Current procedures, challenges and opportunities for collection and analysis of Criminal Justice statistics – CERT-GH

**International Workshop on Criminal Justice Statistics on
Cybercrime and Electronic Evidence
Accra, Ghana
29 -31 March 2016**

By

Eric Akumiah

Member, GLACY+ National Team Member

Agenda

- CERT-GH

- Collection of Statistics

- Processing Statistics

- Reporting and Analysis

- Challenges

- Conclusion

CERT-GH
Ghana Computer Emergency Response Team

CERT-GH Charter & Mission

"CERT-GH provides information and assistance to its constituents in implementing proactive measures to reduce the risks of computer security incidents."
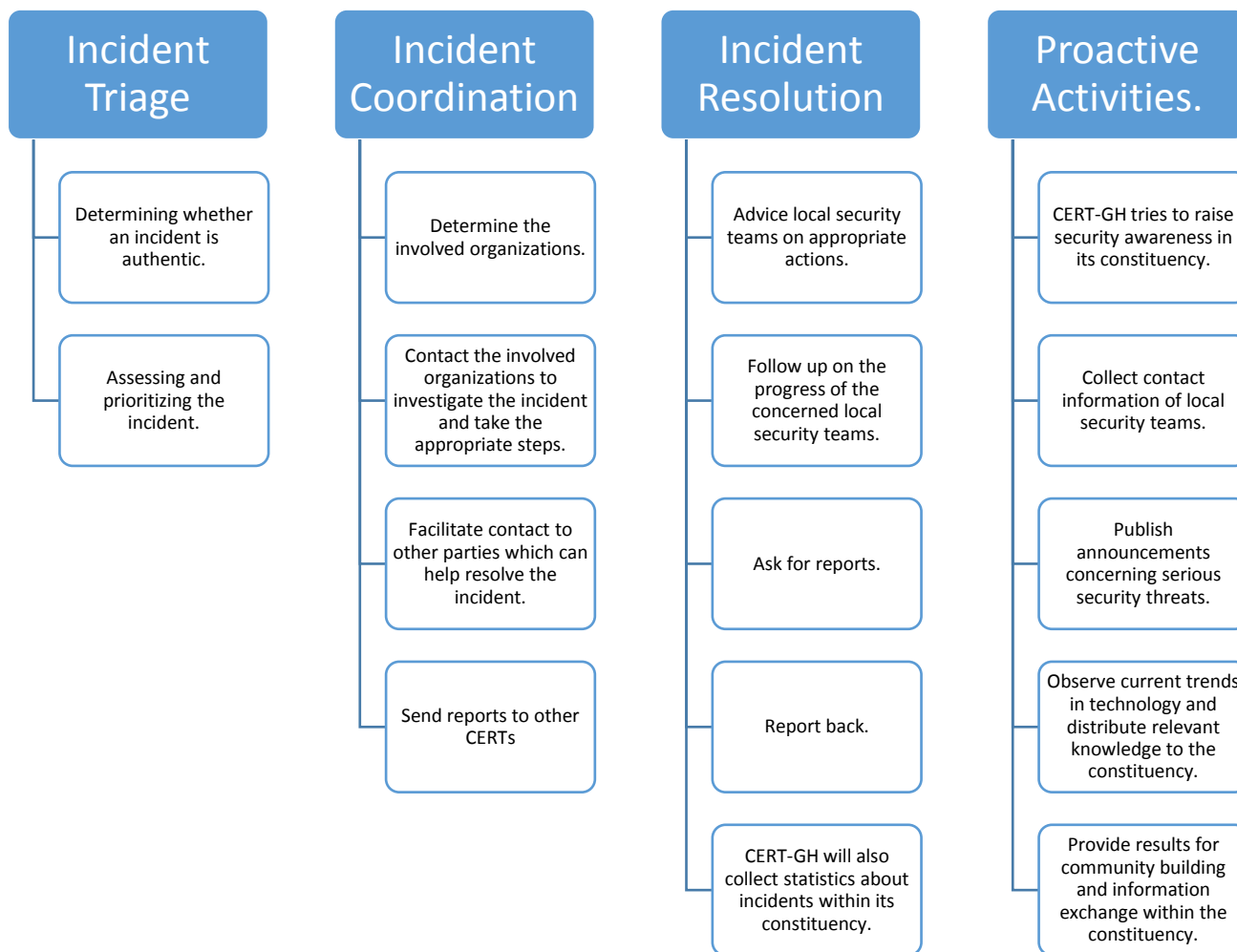
Functions of CERT-GH

| Provide a single point of contact for reporting security incidents | Assists the organizational constituency and general computing community in preventing and the handling of computer security incidents | Shares information and lessons learnt with other response teams | Collaborate with law enforcement agencies and local authority bodies |

CERT-GH
Ghana Computer Emergency Response Team

Services of CERT-GH

Incident Triage	Incident Coordination	Incident Resolution	Proactive Activities.
Determining whether an incident is authentic.	Determine the involved organizations.	Advice local security teams on appropriate actions.	CERT-GH tries to raise security awareness in its constituency.
Assessing and prioritizing the incident.	Contact the involved organizations to investigate the incident and take the appropriate steps.	Follow up on the progress of the concerned local security teams.	Collect contact information of local security teams.
	Facilitate contact to other parties which can help resolve the incident.	Ask for reports.	Publish announcements concerning serious security threats.
	Send reports to other CERTs	Report back.	Observe current trends in technology and distribute relevant knowledge to the constituency.
		CERT-GH will also collect statistics about incidents within its constituency.	Provide results for community building and information exchange within the constituency.

Services of CERT-GH – Cont'd

Proactive Services (80%)	Preventing criminal from Exploiting software vulnerabilities to attack systems	Receive real-time (+24hrs) feed from International probes on issues on Ghana networks
		Prepare Alerts and Advisories to network operators on how to keep networks clean
		Provide to network operators latest updates from Original Equipment Manufacturers (OEM) and software manufacturers on latest updates
		Newsletter to inform
Reactive Services (20%)	Coordinate Incident handling with constituents for cyber Attacks	Government Website defacements
		Malware attacks (e.g. Ransomware attacks)

CERT-GH
Ghana Computer Emergency Response Team

Collection of Statistics

Phone & *Email*

Webform

Other Forms of Collection

Receive Intelligent feed from International Cyber Monitoring Servers and probes on Ghana

Receive Direct request from other National CERTs

- US-CERT
- Canada CERT
- Australia
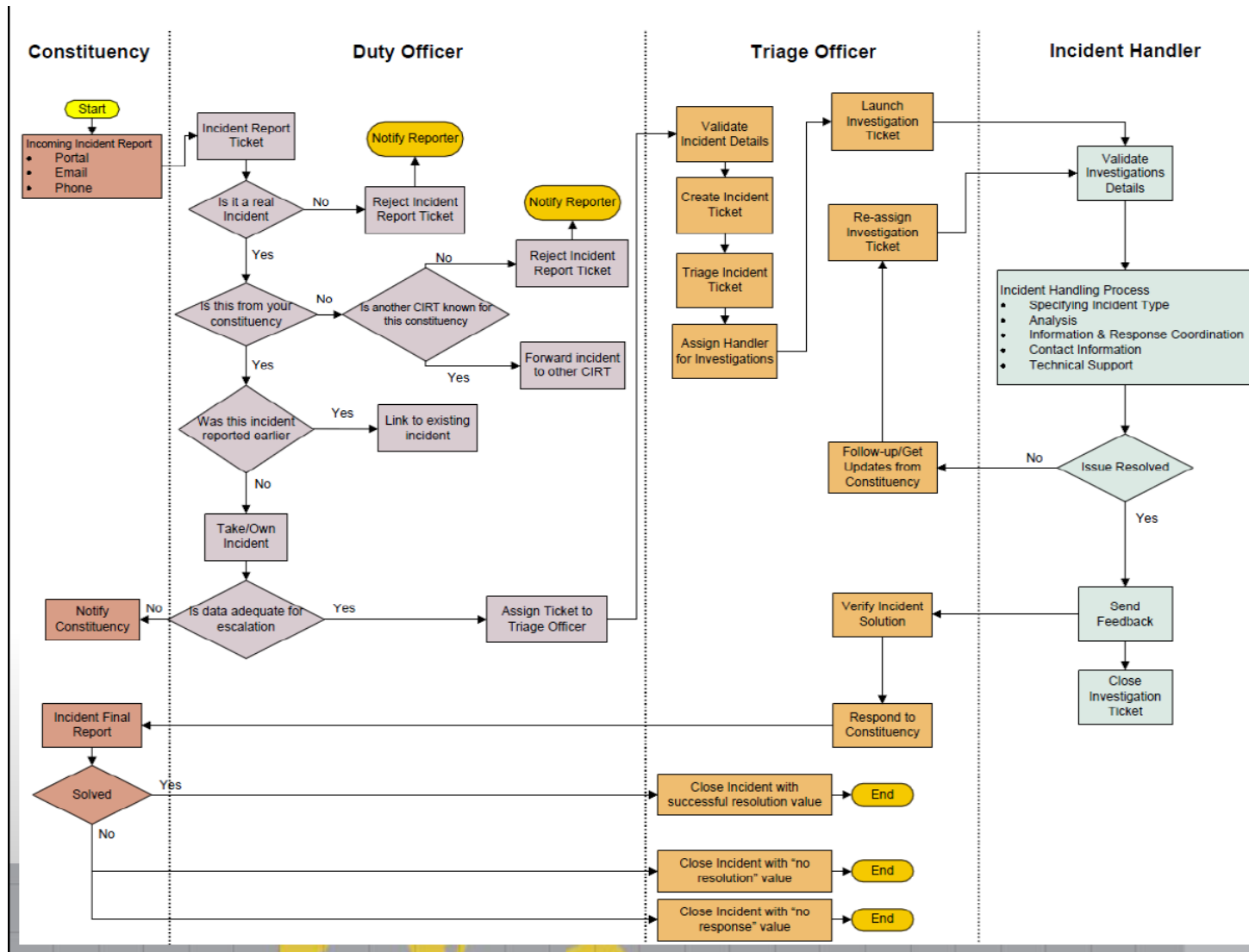- AfricaCERT
- CERT/CC

mation for enhance Cyber security
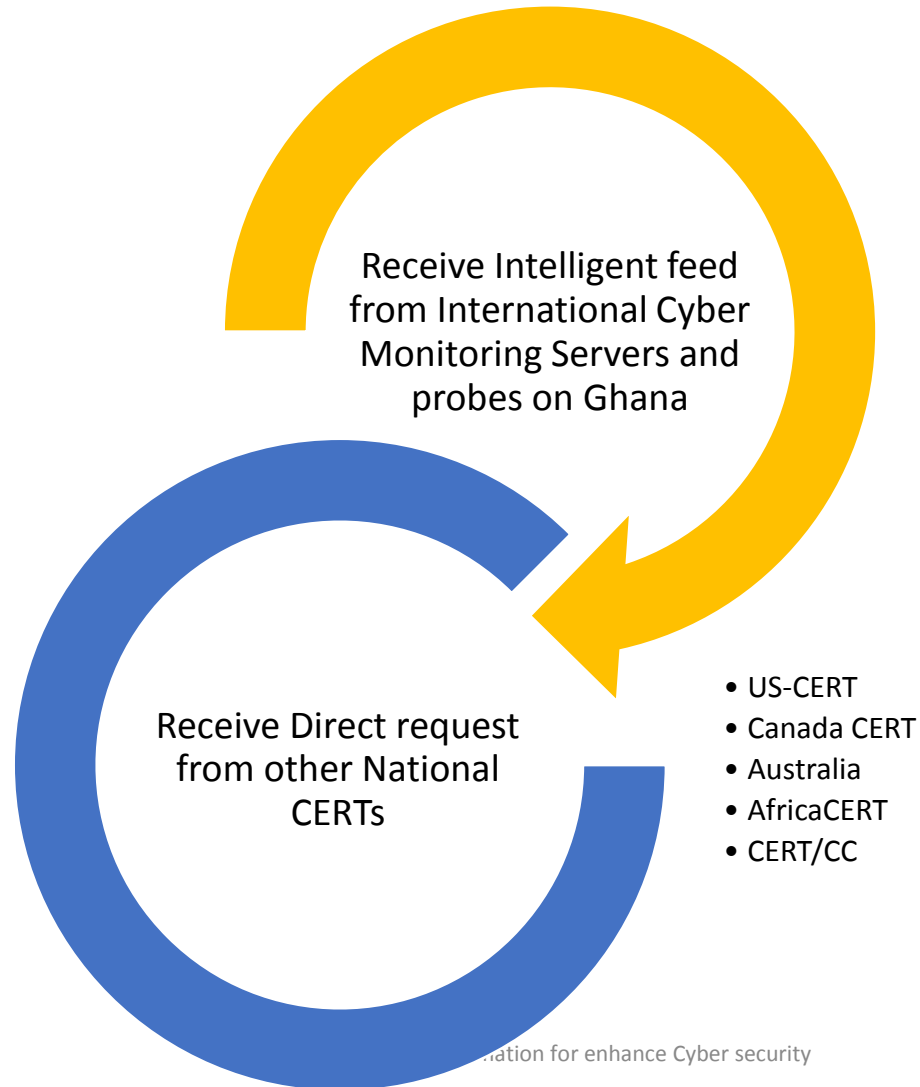
Processing Statistics

- All incidents received inputted into the Incident Request Handling Systems
    - Ticketing System to track case from start to end
    - Systems categorize request
    - Reports generated from Systems on demand

- CERT-GH has automated feed from international probes (Cyber Risk and attacks)

- Reports generation
    - Daily Report
    - Weekly Report
    - Monthly Report
    - Designated period desired (Quarterly, Annual etc)

CERT-GH
Ghana Computer Emergency Response Team

RTIR Ticketing Systems

CERT-GH Automated Feed Platform

Reporting & Analysis

...CERT-GH, Sharing Information for enhance Cyber security

Threat Landscape : Ghana National Networks 2015

Ghana National Network Attacks and Vulnerabilities

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
Botnet Infections	49960	43395	36370	65151	57481	54126	46162	62828	58478	86172	48394
Website Defacements	162	140	184	121	236	46	59	8	31	44	178
SSL Breaches	449	71852	178822	72403	38389	28246	29874	41117	38613	33246	37182
DNS Open Resolver Vulnerabilities	10950	10587	7575	10026	12882	10516	11662	12475	16236	29008	27778
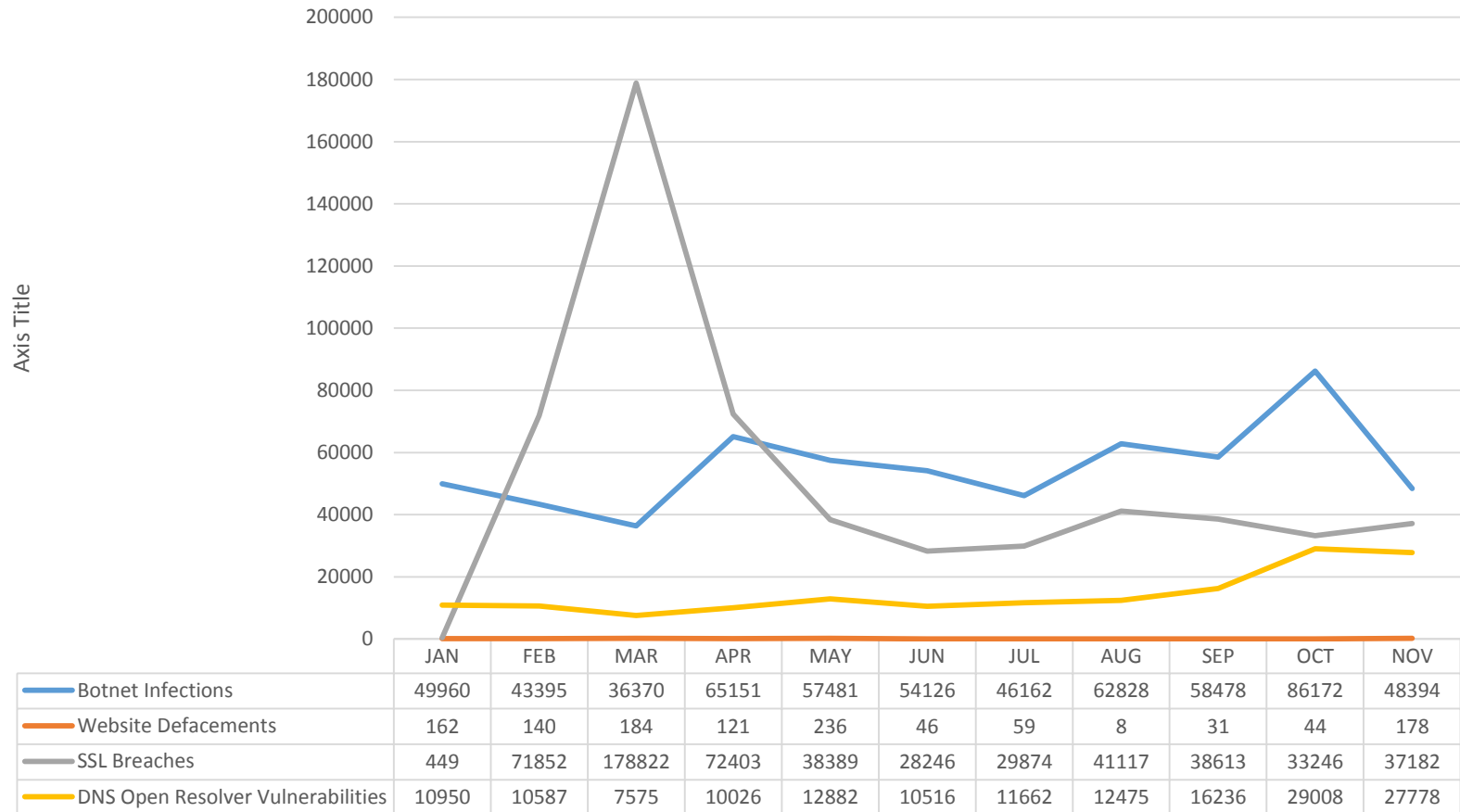
Threat Landscape : Government Networks 2015

Ghana Government Network Attacks & Vulnerabilities

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
Botnet Infections	370	336	305	182	218	22	45	13	18	25	45
DNS Open Resolver Vulnerabilties	125	81	63	56	103	92	108	155	126	126	131
SSL Breaches	0	0	71	171	221	120	143	101	92	77	81
Compromised Websites	11	1	0	0	0	0	1	0	0	0	1

CERT-GH
Ghana Computer Emergency Response Team
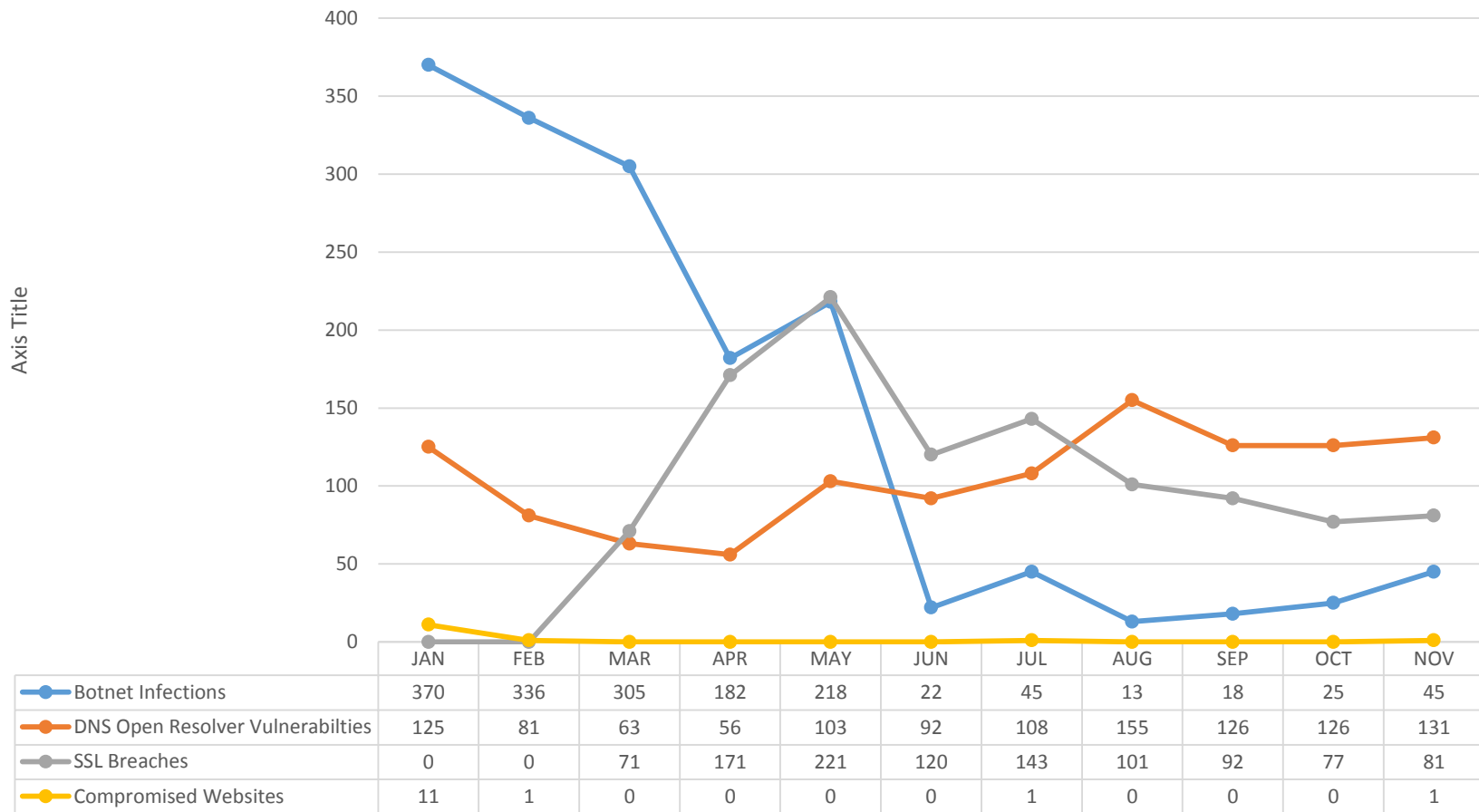
Early Warning on Ghana Networks
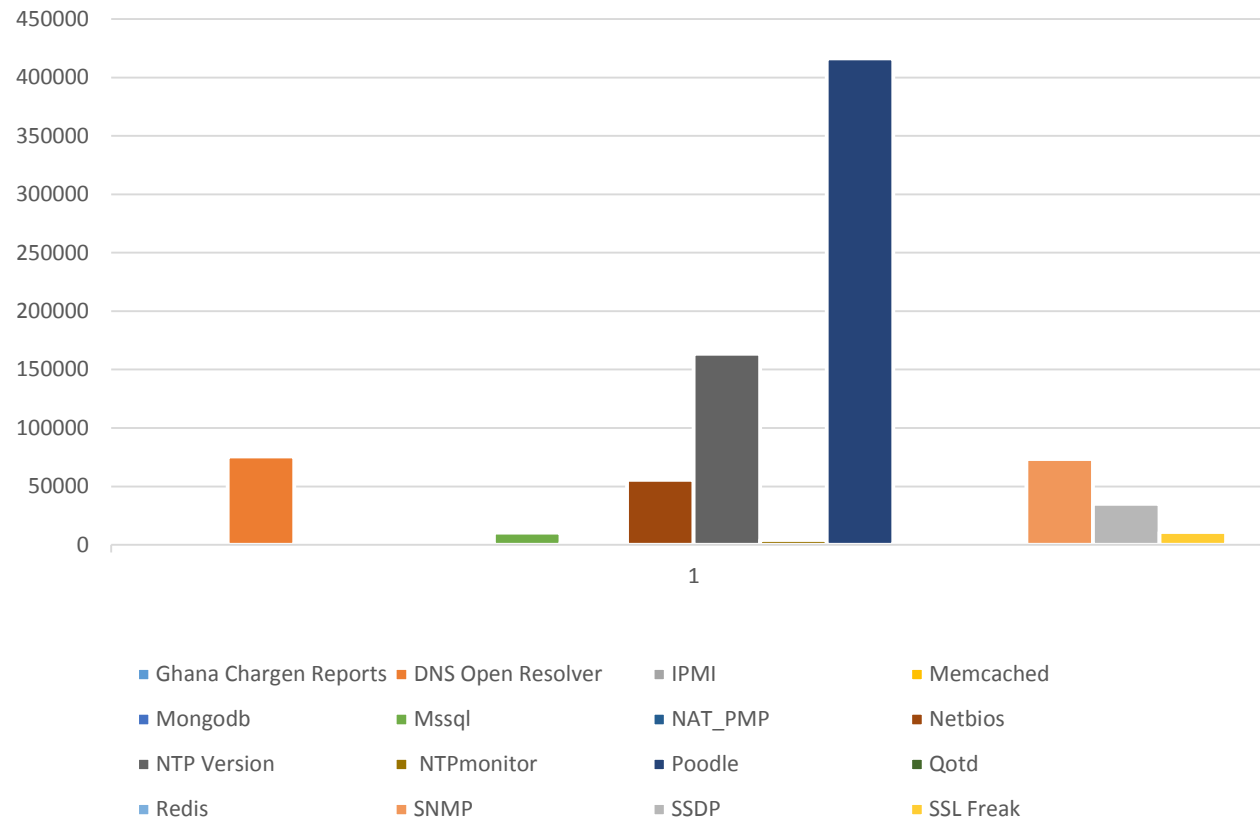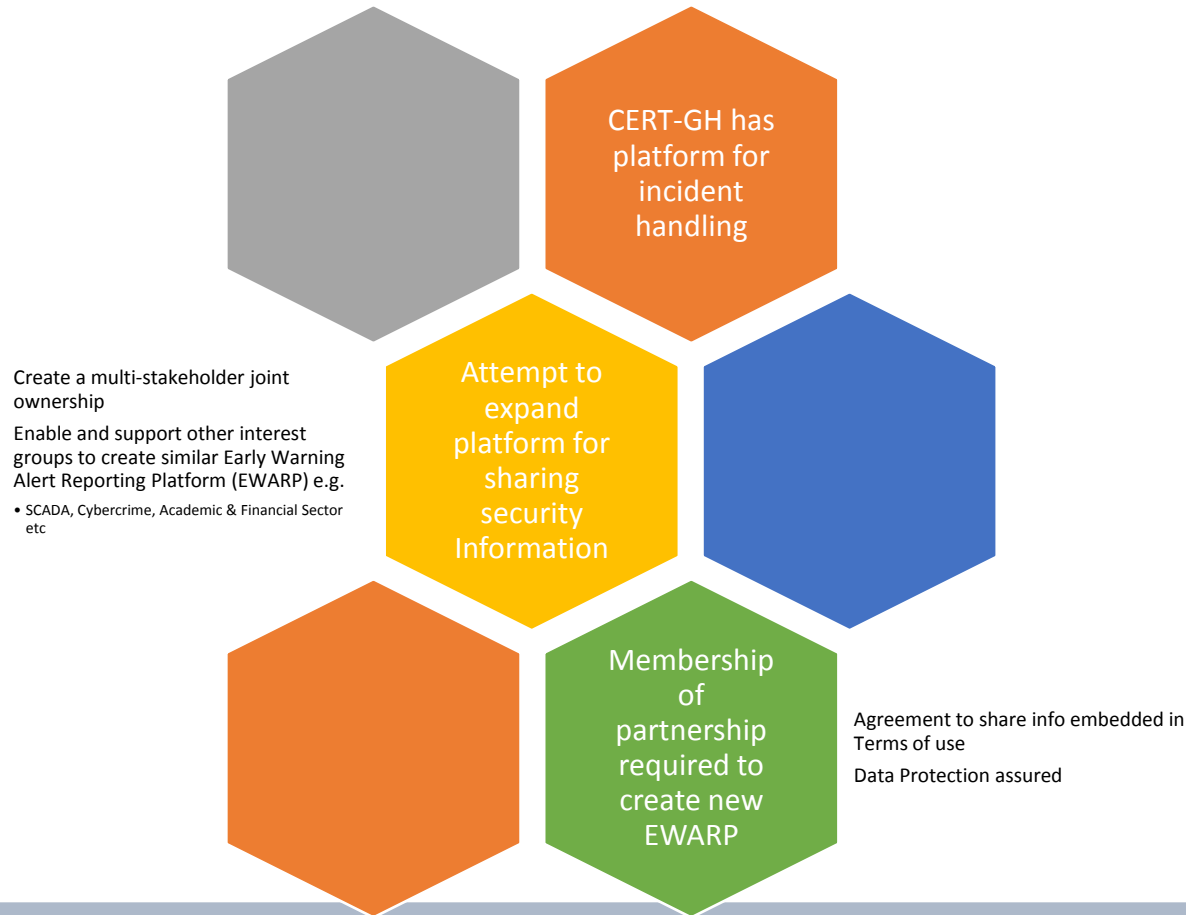
Uses of Statistics

- Indication of Ghana's Cyber hygiene
- Inform Policy decision
  - 2015 Annual report informed organization of National Cyber Awareness week with capacity building on incident handling
- Provides good bases on how National Cyber security Strategy can be implemented.
  - What type of national Awareness for what stakeholder?
  - What must Network operators focus on?
- Information Sharing for improved cybersecurity

CERT-GH
Ghana Computer Emergency Response Team

Challenges

- Lack of visibility of the CERT-GH reporting mechanism on Portal
- Lack of response from constituencies when Alerts and advisorirees are sent to them

CERT-GH
Ghana Computer Emergency Response Team

Information Sharing: Ghana Cybersecurity Information exchange Platform(GCIXP)

Create a multi-stakeholder joint ownership

Enable and support other interest groups to create similar Early Warning Alert Reporting Platform (EWARP) e.g.

• SCADA, Cybercrime, Academic & Financial Sector etc

CERT-GH has platform for incident handling

Attempt to expand platform for sharing security Information

Membership of partnership required to create new EWARP

Agreement to share info embedded in Terms of use

Data Protection assured

CERT-GH
Ghana Computer Emergency Response Team

Conclusion

- Awareness creation for CERT-GH incident reporting mechanism will improve cybersecurity in Ghana and minimize incident of cybercrime.

- Government can use statistics reported in CERT-GH to inform public policy on cybersecurity.

- Public private collaboration can improve sharing of cyber intelligence to improve cybersecurity

CERT-GH
Ghana Computer Emergency Response Team

Thank you ?

team@cert-gh.org

www.cert-gh.org