2024 CYBER THREAT REPORT
RBC ENTERPRISE LIMITED

EXECUTIVE SUMMARY

This comprehensive report examines the evolving cybersecurity threat landscape across East Africa throughout 2023 and into early 2024. Based on data collected from over 500 organizations and analysis of more than 2,000 security incidents, we have identified significant shifts in threat actor tactics, techniques, and procedures (TTPs) that organizations in the region must address to maintain effective security postures.

The digital transformation agenda across East Africa has accelerated dramatically, with Kenya, Rwanda, and Tanzania leading regional technology adoption. However, this rapid digitalization has created an expanded attack surface that sophisticated threat actors are actively exploiting. Organizations face challenges from both opportunistic cybercriminals and advanced persistent threats (APTs) targeting critical infrastructure, financial systems, and sensitive data.

This report provides decision-makers with actionable intelligence to understand the current threat environment, anticipate emerging risks, and implement effective countermeasures appropriate for the East African context.

KEY FINDINGS

- Ransomware attacks increased by 157% across East Africa in 2023, with average ransom demands rising to $95,000 USD

- 64% of breaches exploited vulnerabilities that had available patches for more than 30 days

- Financial services (37%), healthcare (24%), and government sectors (18%) were the most heavily targeted

- 78% of organizations experienced at least one successful phishing attack

- Mobile-based attacks grew by 213% alongside the expansion of mobile payment systems

- Supply chain attacks have become more sophisticated, with 42% of major breaches originating through third-party vendors
- Cloud security misconfigurations accounted for 31% of data breaches
- Average dwell time (time between initial compromise and detection) stands at 24 days
- The cybersecurity skills gap across East Africa exceeds 10,000 professionals

THREAT LANDSCAPE OVERVIEW

Ransomware Evolution

Ransomware remains the most significant threat facing East African organizations. Beyond the traditional encryption of data, ransomware groups have evolved to employ double and triple extortion tactics. These include data theft before encryption, threats to publish sensitive data, and distributed denial-of-service (DDoS) attacks to pressure victims into paying ransoms.

The LockBit, BlackCat, and Royal ransomware variants were particularly active in the region. A major financial institution in Kenya experienced a sophisticated ransomware attack in November 2023 that disrupted services for nearly three days and resulted in significant financial and reputational damage.

Initial Access Vectors

Email phishing remains the primary initial access vector, accounting for 47% of successful breaches. However, we've observed a significant increase in sophisticated social engineering attacks targeting executives through WhatsApp and other messaging platforms. These attacks often leverage AI-generated content to create convincing impersonations.

RDP (Remote Desktop Protocol) exploitation accounts for 23% of initial access, followed by exploitation of internet-facing applications (18%) and compromised credentials (12%).

Emerging Threats

Several emerging threats have gained prominence:

1. Mobile Malware: With mobile penetration rates exceeding 85% in many East African countries, cybercriminals are increasingly targeting mobile devices through malicious applications, SMS phishing (smishing), and exploiting vulnerabilities in popular mobile payment systems. Banking trojans like Alien and Cerberus have been modified specifically to target East African mobile banking applications.

2. Supply Chain Compromises: As businesses digitize their supply chains, attackers are targeting vulnerable links in these ecosystems. By compromising smaller vendors or service providers with access to larger organizations, attackers can bypass robust security measures. The SolarWinds-style attacks have inspired regional threat actors to adopt similar techniques.

3. AI-Enhanced Attacks: Cybercriminals are leveraging artificial intelligence to enhance their attacks. AI-powered phishing campaigns that mimic legitimate communications with remarkable accuracy have been particularly effective against organizations in the region. These attacks feature grammatically correct emails that closely resemble authentic organizational communications.

4. Cloud Security Vulnerabilities: As organizations migrate to cloud-based solutions, misconfigured cloud environments have become a significant vulnerability. In 2023, several data breaches in the region resulted from improperly secured cloud storage buckets and inadequate access controls, particularly in S3 buckets and Azure Blob storage.

REGIONAL FOCUS: KENYA, TANZANIA, RWANDA, AND UGANDA

Kenya

Kenya continues to lead the region in both technology adoption and cybersecurity maturity. The implementation of the Data Protection Act has driven improved security practices, though compliance remains inconsistent. Financial services and mobile money platforms face the highest attack volumes, with fraudulent transactions increasing by 32% in 2023.

The Communications Authority of Kenya reported over 278 million cyber threats detected in Q4 2023 alone, representing a 47% increase from the previous quarter. Notable incidents included multiple DDoS attacks against government portals and a major data breach affecting a healthcare provider.

Tanzania

Tanzania has seen a rapid increase in cyber threats as digital transformation initiatives expand. The Tanzania Communications Regulatory Authority (TCRA) reported a 67% increase in reported cybersecurity incidents in 2023. The energy sector and government services have been particularly targeted, with several ransomware incidents affecting critical infrastructure.

The lack of comprehensive data protection legislation creates additional challenges for organizations operating in Tanzania, though this is expected to be addressed with new regulations in late 2024.

Rwanda

Rwanda maintains the most comprehensive cybersecurity framework in the region, with strong government leadership in digital initiatives. The National Cyber Security Agency has implemented proactive measures that have reduced successful attacks by 23% year-over-year.

Despite these successes, Rwanda's position as a growing financial hub has attracted sophisticated threat actors. Targeted spear-phishing campaigns against financial institutions increased by 78% in 2023, though the average time to detection was significantly better than regional averages at 9 days.

Uganda

Uganda faced substantial challenges from both cybercriminals and hacktivism in 2023. The Uganda Computer Emergency Response Team reported a 112% increase in security incidents, with government agencies and telecommunications providers facing the most significant pressure.

Mobile money fraud remains a persistent issue, with over 7,000 reported cases affecting Ugandan citizens. The implementation of the Data Protection and Privacy Act has begun to improve organizational security practices, though enforcement remains limited.

PREDICTIONS FOR 2024-2025

Based on current trends and threat intelligence, we anticipate the following developments in the East African cybersecurity landscape:

1. Regulatory Evolution: Data protection regulations will mature across the region, with increased enforcement actions and potential penalties for security failures. Organizations should expect regulatory harmonization efforts across the East African Community.

2. Ransomware Specialization: Ransomware groups will increasingly target specific industries with customized malware designed to exploit sector-specific technologies and processes.

3. Critical Infrastructure Focus: Attacks against energy, telecommunications, and water management systems will increase as these sectors continue digital transformation without commensurate security investments.

4. Mobile Platform Targeting: The dominance of mobile-first services will drive increased sophistication in mobile malware, particularly targeting financial applications and two-factor authentication mechanisms.

5. AI-Powered Defense: Organizations will increasingly leverage artificial intelligence and machine learning to enhance threat detection and response capabilities, though this will be constrained by the skills gap.

6. Cloud Security Maturity: As cloud adoption accelerates, security practices will mature, though misconfigurations will remain a significant risk factor throughout 2024.

7. Collaborative Defense: Industry-specific security alliances and information sharing initiatives will become increasingly important in addressing shared threats, with financial services leading this trend.

RECOMMENDATIONS FOR ORGANIZATIONS

Strategic Recommendations

1. Implement Zero Trust Architecture: Adopt a zero trust security model that requires strict identity verification for every person and device attempting to access resources, regardless of location.

2. Develop Comprehensive Security Awareness: Create role-specific training programs that address both technical and non-technical staff needs, with particular focus on phishing recognition.

3. Establish Security Operations Capability: Whether internal or outsourced, organizations need dedicated security monitoring and incident response capabilities appropriate to their risk profile.

4. Create Business Continuity Plans: Develop and regularly test business continuity and disaster recovery plans that address ransomware and other disruptive cyber attacks.

5. Engage with Industry Partners: Participate in information sharing communities and establish relationships with peer organizations to enhance threat intelligence capabilities.

Tactical Recommendations

1. Implement Multi-Factor Authentication: Deploy MFA across all systems, particularly for remote access, privileged accounts, and email.

2. Establish Vulnerability Management: Develop processes to identify, prioritize, and remediate vulnerabilities, with critical patches applied within 14 days.

3. Segment Networks: Implement network segmentation to contain potential breaches and limit lateral movement by attackers.

4. Secure Cloud Environments: Implement cloud security posture management tools and processes to prevent misconfigurations and excessive permissions.

5. Deploy EDR/XDR Solutions: Implement endpoint or extended detection and response solutions to enhance visibility and response capabilities.

6. Secure Backup Strategy: Implement the 3-2-1 backup strategy with offline copies that cannot be affected by ransomware.

ABOUT RBC ENTERPRISE LIMITED

RBC Enterprise Limited is a leading provider of cybersecurity solutions in East Africa, offering comprehensive security services, training, and consulting to organizations across multiple sectors. With offices in Nairobi, Kigali, and Dar es

Salaam, our team of certified security professionals delivers practical, contextualized security solutions that address the unique challenges of the East African technology landscape.

For more information about how RBC Enterprise Limited can enhance your organization's security posture, contact us at security@rbc-enterprise.com or visit our website at www.rbc-enterprise.com.