مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Bolstering Defenses Against Ramadan Festive Season Cyber Threats

Date: 05-03-2025

Executive Summary

The Ramadan season has arrived, bringing joy and celebration across the UAE. However, during this period, organizations and individuals are more vulnerable to digital threats due to reduced staffing, a distracted workforce, and operational changes that are common during Ramadan. UAE Council Threat Intelligence has observed active campaigns, ranging from financially motivated phishing to state-sponsored espionage, which pose risks to financial stability, operational continuity, and national security.

The rise in e-commerce, charitable donations, and remote work, combined with reduced staffing, creates new vulnerabilities during the Ramadan season, amplifying the UAE's digital attack surface.

The UAE's position as a global hub further attracts both opportunistic cybercriminals and strategic adversaries. This circular consolidates vital insights and offers clear, actionable steps to mitigate these risks.

Key Threat Vectors

1. Financial Fraud (UNC6055):

- **Profile:** Targeting credit card data via fake Ramadan donation and retail sites.
- **Tactics:** AI-enhanced phishing with lures like "Zakat Relief" or "Eid Offers," hosted on UAE IPs.
- **Impact:** Direct financial loss and customer trust erosion.

2. Espionage (UNC6068):

- **Profile:** China-linked, with espionage intent.
- **Tactics:** Spear-phishing with malware (e.g., TINYSHELL, MD5: 0007a47738a8ca8b122e671ee9a0b6aa) disguised as official Ramadan communications.
- **Impact:** Theft of sensitive data from government and critical sectors.

3. Systemic Risks:

- **Profile:** Opportunistic ransomware and infrastructure exploits.
- **Tactics**: Targeting unpatched edge devices and understaffed operations.
- Impact: Operational downtime and recovery costs.

Necessary Security Measures

By enhancing vigilance and utilizing the latest technology, individuals can experience a safer Ramadan season. To protect your organization, the Cyber Security Council advises the prompt implementation of the following measures:

- **Strengthen Email and Network Security:**
  - Deploy advanced email filtering tools to detect and block phishing attempts.
  - Configure firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to monitor unusual network activity.
- **Implement a Backup and Recovery Plan:**
  - Regularly back up all critical data to secure, offline storage solutions.
  - Test your recovery procedures to ensure data can be restored quickly.
- **Patch Management and Vulnerability Assessment:**
  - Ensure all systems, software, and applications are updated with the latest security patches.
  - Conduct regular vulnerability assessments and penetration testing to identify potential weaknesses.
- **Educate Employees:**
  - Train staff to recognize and report phishing emails, suspicious links, or unexpected attachments.
  - Encourage the use of strong, unique passwords and multi-factor authentication (MFA) for all accounts.
- **Segment Network Access:**
  - Monitor access logs to detect unauthorized activities.
  - Restrict access to sensitive data by implementing network segmentation and the principle of least privilege.
- **Develop and Test an Incident Response Plan:**
  - Create a detailed response plan specifically for ransomware attacks.
  - Simulate ransomware incidents to ensure readiness and improve coordination across teams.

Action Required

Please disseminate this circular to all relevant departments and stakeholders within your organization. Immediate implementation of Security measures will significantly enhance your resilience against cyber threats and significantly reduce risk of compromise.

Threat Intelligence recommends activating Immediate Response Playbook:

- **Contain the Threat:** Block shared IOCs across firewalls, IDS/IPS, and endpoints.
- **Empower Your Workforce:** Issue an all-staff alert: “Verify all Ramadan-related emails and websites; report suspicious activity.”
- **Fortify Operations:** Ensure 24/7 security monitoring and patch edge devices.

The UAE Cybersecurity Council remains committed to supporting your organization in maintaining a secure and resilient digital infrastructure.