IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Global Response Centre (GRC)

Regional Cyber security Forum for Africa and Arab States, Tunis, Tunisia

4th - 5th June 2009

Need for GRC

- Access to the right information at the right time
  - Too many sources of information
  - Information is duplicated across various information sources
  - Very few security incident feeds are customised for a country or region
- No effective collaboration channels
  - Any single country is vulnerable against a well co-ordinated international cyber attack
  - There is a significant pool of untapped expertise within the security industry and the academia

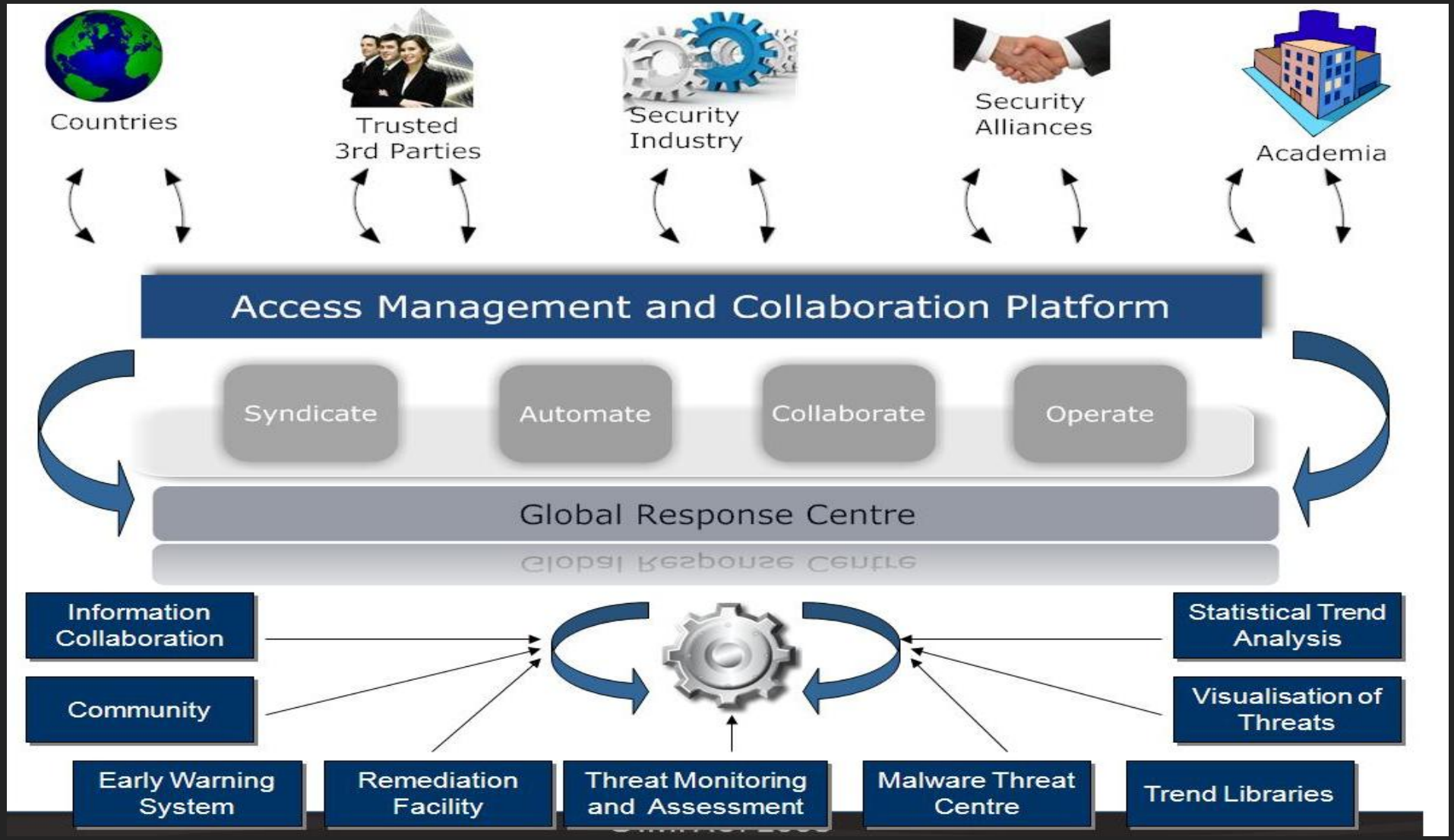
What does the GRC offer?

- *Syndicate* information from various trusted sources to enable effective remediation of security incidents
- *Automate* the process of collecting, monitoring, selecting, retrieving, tagging, cataloging, visualising and disseminating data on security incidents
- *Collaborate* with member Governments' agencies, members of academia, members of the security industry and trusted experts to provide resolution to security incidents
- *Operate* a 24x7 Response Centre

Value to member Governments

- **Rich source of cyber-threat feeds.**
- **Co-ordinated response to –** private sector/academia/public sector.
- **Providing a framework for national CERTs to collaborate and remediate problems across-borders.**

GRC Architecture



GRC Features

Current	Future
Network Early Warning System (NEWS)	Visualization of Threats by Countries
Expertise Finder	IMPACT Scorecard
IMPACT Community	Trend Libraries
Malware Threat Analyzer	Trend Monitoring & Analysis
Global Visualization of Threats	Remediation Facility
Incident & Case Management (cross-CERT compliant)	IMPACT Honeynet
Knowledgebase	Video Broadcasting
Reporting	Threat Route Plotter
	Remote GRC Integration
	Resolution Finder

GRC Features Definition

Early Warning System	Real-time Information mashup from various sources
Expertise Finder	Facilitates Expert Knowledge Exchange Network and Real-time communication
IMPACT Community	Social Networking Facility for IMPACT members
Remediation Facility	Research and Development Lab
Malware Threat Analyzer	Malware Submission Facility - Automated Threat Analysis System
Trend Libraries	Trend Archive
Global Visualization of Threats	Global Security Health Check. Global Threat Map
Visualization of Threats by Countries	Threats by Countries
Incident & Case Management	Case Management and Incident Escalation (Cross-CERT compliant)
Trend Monitoring & Analysis	Trend Dynamic Data Analysis and Assessment
Knowledgebase	Libraries of Security Documents and Information
Reporting	Executive and Technical Report Generation Facility
IMPACT Honeynet	IMPACT Integrated Honeynet Framework
Video Broadcasting	Video broadcasting of emergency news from IMPACT
Threat Route Plotter	Security Threat Trails
Resolution Finder	Map Resolution to Security Threats
Remote GRC Integration	Country based GRC integration with IMPACT

Information sources for NEWS

Symantec

SANS

Secunia

Kaspersky

Arbor Networks

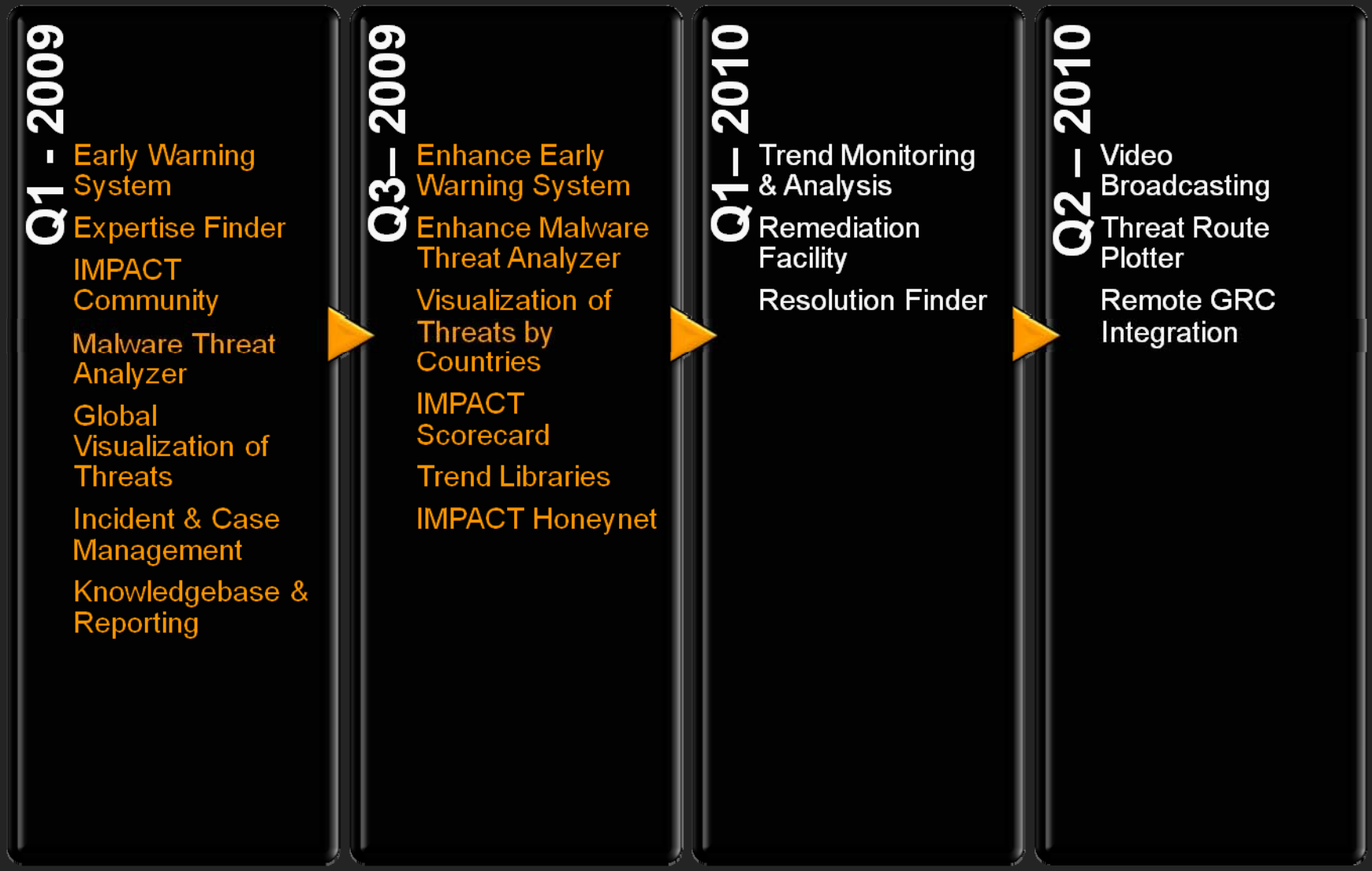
SOPHOS

SRI-MTC

F-Secure

Trend Micro

Development phases for NEWS & ESCAPE



IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER-THREATS

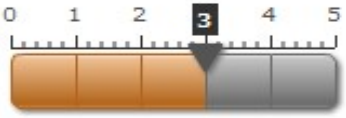
Search: Go

Home | Incidents | EWS | Submit Sample | Library | Support | Search | Meetings | About IMPACT | Team Management | Document Center | News | Reports | Sites

My Site | My Links | Site Actions

Current Threats

C & C Servers | Sources | Phishing | Malware | All



IMPACT | GLOBAL THREAT STATUS

This Week in Pictures

Mohd Noor Amin, IMPACT Chairman and ITU Secretary-General Dr Hamadoun Touré sign the MoU on Wednesday, 3 September at ITU Telecom Asia 2008 in Bangkok

View slide show

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER-THREATS

Search: Go

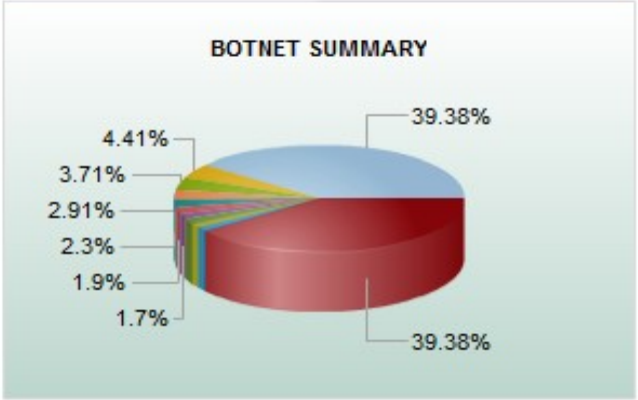
Home | Incidents | EWS | Submit Sample | Library | Support | Search | Meetings | About IMPACT | Team Management | Document Center | News | Reports | Sites

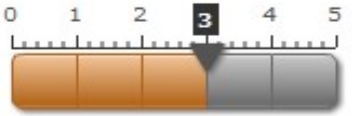
My Site | My Links | Site Actions

IMPACT Intranet > EWS

Ports

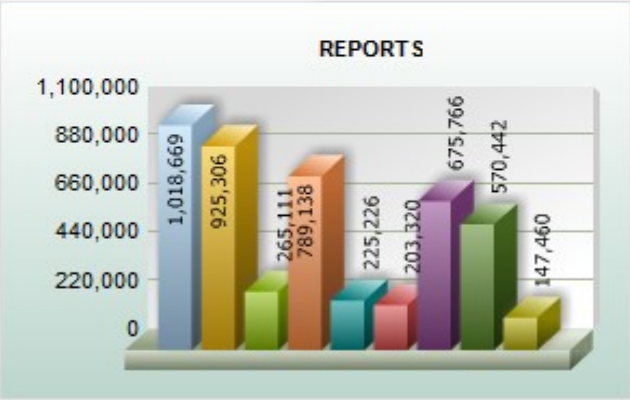
Botnets



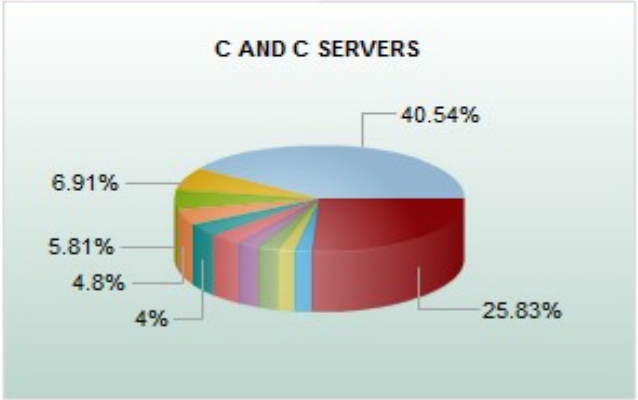


IMPACT | GLOBAL THREAT STATUS

Sources



Command & Control Servers



Virus Info

Trojan-Spy:W32/ZBot.XF
Trojan:Java/Konov.A
Trackware:W32/Tracking Cookie
Trojan-Spy:W32/Gimmiv.A
Trojan-Downloader:W32/FakeAlert.BG
Trojan-Downloader:W32/Renos.GEN
Worm:W32/AutoRun.NOI
Net-Worm:W32/Koobface.BM
Rootkit:W32/Agent.UI
Backdoor:W32/Hupigon.OGA

IMPACT

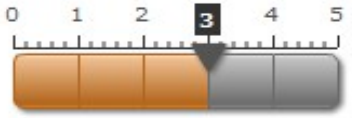
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER-THREATS

Search: Go

Home | Incidents | EWS | Submit Sample | Library | Support | Search | Meetings | About IMPACT | Team Management | Document Center | News | Reports | Sites

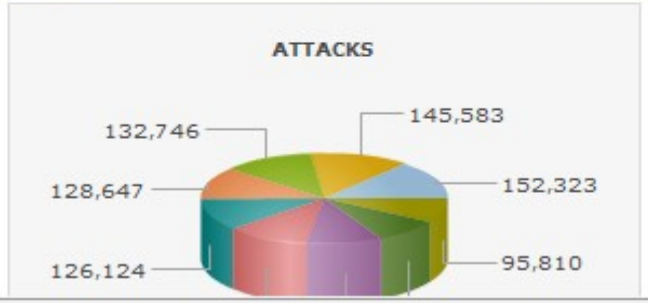
My Site | My Links | Site Actions

Sources (past 24 hours)



IMPACT | GLOBAL THREAT STATUS

Attacks



Sources

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER-THREATS

Search: Go

Home | Incidents | EWS | Submit Sample | Library | Support | Search | Meetings | About IMPACT | Team Management | Document Center | News | Reports | Sites

My Site | My Links | Site Actions

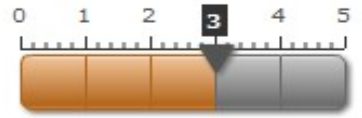
Early Warning System

- EWS Home
- Botnet
- Command and Control Servers
- Top Ports
- Virus
- Vulnerabilities
- Sources
- Spyware
- Phishing
- Malware
- Submit Sample
- Threat Map

Top Ports (pa

By Reports

Ports	Report
993	16464
139	21026
445	24137
64471	15088
80	11803
135	9970
51413	7050
45644	6062
8000	4400



IMPACT | GLOBAL THREAT STATUS

By Sources

Ports	Sources
4899	1533
53	1350
445	1188
135	1013
2967	802
23	622
1433	468
1434	460
25	457

By Targets