QUEST CYBERSECURITY INTELLIGENCE SERIES

GLOBAL CYBER THREAT LANDSCAPE REPORT 2025

Executive Security Intelligence Brief

Prepared by Quest Technologies Ltd – Cybersecurity Advisory & Risk Management

Website: www.questtechltd.com

GLOBAL CYBER THREAT LANDSCAPE REPORT 2025

Cybersecurity Intelligence for Risk Leaders, CIOs and CISOs

Prepared for organizations seeking to understand emerging cyber threats, attacker behavior, and defensive strategies required to protect enterprise infrastructure.

Prepared by Quest Technologies Ltd

Cybersecurity Advisory | Security Monitoring | Incident Response | Cyber Risk Readiness

QUEST EXECUTIVE ADVISORY

Cyber threats are evolving faster than most organizations can respond. Attackers now operate with industrial-scale automation, artificial intelligence, and global criminal infrastructure.

The 2025 Global Threat Landscape Report highlights how adversaries have significantly increased the speed, scale, and sophistication of cyberattacks across industries worldwide.

Threat actors now rely heavily on automated reconnaissance, AI-assisted cybercrime, cybercrime-as-a-service marketplaces, credential theft and identity compromise, exploitation of exposed infrastructure, and cloud misconfiguration attacks.

These trends confirm that cybersecurity is no longer only an IT issue — it is a business risk management priority.

Quest Technologies Ltd works with organizations to strengthen cyber resilience through cybersecurity risk assessments, security architecture design, security monitoring & SOC services, incident response readiness, and cyber insurance readiness alignment.

The objective is simple: Reduce cyber exposure before attackers exploit it.

KEY FINDINGS FROM THE GLOBAL THREAT LANDSCAPE

Recent cybersecurity intelligence reveals several developments shaping the global threat landscape.

1. Cyber reconnaissance is accelerating – attackers aggressively scan the internet to identify vulnerable systems before launching attacks.

2. Artificial Intelligence is enabling cybercrime – AI tools now automate phishing, malware creation, and social engineering.

3. Cybercrime-as-a-Service – underground marketplaces sell ready-made cyberattack capabilities.

CREDENTIAL THEFT & INITIAL ACCESS

Credentials remain one of the most valuable commodities in cybercrime ecosystems.

Stolen credentials originate from phishing attacks, malware infections, credential stuffing, and previous data breaches.

Criminal markets sell VPN access, RDP access, corporate admin credentials, and internal network access.

Infostealer malware extracts browser passwords, financial data, and corporate login credentials from compromised systems.

EXPLOITATION OF VULNERABILITIES

Cybercriminals increasingly exploit vulnerabilities within days of disclosure.

Common targets include outdated operating systems, unpatched applications, IoT devices, and exposed web services.

Delayed patching and weak asset visibility increase organizational risk exposure.

IoT SECURITY RISKS

Internet of Things devices such as routers, cameras, and smart infrastructure are increasingly targeted by attackers.

Many devices contain default credentials, outdated firmware, or exposed management interfaces.

Compromised devices are often used for botnets, DDoS attacks, and persistent network infiltration.

CLOUD SECURITY RISKS

As organizations migrate infrastructure to the cloud, attackers are targeting misconfigured cloud environments.

Common attack vectors include exposed credentials, misconfigured storage services, weak identity access control, and insecure APIs.

Once inside, attackers attempt privilege escalation, lateral movement, and data exfiltration.

RANSOMWARE & CYBER EXTORTION

Ransomware continues to dominate the cyber threat landscape.

Modern ransomware operations run as organized criminal enterprises where affiliates execute attacks and share profits.

Many attacks now involve double extortion where attackers both encrypt systems and threaten to leak stolen data.

STRATEGIC DEFENSE RECOMMENDATIONS

Organizations should prioritize continuous attack surface monitoring, identity security, vulnerability management, and proactive threat detection.

Cyber incident preparedness is critical for reducing operational disruption during attacks.

QUEST CYBERSECURITY SERVICES

Quest Technologies Ltd provides cybersecurity advisory and implementation services including:

- Cybersecurity Risk Assessments

- Security Architecture Design

- Security Monitoring & SOC

- Incident Response & Recovery

- Cyber Insurance Readiness Alignment

Our mission is to help organizations reduce cyber exposure, strengthen cyber resilience, and align with global security best practices.

DISCLAIMER

This report contains cybersecurity intelligence and research insights intended for educational and risk awareness purposes.

Quest Technologies Ltd is not an insurance provider. Our role is to help organizations strengthen cybersecurity posture and reduce cyber risk exposure through advisory and technology implementation services.

CONTACTS

Quest Technologies Ltd

Website: www.questtechltd.com

Email: info@questtechltd.com

Cybersecurity Assessments | Security Monitoring & SOC | Incident Response | Cyber Insurance Readiness