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

Deliverable:	**D1.6.2 Specification: End Customers Reporting Tools**
Work package	WP1 Requirements & Specification
Due date	M30
Submission date	31/07/2015
Revision	V 2.0 | 2015.07.07
Status of revision	
Responsible partner	Signal Spam
Contributors	FCT-FCCN (Reviewer)
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	01/02/2013

Introduction

This document aims at providing requirements for end customer spam and online abuses reporting tools, usable for Work package 2 (WP2) during the process of choosing solutions and technologies to actually develop those tools.

Spam and online abuses reports can provide useful data regarding botnets identification and infected devices. As some countries may already have a national spam reporting centre or equivalent organisation, we recommend ACDC work with these in order to retrieve the intelligence and offers them the opportunity to equip themselves with the tools they are lacking to cover all threats reports possibilities.

Content

Tables

Figures

1. General requirements

In the following we have identified some requirements for the end customers reporting tools, defined as general as they can be applicable to all the type of tool categories.

Part of the requirements is related to the tool design in term of usability, compatibility and so on.

Other requirements are related to the design of the tool with respect to the users' privacy and compliance to the relevant privacy regulations, in part taken from the set of universal Mobile Privacy Principles published in January 2011 by the GSMA. This set describes the way in which mobile consumers' privacy should be respected and protected when they use mobile applications and services that access, collect and use personal information [http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples2012.pdf]. In addition, the GSMA has released a set of Privacy Design Guidelines for Mobile Application Development intended to help drive a more consistent approach to user privacy across mobile platforms, applications and devices fostering the development of a common set of functional requirements. That guidelines have also the intent to enable mobile users to benefit from a consistent functional treatment of their privacy across platforms and devices, strengthen their awareness and help them make decisions relevant to their interests.

The term personal information has been used in the following requirements to include (but not limited to) the information related to a user and their use of services and information which may be considered private by users even though it may not be strictly protected in law. Some example are data that is collected directly from a user (e.g. entered by the user via an application's user interface and which may include name and address, credit card details), any data about a user that is gathered indirectly (e.g. mobile phone number, email address, name, location data, IP address, unique phone ID, and so on), any data about a user's behaviour (e.g. location data, service and product use data, website visits), any user-generated data held on a user's device (logs, messages, user-generated images, contact lists or address books, notes, and security credentials).

G1.The tool shall be installed in an easy way. It shall ensure usability and avoid excessive user prompts that will burden the user. It shall take in consideration the user experience.

G2.For each operating system, the tool shall respect standard installation procedures (certified applications for Microsoft, App Store, or RPM Linux).

G3.When installed the tool shall not degrade the end-user terminal's performance

G4.The tool shall be "universal" that means shall be adaptable for example to the different web browsers, mail clients and so on. It may be necessary to adjust the tools to the various environments, for instance different e-mail client software or internet browsers.

G5.The tool shall have an easy (user-friendly) and configurable GUI (Graphical User Interface).

G6.The information collected by the tool shall be transferred to the remote server (such as the clearinghouse) in a protected way, such as using a TLS connection. Personal data collect will be submitted to exhaustive terms of use in compliance with European Data Protection Policy related to tackling cyber threat issues. The tool shall keep data secure. The tool shall take appropriate steps to protect users' personal information from unauthorised disclosure or access. It shall adopt technical

measures to prevent the misuse or corruption of personal information. Where the application or tool creates or collects personal information considered sensitive, such information must be stored and transmitted in a secure manner.

G7.The tool must provide the users with the information about who is collecting or using their personal information. Before the download or tool activation, the user must be made aware of the identity of any entities that will collect or use personal information in the scope of the tool and their data privacy practices. The tool shall have to explicitly declare its purpose and use. The access, collection, sharing, disclosure and further use of the collected users' information shall be limited to meeting legitimate purposes (such as ACDC purpose). To comply with this requirement, the tool shall provide the users with information about the collection and use of their personal information upfront (purposes of the ACDC reporting tool or application), enabling them to make informed decisions about using the application or tool. Before the tool download or activation, the user must be presented with information about what personal information the tool will access, collect and use, what personal information will be stored (on the device and remotely), what personal information will be shared, with whom and for what purpose. Finally any terms and conditions of use affecting a user's privacy shall be given. The tool shall enable the user to reject the installation or activation if they do not wish their personal information to be used as explained to them

G8.The tool must be designed to permit user choice and control. Users shall be given opportunities to exercise meaningful choice, and control over the collected data.

G9.Data Minimisation and Retention. Information collected by the tool or application must be reasonable, not excessive, so as to not frighten end user, and used within the scope of the user's expectations and the legitimate purposes as notified to users. Only the minimum information necessary to meet legitimate purposes (such as the purpose defined within the ACDC) and to deliver, provision, maintain or develop services (such as the malware monitoring and mitigation service), should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.

G10.The tool must gain the user's active consent when necessary. In the majority of cases, it will be obvious to users what personal information will be needed to support an application. However, where access, collection and use of personal data is not necessary to the application's primary purpose and would be unexpected by the user, then users should be given a choice about whether to allow these secondary and non-obvious uses of their information.

G11.The tool must respect User Rights. Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.

G12.The tool must be secure by design. Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.

G13.Users must be provided with information about privacy and security issues and ways to manage and protect their privacy.

2. Web Browser Reporting Plugin

This kind of tool is intended to be a "universal plugin", capable of extracting data from html source codes. It could be used to report spam on webmail's (for this we would need to have in depth knowledge of the biggest webmail's around) or malicious/infectious websites.

2.1.Context

Identifying spambots is a key part of end users involvement in tackling botnet issues. To complete the reporting frame, end users must be able to report abuses, spam or malicious website through their web browser. It will be up to national spam reporting centres to qualify and to send to ACDC spambot reports.

2.2.Survey

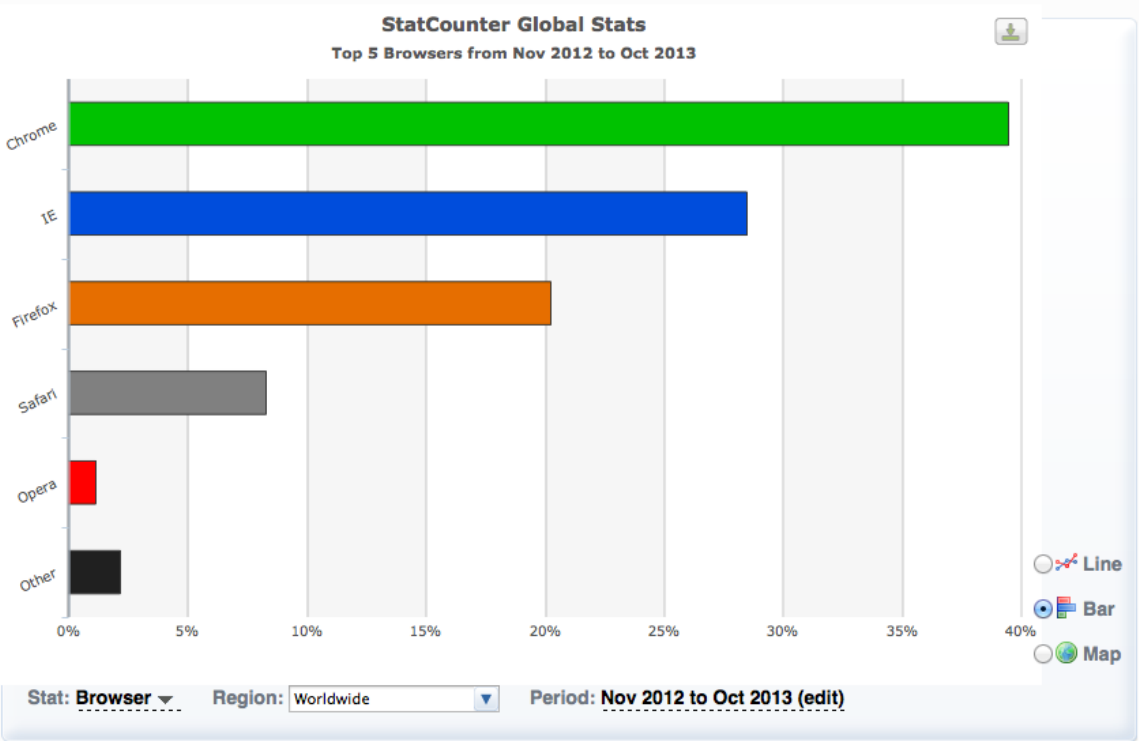


Figure 1 – Most used web browser

2.3. Web Browser Plugin Requirements

WBPR 1 : Versions	Each web browser should have its own version of the plugin. In case of too many incompatible versions of the same web browser, various plugins for the same web browser must be considered.
WBPR 2 : Web browser implementation	The plugin must be easily incorporated in a web browser, accessible to end user through a simple button that will launch the whole script.
WBPR 3 : Link through API connection	The plugin will link with ACDC (or the national relays) through an API connection.

WBPR 4 : Authentication	During installation, the plugin must ask the end user to authenticate himself in order to link the plugin button with its ACDC profile, and store this data in order not to ask the end user for it again. If the end user has no profile, the plugin must offer the possibility to create it.
WBPR 5 : Network connection through proxy	When the plugin is installed on all computers of a company, the plugin must allow a connection to the network through a proxy and authorized proxy.
WBPR 6 : Network cut-off	Should a network cut-off occur, the plugin must still function and keep reports waiting to be process in a queue without affecting overall performances of the Web Browser. When network connection is re-established, the plugin must ensure reports are normally delivered to the spam reporting centre.
WBPR 7 : Content of reports	The plugin must transmit the full report without altering its content, i.e. html source code, full header of spam and raw content.
WBPR 8 : html reports	When reporting a malicious website, the plugin must send the source code and the URL.
WBPR 9 : Webmail reports	When reporting a spam on a webmail, the plugin must activate a script enabling viewing of the source code inside the webmail interface, retrieve it, and send it to the ACDC (or its national relay).
WBPR 8 : Notification	Once the plugin has transmitted the report, it should notify the end user that its report was correctly made and transmitted to ACDC.
WBPR 9 : Intelligence & qualification	Data processing requires intelligence in order to detect the category of the report. The plugin itself must be able to determine the content of the report whether it is illegal content on a web page, or an e-mail viewed on a webmail.
WBPR 10 : Scripts & knowledge of webmails	In case of a spam report, the plugin must be familiar with the top used webmail in order to be able to launch a specific script that will extract the source code and the full header. *We recommend conducting a survey to determine in each country which e-mail domains are the most used, aside Outlook (and all other Microsoft messaging related domains), Yahoo, AOL and Gmail which the most used worldwide : the plugin button will have to be able to launch a specific script for each of those.*

Table 1- Web Browser Plugin Requirements

3. E-mail Clients Reporting Plugins

3.1.Context

This set of tools is designed for end users using a desktop e-mail client to read their e-mails. The plugins described below aim at adding a new functionality in the software, enabling end users to report their spam (full source, header and body) in an one-click easy and convenient way.

3.2. Survey

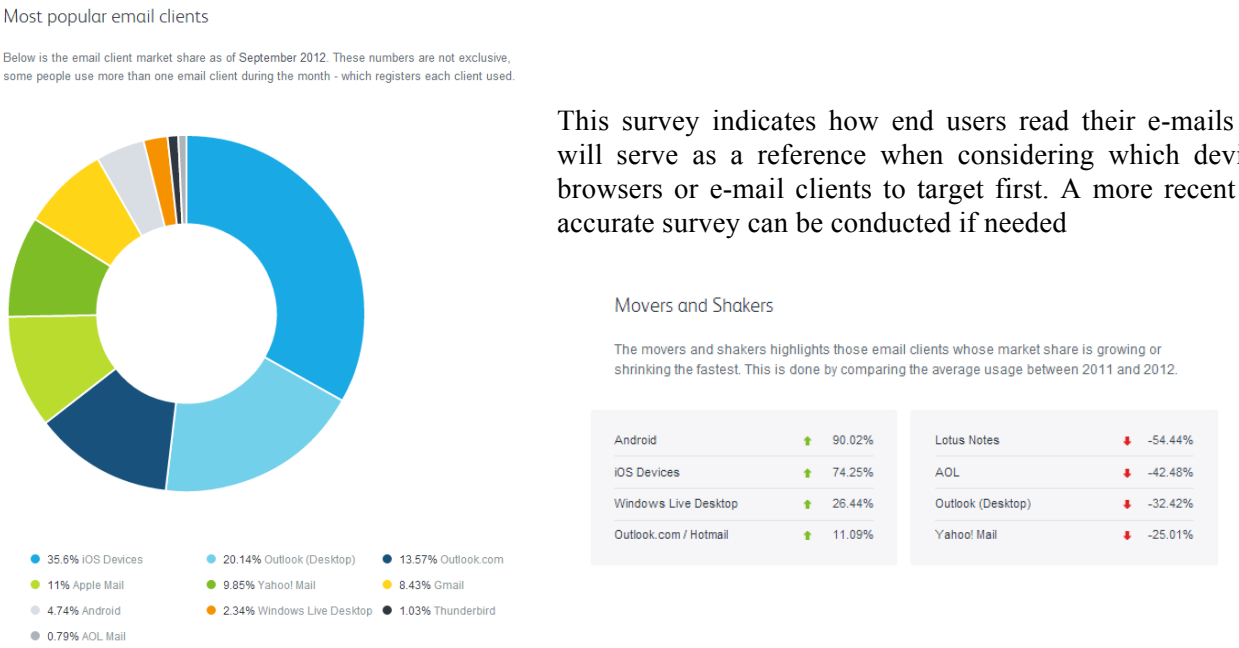
Within the Advanced Cyber-Defence Centre activity, Internet's Users must be able to report spam they receive to a central clearing house in order to identify IP addresses that may be corrupted sending spam. To do so, in addition to a general web form on ACDC website, e-mail client plugins are needed to report spam in a convenient and user-friendly way.

To establish a list of priorities, we recommend benchmarking the most used e-mail software.

From the survey above, it appears the most used desktop e-mail clients are:

1. Outlook (2003, 2007, 2010, 2013): 20,14%
2. Apple Mail: 11%
3. Windows Live: 2,34%
4. Thunderbird: 1,03% (Operating Systems: Windows, Mac OS X, Linux)

Additional desktop e-mail client to take in consideration: Outlook Express, Lotus Notes.



This survey indicates how end users read their e-mails and will serve as a reference when considering which devices, browsers or e-mail clients to target first. A more recent and accurate survey can be conducted if needed

Figure 2 – Most popular e-mail clients and trends

Email Client	Popularity
iOS Devices	35.60%
iPhone	25.05%
iPad	9.74%
iPod Touch	0.81%
Microsoft Outlook	20.14%
Outlook 2000, 2003, Express	7.68%
Outlook 2007	6.51%
Outlook 2010	5.96%
Outlook.com	13.57%
Apple Mail	11%
Apple Mail 5	4.31%
Apple Mail 4	3.75%
Apple Mail 6	1.70%
Apple Mail 3	1.04%
Apple Mail 2	0.20%
Yahoo! Mail	9.85%
Gmail	8.43%
Android	4.74%
Windows Live Desktop	2.34%
Thunderbird	1.03%
AOL	0.91%
AOL Mail	0.79%
AOL Desktop 9.1	0.12%
Sparrow	0.19%
Windows Phone 7	0.14%
Lotus Notes 6 & 7	0.07%
Blackberry	0.05%
Excite	0.02%
Palm WebOS	0.01%
Entourage 2004	0.01%
Unable to detect email client	10.25%

Table 2 - Sources: E-mail Client Popularity (2012)*1*

[1] http://www.campaignmonitor.com/resources/will-it-work/email-clients/

3.3. E-Mail Clients Reporting Plugin Requirements

The concept is to develop a plugin for desktop e-mail software.

ECRPR 1 : Easy Installation	The plugin should be easy to install on the end user's desktop e-mail software.
ECRPR 2 : Multi-reporting	End users must be able to select one or several e-mails they want to report to ACDC's spam reporting centre (or national relays).
ECRPR 3 : Background treatment	When reporting e-mails, desktop e-mail software must not be slowed by the process. We recommend a background treatment.
ECRPR 4 : Authorized proxy connection	When desktop e-mail software is installed on all computers of a company, the plugin must allow a connexion to the network through a proxy and authorized proxy.
ECRPR 5 : Authentication	When configuring the plugin, end users must have the possibility to authenticate themselves (linking their account to the spam reporting centre). Authentication data must be stored and used when starting the desktop e-mail software.
ECRPR 6 : Anonymous reports	The plugin must also give the possibility to the end user to report its e-mails anonymously (although this will undermine the quality of the report).
ECRPR 7 : Network cut-off	Should a network cut-off occur, the plugin must still function and keep reports waiting to be process in a queue without affecting overall performances of the desktop e-mail client. When network connexion is re-established, the plugin must ensure reports are normally delivered to the spam reporting centre.
ECRPR 8 : Full transmission	The plugin should at all times transfer the full reported message without alteration regarding the header and the body.
ECRPR 9 : Move to different folder	Once undesired e-mails have been reported, the plugin should remove the messages to the "undesired messages folder" or "spam folder".
ECRPR 10 : Secured connection	The connexion between the plugin and the spam reporting centre should be secured, using https protocol.

Table 3- E-Mail Clients Reporting Plugin Requirements

Note : Signal Spam can provide spam reporting plugins for Thunderbird, Outlook, and Live Mail.

4. Mobile Devices Reporting Plugins

4.1. Context

Identifying spambots is a key part of end users involvement in tackling botnet issues. To complete the reporting frame, end users must be able to report spam on their mobile devices through mobile apps. It will be up to national spam reporting centres to qualify and to send to ACDC spambot and botnet related reports.

4.2. Survey

Most popular operating systems are Android, iOS and Windows 8. Developments must take into account the compatibility with different versions of the operating systems on the different devises available. The survey conducted in 3.2 in also relevant.

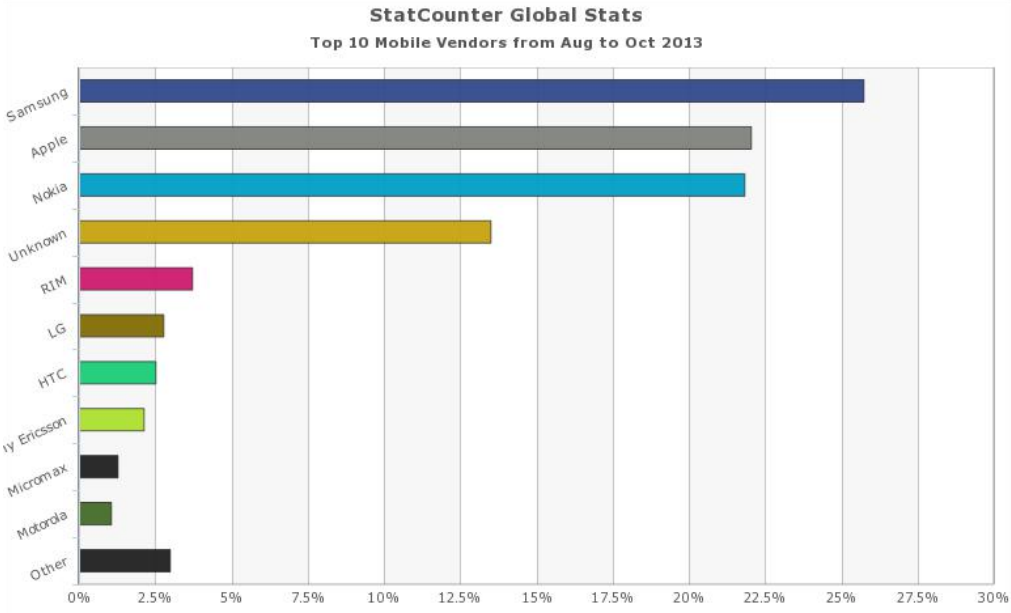


Figure 3 – Top mobile vendors

4.3. Mobile Devices Spam Reporting App Requirements

MDRAR 1 : Autonomous App	The application must be able to function autonomously.
MDRAR 2 : Authentication	The application must allow end user to authenticate himself to the centralized system such as the mobile botnet sensor.
MDRAR 3 : Reporting	The application must allow end user do report one or several e-mails or malicious websites.
MDRAR 4 : Link with messaging system	The application must link with the e-mail account of the end user in order to allow him to scroll his e-mails and report one or several of them.
MDRAR 5 : Report processing 1	The application must transmit reported e-mails without alteration, that is to say full message including full header and raw content.
MDRAR 6 : Report processing 2	Once an e-mail has been reported, the application must move the e-mail into the trash folder of the e-mail account.

Table 4 - Mobile Devices Spam Reporting App Requirements

4.4.Thoughts on closed mobile operating systems

Some operating systems are known to be closed to application modifying their key features.

For these systems, ACDC could provide a dedicated IMAP folder in which end user could drop their malicious spam.

The various messaging clients on mobile devices include this feature. It would be fairly easy for end users to configure a new IMAP account in order to push malicious e-mails in it.

Although this method would target knowledgeable end users, it would ensure a solution for all mobile operating systems.

4.5.Mobile Devices Anomaly Reporting App Requirements

The main goals of this tool/app is to detect any anomalies happening on the mobile device and send the collected data to the centralized ACDC component (e.g. the mobile botnet sensors) for further investigation and deep analysis. The idea is to have the detection algorithms running remotely and centralized in order to limit resource consumption on the mobile device leaving to them only the monitoring and reporting capacity of any detected anomalous behaviour.

MDARAR 1 : monitoring and detection functionality	The tool/app should be able to detect any anomalies happening on the mobile device using the data gaining from the device (anomaly detector) and/or malware signatures (misuse detector). To achieve this object the app/tool should be able to extract any usable information (such as device information, battery level, installed applications list, application logs, system calls invoked by the mobile application, result of monitoring applications,…) from the mobile device. The app/tool should be provisioned also with the malware signatures (e.g. from a centralized ACDC system). The app/tool upon detection of an anomaly, should report it to the user and send the collected data to the centralized system (e.g. to the mobile botnet sensors for further investigation). The module should run on various end-user devices (e.g. smartphones, tablets) and various OSs (e.g. Android, iOS).
MDARAR 2: light-weight detection module	The app/tool should provide "light-weight detection" functionality to limit computational power and energy sources on the mobile devices. That is the module should collect and examine a wide range of system events (such as, for example, Telephony module events, network events, i/o events, etc.) and anomalies in user/device behaviour that will be potentially useful to a centralized system (e.g. the mobile botnet sensors) to detect unknown threats. This provides functionality for on-device light-weight

	detection by running the detection algorithms (resource exhaustive) remotely in the centralized system.
MDARAR 3 : low impact on performance	The app/tool should have a low impact on the end-user device performance (e.g. battery life, processing power) caused by the anomaly detection engine.
MDARAR 4 : reporting functionality	The app/tool should report the collected data to a centralized system (could be the mobile botnet sensor) where the most algorithms are running for analyzing these features in order to avoid resource exhaustion on the mobile device and to improve the efficiency. Also the app/tool should provide to the user the option to upload a suspicious mobile application to the centralized system (could be the mobile botnet sensor) for further investigation.
MDARAR 5 : limited exchange of traffic	The tool/app should be able to limit the info exchange (e.g. short log files) to the minimum useful and should prefer the network connections available with minimum charging implications on the user (e.g. automatic log file upload via WiFi could be foreseen).
MDARAR 6 : API communication to ACDC infrastructure	The app/tool should provide the necessary API to connect to the centralised system (e.g. the mobile botnet sensors).
MDARAR 7 : custom configuration	The tool/app should be custom's configurable giving the user the ability to choose the running mode of the app/tool (e.g. only an event's notification, a notification and dis-installation of suspicious applications that have infected the device…). In addition the app/tool should give the user the ability to decide if to be always notified (e.g. on the light-weight detection module behaviour in terms of the event detection, the data sent to the centralized system, etc.) or to be completely unaware.
MDARAR 8 : robuste and trust	The lightweight malware detection module should be reliable and robust to reduce the vulnerabilities to attacks and thus preventing as much as possible its circumvention by malicious applications.

MDARAR 9 : notification	The app/tool should alert the user upon detection of an anomalous event on the user device or in case of an attack detected from the device. When detected, the user can send the logs to the mobile botnet sensor. The app/tool should also provide the functionality to notify the user in case where an uploaded suspected application is detected as malicious by the centralized system (e.g the mobile botnet sensors) so that a countermeasure can be performed.

Table 5 - Mobile Devices Anomaly Reporting App Requirements

5. End-user Data Collection Tool

5.1. Context

Any tool that could allow sharing knowledge of infections by malwares can enter the scope of reporting tools.

For instance, if an end user runs a scan on his device, whether through a security vendor, his ISP, or a mobile security check application, the information should be shared with ACDC. This might not be an end user tool per se, as it involves third parties in the process of retrieving data.

This tool is intended to be a collector of various information retrieved from the terminal that can be associated to suspected activity such as: potential malware samples loaded into memory, enumerates recent system changes, reports basic system configuration, exposes possible backdoors, acquires text copies of all system logs and registry settings, maps all open ports to the processes connected to them, scans for known malware, and captures packets from the IP stack.

5.2. End-User Data Collection Tool Requirements

CTR1. Fully Modular Design	Allows for development of new information gathering methods. Can be custom tailored to any environment
CTR2. Easy and configurable GUI (Graphical User Interface)	The user must have the possibility to configure the types of information they consent to be collected, to enable/disable the automatic uploading of the reports, to select the running modules (fast scan or slow scan) and other similar options.
CTR3. Compressed report transferring	The collected results shall be compressed to reduce transfer times. The compressed file should be password protected with a unique user password.
CTR4. User explicit consent for the reports uploaded to the clearing house	The consent must be given at the installation time or each time the reports are downloaded (the first approach is better)
CTR5. Automatic-upload of the reports to the clearing house repository	When the user consent has been obtained the collected reports shall be automatically sent to the central repository clearing house where it can be analysed
CTR6. Protected transferring of the collected reports	
CTR7. Email notifications	Users are notified immediately on successful reports upload using a standardize template

Table 6 - End-User Data Collection Tool Requirements