National Computer Board

CERT-MU

Approaches for Securing IoT Infrastructure

Dr. Kaleem Usmani
Officer-In-Charge
Computer Emergency Response Team of Mauritius
(CERT-MU)

June 2017

Presentation Outline

- About CERT-MU
- IOT Threat Landscape
- Cybersecurity Initiatives
- Approaches for Securing IoT Infrastructure

About CERT-MU

- CERT-MU was setup in May 2008 under the umbrella of the National Computer Board.
- It is a National CERT and is the second oldest CERT in Africa after Tunisia (TunCERT).
- CERT-MU is the main engine driving cybersecurity initiatives in the country.
- It assists the Ministry of TCI on the development and implementation of cybersecurity policies and promotes cybersecurity at the national level.
- CERT-MU is ISO 27001 certified.
- CERT-MU has played an active role in the ITU's Global Cybersecurity Index Survey ranking published in June 2017, where Mauritius is placed 1st in Africa and 6th in the world.

About CERT-MU (Contd.)

- CERT-MU has been affiliated to CERT/CC and Forum of Incident Response and Security Teams (FIRST).

- Memorandum of Understanding has been signed between CERT-India, Japan CERT/CC, STQC-India, Symantec-Mauritius and EMTEL Ltd-Mauritius in the area of cyber security.

- CERT-MU is also the member of Cybersecurity Alliance for Mutual Progress (CAMP), coordinated by Korean Internet Security Agency (KISA), Seoul, South Korea.

CERT-MU Services

- Incident Handling
- Vulnerability Scanning and Penetration Testing
- Dissemination of virus alerts, advisories, vulnerability notes on a daily basis
- Assistance to organisations for the implementation of Information Security Management System based on ISO 27001
- Third party information security audits
- Technical security assessment of organization's IT infrastructure

CERT-MU Services (Contd.)

- Cyber Security Drill
- Organisation of Information Security Trainings
- Sensitization on Information Security

IOT Threat Landscape

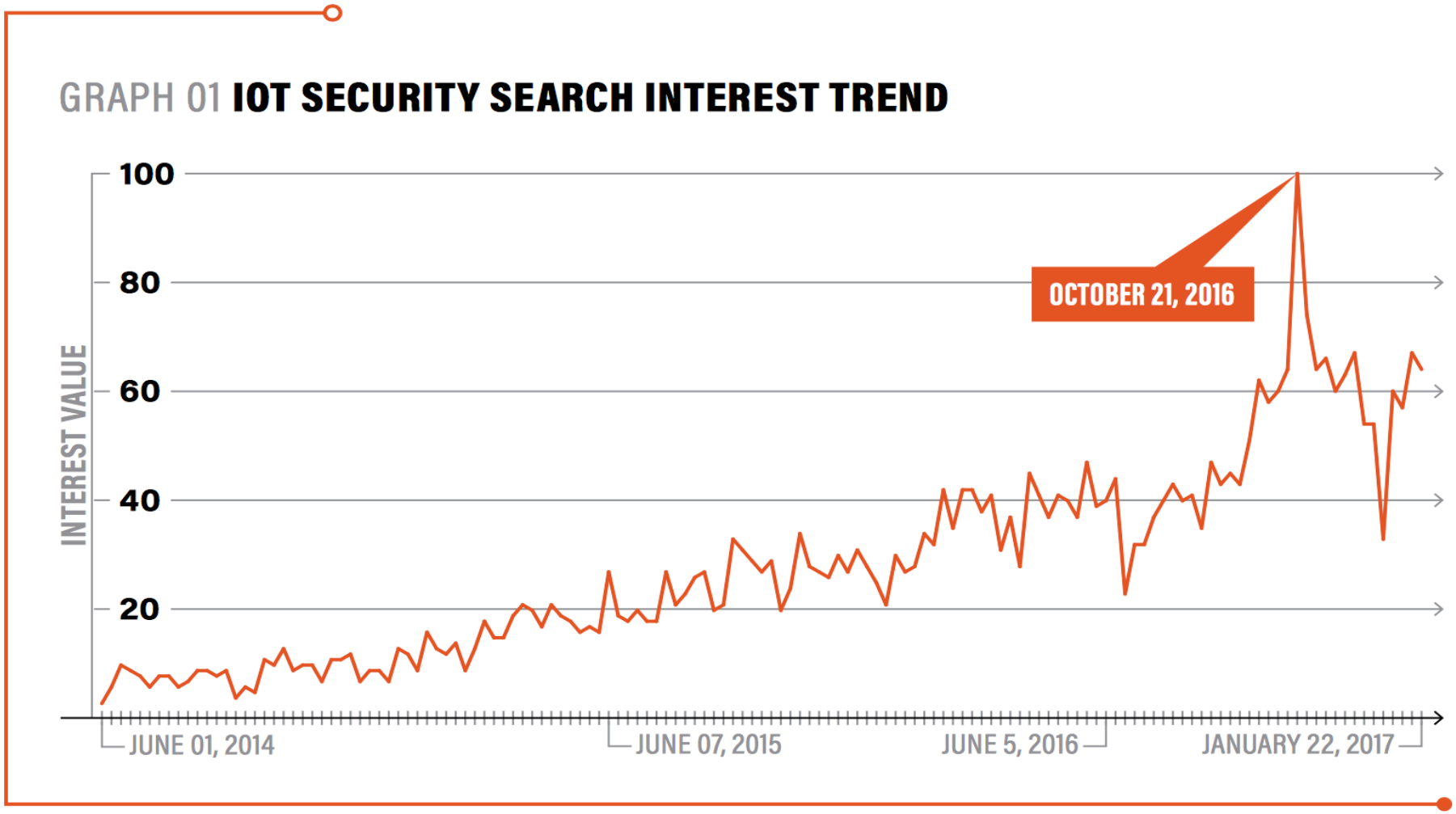
- Research firm Gartner Inc. predicts that 8.4 billion connected devices will be in use worldwide this year (2017), a 31 percent increase over 2016.

- According to an HP study, *Internet of Things Security: State of the Union 2014 Report*, 70 percent of IoT devices are vulnerable to attack.

- Companies have not stopped producing products with insecure default configurations. For e.g. common routers like “linksys” and “Netgear”.

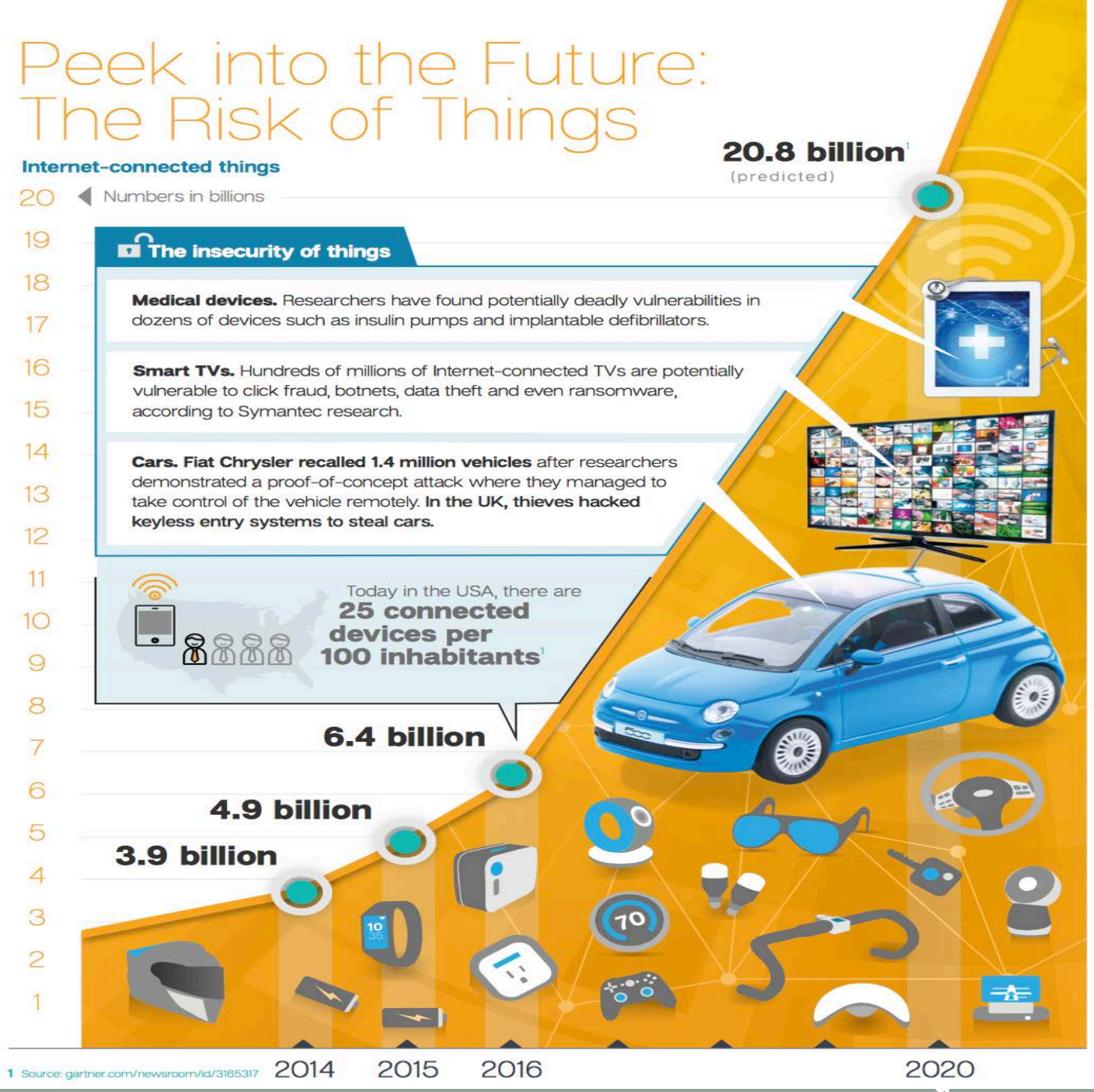
- **Mirai** has changed the perception of IoT device threats

IOT Security Search Interest Trend



Source: Internet of Evil Things 2017 Report by Pwnie Express

(Source: Gartner.com)

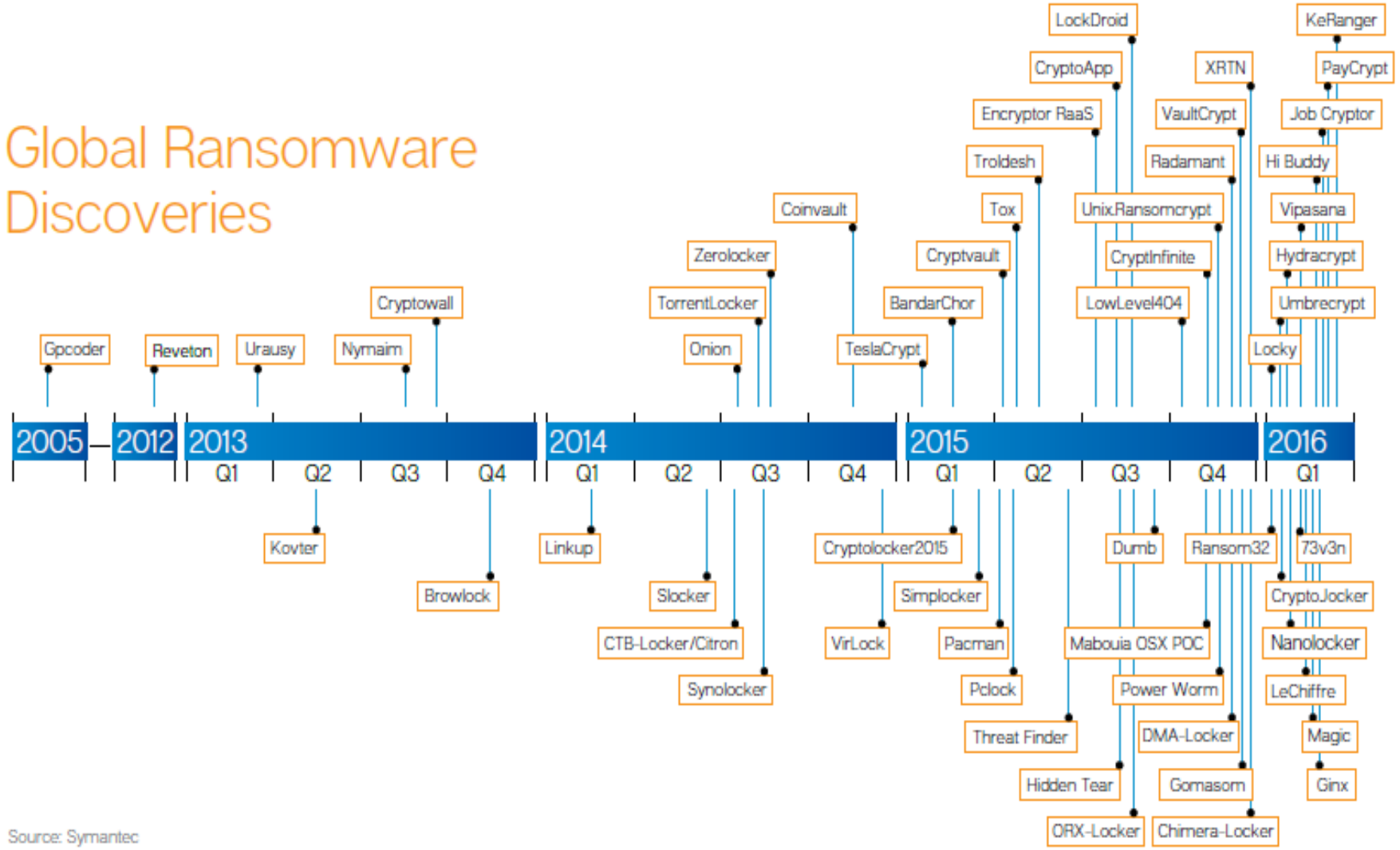


Security Threats to the IOT Infrastructure

- Ransomware (e.g. WannaCry and Petya)
- Malware (Mirai)
- Deploying a botnet
- Denial of Service
- Phishing
- Data Integrity Attacks (Stuxnet 2010)
- MITM

Evolution of Ransomware

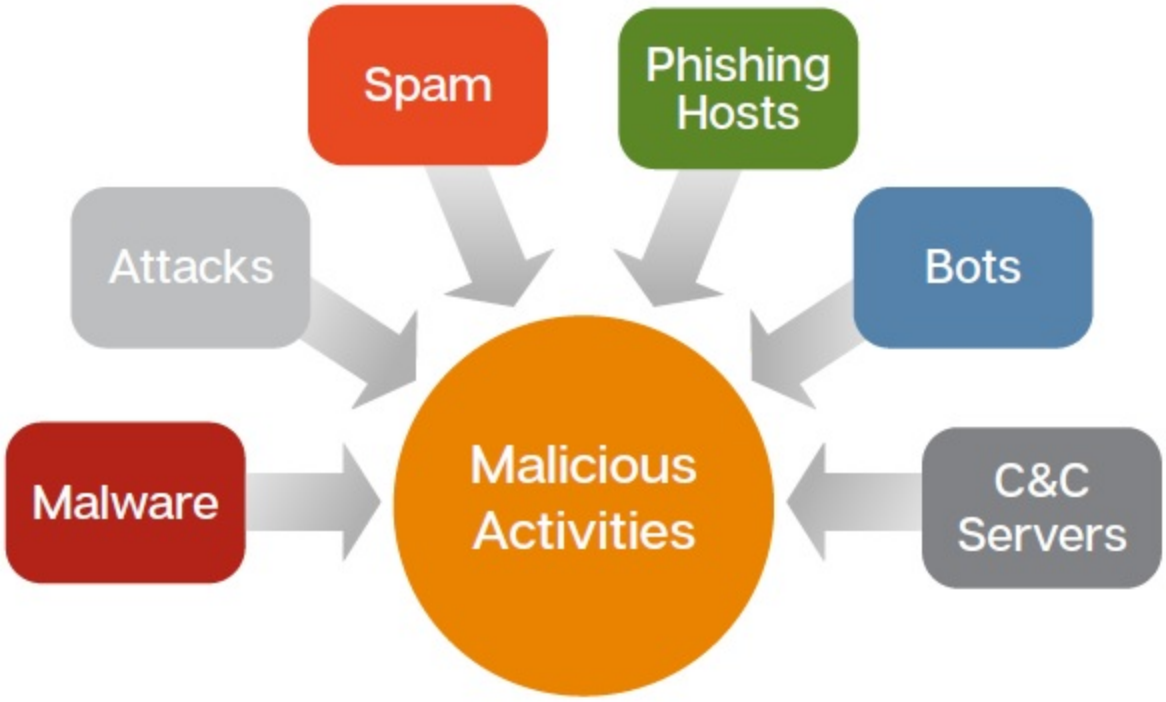
(Source: Symantec Cybersecurity Trends Africa Report)



Overall Malicious Activity-Africa

(Source: Symantec Cybersecurity Trends Africa Report)

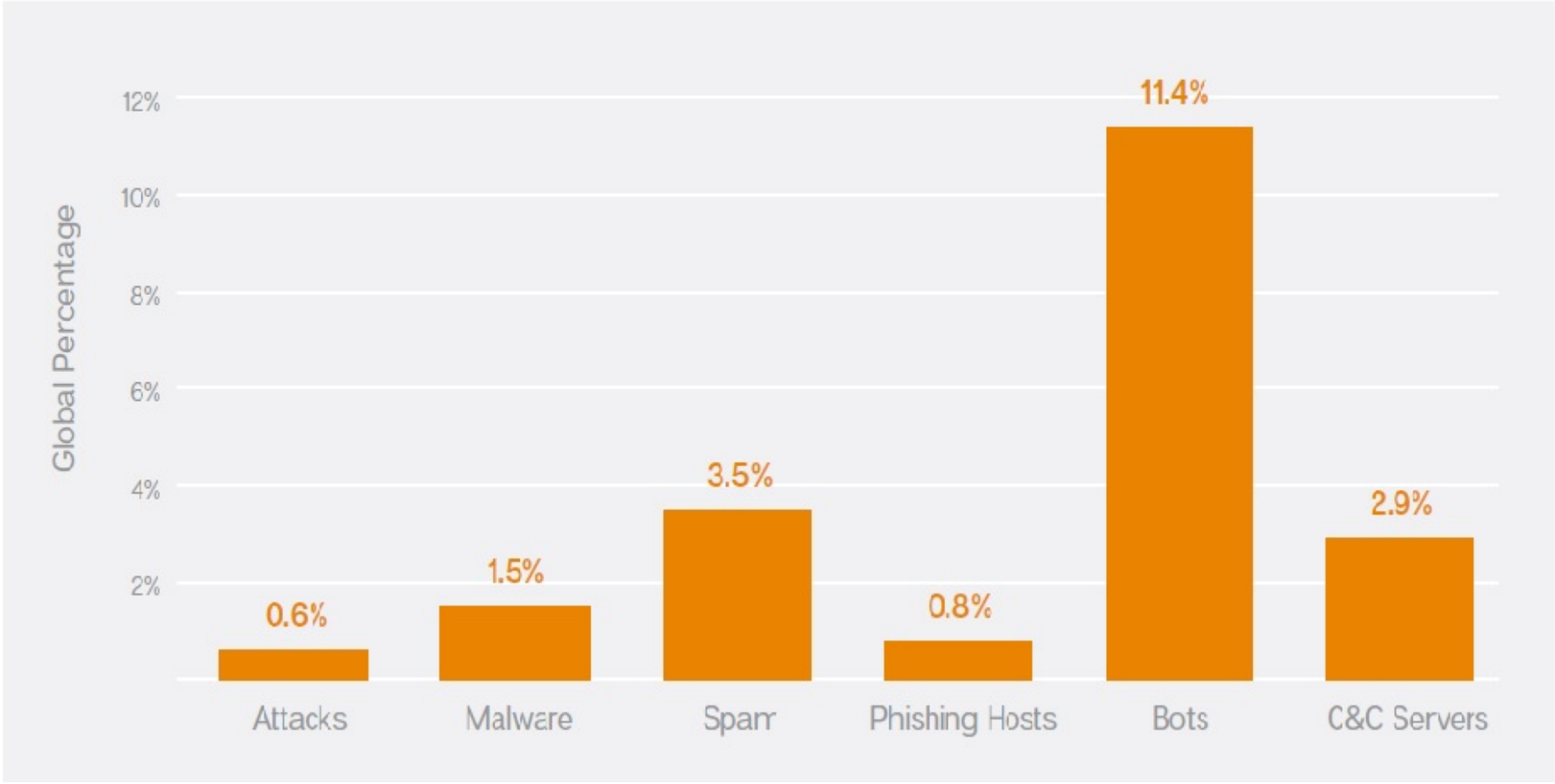
Figure 1: Malicious Activity Types



Malicious Activity originating from Africa

(Source: Symantec Cybersecurity Trends Africa Report)

Figure 2. Malicious Activity Originating from Africa–2016



Overall Malicious Activity-Africa

(Source: Symantec Cybersecurity Trends Africa Report)

Table 1. Overall Malicious Activity Originating from Africa–2016

MALICIOUS ACTIVITY	INCIDENT COUNT		GLOBAL PERCENTAGE
	GLOBAL	AFRICA	
Attacks	201,283,309	1,249,575	0.6%
Malware	559,789,928	8,501,677	1.5%
Spam	32,298,641,930	1,122,760,857	3.5%

MALICIOUS ACTIVITY	INCIDENT COUNT		GLOBAL PERCENTAGE
	GLOBAL	AFRICA	
Phishing Hosts	785,770	6,210	0.8%
Bots	122,605,684	14,006,143	11.4%
C&C Servers	69,872	2,017	2.9%

Top 10 African Countries Under Attack

(Source: Symantec Cybersecurity Trends Africa Report)

Table 2. Top 10 Source African Countries for Attacks–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	25%	314,880
Egypt	2	12%	149,685
Kenya	3	9%	106,265
Nigeria	4	7%	89,100
Mauritius	5	6%	73,134
Algeria	6	5%	60,381
Seychelles	7	4%	45,661
Botswana	8	3%	37,880
Morocco	9	3%	34,464
Tunisia	10	3%	32,187

Top 10 African Countries with Malware Profile

(Source: Symantec Cybersecurity Trends Africa Report)

Table 3. Top 10 Source African Countries for Malware–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	20%	1,716,308
Tunisia	2	14%	1,166,774
Kenya	3	8%	668,194
Nigeria	4	6%	469,018
Cote D'Ivoire	5	5%	407,112
Ghana	6	5%	405,805
Egypt	7	5%	400,679
Algeria	8	4%	304,114
Ethiopia	9	3%	245,172
Cameroon	10	3%	224,546

Top 10 African Countries with Phishing Hosts

(Source: Symantec Cybersecurity Trends Africa Report)

Table 5. Top 10 Source African Countries for Phishing Hosts–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
South Africa	1	74%	4,621
Morocco	2	5%	319
Egypt	3	3%	184
Kenya	4	3%	160
Nigeria	5	2%	136
Tunisia	6	2%	112
Cameroon	7	1%	57
Libya	8	1%	53
Zimbabwe	9	1%	51
Algeria	9	1%	48

Top 10 African Countries with Bots Profile

(Source: Symantec Cybersecurity Trends Africa Report)

Table 6. Top 10 Source African Countries for Bots–2016

COUNTRY	RANK	PERCENTAGE WITHIN AFRICA	INCIDENT COUNT
Egypt	1	48%	6,778,893
Algeria	2	15%	2,117,402
Tunisia	3	6%	798,121
South Africa	4	5%	768,800
Morocco	5	4%	601,180
Nigeria	6	3%	488,416
Kenya	7	3%	435,032
Ghana	8	2%	282,776
Sudan	9	2%	258,914
Cote D'Ivoire	10	2%	247,672

Threat Concerns on the IoT Devices

(Source: Internet of Evil Things Report 2017 by Pwnie Express)

→ **Business Concerns:**

- Brute force attacks on my WiFi networks
- IoT vulnerabilities
- Smartphone attacks
- WiFi and wireless vulnerabilities

→ **Personal Concerns:**

- Wireless Cars
- Wireless home monitoring and safety devices
- Vulnerable connected children's toys
- Smart TV's

Cybersecurity Initiatives

- Following projects are being undertaken to enhance the cyber security posture of the country:
  - Implementation of the National Cybersecurity Strategy
  - Finalisation of the National Cybercrime Strategy
  - Enhancement of the Legal Framework
  - Setting up of the Anti-Cyber Threat Monitoring System
  - Development of the Critical Information Infrastructure Protection Framework

Cybersecurity Initiatives (Contd.)

- Setting up of the Centralised Online Incident Reporting System

- Setting up of a National Cybersecurity Drill Infrastructure

Approaches for Securing IT Infrastructure

- Public Key Infrastructure (PKI)

- PKI has a history as the de-facto standard for Internet security and has the developing specifications to accommodate the requirements of diverse IoT deployments.

Approaches for Securing IT Infrastructure

- PKI Ecosystem implemented in Mauritius in 2012.
- ICT Authority as CCA
- eMudra as foreign CA
- NCB as Local Agent (Local CA)
- Mauritius Post as RA
- DSC’s are issued in Mauritius since 2013

Approaches for Securing IT Infrastructure

- Botnet Tracking and Mitigation System Implementation

Approaches for Securing IT Infrastructure

CERT-MU is in the process of setting up an infrastructure to proactively detect and take appropriate measures against botnets

Implementation of this system will provide safe and secure environment for businesses

The solution can be extended to IOT devices

Benefits:

Mitigation of existing botnets

Prevention of new infections

Minimizing profitability of botnets

Visualize threat landscape of the Mauritian cyberspace

Collaborative Responsibility to Help Secure IOT

THANK YOU!

Contact:

kusmani@cert.ncb.mu

Website: www.cert-mu.org.mu

Hotline: 8002378