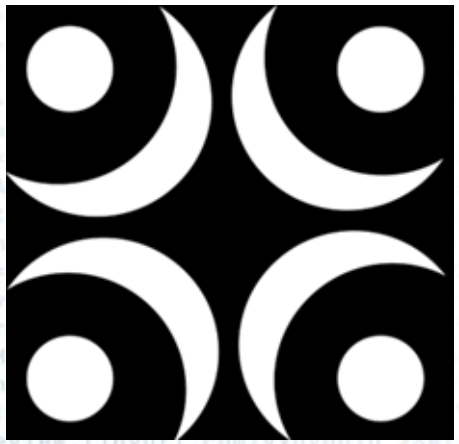
# DDoS Attacks
# A Strategic Threat

Tim Westlake
Principle Enterprise Security Architect

Akamai



INSURANCE TECHNOLOGY FORUMS

# Who is Akamai?

## We make life better for billions of people, trillions of times a day.

**4,400+**
Edge PoPs

**1,200+**
Networks

**130+**
Countries

**700+**
Cities

**38+**
Scrubbing Centers

Customers Include:

- All top 10 brokerages
- All top 10 banking companies
- 9 of the top 10 software companies
- 8 of the top 10 pharma companies
- 8 of the top 10 fintech companies
- 8 of the top 10 retail companies

**100B+**
DNS queries/day

# DDoS Threat Landscape

## Returning to the headlines

CYBERSECURITY

### Report Shows DDoS Attacks Rising, More Manufacturers Targeted

Attackers are putting new pressure on network defenses.

### Aisuru Botnet Shatters Records With 29.7 Tbps DDoS Attack

The Aisuru botnet's massive DDoS assault marks a new era in which hyper-volumetric attacks are both accessible and harder to defend.

United States Attorney's Office
District of Alaska

About USAO-AK | Find Help | Contact Us

About | News | Divisions | Programs | Contact Us

Justice.gov > U.S. Attorneys > District of Alaska > Press Releases > Authorities Disru
Responsible For Record Breaking Attacks Targeting Victims Worldwide

PRESS RELEASE

### Authorities disrupt world's largest IoT DDoS botnets responsible for record breaking attacks targeting victims worldwide

NEWS 20 February 2026

### Dramatic Escalation in Frequency and Power of DDoS Attacks

HACKREAD

Hacking News | Technology | Cyber Crime | Security | Crypto | Surveillance

PRESS RELEASE

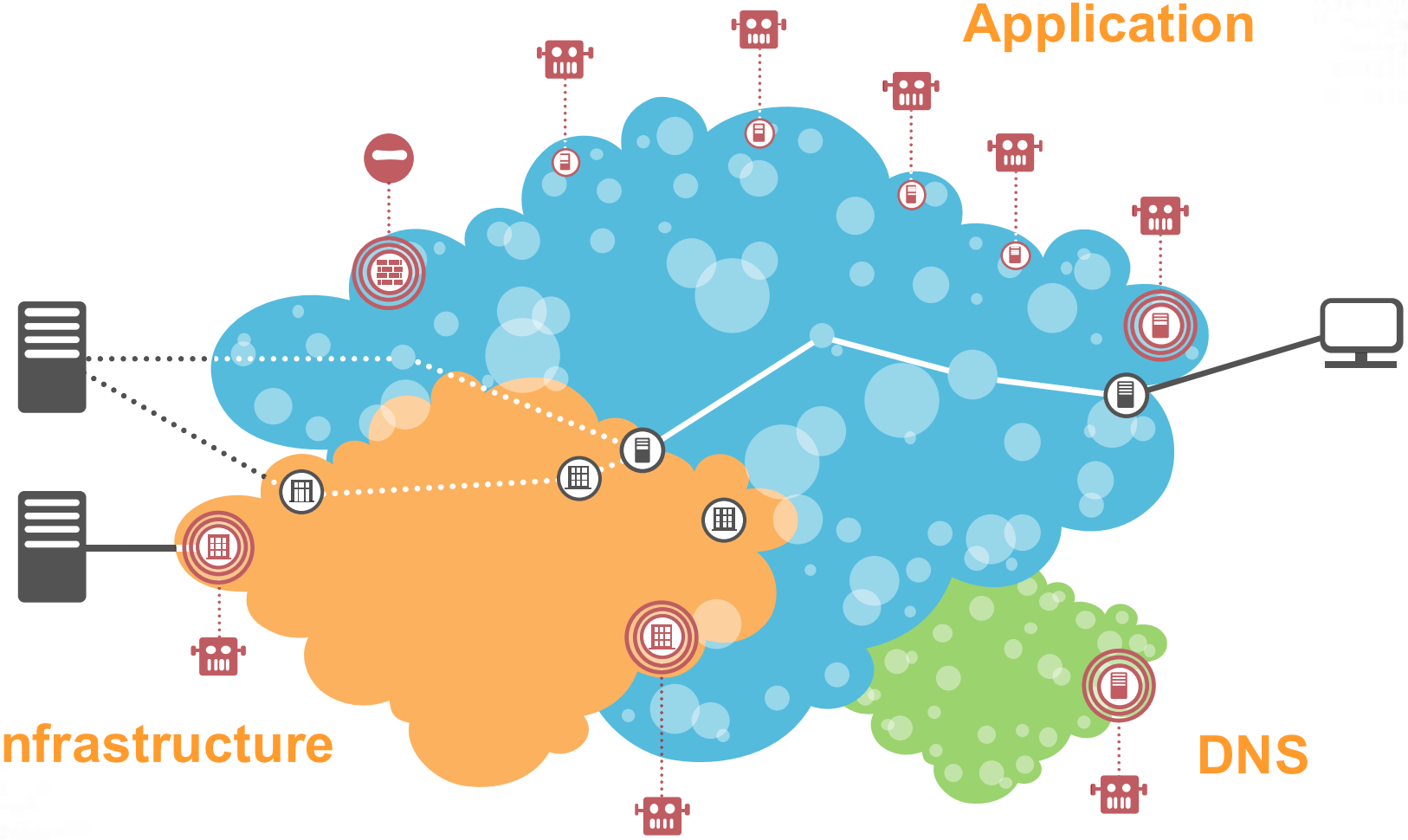
### Link11 Releases European Cyber Report 2026: DDoS Attacks Become a Constant Threat



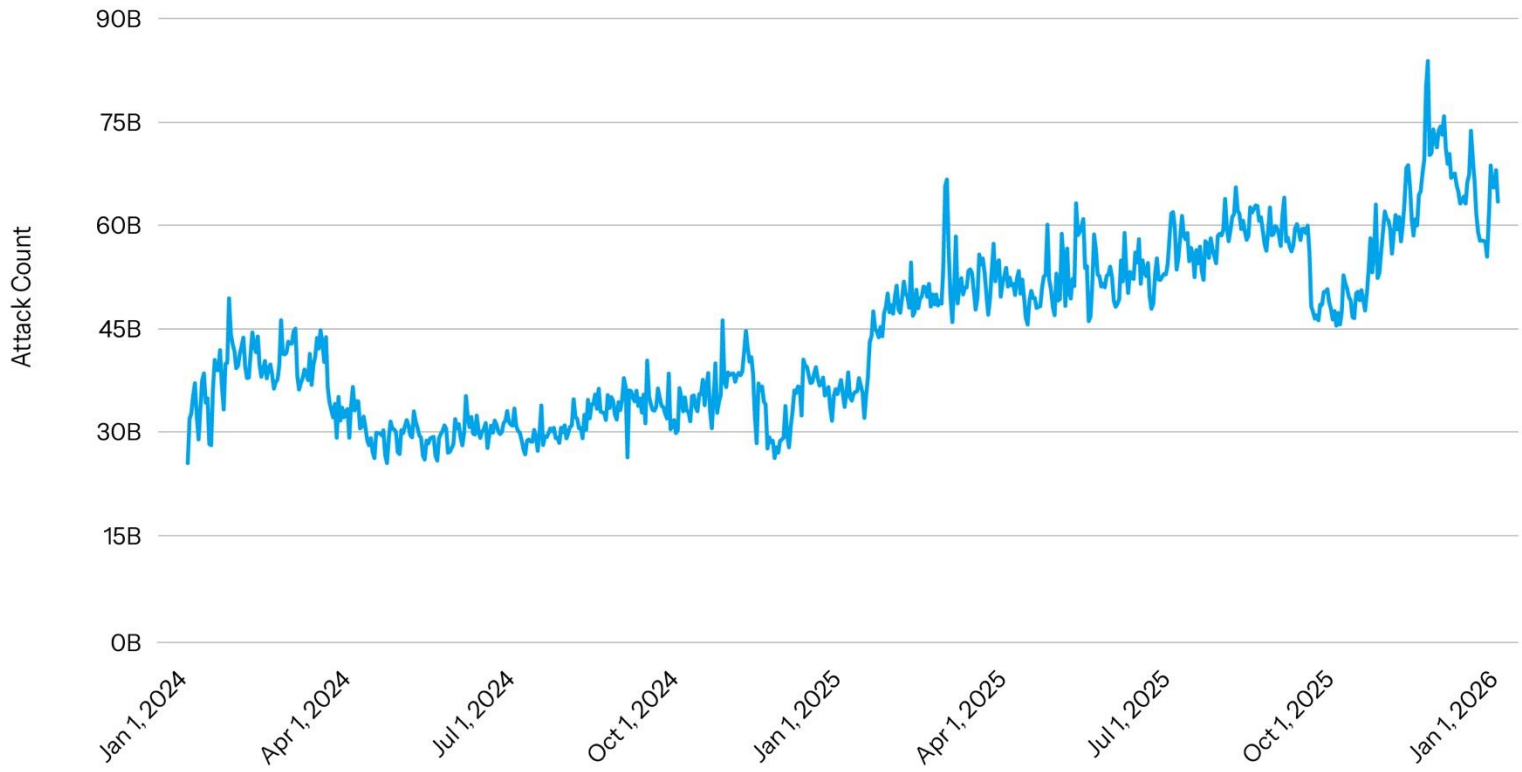

Akamai

# 3 Pillars of DDoS Protection

## Protecting the whole attack surface

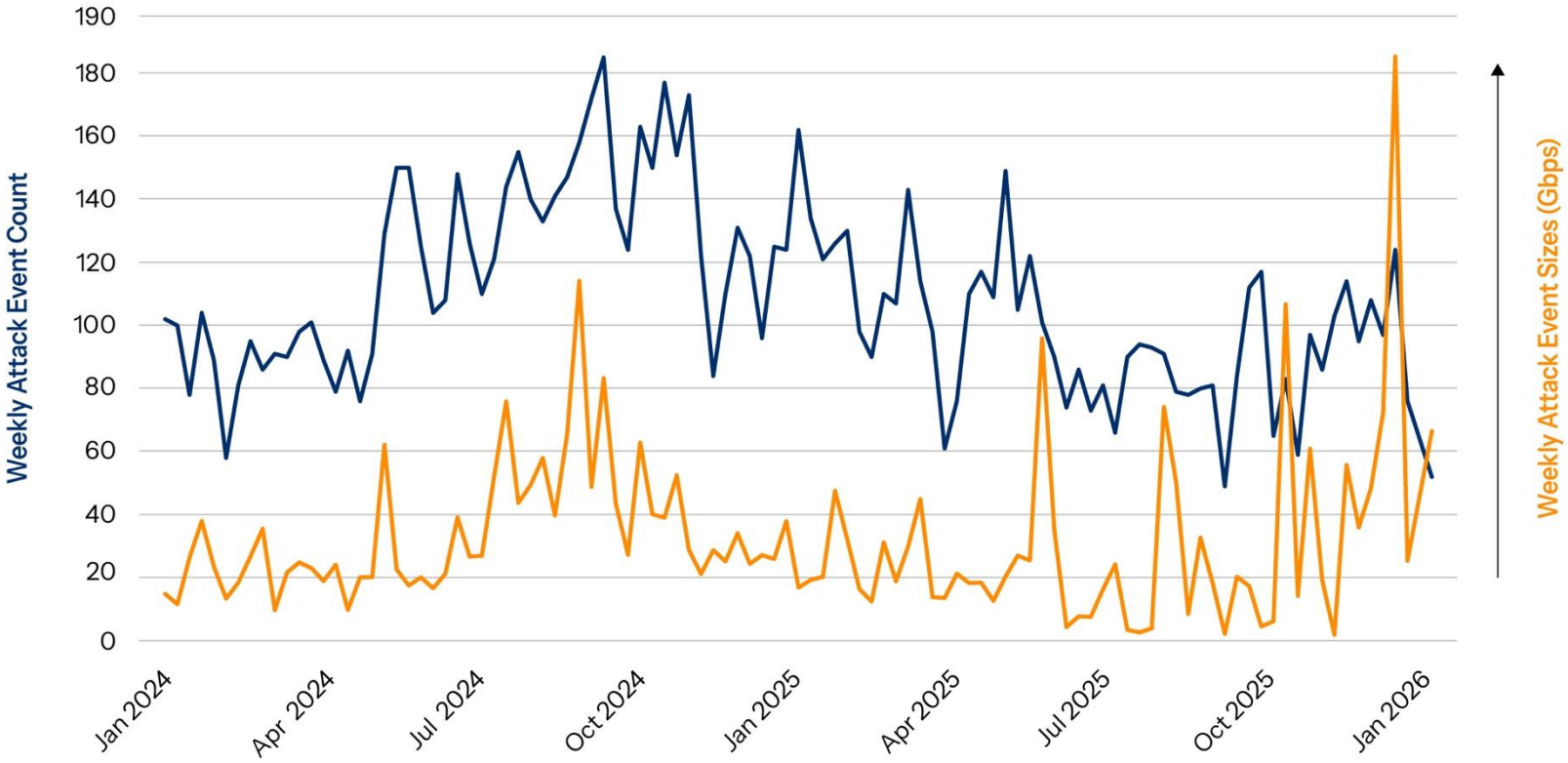


# Layer 7 DDoS Attacks



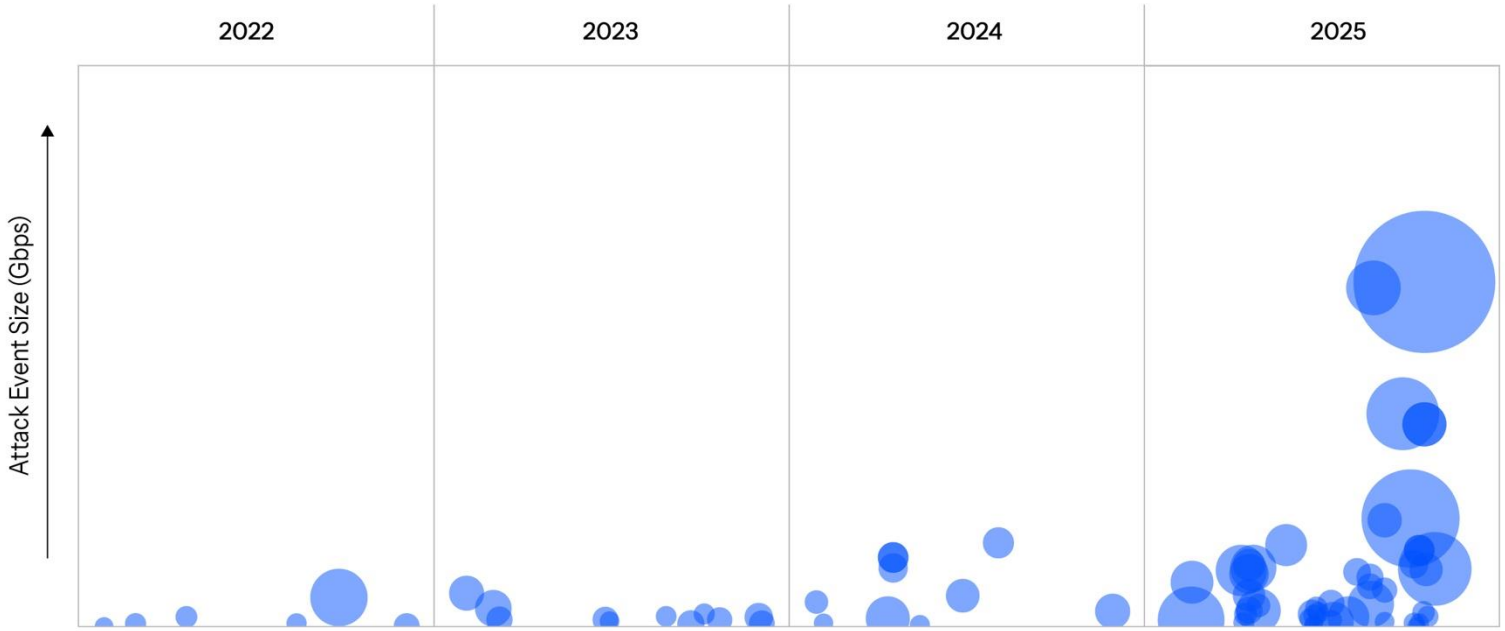

- **104% increase between 2023 and 2025**
- **61% increase between 2024 and 2025**
- **Targeting APIs and Web apps**
- **Botnets assisted by AI**

# Layer 3 / 4 DDoS Attacks



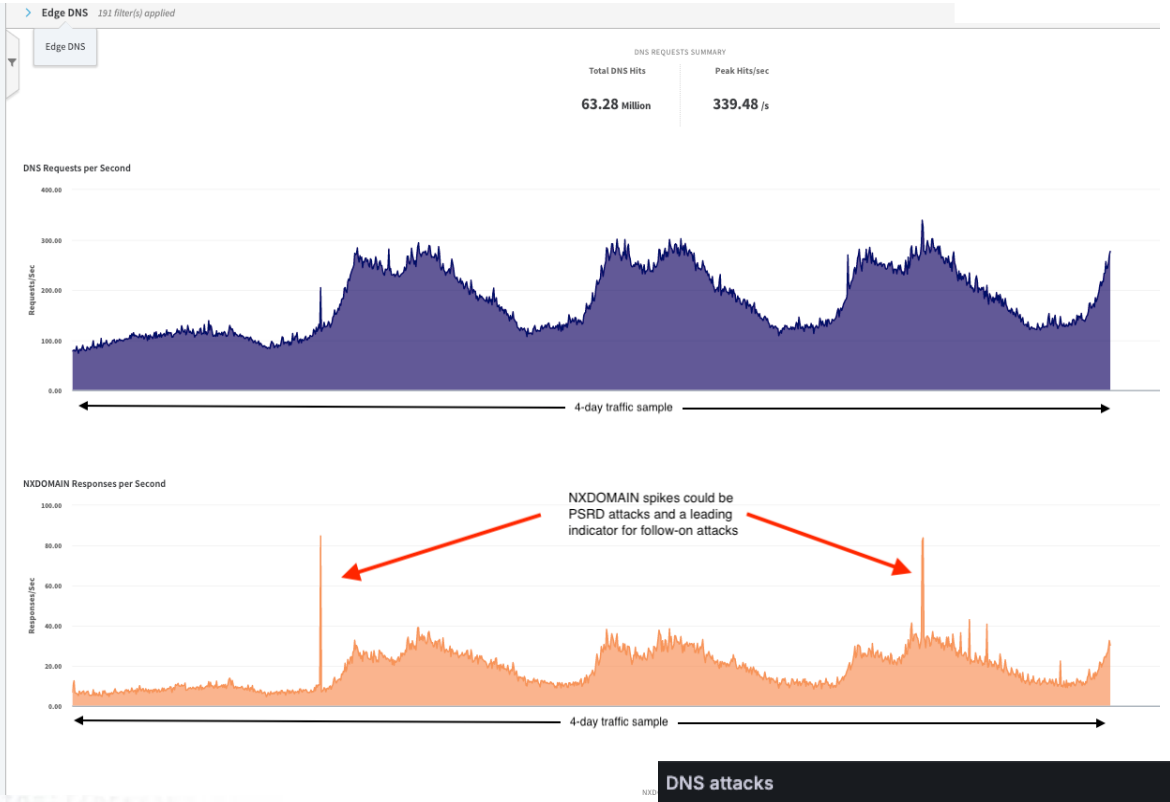

- **Overall frequency of events has reduced**
- **Step change increase in large attacks**
- **Increase in Attack Duration**

# Layer 3 / 4 DDoS Attacks

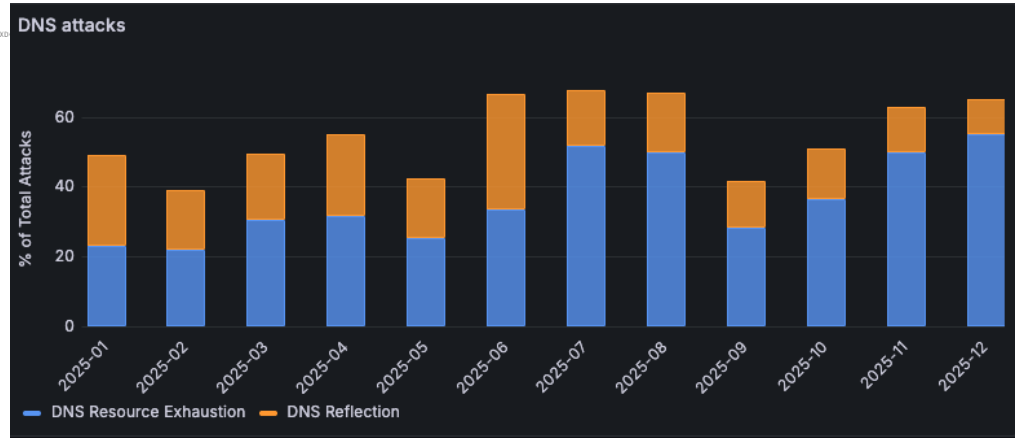



- Steady increase in overall attack volume
- DDoS for Hire services are now businesses
- Latest generation of attack tools have dramatically increased attack size

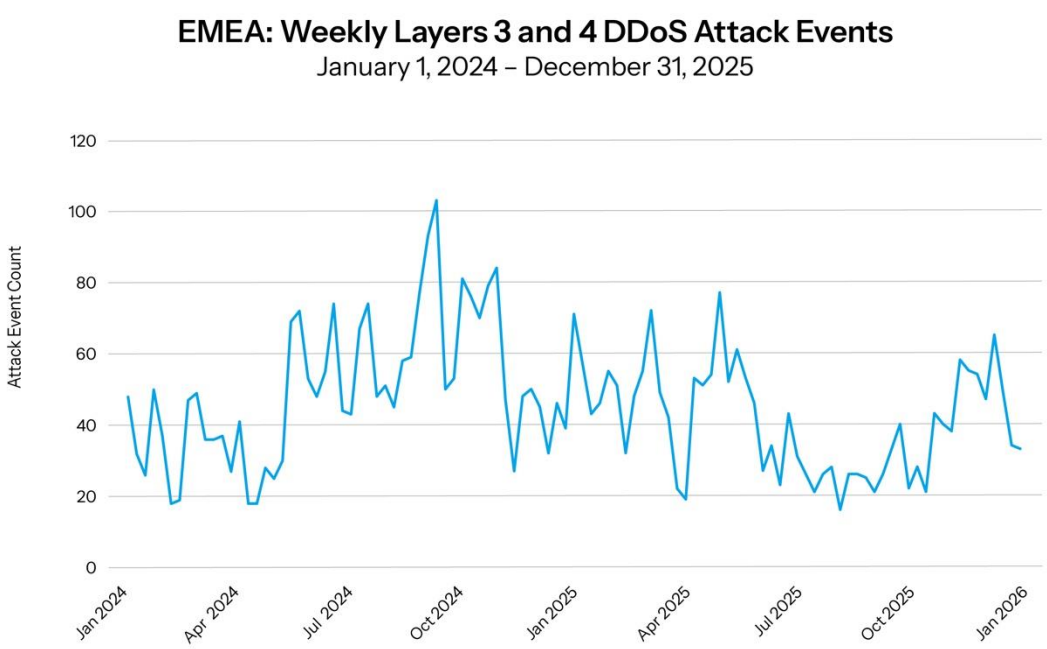
# Attacks against DNS Infrastructure



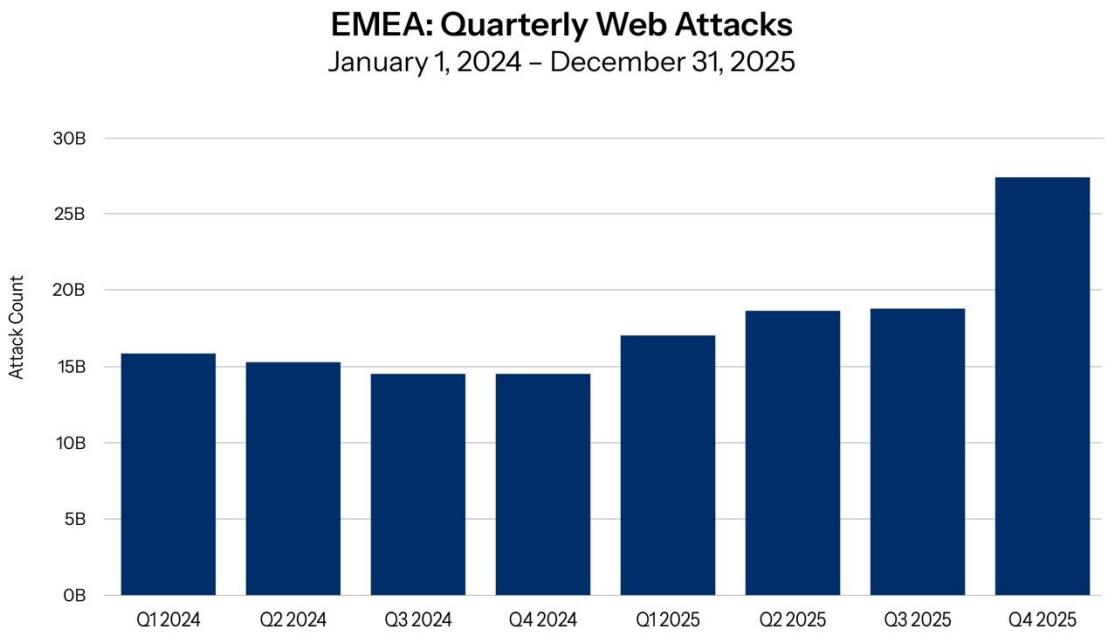

- 60% of DDoS attacks had a DNS Component
- Attacks against Authoritative DNS Servers
- Attacks against DNS Traffic Management (Load Balancers)
- Vulnerabilities due to DNS misconfiguration



# EMEA Attack Trends

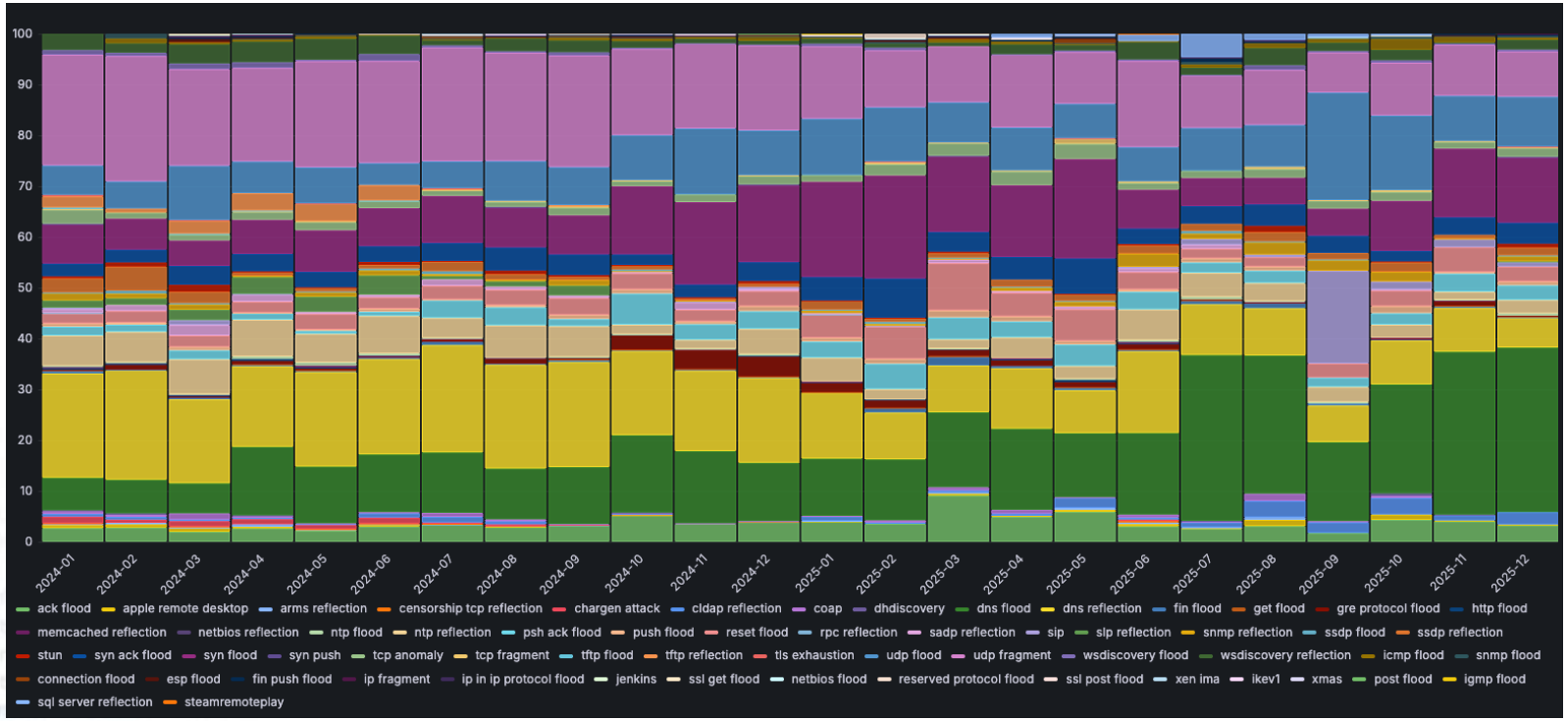



- Consistent level of threat
- Most targeted global region




- Q4 25 – Two year high for attacks
- Supply chain specifically targeted

# Increasing number of layer 3/4 vectors




- **Attackers are using new tools and techniques**
- **Over 140 different vectors seen in 2025**
- **Multi-vector attacks are the norm**
- **Increase in Sophistication**

# AI Assisted DDoS

## AI is not just an attack surface

**Roger Barranco, Vice President of Global Security Operations**

**"AI has lowered the barriers to entry for attackers. Threat actors no longer need to be skilled coders; they can use AI to verbally build and mount an attack."**

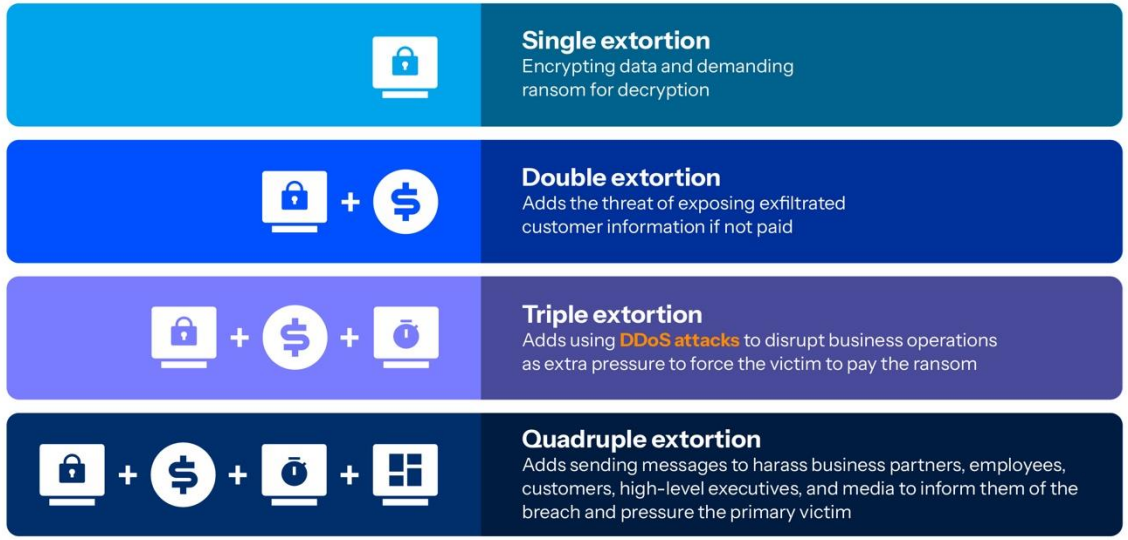
**Reuben Koh, Director of Security Technology, APJ Region**

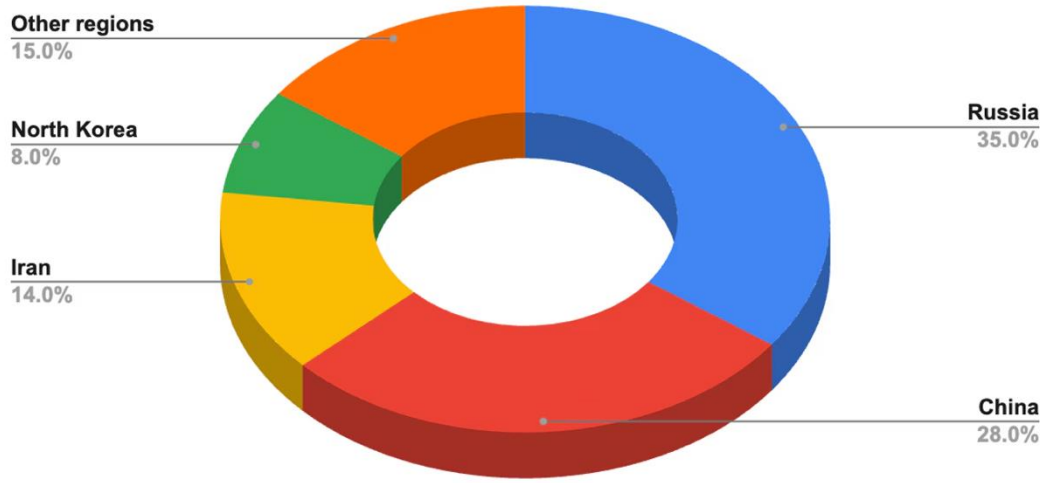
**"AI is powering successful attacks and posing challenges for conventional defenses and security teams because the attacks are harder to detect, have more impact, and achieve their objectives faster. "**

**Tricia Howard, Scrybe of Cybersecurity Magicks**

**"The more AI is used by attackers, the more important it becomes to understand the people and psychology behind the attacks. "**

# Motivation: Crime and Politics




- DDoS as a tool of or part of extortion
- Smokescreen for other activities

- Attacks rise in parallel to recent geo-political activities
- Highly resourced state sponsored teams
- Hacktivism from academic institutions

# Protecting Yourself – Be Prepared

## Three key process areas to prioritize

### 1. Stakeholder Alignment

Internally, ensure that teams (security operations center, IT, incident response, crisis management) collaborate seamlessly to detect and mitigate threats. Externally, confirm that vendor SLAs define clear escalation paths for rapid response.

### 2. Incident preparedness

Establish a well-defined playbook, eliminating ambiguity during an attack. This playbook should include:

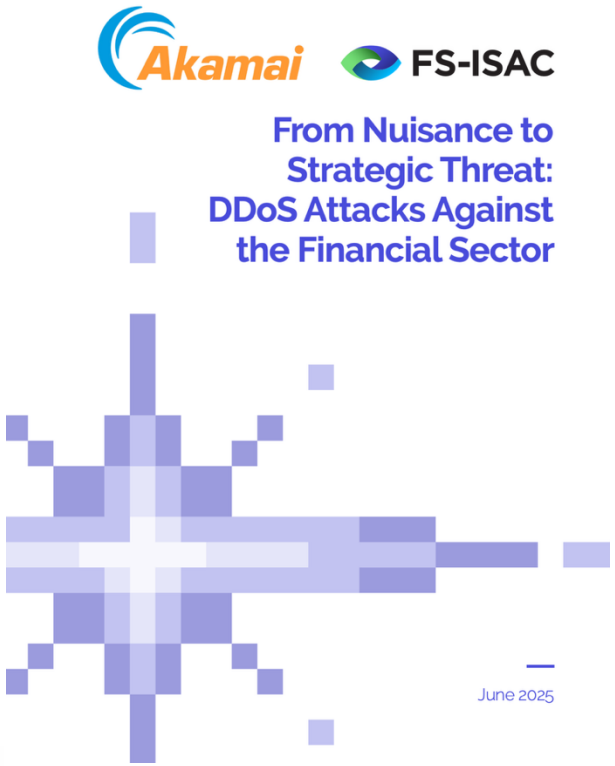
- Designated decision-makers and contacts at every level (with up-to-date contact lists)
- Step-by-step response protocols for varying attack scenarios

### 3. Multilayered defence

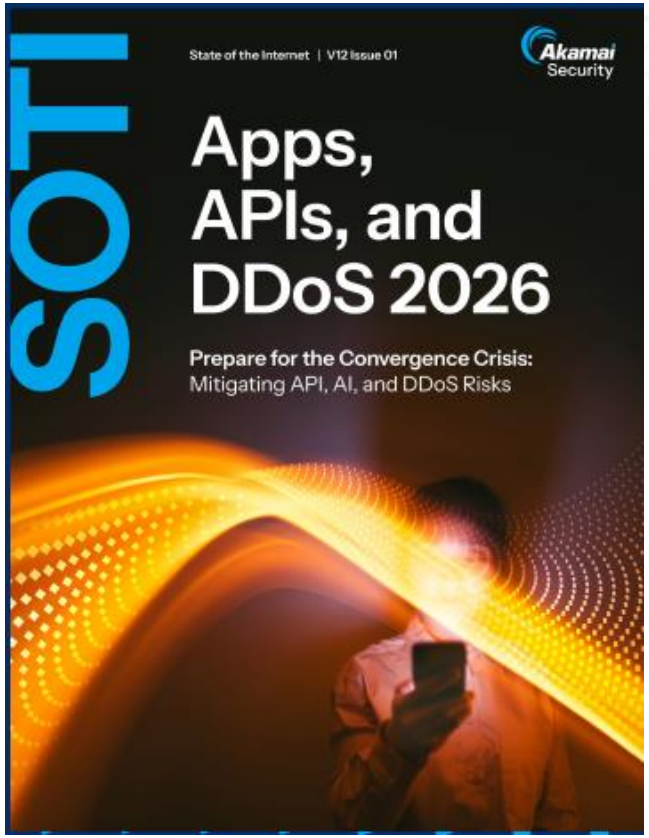
Protect against all potential vectors:

| | |
|---|---|
| DNS | - Ensure that DNS is resilient by using a cloud provider or multiple cloud providers<br>- DNS Implement Domain Name System Security Extensions (DNSSEC)<br>- Implement DNS posture management, firewall, and filtering |
| Infrastructure (Layer 3 & 4) | - Ensure that the company is keeping its attack surface small by pushing as much of the Layer 4 rules to the DDoS provider as possible<br>- Have a proven strategy for the ports and protocols that must be open to the internet |
| Application layer (Layer 7) | - The organization's critical host names should all be resolving to a CDN with a web application and API protection (WAAP) solution that is able to mitigate millions of requests per second without leaking traffic to the origin |

# Reports




FS-ISAC Members can access the full report in the member portal, or at this URL: https://www.fsisac.com/ddos-akamai-2025




https://www.akamai.com/lp/soti/app-api-ddos-security-report-2026


Akamai