10 Defining Moments of the 2025 Cyber Threat Landscape

A 360° retrospective as we close the year

The battlefield moved.
Here's what changed.

Swipe

In 2025, the question changed

From: "How do we prevent breaches?"
To: "How fast can we detect and recover?"

Attacks became continuous operational pressure, not exceptional events.
The institutions that thrived were those who built resilience through visibility, rapid response, and assumed breach mentality.

Swipe

The Identity Takeover

Attackers stopped breaking in. They logged in.

What we observed in 2025:

- 32% increase in identity-based attacks (H1 2025)
- 97% involved password spray or brute force
- Credentials and tokens replaced traditional exploits
- 80% of access broker intrusions were credential-based

The defense that worked: MFA blocked 99%+ of identity attacks

Swipe

AI Scaled Social Engineering to Industrial Levels

"What changed wasn't the tactic—it was the scale and precision"

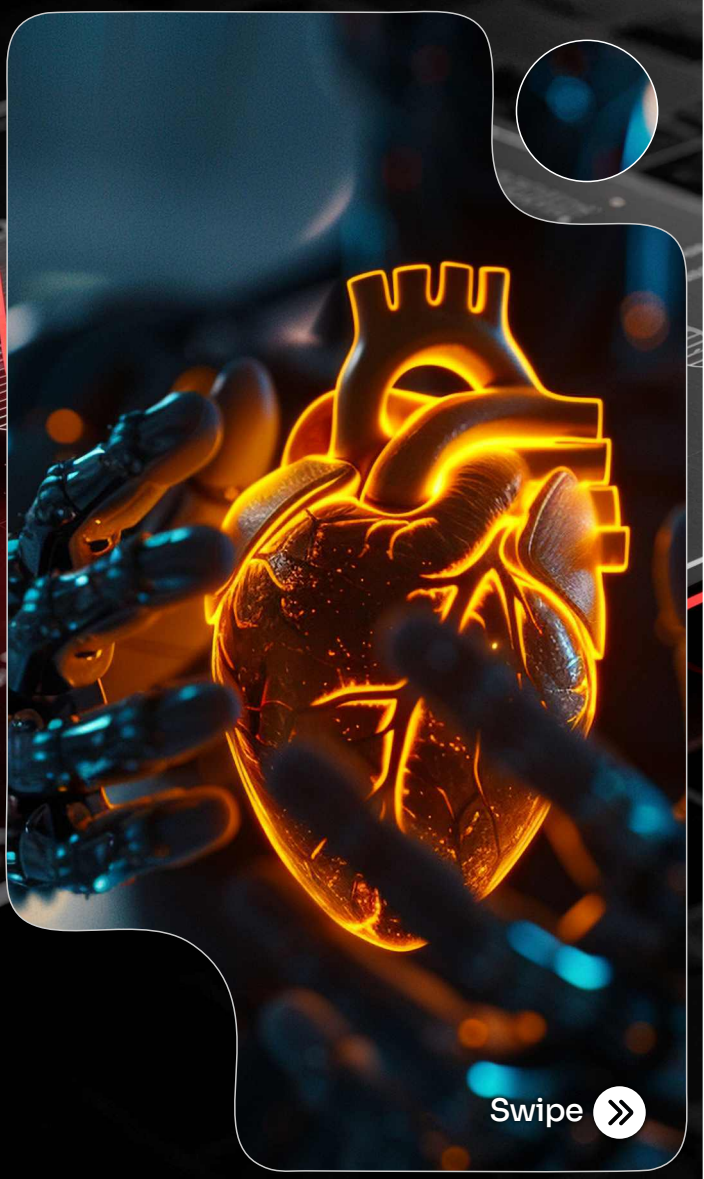
The 2025 evolution:

- Over 80% of social engineering incorporated AI support.
- Attackers combined leaked data + public OSINT + AI processing.
- Result: Hyper-personalized scams at industrial scale

Real impact in Africa:

- BEC attacks with accurate org charts and internal context
- Customer fraud in local languages referencing actual transactions
- SIM swap operations enhanced with AI-gathered intelligence

OSINT existed before. AI made it scalable, faster, and devastatingly precise.



Swipe

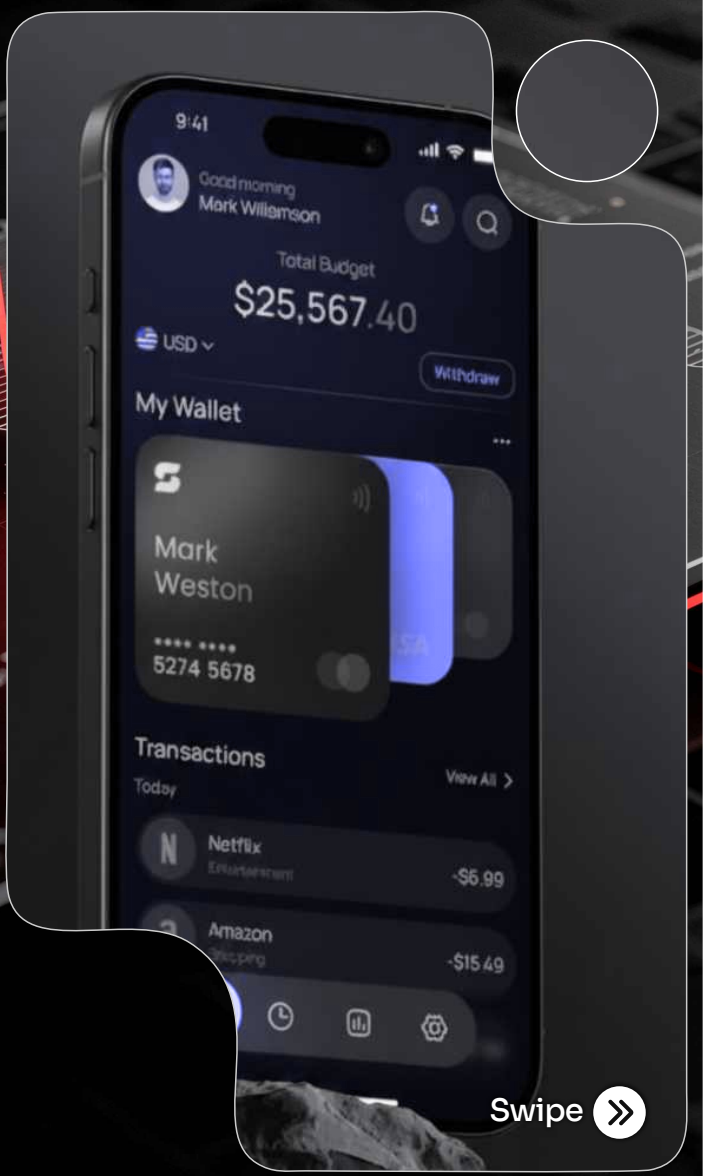
Mobile Banking Became the Primary Battlefield

"In Africa, where the money moved, fraud followed at scale"

What dominated 2025:

- SIM swap fraud executed at industrial levels
- Automated bot attacks on compromised devices
- Payment infrastructure API vulnerabilities systematically exploited
- Mobile transaction dominance = massive attack surface expansion

60% of initial access still came through phishing,now optimized for mobile delivery



Swipe

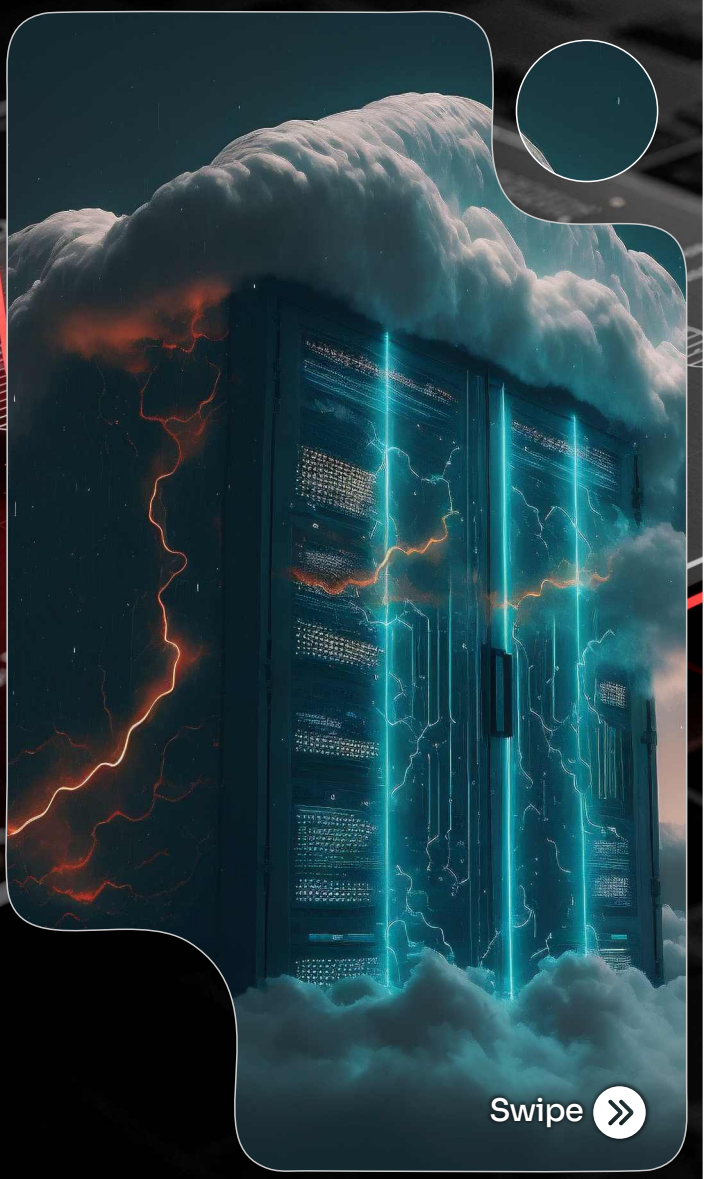
The Cloud Became a Warzone

"87% increase in destructive cloud-focused campaigns"

Critical shifts we tracked:

- 40%+ of ransomware targeted hybrid (on-prem + cloud) environments
- Mass VM deletion and OAuth app abuse became standard tactics
- Identity and access management gaps proved catastrophic
- Legacy authentication protocols in cloud environments = open exposure

On-premise security ≠ cloud security



Swipe

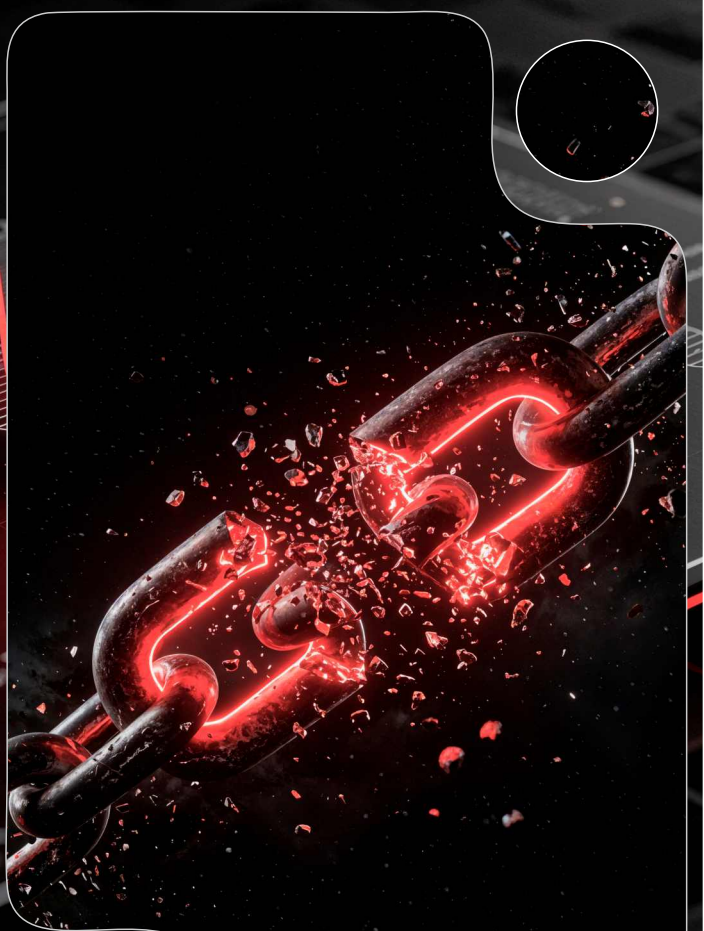
Supply Chain Became the Weakest Link

"You're only as secure as your weakest vendor"

What we witnessed:

- Vendor integrations exploited as primary entry points
- API misconfigurations in open banking ecosystems
- Third-party service provider compromises cascaded across clients
- Shared infrastructure vulnerabilities amplified blast radius

368 access brokers operated across 131 countries, 68 industries—targeting your vendors to reach you



Swipe

Infostealers Became Foundation Tools

"They evolved from nuisance to enterprise threat"

The 2025 pattern:

- Infostealers harvested credentials, cookies, tokens, system context.
- Fed directly into ransomware and extortion operations.
- Lumma Stealer alone accounted for 50%+ of observed activity.
- One infostealer infection signaled high probability of future breach.

Detection shifted from "clean the malware" to "assume enterprise compromise

Swipe

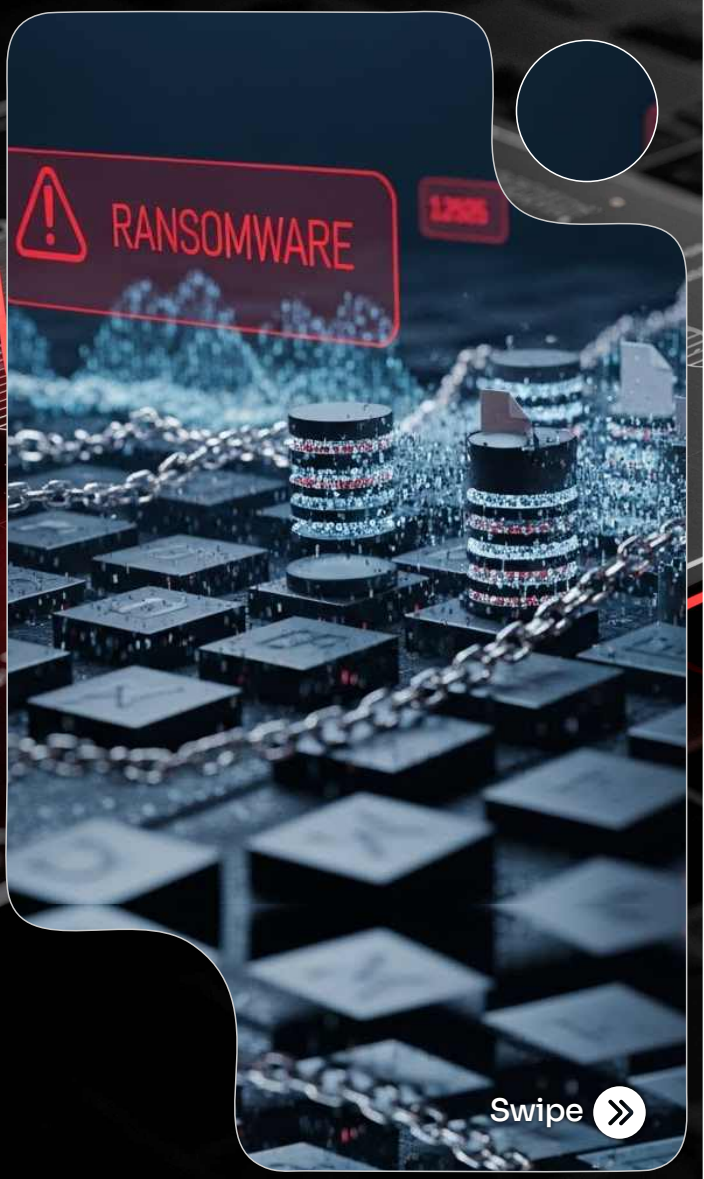
Ransomware Stopped Being About Malware

"It became about privileged access abuse"

Tactics that defined 2025:

- OSINT reconnaissance mapped organizational structures
- AI-powered helpdesk impersonation and vishing
- Teams-based social engineering with insider context
- RMM tool abuse in 79% of cases
- Deliberate targeting of antivirus exclusions (30% of incidents)

The payload mattered less than knowing who to impersonate and what to say



Swipe

Cybercrime Fully Industrialized

"The service economy matured"

What 2025 proved:

- Phishing-as-a-Service drove 60% of initial access
- Access as a Service brokers specialized and scaled
- Ransomware as a Service lowered barriers to entry
- 80% of intrusions relied on commercialized, credential-based operations

Lower barriers + specialization = relentless, high-volume pressure