ITS - Cyber Security

www.ITS.ws

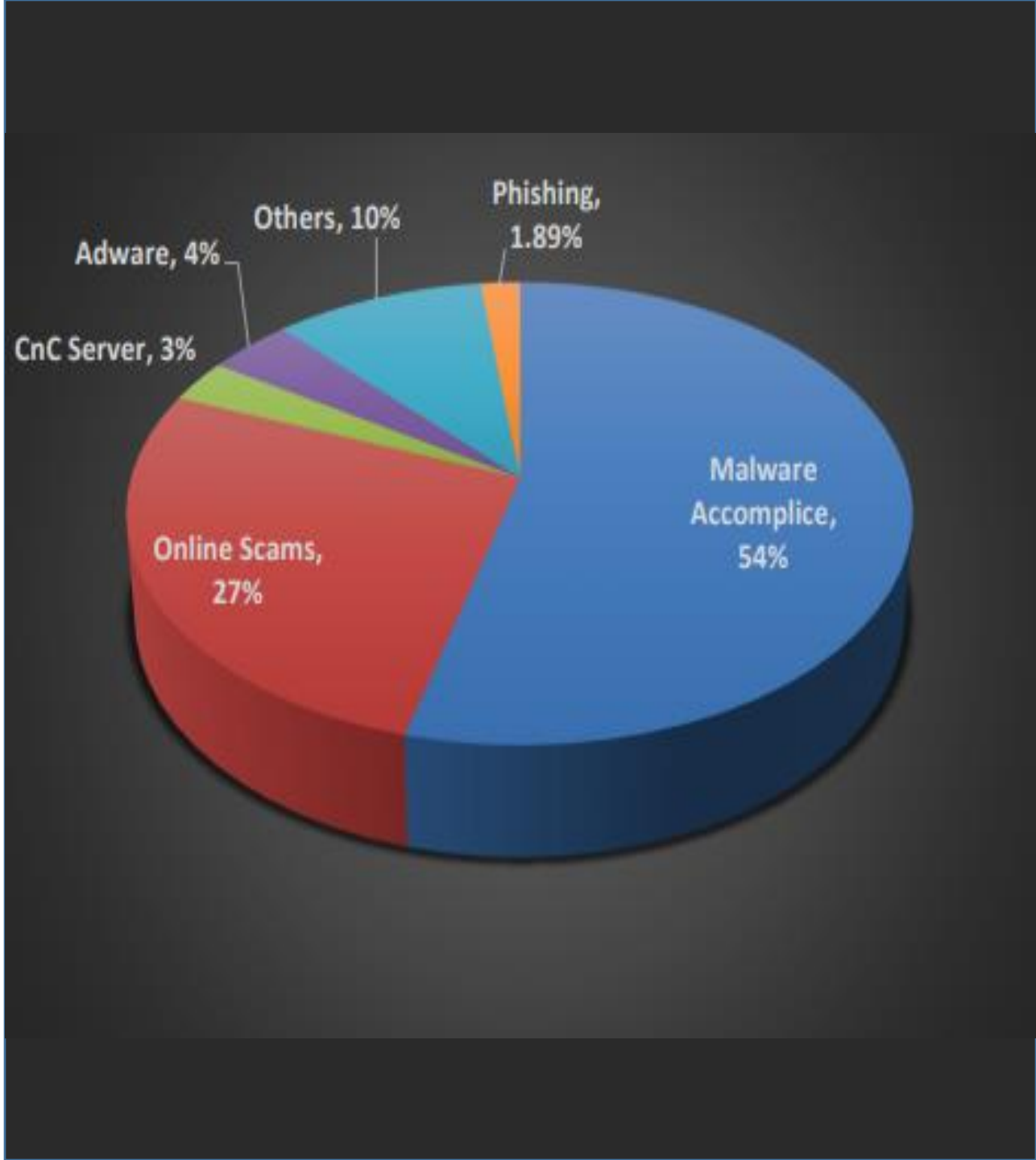
The main cyberthreats in Africa

- **Online scams**: fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information.
- **Digital extortion**: victims are tricked into sharing sensitive information that will be used later on for blackmail
- **Business email compromise**: criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account
- **Ransomware**: cybercriminals block the computer systems of banks, hospitals and public institutions, then demand money to restore functionality
- **Botnets**: networks of compromised machines are used as a tool to automate large-scale cyberattacks

www.ITS.WS

Business email compromise

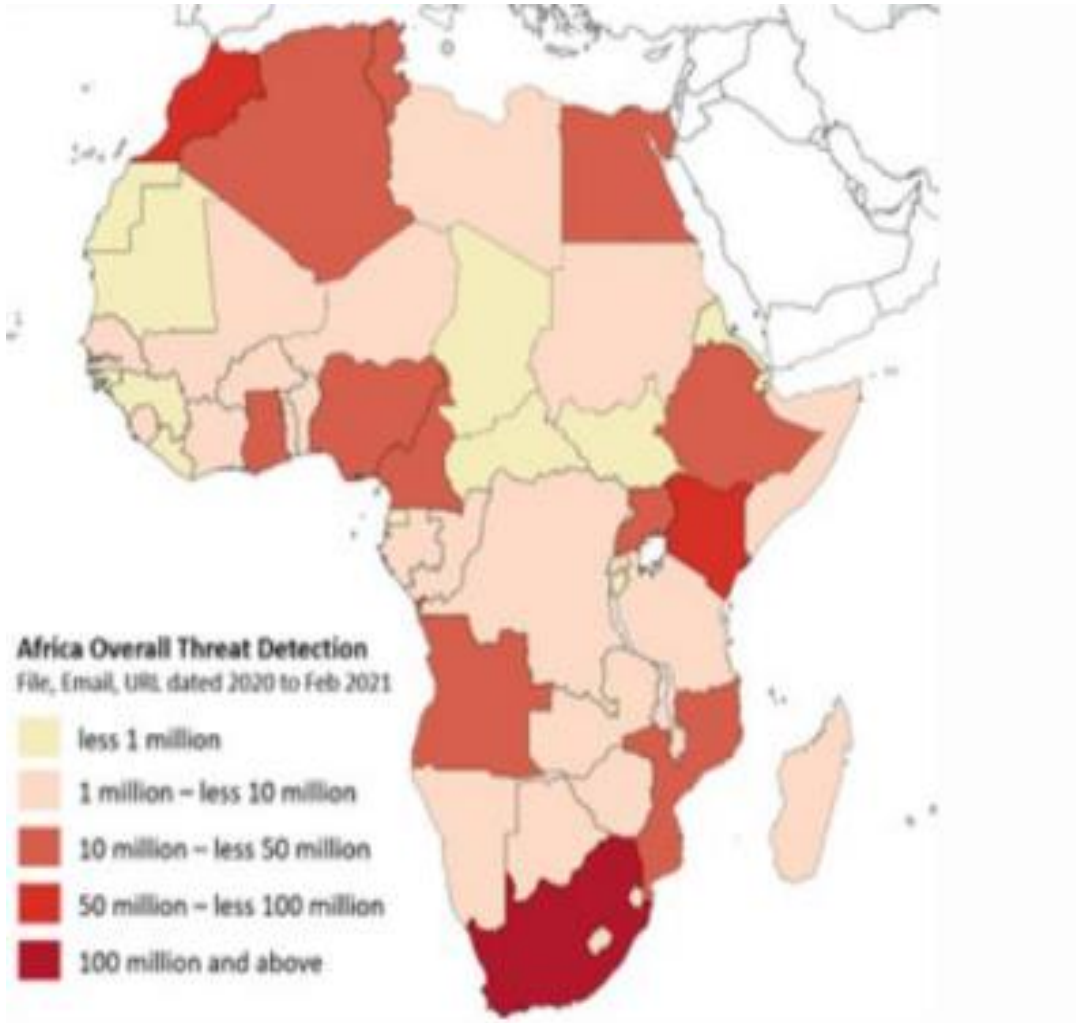
- Business email compromise (BEC) is one of the most financially damaging online crimes
- 28.14% of respondents reported that they had previously clicked on a phishing email
- 27.71% had previously fallen for a scam
- 19% had forwarded a spam or hoax email. alone.



www.its.ws

Threat Detection

- INTERPOL recorded millions of threat detections in Africa from January 2020 to February 2021
- Email: 679 million detections
- Files: 8.2 million detections
- Web: 14.3 million detections



Cost of Data Breach

$3.86M

Global average cost of a data breach

- 1.5%
decrease from 2019

$392 million

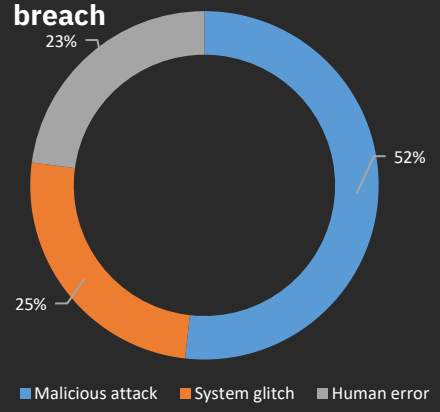
Average total cost of a breach of >50M records

$150

Cost per record for compromised customer PII

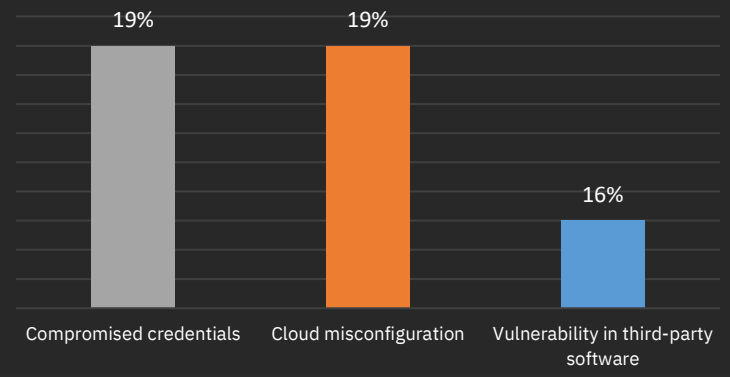
#1
Healthcare and U.S. costliest industry and country

Root causes of a data breach



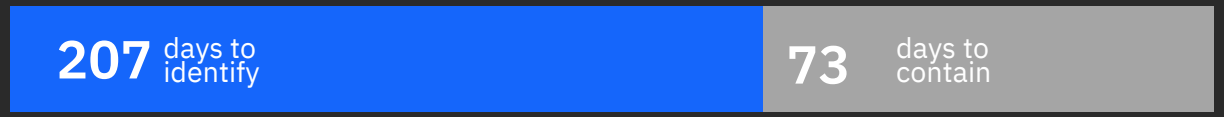
Top 3 initial attack vectors

(percentage of malicious attacks)



Time to identify and contain

Global average: 280 days



$2 million

Average cost savings with incident response teams and IR testing vs. no IR teams or testing

Cyber Security Challenges

"I don't have enough **time** to go after every new **threat**, **alert**, **patch and compromised devices accessing** critical apps."

"We can't always get to the **root cause** of every **attack**, **stolen credentials**, or find the best **security/productivity** balance."

"My team can't be **experts** on every new **threat, threat hunting**, and all **compliance and privacy** mandates."

www.its.ws

ITS-NIST Alignment

www.its.ws

Cybersecurity Services

Managed SOC

Tailored services to design, build, staff, and operate a 24/7 security operations center that meets your specific needs.

SOC-as-a-Service

All the benefits of a modern SOC, but without the cost or complexity of designing, staffing, and operating one.

Red Team

Penetration testing and other red team services that strengthen your security by finding vulnerabilities before an attacker exploits them.

Blue Team

Assessment and audit services that identify your security gaps and improve your defenses against an attack, without adding staff.

www.its.ws

Alliances


RSA


Secureworks


IBM


THREATQ


SWIMLANE


paloalto
NETWORKS


exabeam


Carbon Black.


zscaler


DARKTRACE


CITRIX


ATTACKIQ


Check Point
SOFTWARE TECHNOLOGIES LTD


CISCO


CYSIV


FORTINET


DELL Technologies


VERITAS


ITS
www.ITS.ws

Thank You

Let’s Stay Connected


ITSCorporate


ITS_Corporate


ITSCorporate


ITSGroup


info@its.ws