Serianu Cyber Security Advisory

Christmas Season Security Advisory

SOC Advisory Number:

TA – 2024/012

Date(s) issued:

16th December 2024

As we embrace this festive season; a time to pause, recharge, and connect with loved ones while reflecting on the year gone by, it is essential to remain vigilant. Cybercriminals have increasingly leveraged this period of reduced activity and heightened online transactions to exploit vulnerabilities in systems and processes.

At Serianu Cyber Command, our analysis reveals that the holiday season consistently presents a high-risk period for cyberattacks, with threat actors exploiting remote working, holiday giveaways, reduced vigilance, heightened financial activity and weakened monitoring across industries. This year, cyber threats in Africa have grown more sophisticated, with attackers forming syndicates and deploying advanced techniques to target critical infrastructures, financial institutions and operational controls. Cybercriminals have embraced AI-driven tools enabling automated phishing, ransomware and fraud operations. These innovations have fueled the surge in deepfake scams and social engineering techniques which are now increasingly affecting African markets.

The recent INTERPOL-led *Operation Serengeti* targeting cybercrime across Africa revealed that **credit card fraud** was a major attack vector. In Kenya, for example, cybercriminals employed fraudulent scripts to bypass banking security protocols, facilitating the theft and redistribution of approximately $8.6 million through systems like **SWIFT**. These attacks exemplify the sophisticated tactics being used, including the manipulation of core financial infrastructures to exploit vulnerabilities. The report further revealed a notable increase in ransomware, business email compromise (BEC), digital extortion and SIM card fraud, underscoring the diverse and evolving strategies of cybercriminals.

To help safeguard your operations, we have outlined key actions to ensure you **Anticipate, Detect and Respond** to potential threats effectively. Below, we provide a concise list of IT and operational recommendations designed to maintain a strong security posture throughout the holiday period.

Key areas to focus on this season include:

1. Database and Transaction Monitoring

Prioritize monitoring for unusual patterns such as:

- Database connections coming from New or Unauthorized IP address
- Successful and failed logins into the database
- Modifications involving dormant accounts, including [inserts/deletes/updates]
- Modifications targeting recently registered or activated accounts
- Modifications to customer mobile banking data
- Modifications to customer card application data
- Source account initiating more than 3 transactions per day
- Receiving account credited more than 3 transactions per day
- Transfers into a recently registered or re-activated account
- Withdrawals from a recently registered or re-activated account
- Analyze database activity for anomalies that could indicate AI-driven fraud

2. Channels Monitoring

a) Mobile and Agency Banking Monitoring

Leverage real-time financial dashboards, enhanced with visual color-coding where applicable and daily activity reporting to efficiently monitor mobile and agency banking operations.

Block, Alert and Investigate:

- Transactions initiated by phone numbers NOT registered as subscriber numbers.
- Single transactions that exceed approved limits.
- Daily transaction volumes exceeding daily approved limit
- Phone numbers receiving funds from multiple accounts in a short timeframe.
- Source account transacting with multiple phone numbers.
- Transactions involving phone numbers registered within the last 10 days.
- Remain alert for deepfake enabled scams and AI-crafted phishing attacks targeting mobile money users.
- Educate customers on verifying the authenticity of suspicious messages and promotions.

b) ATM and POS Banking

Use comprehensive monitoring tools/reports to track and respond to unusual activity in ATM and POS channels.

Block, Alert and Investigate:

- Single transactions exceeding approved limits.
- Daily cumulative transactions exceeding set thresholds.
- Source account transacting with multiple card numbers.
- Newly issued card numbers transacting (suspiciously) within 10 days of issuance/registration.

c) Account to Account Transfers

Strengthen vigilant oversight on core banking systems by implementing detailed alerts and periodic reports.

Monitor, Alert and Report:

- Source accounts initiating more than 3 transactions per day.
- Receiving accounts credited with more than 3 transactions per day.
- Transfers directed to recently registered or re-activated accounts.
- Withdrawals from recently registered or re-activated accounts.
- Daily and weekly transaction summary reports highlighting accounts exceeding agreed thresholds.
- Activity transaction summary reports providing details on privileged user activities in the system - including approvals, creations and deletions.

d) Review Transactional Data Validation

Enhance thorough review and approvals of all transactional data changes before implementation by internal teams and service providers.

3. Strengthen Remote Access Management

- Restrict VPN access to only essential personnel and trusted vendors only.
- Ensure thorough vigilance for public facing devices and disable Manager interface for these devices.
- Implement Multi-Factor Authentication (MFA) on all critical applications including VPNs and emails.
- Use jump servers for access to critical and sensitive business systems, ensuring clear attribution to all activities.
- Audit cloud configurations regularly to prevent misconfigurations, a leading cause of breaches in 2024.

- Strengthen security protocols for supply chain vendors to mitigate risks from third-party software updates and integrations.
- Limit use of multiple different remote access tools (e.g AnyDesk, TeamViewer, RDP) through the firewall, instead standardize on a single approved tool for remote operations.

4. Default Accounts Management

- Avoid reliance on default system accounts like “**Administrator**” on Active directory or “**Root**” on Linux systems.
- Enforce access to critical systems exclusively through personal user credentials allowing default account use only under exceptional circumstances and with explicit approval.

5. Physical Access Restriction and Change Management

- Limit physical access to environments strictly to scheduled shifts or formally approved requests.
- Maintain an updated asset register for all devices brought on premises.
- Coordinate with the Serianu team or persons working from home and on shift during the holiday.
- Continuously monitor critical service availability and report outages promptly to the SOC team.
- Enforce a change freeze for business-critical systems to minimize operational risks.

6. User awareness Training and Critical Technology Updates

- Ensure employees can identify and report phishing attempts, particularly holiday-themed scams.
- Educate users on identifying deepfake-enabled scams, voice impersonation, SIM Fraud tactics and other social engineering techniques.
- Stay updated on critical patch releases and apply them immediately to mitigate vulnerabilities.
- Restrict work environment access to authorized personnel only, ensuring formal approval for anyone not on shift.
- Instruct employees to power down workstations when leaving the office or before going on holiday.

Conclusion

The 2024 cyber threat landscape underscores the importance of adapting defenses to new attack vectors, including AI-powered threats and cloud misconfigurations. It is critical you perform an analysis of your environment, validate that these controls have been implemented and that you have visibility on all transactions, vendor activities and changes being made to critical systems by your internal team. This will require the collective cooperation of IT, Risk and Audit.

We encourage recipients who are unsure of their security posture, unsure of their technical capabilities to implement the above recommendations and/or identify malicious activity or use of tools or techniques that seem malicious to contact us on the following:

Cybercrime hotline *+254(0) 771949475,* ***email****: Info@serianu.com.*