and customization of the German ABBZ website, project partner ECO supported the Bulgarian CERT in setting up this service. The Bulgarian CERT is currently working with several National Internet Service Providers in establishing processes and services similar to Germany, involving and notifying end-users and SME's.

The contribution of Bulgaria to the ACDC support centre network has been setup without any financial contributions out of the ACDC funding.

Laudable in this context is also the dedication from project partner Bulgarian Post (BG Post) to establish the liaison with the national CERT and the voluntary provision of this additional NSC.



antibot.bg
National Support Center

CERT.BG ACDC

Начало Информация Почистване Предпазване За проекта Участници в проекта Контакт

Анти Ботнет център

Ние Ви информираме за ботнетите и как да се предпазите от тях.

ИНФОРМАЦИЯ
Научете повече за ботнетите и щетите, които нанасят

ПОЧИСТВАНЕ
EU-Cleaner и System Rescue DVD

ПРЕДПАЗВАНЕ
Съвети за предпазване от заразяване

БЛОГ

ФОРУМ

Добре дошли в antibot.bg!

Figure 43: Antibot.bg

7 Botfree.eu

The central website Botfree.eu is a basic and static landing page, directing users to their national support centre. The website only displays a map with the participating countries and lists and links the operating partner organisation.

The website includes the mandatory imprint, data privacy statement and the terms of use, besides basic information and technical backgrounds of the ACDC project.

This minimal service of Botfree.eu has been a result of two different strategic decisions.

With support of the work started in WP5 on exploitation and sustainability, the majority of the national support centre operators stated in a survey in November 2014, that they prefer a basic website on Botfree.eu only.

This statement has been made due to the intents keeping the national support centres independent and each responsible for own dissemination, mitigation and outreach activities.

Additionally, the NSC operators consider the Botfree.eu website being owned and operated by the planned European Anti-Botnet Support Centre Alliance (EABSCA). Its future purpose should be an information page for the alliance and the participating partners, but not direct or indirect end-user support centre.

The second decision on reducing the initially provided information has been driven by the decision to direct more users to their national support centre and interested project stakeholders to the actual project website or even the animation joining the ACDC service through a registration to the community portal. Therefore, links have been set accordingly and content transferred. During the project, the website has been maintained and designed by eco.

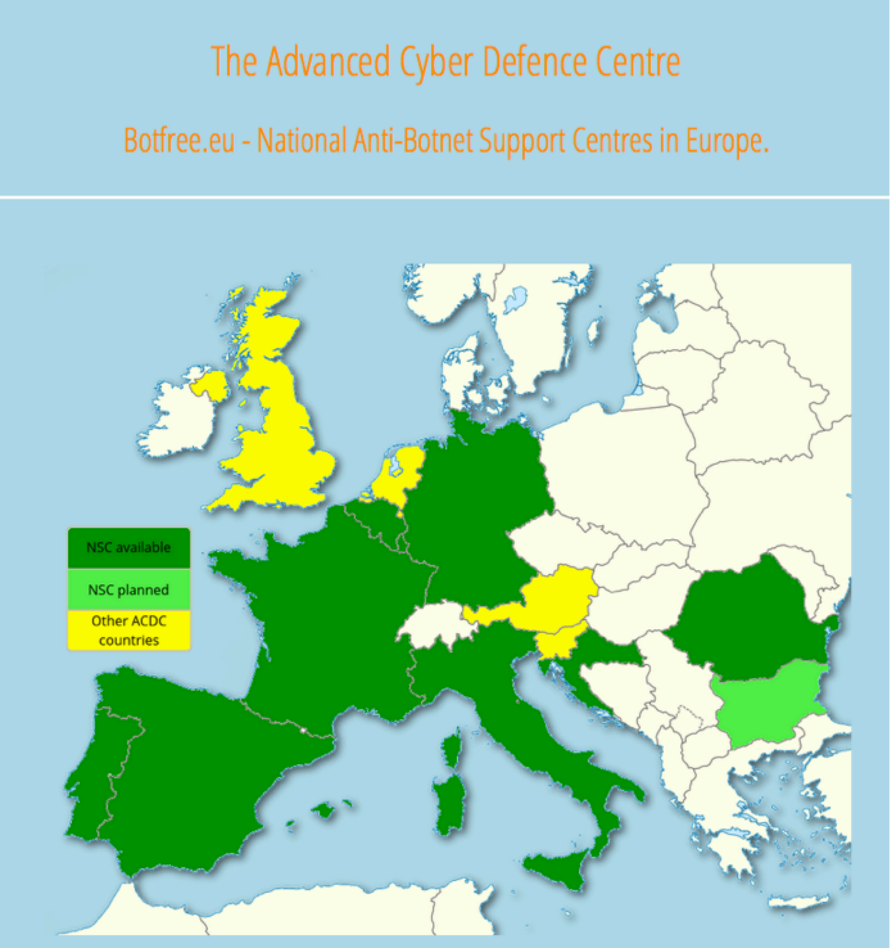

The Advanced Cyber Defence Centre
Botfree.eu - National Anti-Botnet Support Centres in Europe.
NSC available
NSC planned
Other ACDC countries

Figure 44: Botfree.eu

8 Sustainability

The sustainability plan for the ACDC project suggests an own entity for the National Support Centres. This European Anti-Botnet Support Centre Alliance (EABSCA) should be established as a non-profit initiative and its goal is become a coordinating entity for and to the operators of the NSCs.
Besides exchanging knowledge, experience and expertise, the new association should also act as a point of contact for organisations at a European or international level, including ENISA, EUROPOL, CERTs, ISACs or the European Commission.
The Network of National Support Centres should act as a relay point for mitigation campaigns related to Botnet takedowns or for joint awareness campaigns like the Internet Safety Day.
The network should be reaching out to the industry, e.g. to get to new end-user tools like EU-Cleaners.
Also, this network will have the goal to get a member-or partnership with at least one organisation in each state of the European Union, but also beyond. First cooperation with similar projects in Japan, South Korea and Australia has been initialized during the project span and the long term plans might even drive this into the direction of a global alliance. There are several initiatives around the world and the EABSCA could become a relay point of the usage of these global synergies.

Further details on the sustainability plan and the future plans for the Network of National Anti-Botnet Support Centres are described in the second chapter of “Deliverable D5.3 – Sustainability Plan.”