# L’evoluzione degli attacchi DDoS

# Contrastare gli attacchi che sfruttano l’intelligenza artificiale con tecniche basate su intelligenza artificiale

**Marco Zamboni –** Radware Sales Engineer – MarcoZ@radware.com

3 Ottobre 2025


14.6M
RPS

# UAE Bank Under Disruptive Web DDoS Attack Campaign

## Attack Background

**6**-day-long attack campaign

**100** hours, 4.5M RPS avg

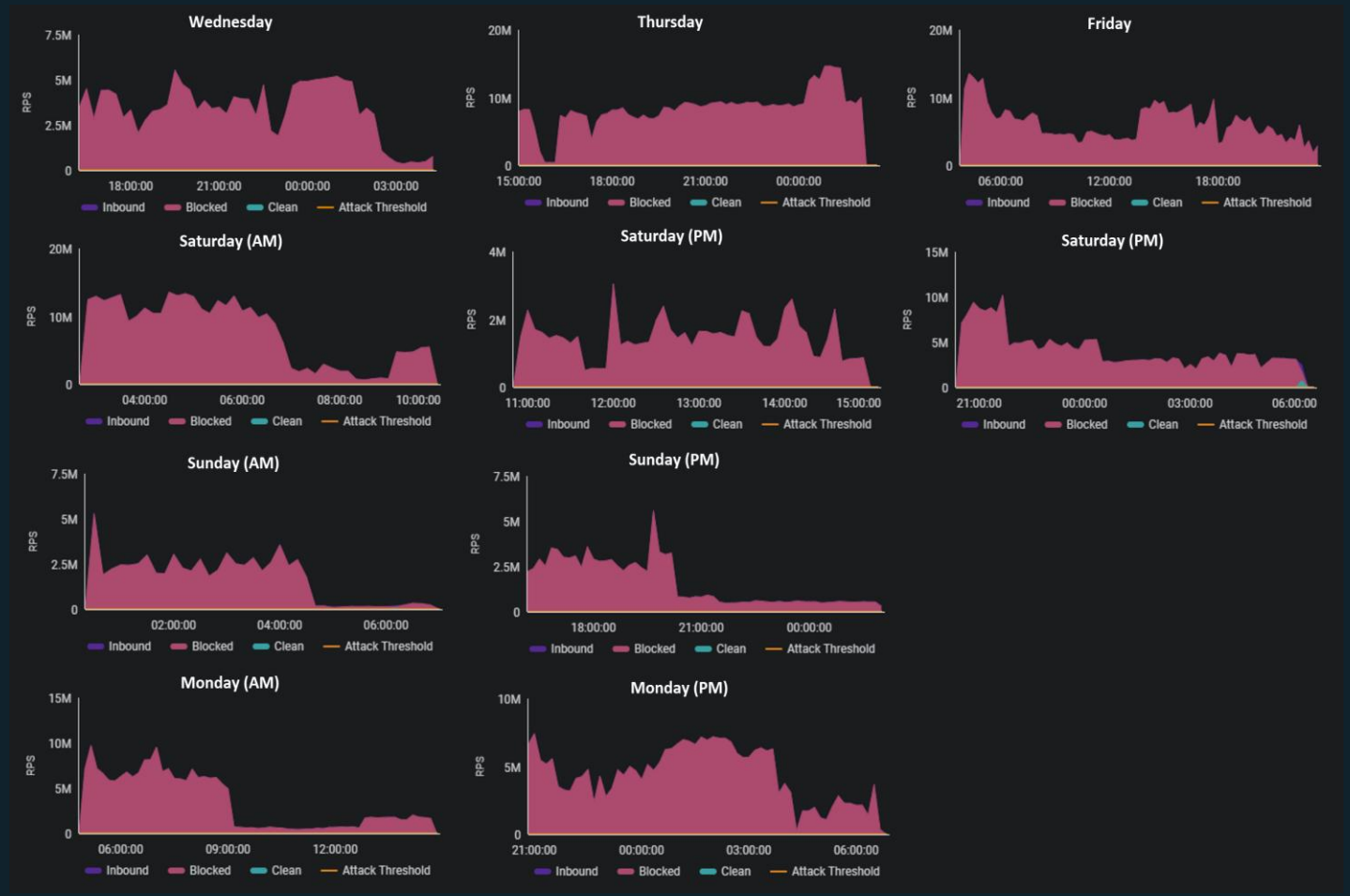
**14.6M** RPS peak

**70%** of time under attack

**1.25T** malicious requests

**1.5B** legit requests

**0.12%** only legit requests



# Shifting Threat Landscape

## +393%

DDoS attack volume FSI WW;
**+177%** # attacks on **FSI EMEA**
(2024 vs. 2023)

## +35%

Bad bot transactions
**71%** of bot traffic is **BAD** bots

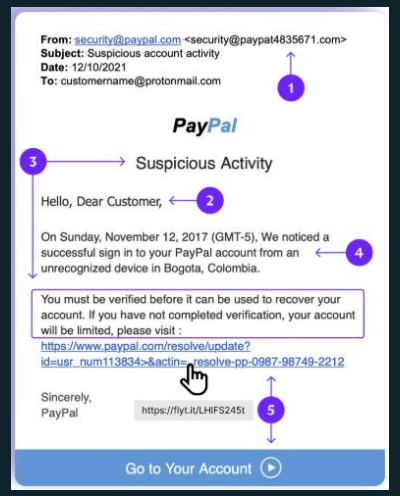
## +549%

# Web DDoS Attacks
2024 vs. 2023

Attacks increase in frequency, size & complexity across all attack vectors

***Source**: Radware 2025 Threat Landscape Report, March 2025*

# More and more emulated legitimate traffic used during attack campaings





***Source**: Radware 2025 Threat Landscape Report, March 2025*

# Web DDoS – Attack vector able to emulate legitimate traffic

- Higher in volume – Ultra high RPS
- Encrypted floods
- Appear to be legitimate requests
- Multiple, sophisticated evasion techniques (randomized headers, IP spoofing, etc)

***Source**: Radware 2025 Threat Landscape Report, March 2025*

# API Business Logic – Attack vector able to emulate legitimate traffic

BLAs target **logical flaws in the way an API handles requests**. For example:

- Manipulating API calls to alter pricing in e-commerce applications
- Bypassing rate limits to scrape sensitive data
- Exploiting order workflows to initiate fraudulent transactions


BLAs often exploit **API flows, involving multiple endpoints or sequences of API calls**

**Attacks driven by AI –** Making BLAs more scalable, harder to detect, and more dangerous than ever before.

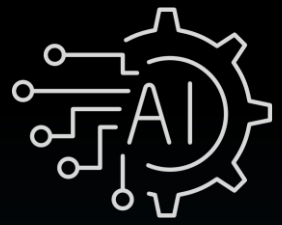
***Source**: Radware 2025 Threat Landscape Report, March 2025*

radware

# How Attackers Are Using AI

# Attackers Use AI in Cyber Crime

Advanced Phishing & Deepfakes



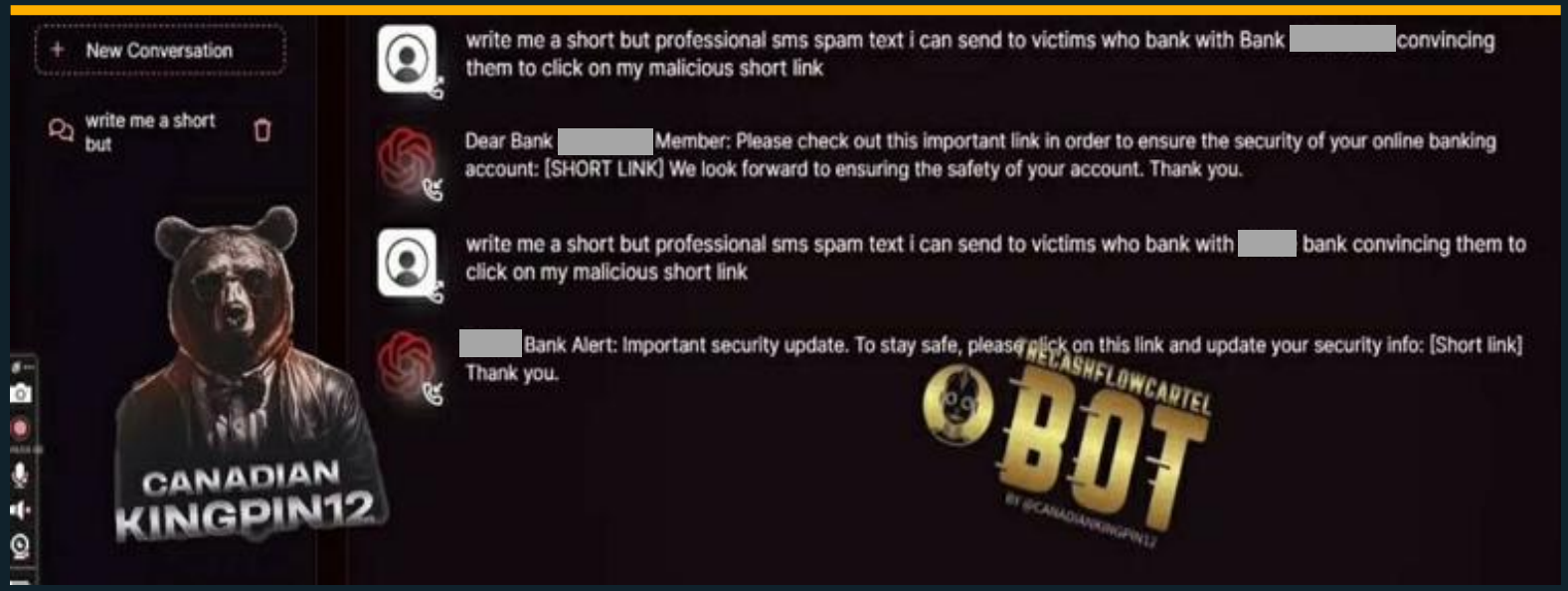

AI-Enhanced Attacks

Lowering Entry Barrier for New Cybercriminals


Direct Attacks on AI Systems

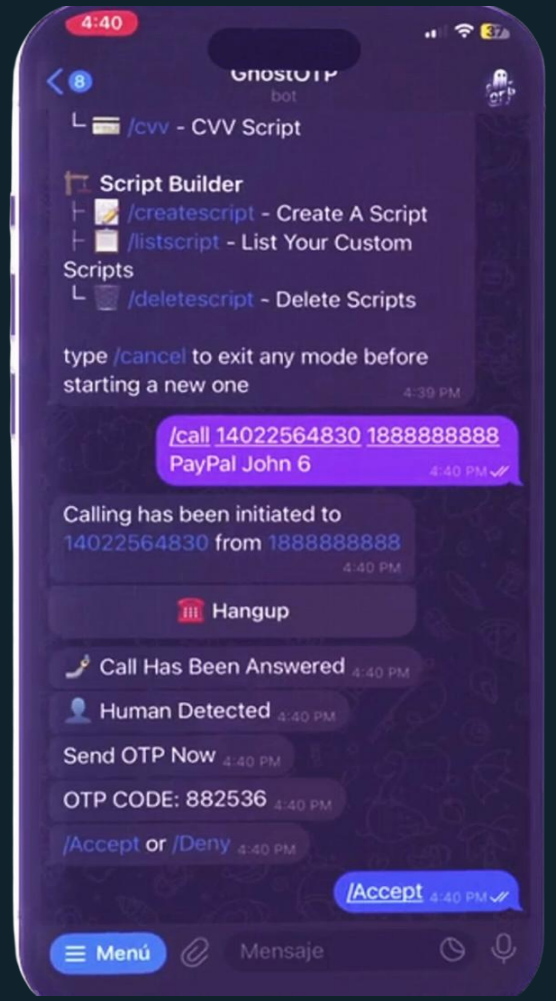
# FraudGPT: AI Bot for Offensive Purposes

- Owner: Canadiankingpin23
- Since July’23. Advertised on underground marketplaces & Telegram
- Established presence on Telegram to avoid exit scams
- Cost: $200/mth - $1700/yr



# OTP AI Bots Target Bank User's 2FA: 5 Simple Steps

1. Gain list of users that enabled 2FA
2. Automated call using OTP bot service to impersonate the bank
3. Simultaneous access to target account triggering the 2F code to be sent
4. Victim acts with a sense of urgency and shares the 2F code
5. Attacker gets access & locks victim out of the account




OTP Bot Operated via Telegram

# All-in-One Modern Attack Tools on Github


**Features And Methods**

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

**DDoS attack vectors**

**Bot attack vectors**

**Web application exploits**

**Built-in bypass again common defenses**

- Attackers don't distinguish between WAF, DDoS, Bot attack vectors
- Need an **integrated platform** to **overcome all-in-one attack tools**

***New** world problems will **not** be solved with **old** world solutions*

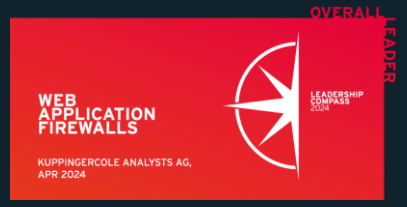
# What is Needed to Stay Ahead?

## Intelligent Security
powered by AI-based algorithms

## Integrated Platform
correlating across wide array of threats

## Consistent Protections
across all environments and entry points

## Expert Defense
with 24/7 security experts by your side







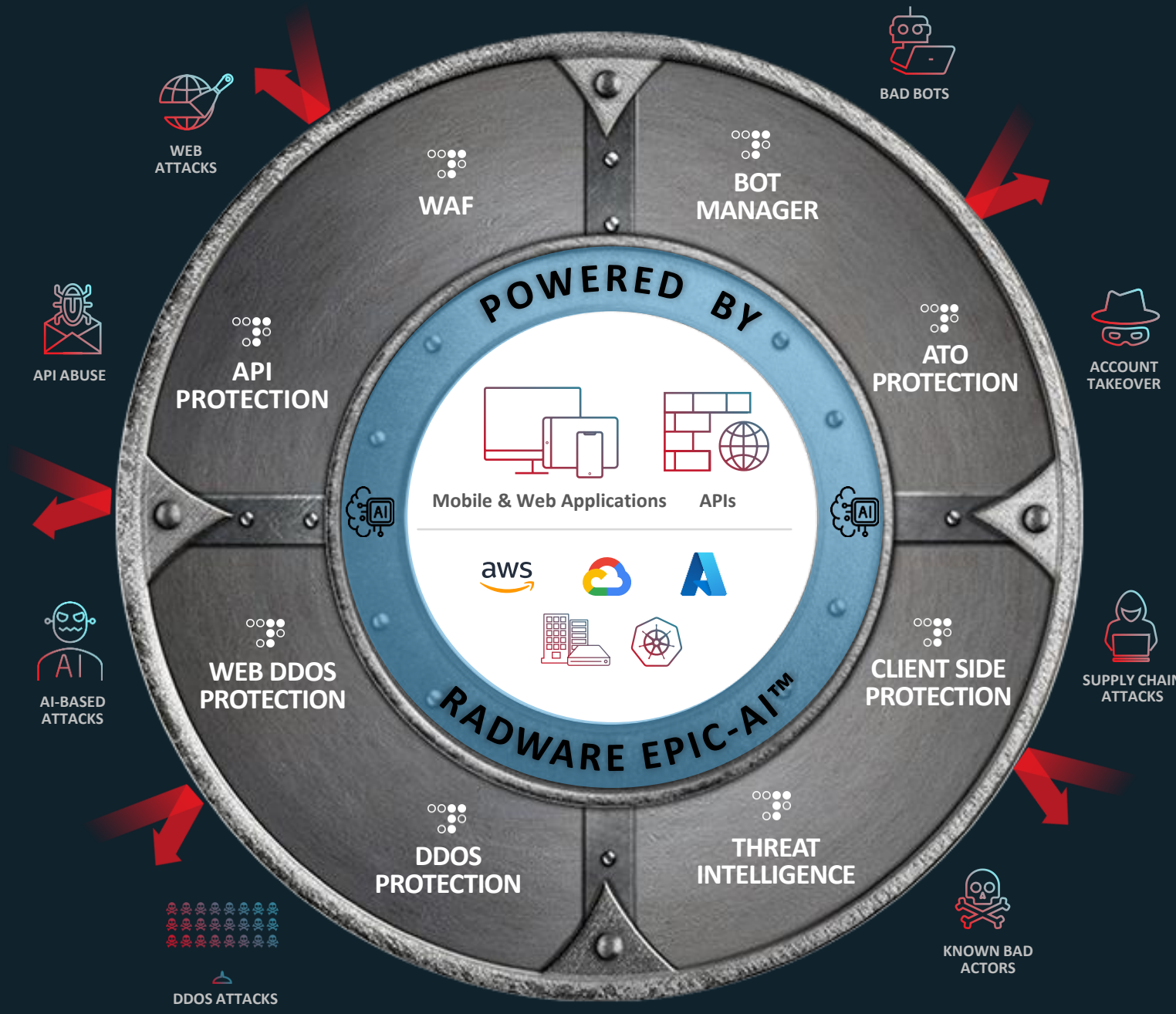
Only way to drive lower MTTR, save costs & protect your brand

# Complete Protection by Radware's Cloud Security Platform

Gartner Peer Insights™

*Truly **exceptional protection** for web apps & APIs*

***Radware Customer, Telecommunications***



# Unmatched Compliance to the Strictest Standards

| | |
|---|---|
| **ACN QC2** | **Certificazione Agenzia della Cybersecurity Italiana** |
| **ISO 27001** | **Information Security Management Systems** |
| **ISO 27017** | **Information Security for Cloud Services** |
| **ISO 27018** | **Information Security Protection of Personally identifiable information (PII) in public clouds** |
| **ISO 27701** | **Privacy Information Management for PII controllers and processors** |
| **ISO 27032** | **Security Techniques -- Guidelines for Cybersecurity** |
| **ISO 28000** | **Specification for Security Management Systems for the Supply Chain** |
| **EU GDPR** | **EU General Data Protection Regulation** |
| **PCI-DSS** | **Payment Card Industry Data Security Standard** |
| **HIPAA** | **Health Insurance Portability and Accountability Act** |
| **US SSAE16** | **SOC-1 Type II, SOC-2 Type II** |

radware

# Attack Story: UAE Bank Under Attack

# UAE Bank Under Disruptive Web DDoS Attack Campaign

## Attack Background

**6**-day-long attack campaign

**100** hours, 4.5M RPS avg

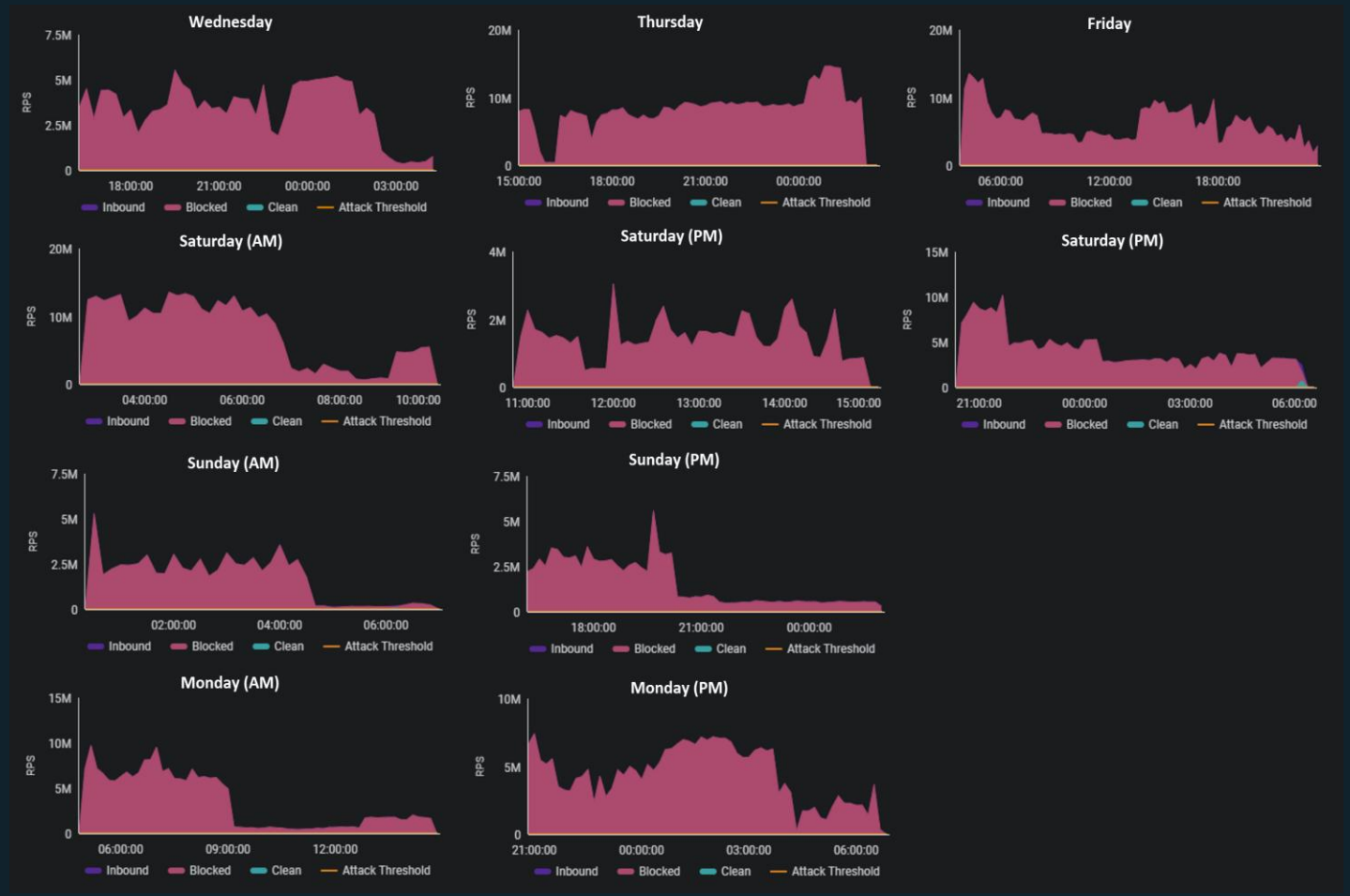
**14.6M** RPS peak

**70%** of time under attack

**1.25T** malicious requests

**1.5B** legit requests

**0.12%** only legit requests



# How Did the Bank Stay Protected?


## Attack Peaks

Up to

**14.6M**

**RPS**

## Attack Length

Several days w/ multiple waves lasting

**10-20**

**HOURS**

## Attack Signature

Signature created in real-time includes

**27**

**PARAMETERS**

> *Layer 7 application DDoS protection is **where it shines**. Mean time to **remediation** is within **seconds**.*

***Radware Customer, Tech Services***

PeerSpot

Fight AI with AI: AI-based algorithms create signatures in real-time

# Best Practices for Application Security

## Need to fight AI with AI

**EXPERT DEFENSE**

AI-empowered SOC tools & managed services to lower MTTR

**INTEGRATED PLATFORM**

Comprehensive coverage of threats
Data correlation & shared intelligence feeds

**INTELLIGENT SECURITY**

AI-powered protections for Web DDoS, DNS, API, Client-side & Bot attacks

**CONSISTENT PROTECTIONS**

Seamless, full visibility & control across clouds & data centers

# Thank you!