CRYPTOTECH
SECURING YOUR SUCCESS

NETSCOUT

Libya Cyber Threat Intelligence Report

Jul – Dec 2024

info@cryptotech.ly

حي الأندلس - طرابلس

0913187693

Cryptotech.ly

Executive Summary

In the second half of 2024, Libya experienced a significant increase in Distributed Denial-of-Service (DDoS) attacks, characterized by higher bandwidth, longer durations, and a broader range of attack vectors. These developments underscore the evolving sophistication of cyber threats targeting the country.

Key Statistics

- **Maximum Attack Bandwidth:** 172.68 Gbps
- **Maximum Throughput:** 27.46 million packets per second (Mpps)
- **Average Attack Duration:** 59.19 minutes
- **Total Number of Attacks:** 1,635
- **Peak Aggregate Throughput:** 47 Mpps on December 22, 2024
- **Peak Aggregate Bandwidth:** 379 Gbps on August 21, 2024

Predominant Attack Vectors

The most frequently observed attack vectors during this period included:

1. **DNS Amplification:** 854 attacks
2. **STUN Amplification:** 786 attacks
3. **TCP ACK Flood:** 600 attacks
4. **NTP Amplification:** 581 attacks
5. **ICMP Flood:** 566 attacks

These vectors highlight the diverse methods employed by attackers to disrupt services and infrastructure.

Targeted Sectors

The sectors most frequently targeted by DDoS attacks in Libya were:

1. **Web Search Portals and Information Services:** 151 attacks
2. **Wired Telecommunications Carriers:** 120 attacks
3. **Other Gasoline Stations:** 22 attacks
4. **Telecommunications Resellers:** 1 attack

These statistics indicate a concentrated effort to disrupt communication and information dissemination channels.

Attack Complexity

- **Maximum Number of Vectors in a Single Attack:** 23
- **Average Number of Vectors per Attack:** Approximately 4

The use of multiple attack vectors in single incidents demonstrates a strategic approach to overwhelm defense mechanisms.

Strategic Implications

The escalation in DDoS activities in Libya during the latter half of 2024 suggests a trend towards more complex and sustained cyberattacks. Organizations are advised to enhance their cybersecurity posture by:

- **Implementing Multi-Layered Defense Mechanisms:** Deploying a combination of network-level and application-level defenses to mitigate diverse attack vectors.
- **Regularly Updating Security Protocols:** Ensuring that all systems are equipped with the latest security patches and configurations.
- **Conducting Continuous Monitoring:** Establishing real-time monitoring systems to detect and respond to threats promptly.
- **Engaging in Cybersecurity Awareness Training:** Educating employees and stakeholders about potential threats and safe practices.