Escalating cyber threats in Africa, a top level summary.

Global Research and Analysis Team
Amin Hasbini
Head of research center (META)

kaspersky BRING ON THE FUTURE

The main trends

Demanding money, threatening and blackmailing

- Ransomware developments
- Including the switch to highly-targeted attacks
- Careful selection of targets, big pay-outs
- No sector off-limits
- Ransomware plus doxing to maximize ROI
- Legal sanctions to discourage ransom payments
- Collaboration of ransomware gangs
- The future will be a blend of established practices and a small number of APT-like gangs

APT threat actors buying initial network access from cybercriminals

Targeted ransomware gangs using generic malware, e.g. AgentTesla

Links between targeted ransomware groups and underground markets

APT threat actors to follow suit

The emergence of 5G vulnerabilities

- 5G has attracted a lot of attention this year
- Concerns about Huawei and fake health risks news
- Public and private researchers looking at the products of Huawei and others for implementation problems, crypto flaws and even backdoors
- Any flaws found will have massive impact
- Take-up of 5G will give hackers more incentive to look for vulnerabilities to exploit

More disruptive attacks

Bigger attack surface
than ever before

More disruptive attacks
in the future

Either through deliberate
attack or collateral damage

The African stats

2021 Africa statistics – happening right now

Top attacked countries

- Egypt
- Nigeria
- Algeria
- South Africa
- Kenya
- Tunisia

Top attacked industries

- Government
- Military
- Pharmaceutical
- Defense
- Energy

2021 Africa statistics – happening right now

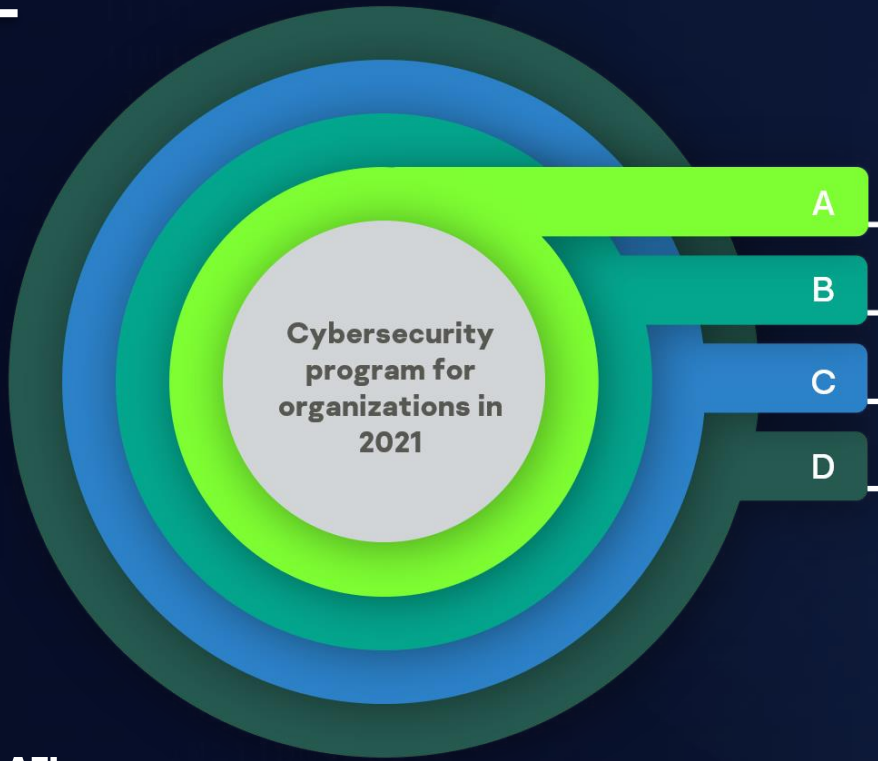
Top attack activities

1. Intelligence espionage
2. Industrial espionage
3. Criminal probing

Top attack groups

1. Lazarus
2. DroppingElephant
3. MuddyWater
4. IndigoZebra

Countermeasures



Advanced employees

Enriched with security trainings, awareness and intelligence on the latest attack methods, IOCs...

Advanced technologies

APT intelligence, SOC, SIEM, Feeds, EDR, AEP, Attribution engine, DFIR capabilities...

Advanced risk management

Vulnerability tracking, penetration testing, data centric classification and assessments...

Advanced compliance

Governance, laws and regulations, procedures, executive management involvement...

GREAT

Thank you!

Contact: amin.hasbini@kaspersky.com

GREAT

kaspersky