



AWARE

Abuse Watch Alerting and Reporting Engine



Introduction

Abuse Watch Alerting and Reporting Engine

- A platform designed to help with incident coordination.
- A tool to monitor cyber threats as a result of malicious activities on the Internet.
- Processes the information in real time and produces actionable reports and visualisations.



Abuse Watch for Alerting & Reporting Engine

Challenges

AWARE

Often time, incident response team faces challenges including:

- Details of an attack not readily available to responders, or they simply doesn't exist.
- Inadequate or absence of tools to provide reliable and comprehensive threat information.
- Data too scattered and not sufficiently filtered to work with.
- Unable to coordinate appropriate actions because the exact threats cannot be identified.
- Lack of expert skills to identify critical data from raw data.

How AWARE Supports CIRT

AWARE

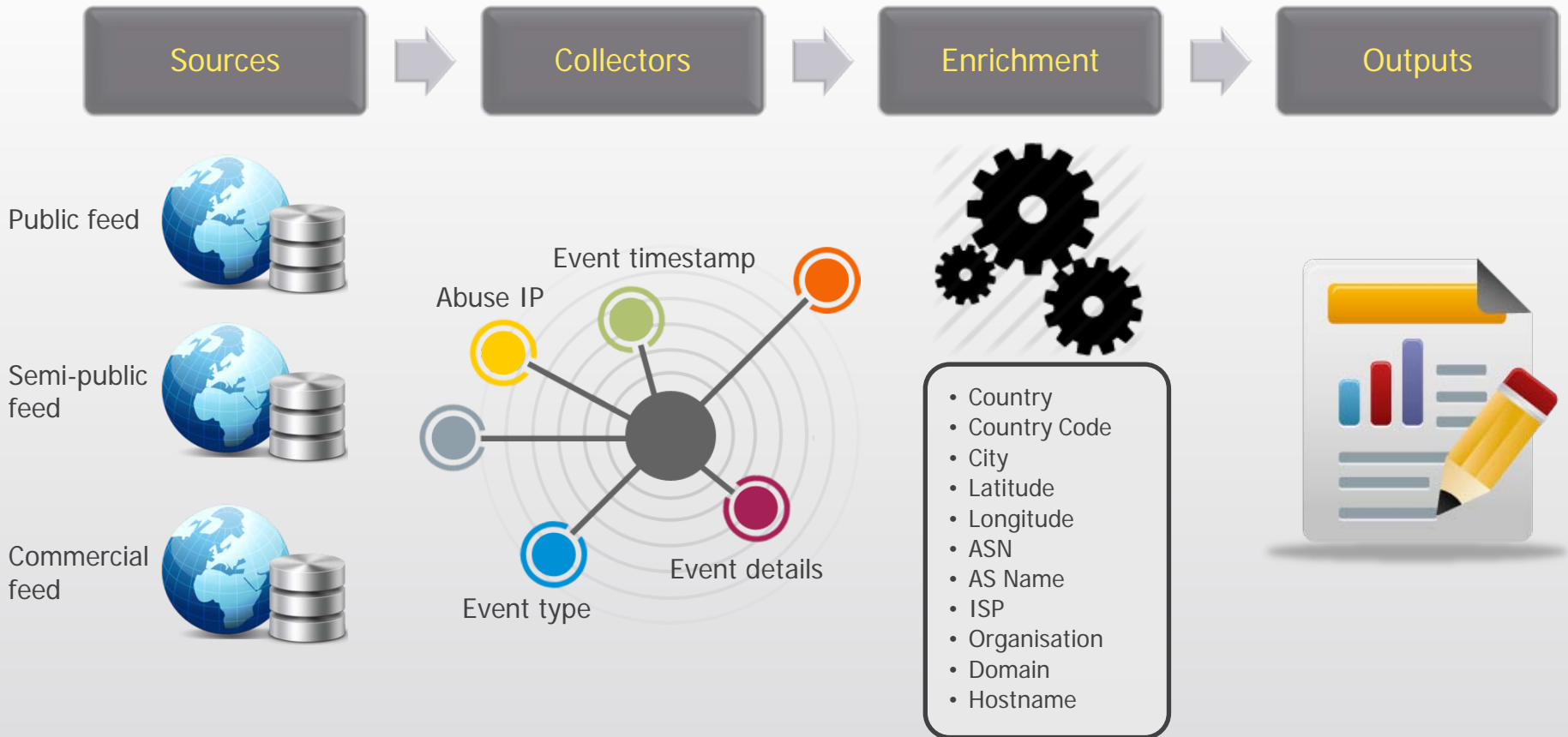
AWARE supports incident response team by:

- Collecting and correlating global data on malicious activities in near real time.
- Making sense of raw data through aggregating and enriching processes.
- Producing actionable intelligence.
- Simplifying incident coordination with relevant agencies.

How It Works

AWARE

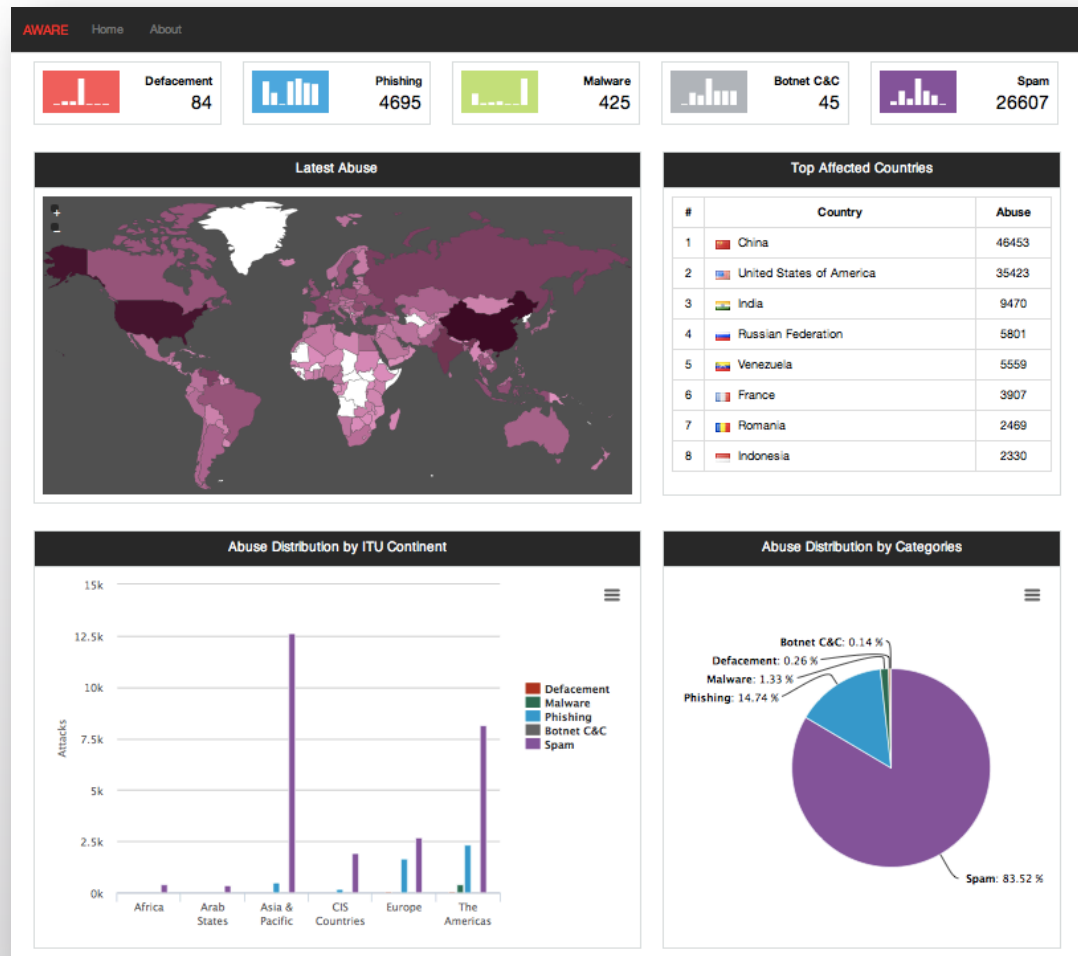
- AWARE fully automates data collection from multiple information sources.



Public Dashboard

AWARE

- The dashboard provides an overview of reported Internet abuse for the last seven days.



Public Dashboard

AWARE

AWARE Home About

Total no. of reported incidents for each abuse category



Defacement
84



Phishing
4695



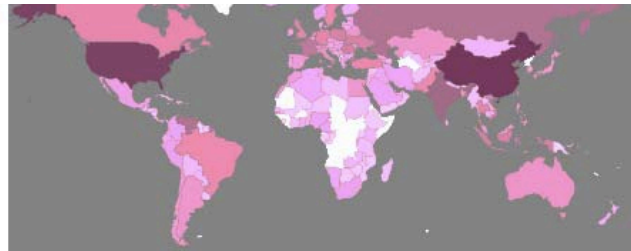
Malware
425



Botnet C&C
45

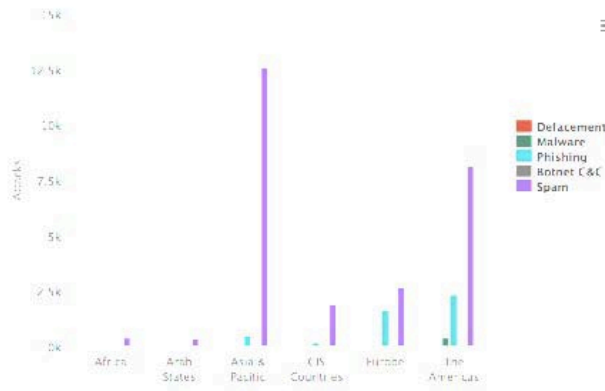


Spam
26607

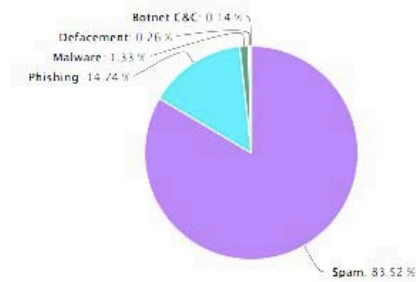


2	United States of America	35423
3	India	9470
4	Russian Federation	5801
5	Venezuela	5559
6	France	3907
7	Romania	2459
8	Indonesia	2330

Abuse Distribution by ITU Continent

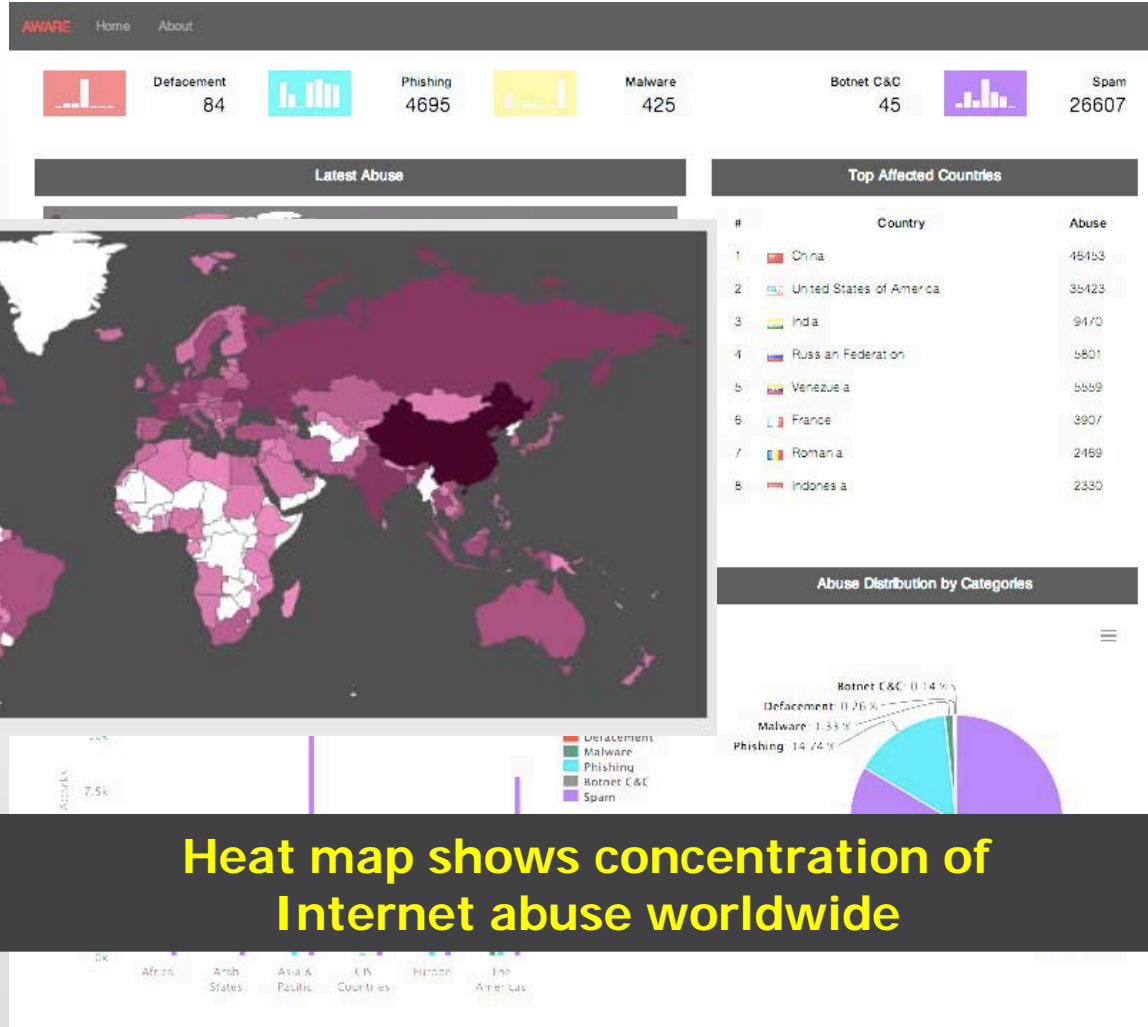


Abuse Distribution by Categories



AWARE

Public Dashboard



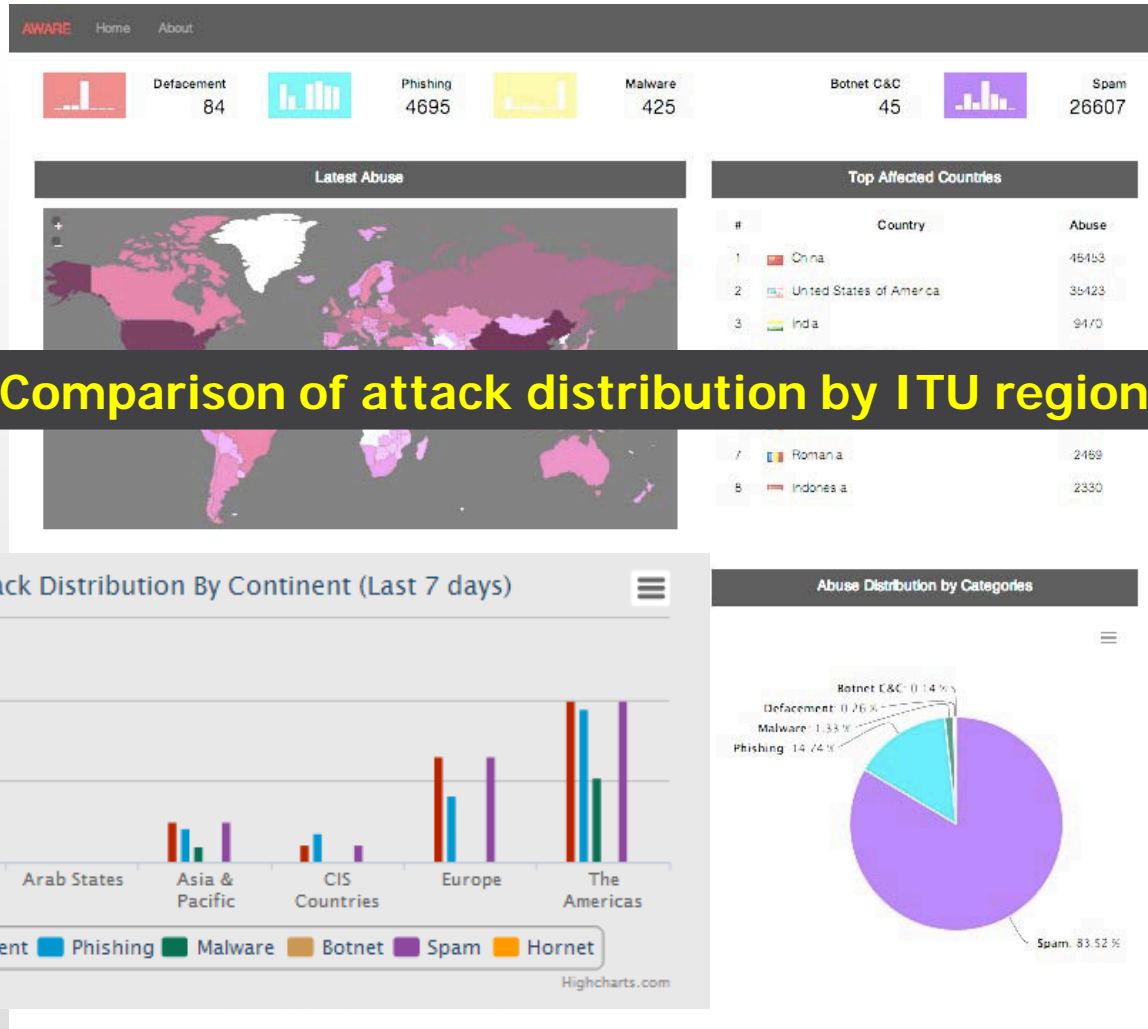
AWARE

Public Dashboard



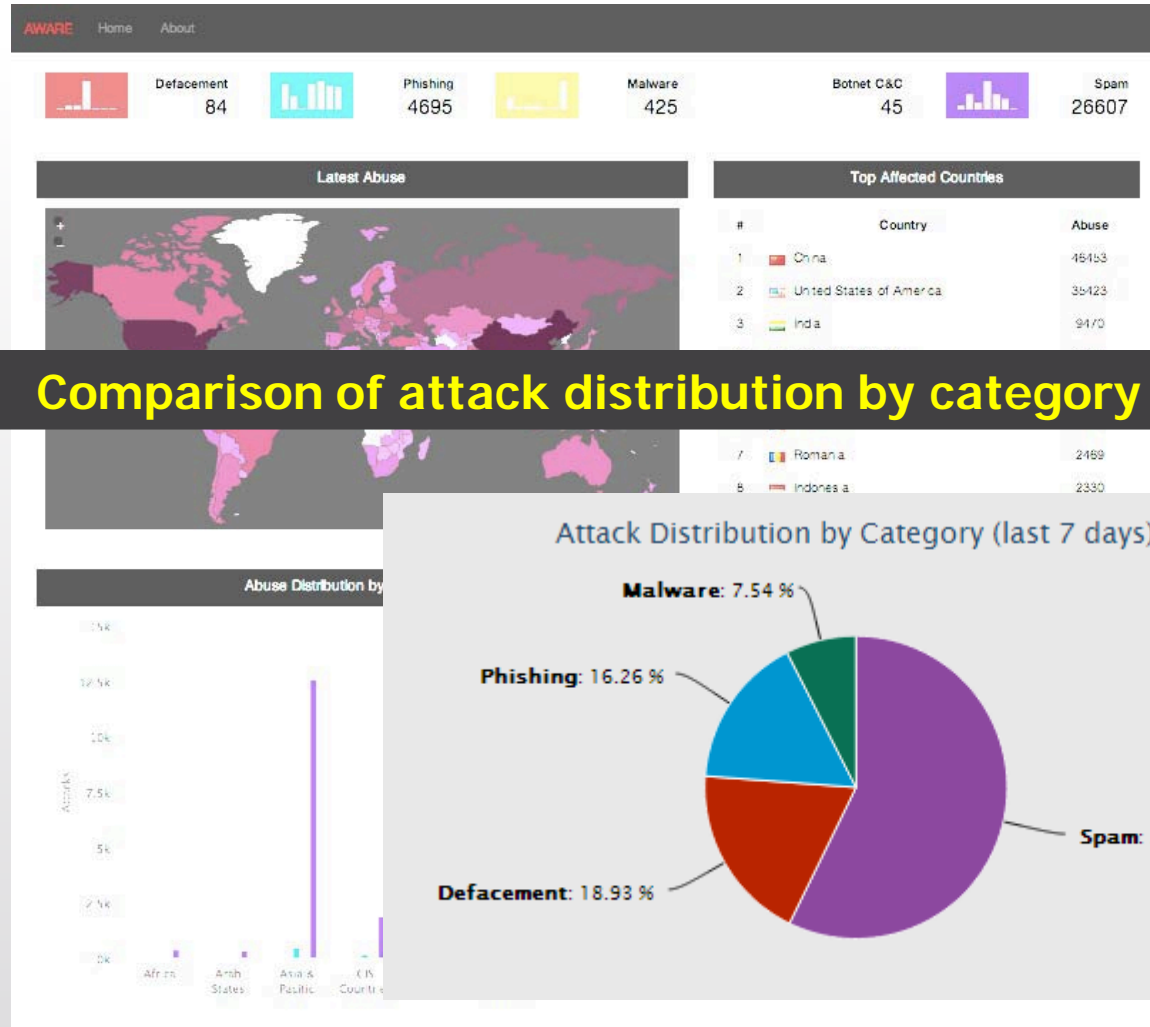
AWARE

Public Dashboard



AWARE

Public Dashboard

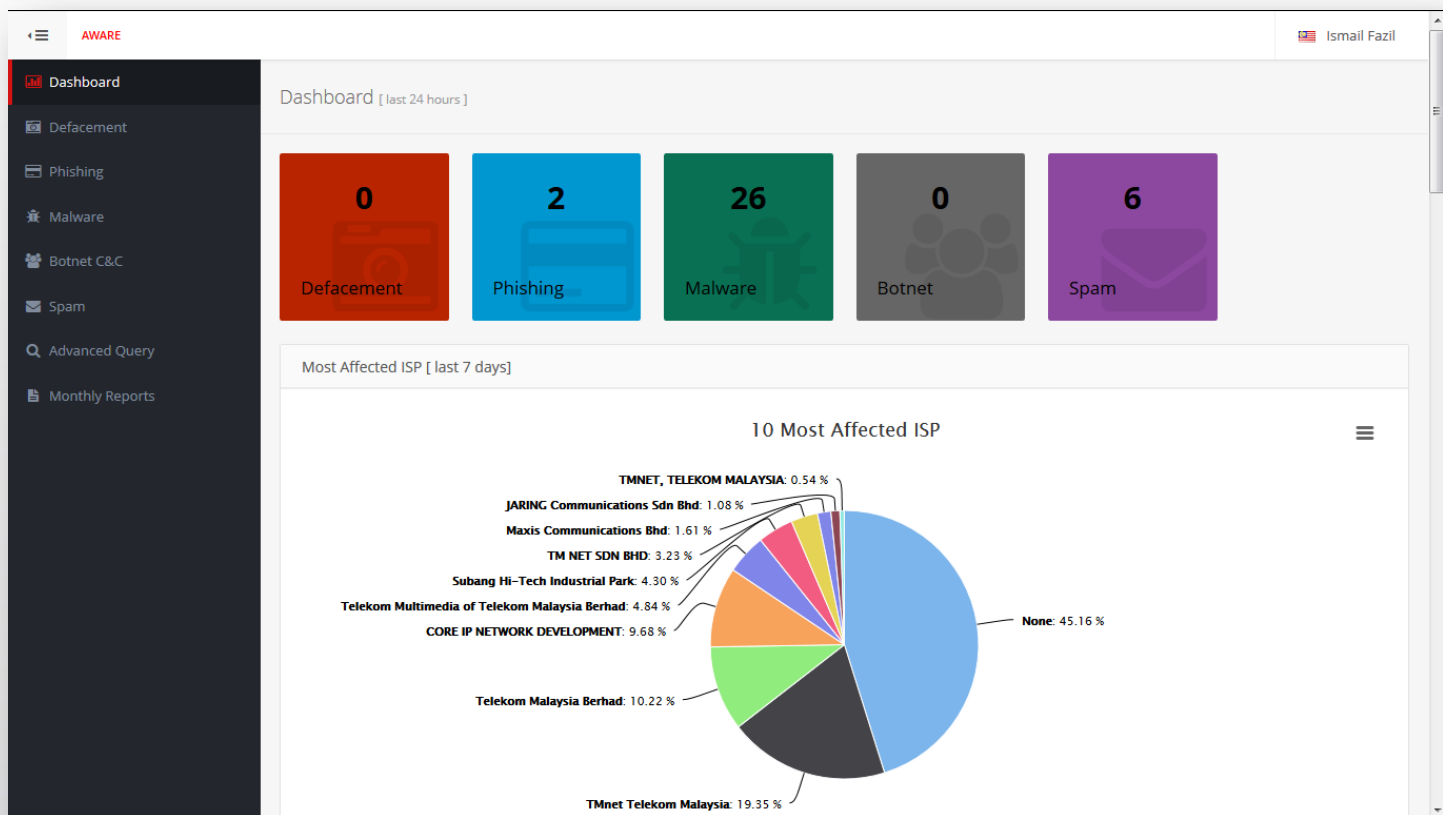


Comparison of attack distribution by category

AWARE

Management Dashboard

- Provides summary of reported Internet abuse in the country for the last seven days.



AWARE

Management Dashboard

- Detail abuse information of each threat category for the last 24 hours.

Defacement latest 24 Hours

All Countries

Total Results: 2,079

#	Date	Details	IP	ISP	CC
1.	25/03/2014	http://skynet.ru	91.195.124.6	LiderHost Ltd.	RU
2.	25/03/2014	http://omskodni.ru	91.195.124.6	LiderHost Ltd.	RU
3.	25/03/2014	http://www.r191.de/ganteng.gif	78.138.89.5	INET-People - Providerservices	DE
4.	25/03/2014	http://www.casanovaweb.it/ganteng.gif	89.96.126.103	Fastweb	IT
5.	25/03/2014	http://poomia.ctnc.es/ganteng.gif	87.106.199.154	Germany	ES
6.	25/03/2014	http://mvitalia.tv	89.163.177.50	UNITED COLO GmbH	IT
7.	25/03/2014	http://godag.no/personal/ganteng.gif	194.63.248.78	Domeneshop AS	NO
8.	25/03/2014	http://my-perfectme.com/ganteng.gif	198.251.74.152	None	US
9.	25/03/2014	http://www.riche.be/ganteng.gif	185.18.9.143	None	NL
10.	25/03/2014	http://www.wiromet.pl/ganteng.gif	89.25.207.149	Telekomunikacja Kopaln Plasku S.A.	PL
11.	25/03/2014	http://www.enerphoneurope.com/ganteng.gif	62.149.140.203	Aruba S.p.A.	IT

Phishing latest 24 Hours

All Countries

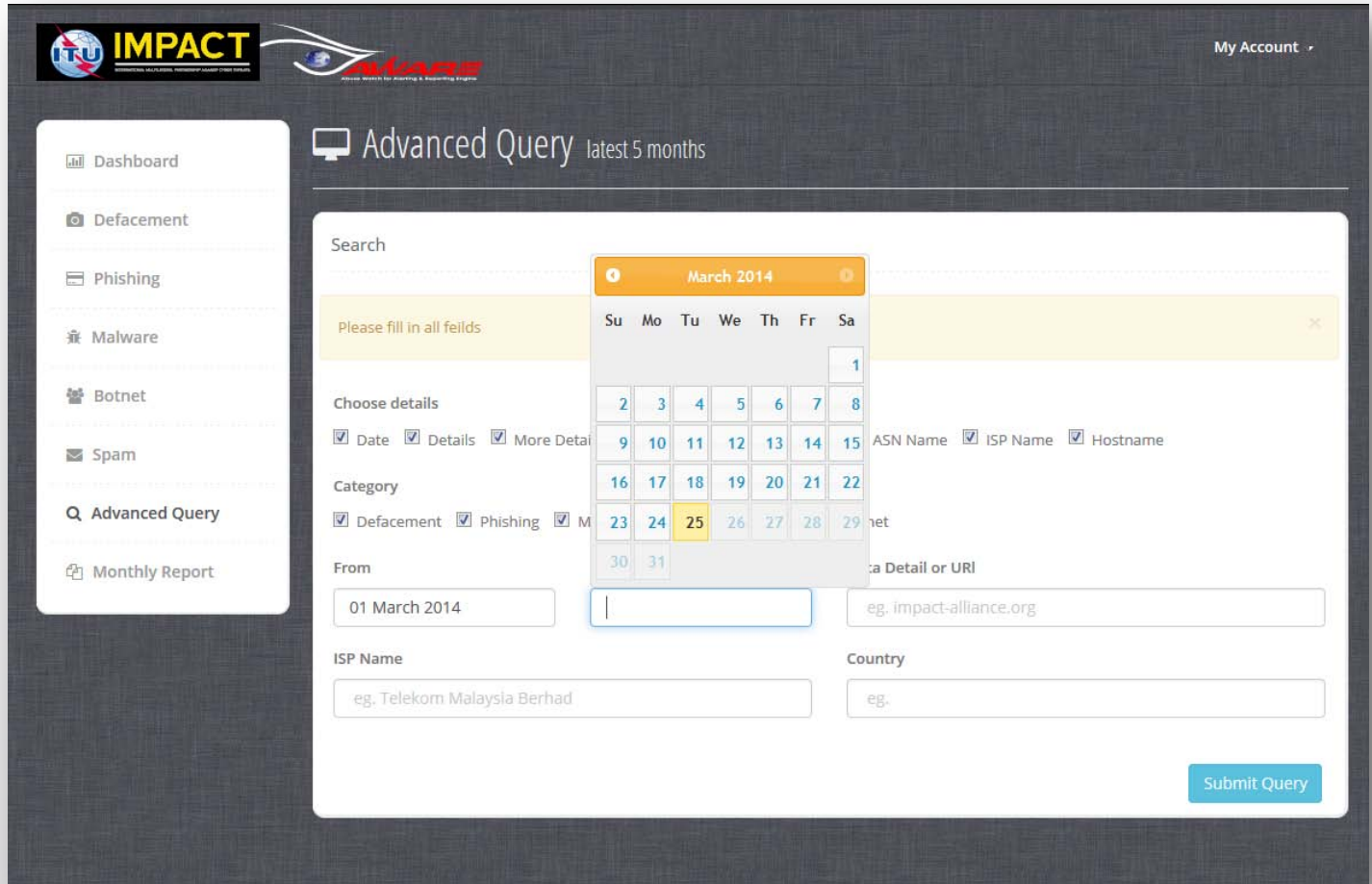
Total Results: 385

#	Date	Details	IP	ISP	CC
1.	25/03/2014	Itau	162.144.3.129	Australia	AU
2.	25/03/2014	Itau	178.248.200.93	None	HU
3.	25/03/2014	Allegro	192.185.225.115	None	US
4.	25/03/2014	Allegro	89.108.67.105	Agava JSC	RU
5.	25/03/2014	Allegro	50.28.17.158	None	US
6.	25/03/2014	Other	76.162.74.2	Ecommerce Corporation	US
7.	25/03/2014	PayPal	50.57.200.12	None	US
8.	25/03/2014	PayPal	50.57.200.12	None	US
9.	25/03/2014	PayPal	50.57.200.12	None	US
10.	25/03/2014	PayPal	50.57.200.12	None	US
11.	25/03/2014	PayPal	50.57.200.12	None	US

AWARE

Advanced Query

- Allows user to generate abuse report based on given parameters.



The screenshot displays the 'Advanced Query' interface on a dark-themed website. On the left is a navigation menu with options: Dashboard, Defacement, Phishing, Malware, Botnet, Spam, Advanced Query (highlighted), and Monthly Report. The main content area is titled 'Advanced Query latest: 5 months'. A search form is visible with a yellow warning box that says 'Please fill in all feilds'. A calendar pop-up for March 2014 is open, showing the date 25th selected. The form includes several sections: 'Choose details' with checkboxes for Date, Details, and More Details; 'Category' with checkboxes for Defacement, Phishing, and Malware; 'From' with a date input field containing '01 March 2014'; 'ISP Name' with a text input field containing 'eg. Telekom Malaysia Berhad'; 'Country' with a text input field containing 'eg.'; and 'Host Name' with a text input field containing 'eg. impact-alliance.org'. There are also checkboxes for 'ASN Name', 'ISP Name', and 'Hostname'. A 'Submit Query' button is located at the bottom right of the form.

AWARE

Monthly Statistics

- Allows user to generate abuse statistics based on date range.

The screenshot displays the AWARE interface for generating monthly statistics. The 'Monthly Reports' section is active, showing a search bar and date range selection. The 'From' date is 06/01/2014 and the 'To' date is 07/31/2014. A calendar for July 2014 is shown, with the 31st selected. The main report area displays a bar chart titled 'Abuse By Categories' and a table titled 'Total Abuse'.

Abuse By Categories

Category	Abuse
Defacement	4
Malware	177
Phishing	169
Botnet C&C	5
Spam	232

Total Abuse

Category	Abuse
Defacement	4
Phishing	169
Malware	177
Botnet	5
Spam	232
Total Abuse :	587

Abuse Distributions

Abuse by categories

Category	Percentage
Defacement	0.68 %
Botnet C&C	0.85 %
Phishing	28.79 %
Malware	30.15 %
Spam	39.63 %

AWARE

Live demo

<https://aware.impact-alliance.org>



Thank you

 www.facebook.com/impactalliance



IMPACT
Jalan IMPACT
63000 Cyberjaya
Malaysia

T +60 (3) 8313 2020
F +60 (3) 8319 2020
E contactus@impact-alliance.org
impact-alliance.org

