مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Bolstering Defenses Against Eid Festive Season Cyber Threats

Date: 04-06-2025

Executive Summary

As the UAE prepares to celebrate Eid, a time of unity, reflection, and generosity, the UAE Cyber Security Council urges all organizations and individuals to remain vigilant against an observed increase in cyber threat activity. The convergence of heightened online engagement—such as digital transactions, charitable donations, and travel-related activity—with reduced staffing and operational changes during the holiday season has significantly expanded the national digital attack surface.

The UAE's strategic position as a regional and global hub continues to attract both opportunistic cybercriminals and state-sponsored threat actors. Intelligence gathered during similar festive periods, including Ramadan, indicates a clear trend of malicious campaigns targeting financial systems, sensitive information, and national infrastructure.

This circular consolidates timely threat intelligence and outlines actionable recommendations to ensure the resilience of the UAE's digital ecosystem during the Eid period.

Key Threat Vectors

1.Financially Motivated Cybercrime

- Threat Profile: Malicious actors are exploiting the Eid season through fraudulent donation portals, fake e-commerce platforms, and SMS/email phishing schemes aimed at harvesting financial credentials.
- Observed Tactics:
  - Use of Eid-themed lures such as "Zakat Gift Card," "Eid Mubarak Offers," or "Charitable Giving Portals."
  - Hosting of fraudulent websites on infrastructure associated with prior phishing operations and UAE-registered domains.
- Impact:
  - Direct financial losses.
  - Erosion of consumer and institutional trust in legitimate donation and retail platforms.

2. Espionage Operations

- Threat Profile: Advanced persistent threat (APT) actors, assessed to be affiliated with state-backed entities, are leveraging the Eid season to target government agencies and critical national infrastructure.
- Observed Tactics:
  - Distribution of malware embedded within Eid greeting attachments and travel advisories.
  - Deployment of *TINYSHELL* variants and other lightweight remote access tools.
- Impact:
  - Exfiltration of confidential information.

3. Systemic Infrastructure Risks

- Threat Profile: Ransomware groups and criminal syndicates are actively exploiting holiday staffing shortages and delayed patch cycles to target essential infrastructure.
- Observed Tactics:
  - Automated exploitation of vulnerabilities in unpatched VPNs, web servers, and remote access protocols.
  - Use of timed payloads to maximize disruption during off-peak periods.
- Impact:
  - Prolonged service outages.
  - Significant economic and reputational damage to affected entities.

Necessary Security Measures

By enhancing vigilance and utilizing the latest technology, individuals can experience a safer Eid Holidays. 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.

Actions 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.

The Eid festive season, while a time of celebration, also presents a window of heightened digital risk. All organizations are urged to adopt a proactive cybersecurity posture to mitigate the risk of cyberattacks that could disrupt essential services, compromise sensitive information, or result in financial harm.

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