SIYINQABA

NOVEMBER

2019 Eswatini National Cybersecurity Awareness Month.

Be Cyber Aware.
Be Cyber Smart.

Outline

- Emerging Technologies and Cyber threats in Telecoms
- What models can protect?
- How safe are we?
- How can we secure our networks?
- Top cyber security threats for ISPs and providers
- Consumer: How to protect yourself

Be Cyber Aware.
Be Cyber Smart.

Importance of cybersecurity in the world of telecommunication

- Telecommunications keep the world connected.
- Economies and entire business infrastructures are built on modern telecoms.
  - Email, messaging, phone and video calls, cloud, XaaS, IoT, OTT
- Intrinsic part of lives, like water / food: fundamental and readily available
- Networks are now highly complex, store large amounts of sensitive data- highly attractive to cyber criminals.
- *Cyber attacks are the 2nd highest global risk, the biggest risk for doing business in Europe and North America according to the World Economic Forum (WEF)(2019)*

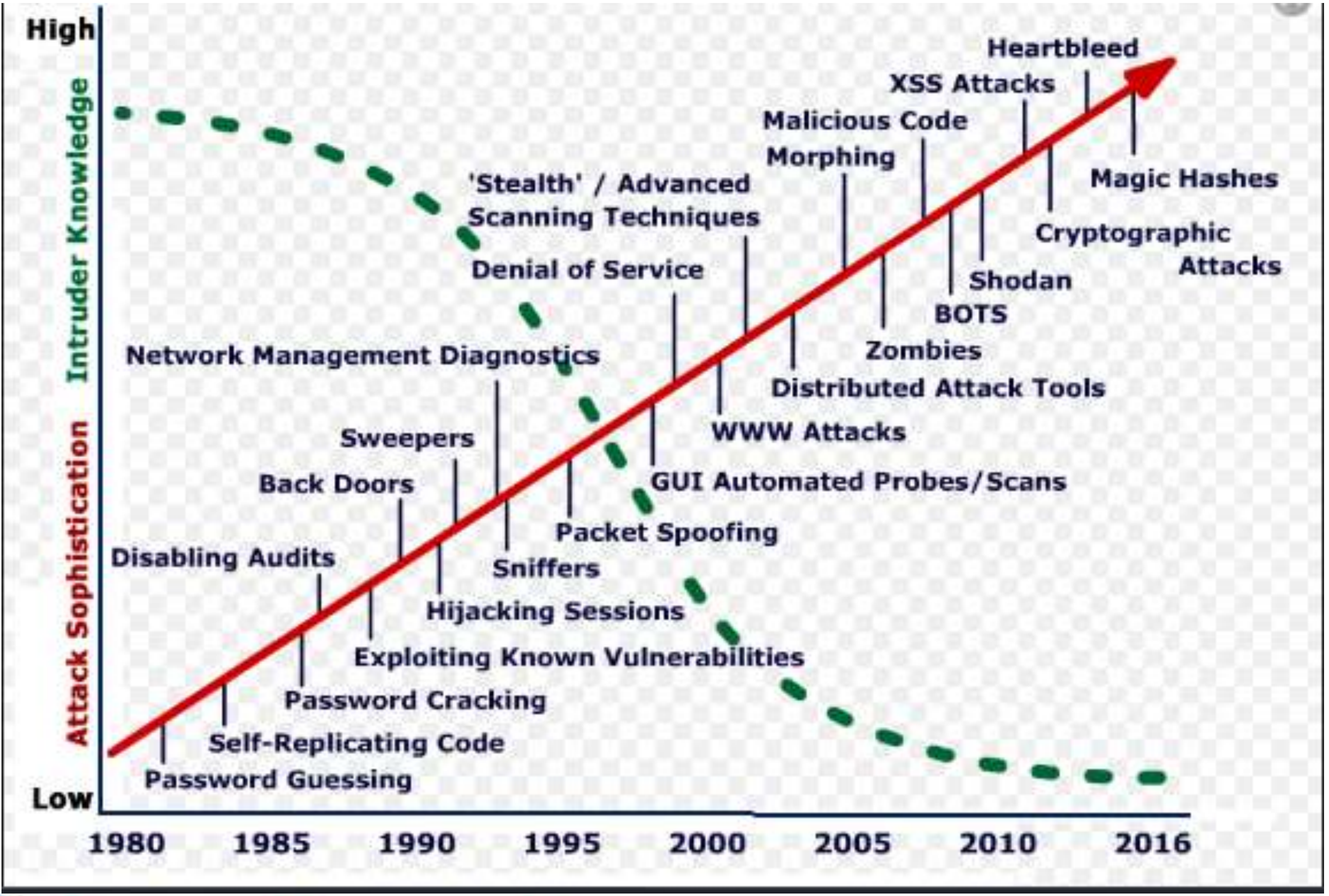
EPTC Transformation
Our People, Our Journey & Our Success

Cyber Threats in the Telecommunications Space

1. Emerging technologies impact on telecommunications cybersecurity

- Proliferation of insecure IoT devices *(Internet of Threats)*
- Cloud Services
- 5G
- Attacks are distributed.
- In the future, AI may be used to finely target victims
  - Two types of attacks:
    - Cyber criminals targeting telecom networks
    - Cyber criminals targeting their subscribers
  - Accessing telco core infrastructure is difficult

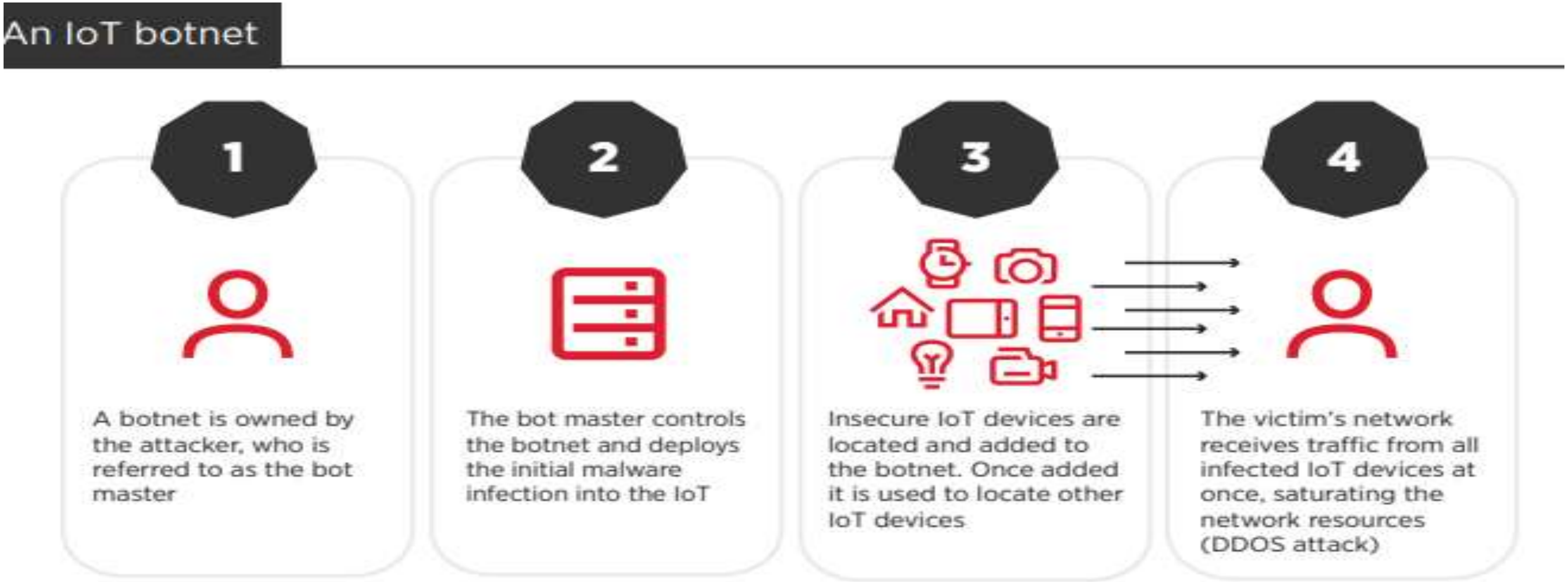
Attack Sophistication vs Attacker knowledge



EPTC Transformation
Our People, Our Journey & Our Success

Cyber Threats in the Telecommunications Space

Example of IoT vulnerability use for botnet and Distributed denial of service



An IoT botnet

1 A botnet is owned by the attacker, who is referred to as the bot master

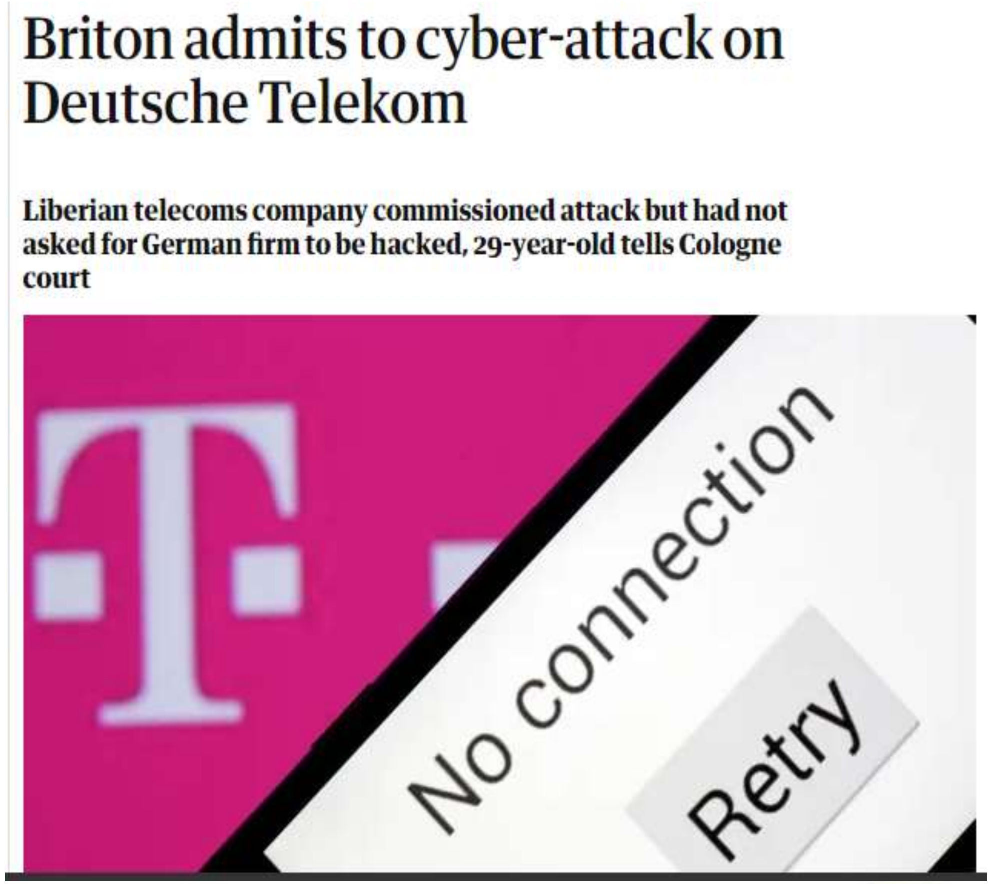
2 The bot master controls the botnet and deploys the initial malware infection into the IoT

3 Insecure IoT devices are located and added to the botnet. Once added it is used to locate other IoT devices

4 The victim's network receives traffic from all infected IoT devices at once, saturating the network resources (DDOS attack)

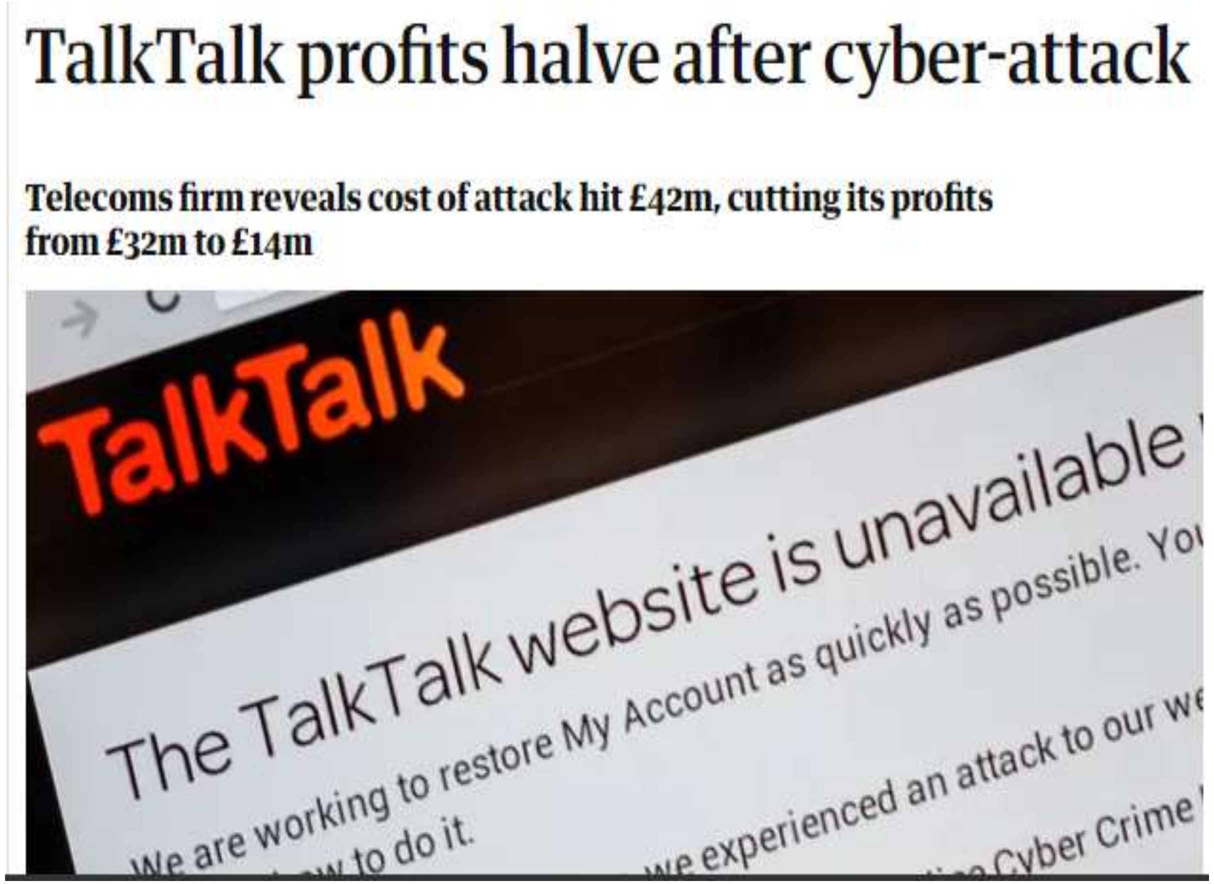
Cyber Threats in the Telecommunications Space

Be Cyber Aware.
Be Cyber Smart.



Briton admits to cyber-attack on Deutsche Telekom

Liberian telecoms company commissioned attack but had not asked for German firm to be hacked, 29-year-old tells Cologne court



TalkTalk profits halve after cyber-attack

Telecoms firm reveals cost of attack hit £42m, cutting its profits from £32m to £14m

TalkTalk
The TalkTalk website is unavailable
We are working to restore My Account as quickly as possible. You
...ow to do it.
...we experienced an attack to our we...
...Cyber Crime

EPTC Transformation
Our People, Our Journey & Our Success

Be Cyber Aware, Be Cyber smart

2. How Do we Defend? – Proactive Defense Models

Organizations must adopt an “active defense” model:

- anticipate attacks before they happen
- detect
- and respond in real time,
- establish traps and alarms to contain attacks
- adopt a tiered approach to protecting critical assets

Assume the worst will happen (someday it will): firewalls will be penetrated, encryption keys will be compromised, hackers will stay a step ahead in deploying malware.

Implement comprehensive, multi-layered security solution – leverage on AI

3. How safe is our telecoms space in the country?

1. **Safety is a function of the whole chain**
   1. Suppliers, hardware, software, people, customers, contractors, peers providers
   2. Enabling and deterring legislation
   3. Multiple routes and redundancies

2. Improvement to increase safety in Telecoms:

a) Adequate budget for cybersecurity

b) National regulatory frameworks on cybercrime

c) Replace insecure legacy protocols

d) Deploy skilled personnel

4. What should we do to secure our networks?

1. Appropriate leadership and processes to drive security measures consistent with digital advancements.
2. Adopt a holistic approach to cyber security (Managed Detection and Response, MDR)
   - Threat detection
   - Prevention measures
   - Incident response methods (CERT)
3. Adhere to standards-based systematic management of cybersecurity across the telecoms sector - eg

   NIST/ISO2701/CIS
4. Awareness: **create internal culture** of cybersecurity awareness (address human risks).

   Educate consumers: securing smart homes and IoT devices.
5. Collaboration and extension of boundaries/defences

Cyber Threats in the Telecommunications Space

5. What are the top Cybersecurity threats for the ICT industry?

Be Cyber Aware. Be Cyber Smart.

1. **Crypto Jacking:** Hijack of computers for the mining of cryptocurrency

2. **Distributed Denial of Service (DDoS) attacks**. vulnerable IoT devices increasingly used in botnets. Direct DDoS degrade performance, disrupt service availability. They can be a cover for a deeper, more damaging secondary attack.
3. **The exploitation of vulnerabilities in network and consumer devices**. new channels for attacks- Vulnerabilities in network devices, consumer or business, exploits for smartphones, poorly configured access controls, inadequate security for xG communications.

4. **Compromising subscribers with social engineering, phishing or malware**. attackers combine data sets from different sources, build detailed pictures of potential targets: (blackmail, social engineering,..)

5. **Insider threat**. Detailed profiles of targets are also used to recruit insiders to help perpetrate cybercrime. Some insiders help voluntarily, others are coerced through blackmail.

EPTC Transformation
Our People, Our Journey & Our Success

Cyber Threats in the Telecommunications Space

Be Cyber Aware.
Be Cyber Smart.

6. Protect thyself & your communications provider

Update your device’s firmware and software

Secure your devices

Have a healthy dose of suspicion

Read & hover before you click

Freebies – are they really free?

Anyone may be hacked: Think Georgia, Joburg Metro, Liberia, etc

EPTC Transformation
Our People, Our Journey & Our Success

Thank You!

Vusi Magagula
Eswatini Posts & Telecommunications corporation
vusi@sptc.co.sz