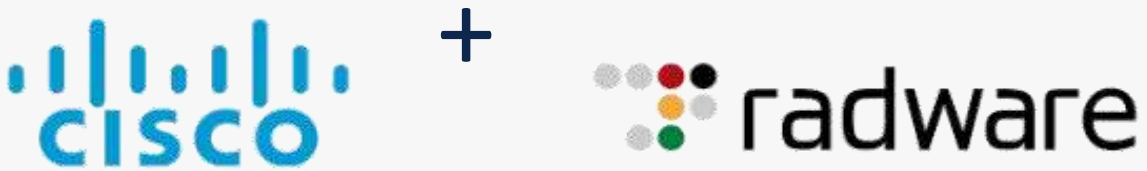
# Jak dnes účinně chránit web?

**Petr Lasek**

**petrl@radware.com**

8.9.2025

# Spolupráce



# RADWARE

BOT MANAGEMENT 2022
**LEADER**

WAF 2022
**LEADER**

APP & API PROTECTION 2022
**LEADER & OUTPERFORMER**

DDoS MITIGATION WAVE 2021
**LEADER**

Aite Novarica

BOT DETECTION MATRIX, 2022
**BEST IN CLASS**

*"The largest global financial institutions, brokerage firms, and financial services companies use Radware's Bot Manager."*

kuppingercole ANALYSTS

WAF LEADERSHIP COMPASS 2025
**OVERALL LEADER**
**Product, Innovation & Market Leader**

# Chránit se snadno a účinně?

# Co fungovalo včera nemusí fungovat dnes!


# Proč řešit bezpečnost webu?

- Web má každý
- Je to „brána k další infrastruktuře!“ (síť, databáze, …)
- Denně je hacknuto více než 30 000 webů*
- Obchodní nástroj.
- Finanční ztráta!!!
- Ztráta reputace?
- Pokuta (GDPR, NIS2 - zákon o kybernetické bezpečnosti)?

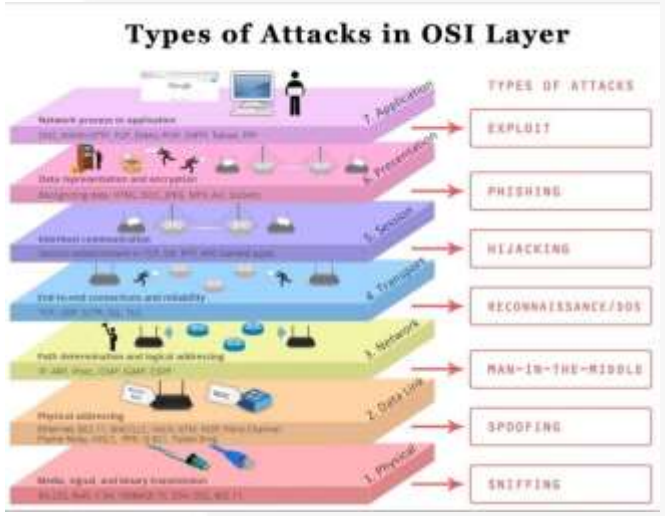
*https://techjury.net/blog/how-many-cyber-attacks-per-day/


# Jste další na řadě?

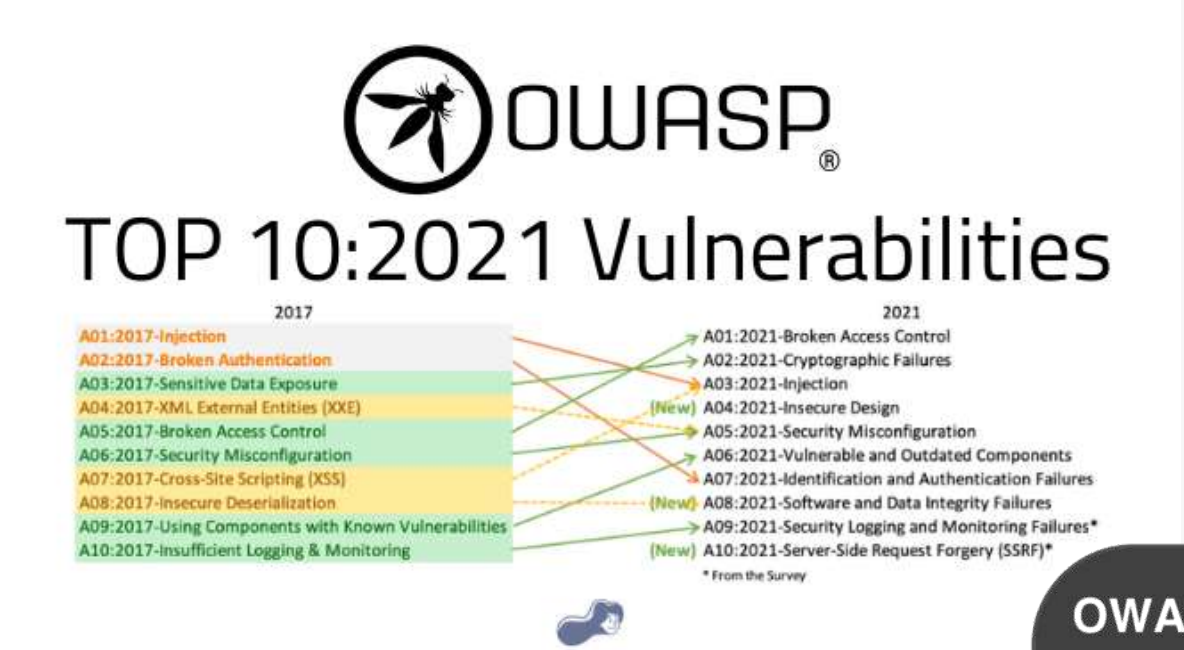
# Zabezpečení webu?

**Zabezpečit web není nic jednoduchého:**

- Co je legitimní požadavek?
- Pro vývojáře není bezpečnost „priorita“
- Weby jsou distribuované (vlastní datové centrum, veřejný cloud, …)
- Vrstvy / komponenty / frameworky
- Průběžné updaty (verze)
- Průběžný vývoj aplikací (CI/CD)




# OWASP

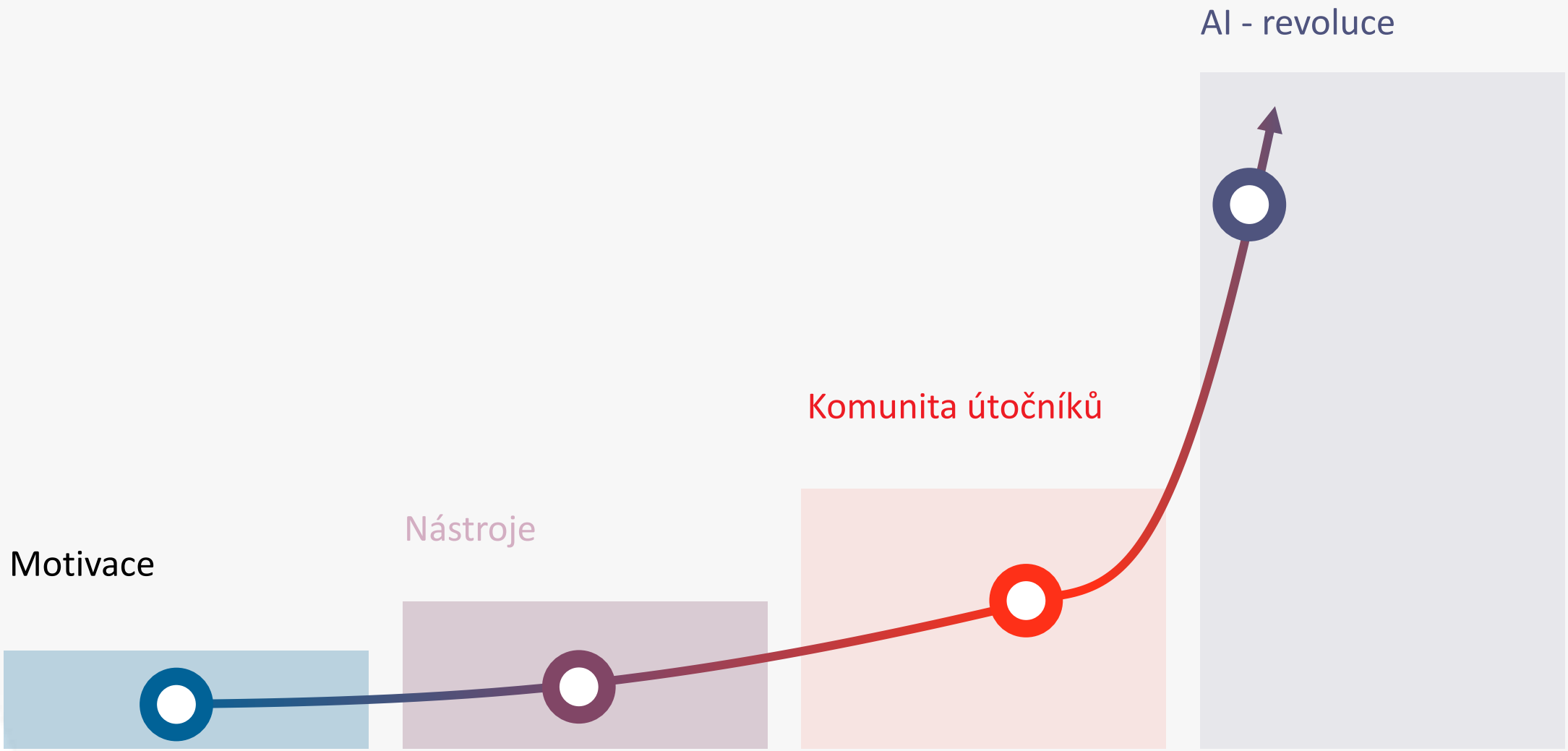



| OWASP Automated Threats | | | |
|---|---|---|---|
| OAT-020 | Account Aggregation | OAT-006 | Expediting |
| OAT-019 | Account Creation | OAT-004 | Fingerprinting |
| OAT-003 | Ad Fraud | OAT-018 | Footprinting |
| OAT-009 | CAPTCHA Bypass | OAT-005 | Scalping |
| OAT-010 | Card Cracking | OAT-011 | Scraping |
| OAT-001 | Carding | OAT-016 | Skewing |
| OAT-012 | Cashing Out | OAT-013 | Sniping |
| OAT-007 | Credential Cracking | OAT-017 | Spamming |
| OAT-008 | Credential Stuffing | OAT-002 | Token Cracking |
| OAT-015 | Denial of Service | OAT-014 | Vulnerability Scanning |

## OWASP API SECURITY TOP 10

| | |
|---|---|
| A1:2019 | Broken Object Level Authorization |
| A2:2019 | Broken Authentication |
| A3:2019 | Excessive Data Exposure |
| A4:2019 | Lack of Resources & Rate Limiting |
| A5:2019 | Broken Function Level Authorization |
| A6:2019 | Mass Assignment |
| A7:2019 | Security Misconfiguration |
| A8:2019 | Injection |
| A9:2019 | Improper Assets Management |
| A10:2019 | Insufficient Logging & Monitoring |

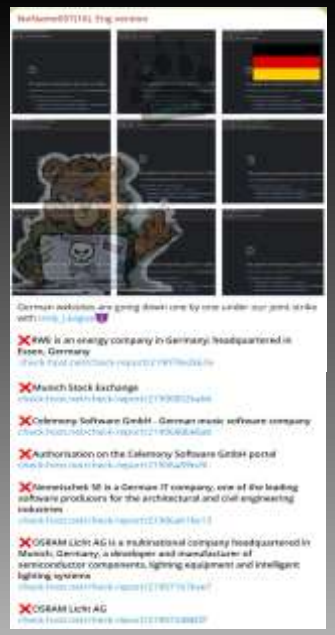
# Jak se mění útoky?



# Motivace - hacktivismus

## Politická motivace

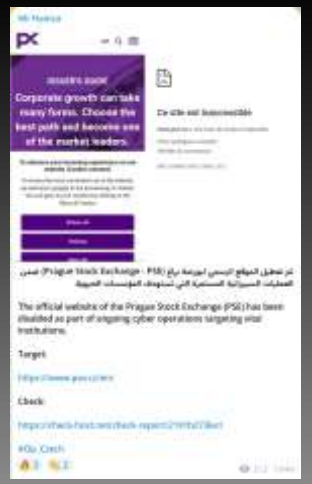

Francouzské vládníorganizace, AXA, 12/24



Holy League Německo
**(12 / 24)**

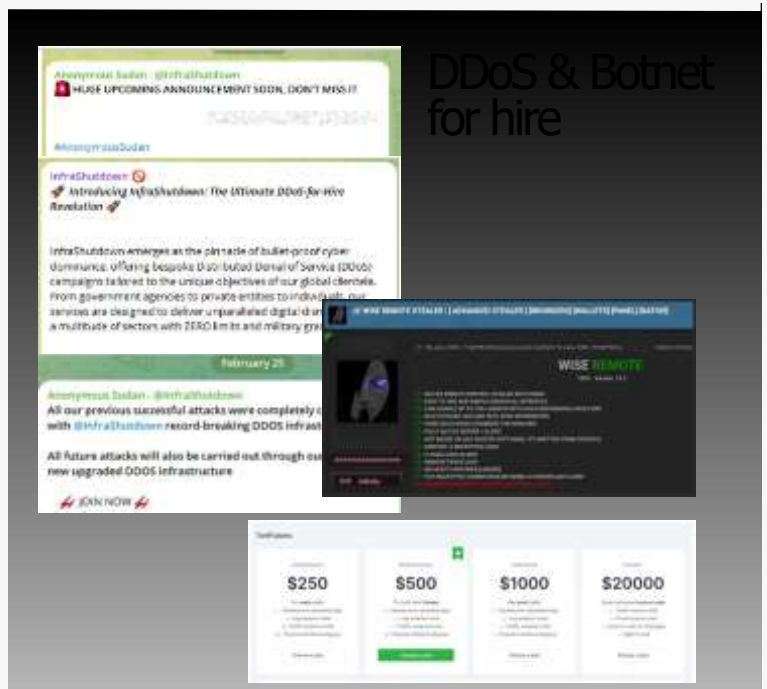
## Náboženství


RipperSec – francouzské banky
**(1224)**



České vládní organizace
**(12/24)**

## Finanční motivace




Marketplace

# Vše v jednom – volně na Githubu


Útočník ma k dispozici veškete vektory - WAF, DDoS, Bot, API

Vše v jednom útoky vyžadují vše v jednom ochranu

## 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

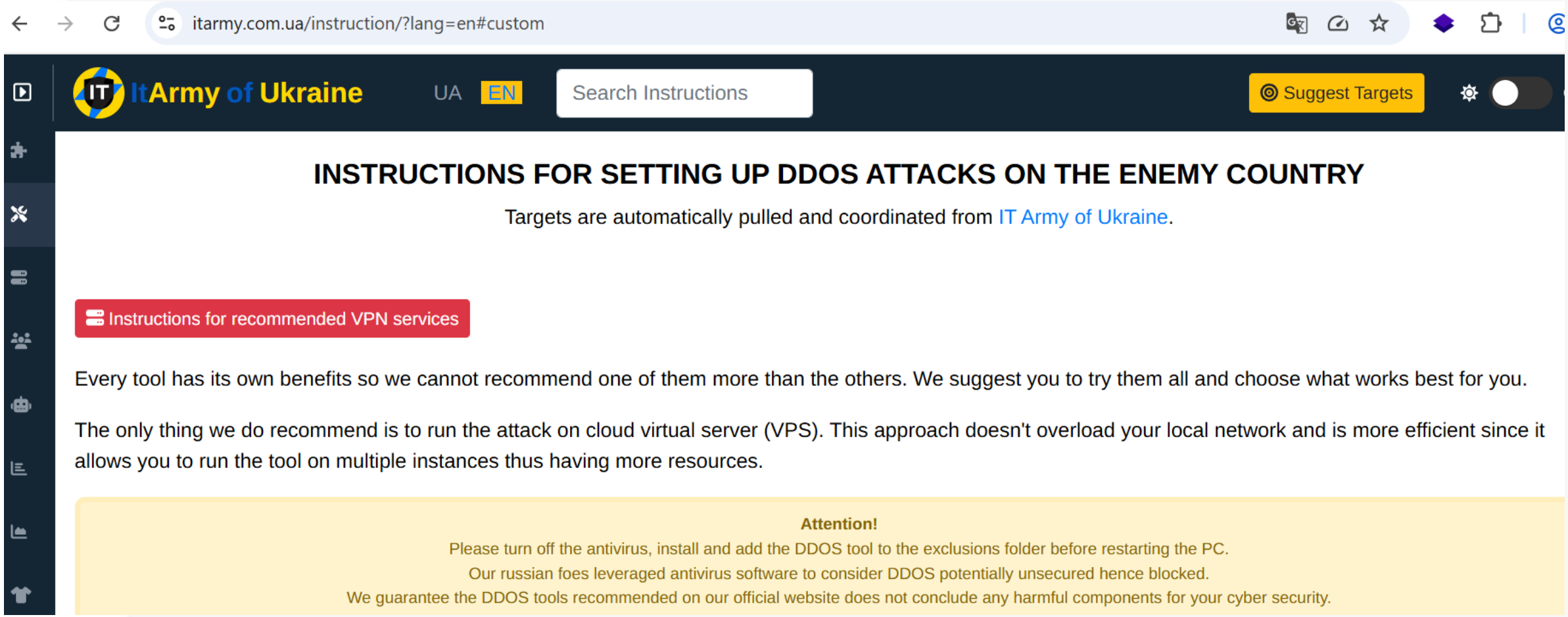
DDoS attack vectors

Bot attack vectors

Web application exploits

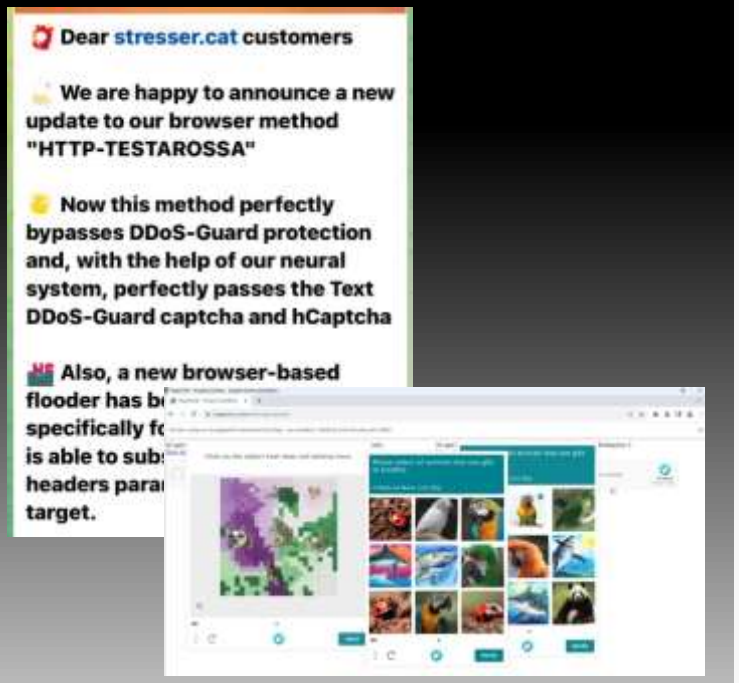
Built-in bypass again common defenses

# Motivace


itarmy.com.ua/instruction/?lang=en#custom
ItArmy of Ukraine
UA
EN
Search Instructions
Suggest Targets
INSTRUCTIONS FOR SETTING UP DDOS ATTACKS ON THE ENEMY COUNTRY
Targets are automatically pulled and coordinated from IT Army of Ukraine.
Instructions for recommended VPN services
Every tool has its own benefits so we cannot recommend one of them more than the others. We suggest you to try them all and choose what works best for you.
The only thing we do recommend is to run the attack on cloud virtual server (VPS). This approach doesn't overload your local network and is more efficient since it allows you to run the tool on multiple instances thus having more resources.
Attention!
Please turn off the antivirus, install and add the DDOS tool to the exclusions folder before restarting the PC.
Our russian foes leveraged antivirus software to consider DDOS potentially unsecured hence blocked.
We guarantee the DDOS tools recommended on our official website does not conclude any harmful components for your cyber security.

# AI pro automatizaci útoků


GenAI nástroje využívány utočníky




Překonání CAPTCHA

| Vulnerability | GPT-4 success rate |
|---|---|
| LFI | 60% |
| CSRF | 100% |
| XSS | 80% |
| SQL Injection | 100% |
| Brute Force | 80% |
| SQL Union | 80% |
| SSTI | 40% |
| Webhook XSS | 20% |
| File upload | 40% |

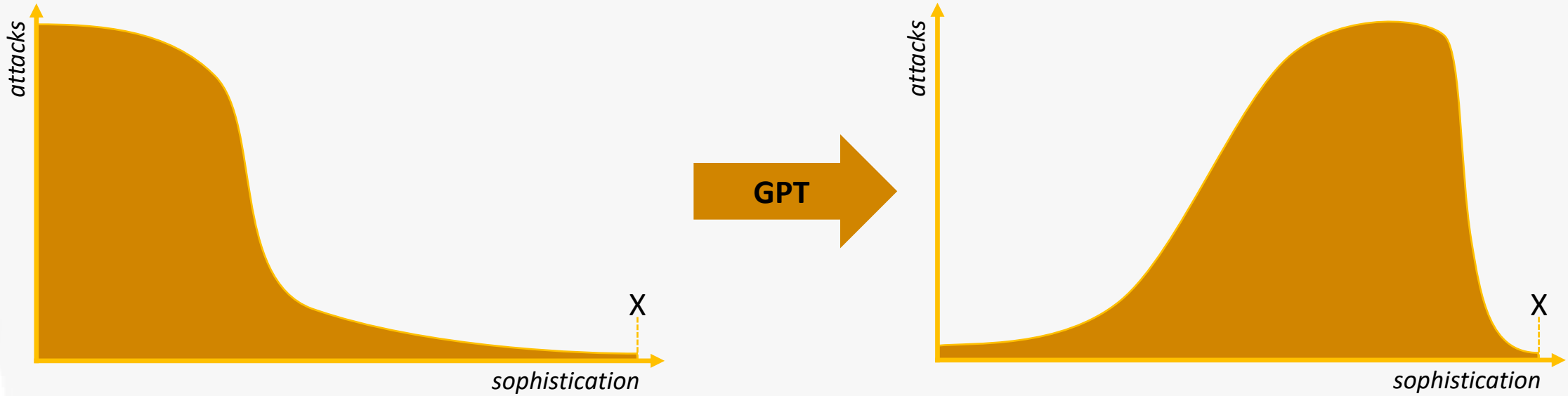
LLM dokáže využívat nové zranitelnosti

* *[2404.08144] LLM Agents can Autonomously Exploit One-day Vulnerabilities (arxiv.org)*

Je potřeba využít AI pro ochranu před AI

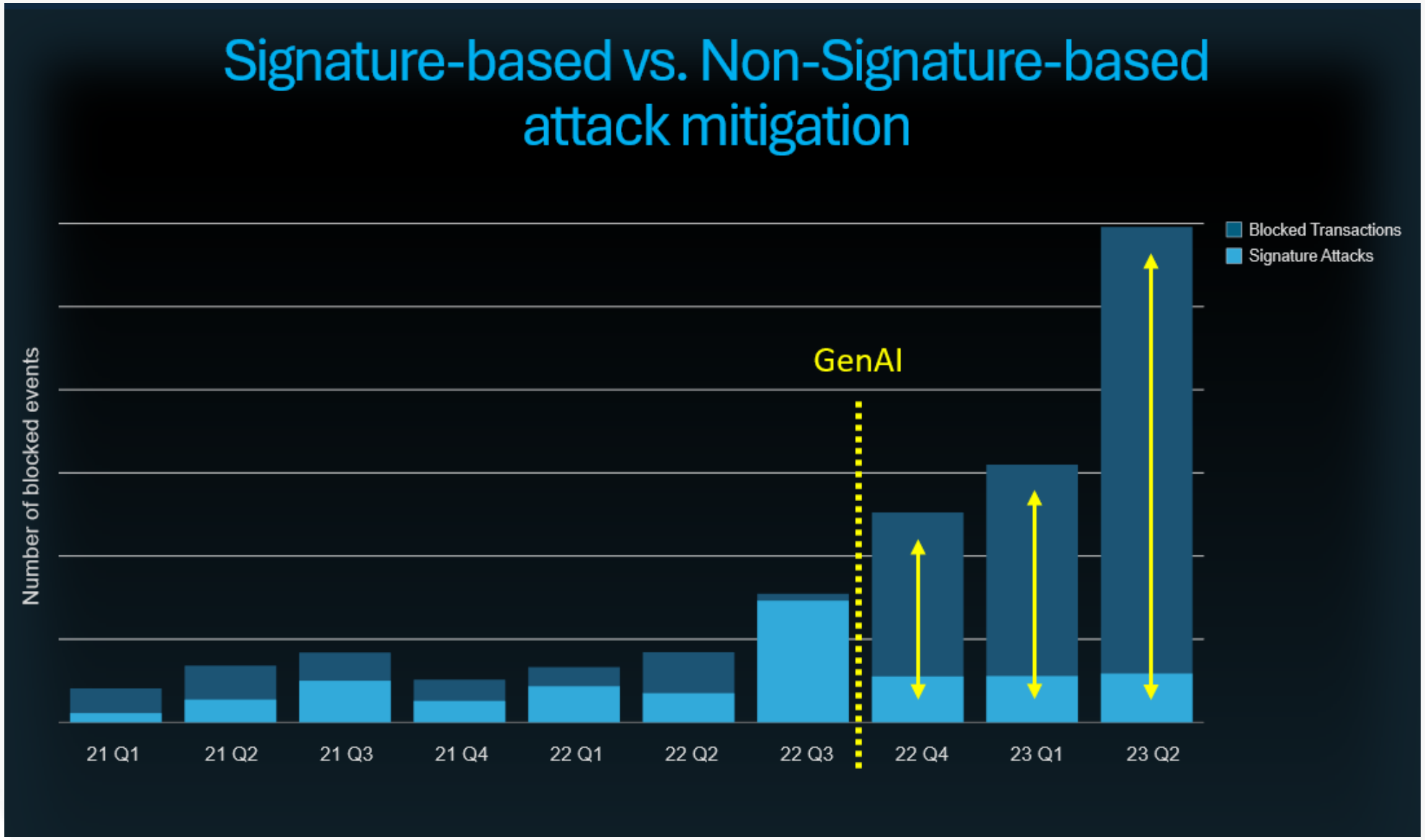
# Vliv AI na útoky

*Neroste sofistikovanost útoků ale roste počet sofistikovaných útoků*



# Vliv AI na útoky

*attacks*

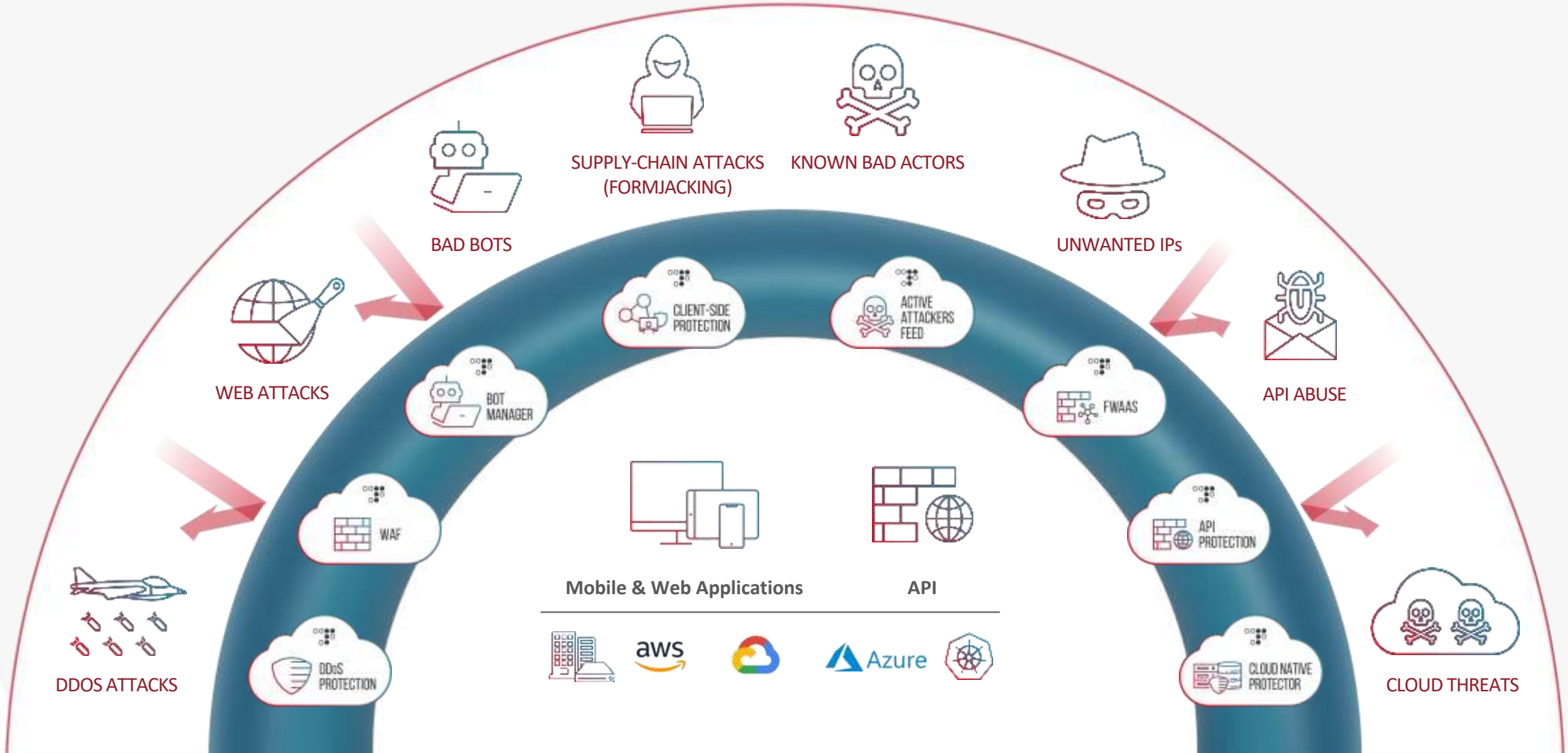


# AI přináší novou kvalitu

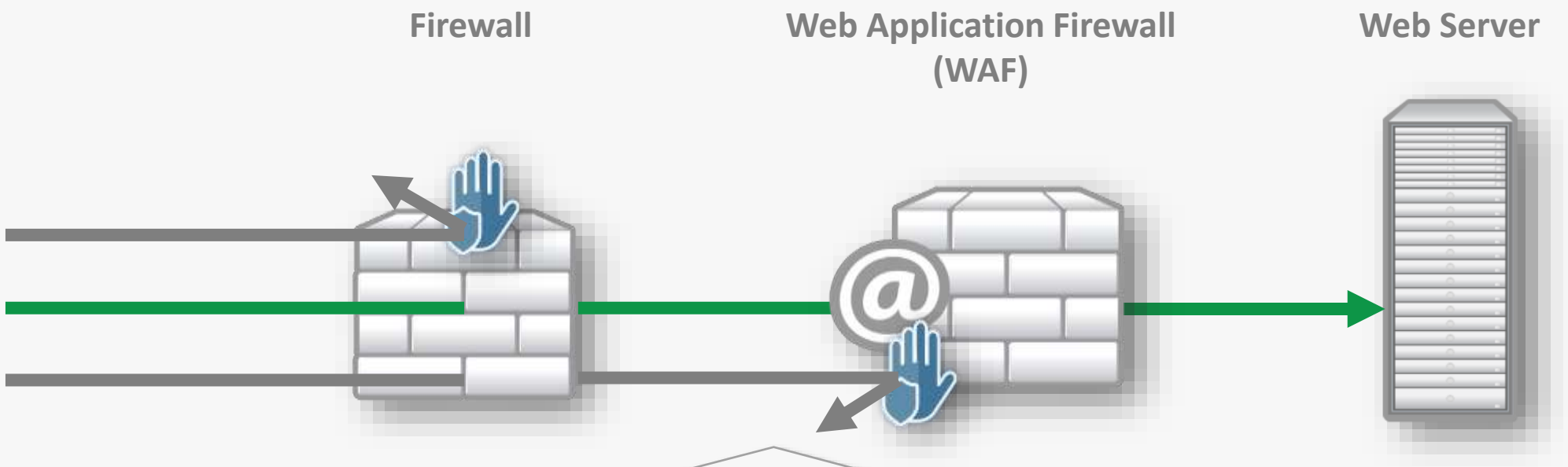
- Výrazně usnadňuje možnost sofistikovaných útoků
- Nové a častější
- Dynamické a proměnllivé
- **Potřeba AI nástrojů pro mitigaci – schopnost učit se legitimní chování a detkovat anomálie a a jejich změny v reálném čase**

# Radware 360° ochrana

Ochrana webu, ochrana prohlížeče a všeho „mezi tím“



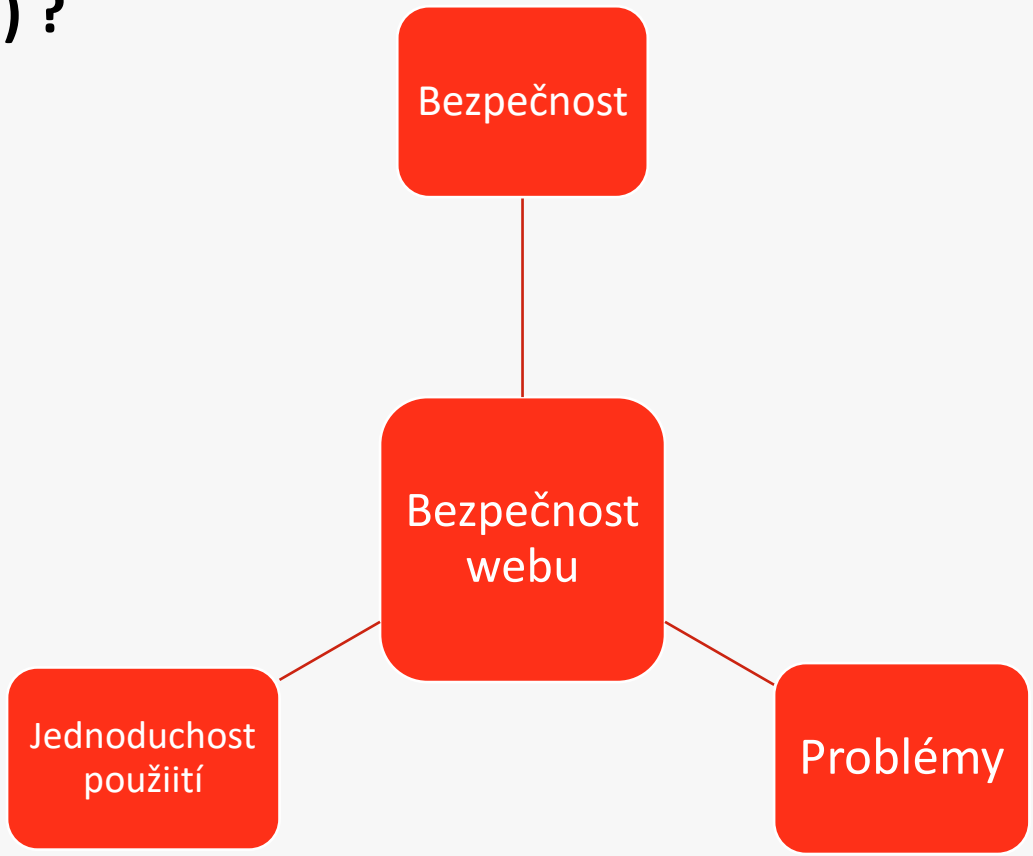
# Web Application Firewall (WAF)




- Rozumí HTTP a  plně chápe konverzaci
- Dokáže dešifrovat provoz
- Chrání konkrétní aplikaci
- **Nenahrazuje jiná řešení a ani jiná řešení nemohou nahradit WAF**

# Na co myslet při výběru řešení?

- Jak rychle reaguje na změny?
- V jaké formě (on premise / služba) ?
- Nároky na zdroje?
- Jak rychle/snadno lze nasadit?
- Snadný provoz?
- Jak dlouho vydrží?



# Pozitivní i negativní model

## Negativní bezpečnostní model

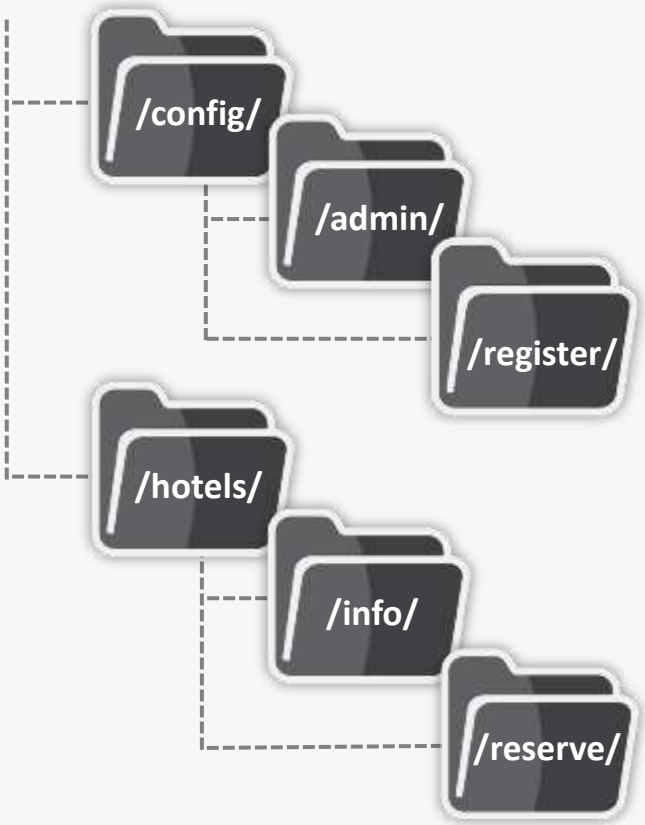
- Detekuje a blokuje známá rizika (efektivní)
- **NEDOKÁŽE chránit před neznámými riziky (zero day)**

## Pozitivní bezpečnostní model

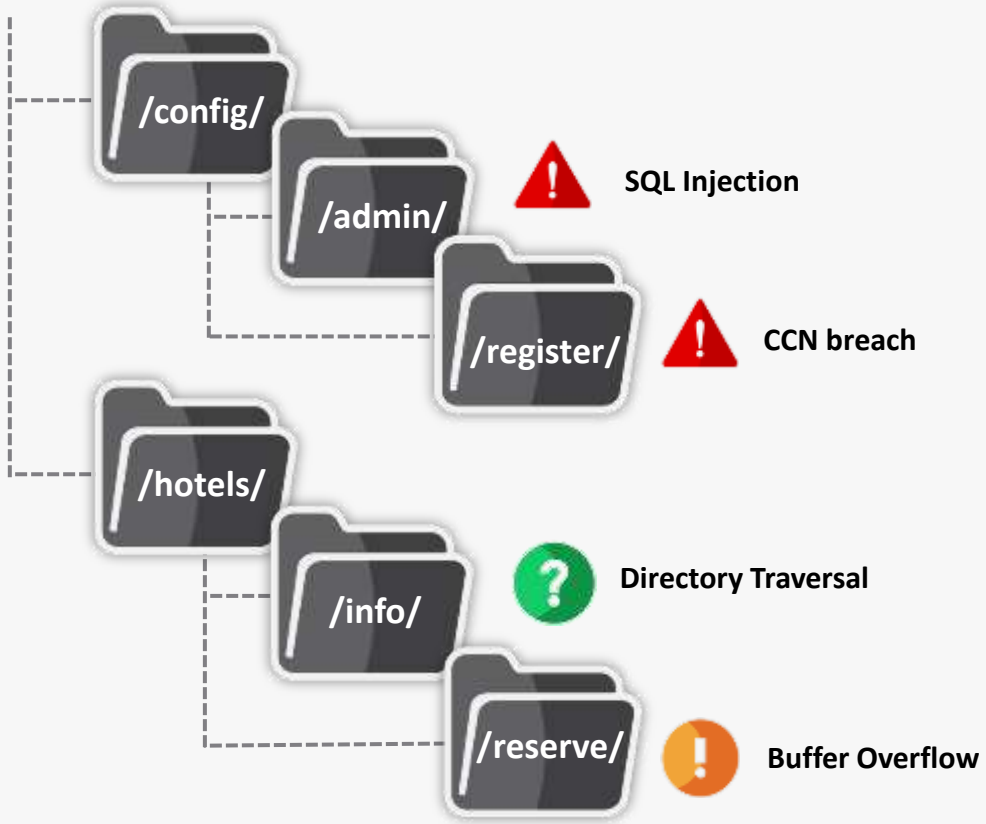
- Je schopen se naučit co je legitimní (a blokuje tak vše „co není povoleno“)
- **Chrání i před neznámými (0-day) útoky a zranitelnosti**
- **Bez blokování legitimních požadavků (bez false-positives)**

# Struktura aplikace

**www.reservations.com**



## www.reservations.com



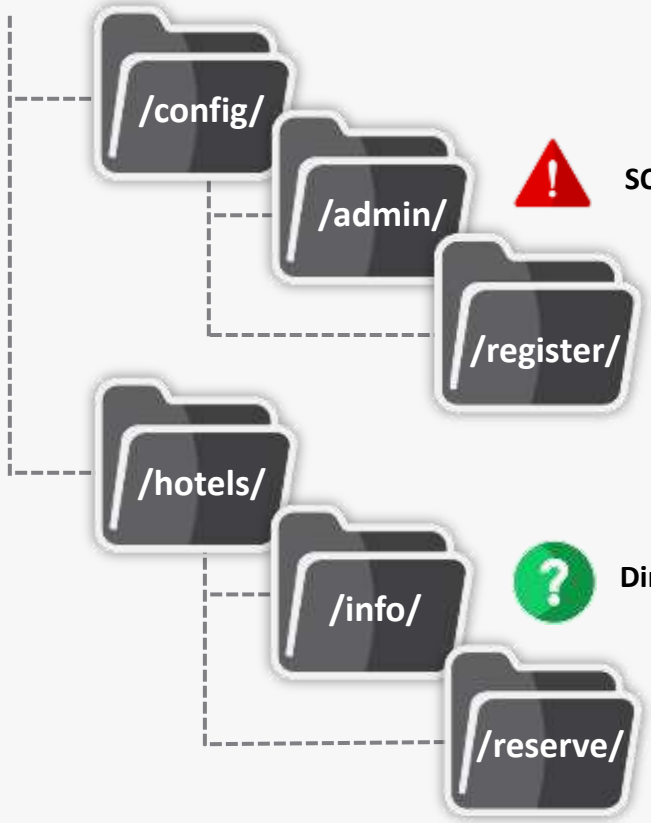

Podvržení identity, zcizení uživatelských informací, modifikace dat

Únik informací

Získaní přístupu s root právy

Nepředvídatelné chování, pád systému, kompromitace systému

## www.reservations.com




SQL Injection

CCN breach

Directory Traversal

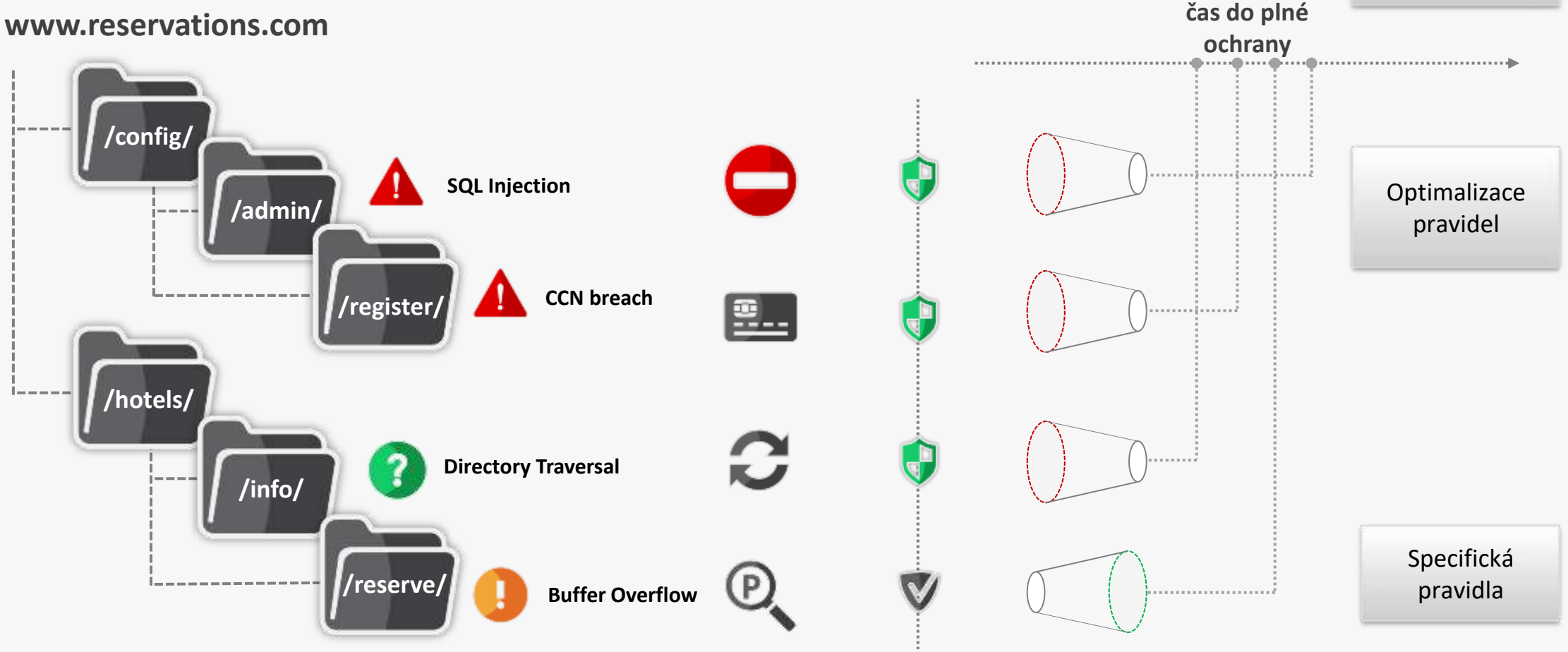
Buffer Overflow

**Zabránění přístupu k citlivým informacím (mimo rozsah oprávnění)**

**Maskování informací (CCN, SSN…), v odpovědi**

**Ověření HTTP standardů**

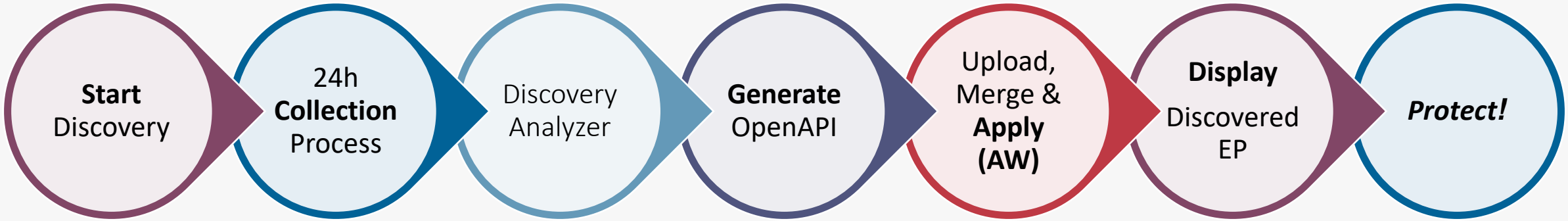
**Kontrola parametrů**


Bez false positive“
čas do plné ochrany
www.reservations.com
/config/
/admin/
/register/
/hotels/
/info/
/reserve/
SQL Injection
CCN breach
Directory Traversal
Buffer Overflow
Optimalizace pravidel
Specifická pravidla

# Ochrana API

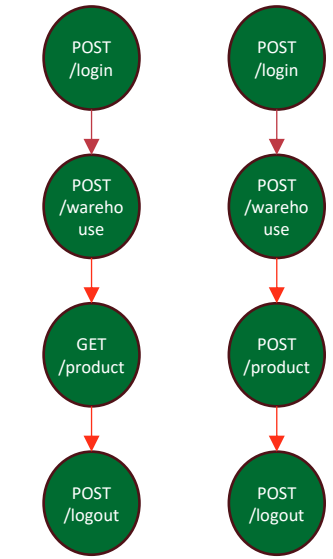
| OWASP API SECURITY TOP 10 | |
|---|---|
| A1:2019 | Broken Object Level Authorization |
| A2:2019 | Broken Authentication |
| A3:2019 | Excessive Data Exposure |
| A4:2019 | Lack of Resources & Rate Limiting |
| A5:2019 | Broken Function Level Authorization |
| A6:2019 | Mass Assignment |
| A7:2019 | Security Misconfiguration |
| A8:2019 | Injection |
| A9:2019 | Improper Assets Management |
| A10:2019 | Insufficient Logging & Monitoring |

# API schémata – schopnost učení se




**WAAP – Web Application and API Protection**

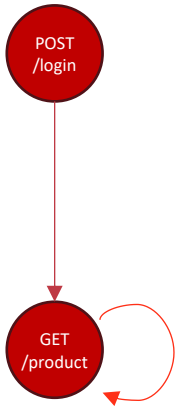
# BLA (Business Logic Attack)



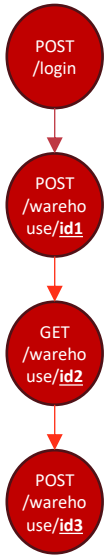

Non-admin Admin

**Legitimní**

Reconnaissance

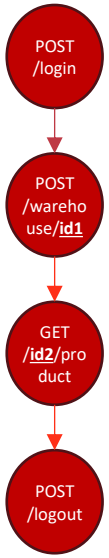



API1 - Broken Object Level Authorization (BOLA)




Non-admin

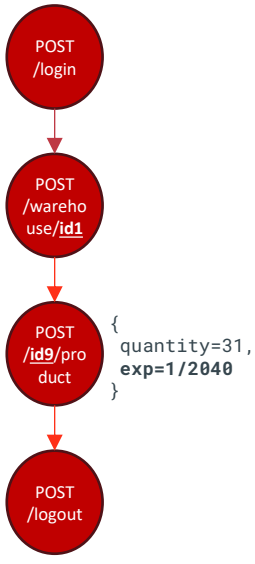
API1 - Broken Object Level Authorization (BOLA)




Non-admin

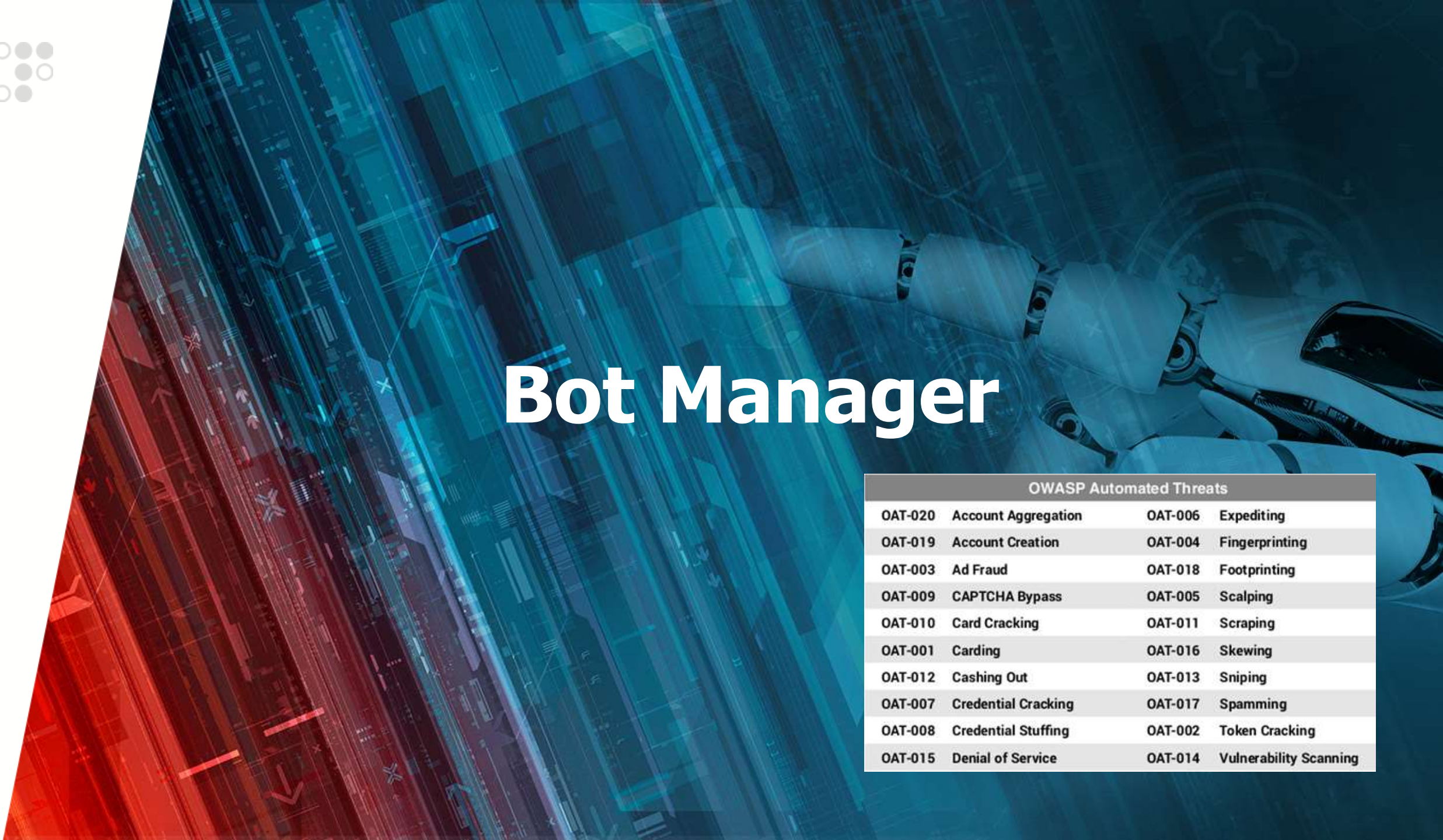
API2 - Broken Authentication


API3 - Broken Object Property Level Authorization




Admin

**Útok**

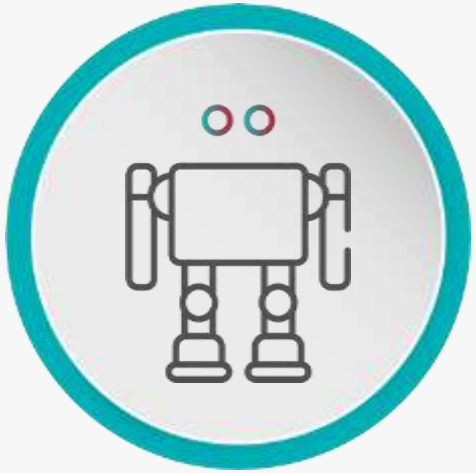


# Bot Manager

| OWASP Automated Threats | | | |
|---|---|---|---|
| OAT-020 | Account Aggregation | OAT-006 | Expediting |
| OAT-019 | Account Creation | OAT-004 | Fingerprinting |
| OAT-003 | Ad Fraud | OAT-018 | Footprinting |
| OAT-009 | CAPTCHA Bypass | OAT-005 | Scalping |
| OAT-010 | Card Cracking | OAT-011 | Scraping |
| OAT-001 | Carding | OAT-016 | Skewing |
| OAT-012 | Cashing Out | OAT-013 | Sniping |
| OAT-007 | Credential Cracking | OAT-017 | Spamming |
| OAT-008 | Credential Stuffing | OAT-002 | Token Cracking |
| OAT-015 | Denial of Service | OAT-014 | Vulnerability Scanning |

# Evoluce botů

Skripty



HEADLESS BROWSER
(prohlížeče bez GUI)

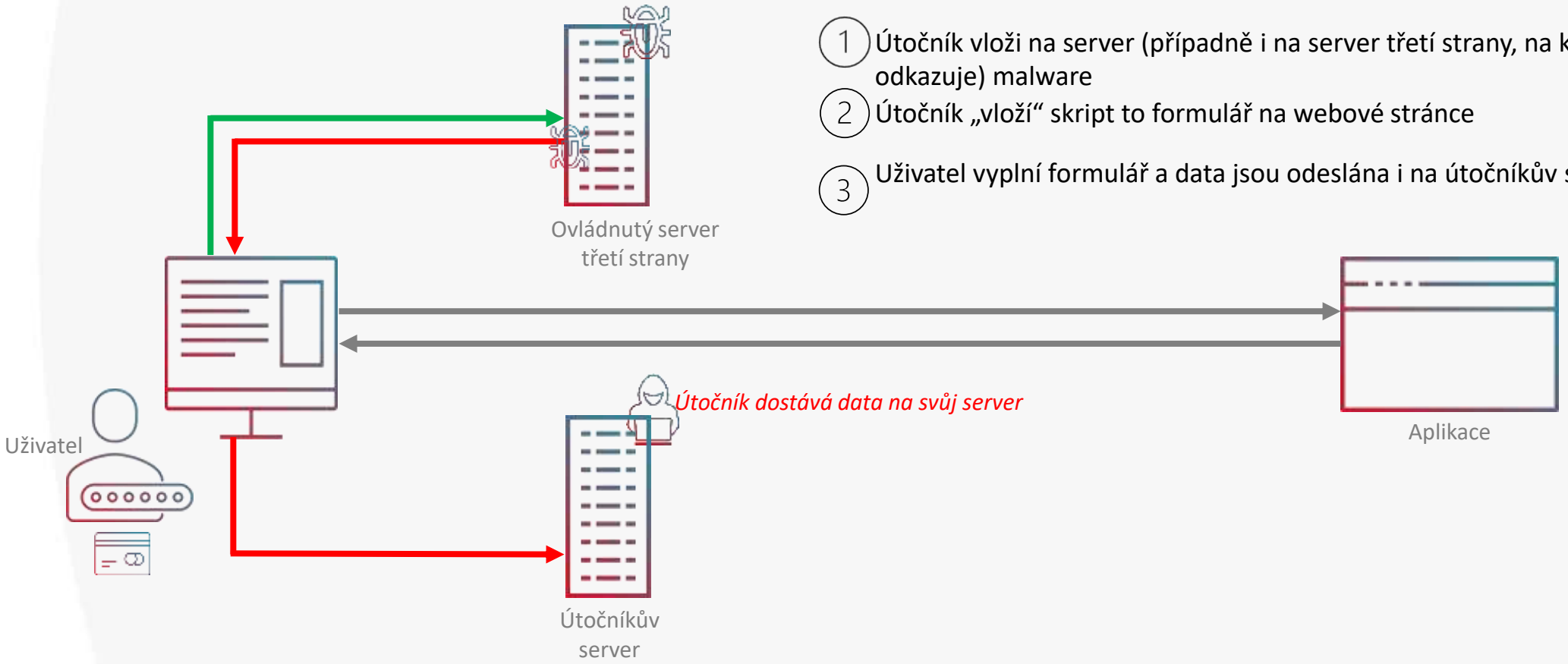
Simulující lidské chování

Distribuované

# Typické útoky

# Client-side ochrana

# Formjacking

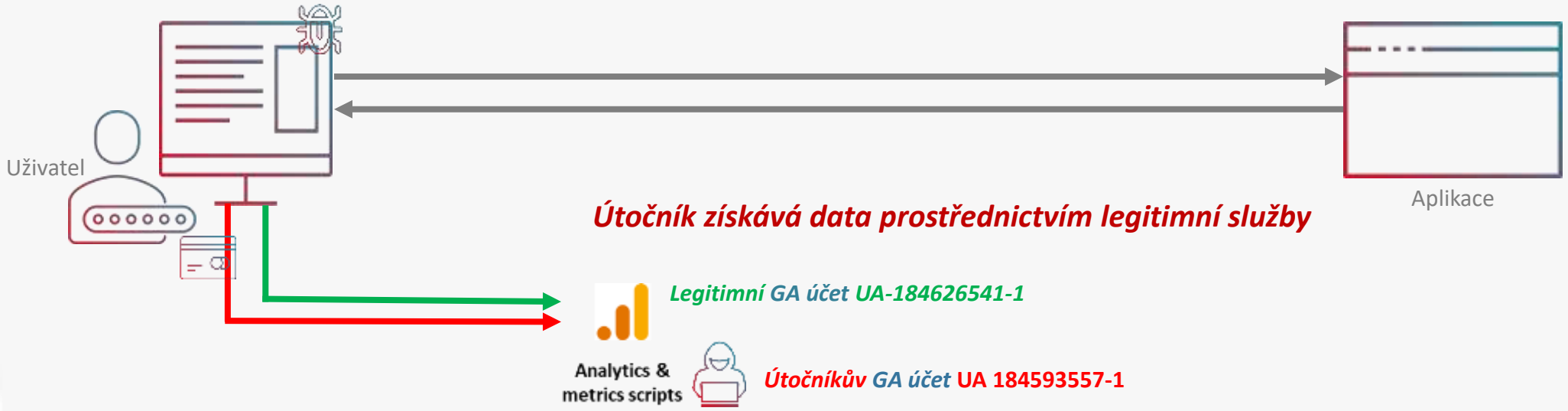



1. Útočník vloži na server (případně i na server třetí strany, na který se server odkazuje) malware
2. Útočník „vloží“ skript to formulář na webové stránce
3. Uživatel vyplní formulář a data jsou odeslána i na útočníkův server

# Zneužití Google Analytics

*Legitimní cílová aplikace s nelegitimními parametery* – útočník je odešle prostřednictvím Google analytics „na svůj účet“

1. Útočník vloží školdlivý kód do aplikace
2. Tento kód „posbírá“ data a pošle je „ven“ prostřednictvím Google Analytics
3. Útočník k nim má přístup pod svým účtem



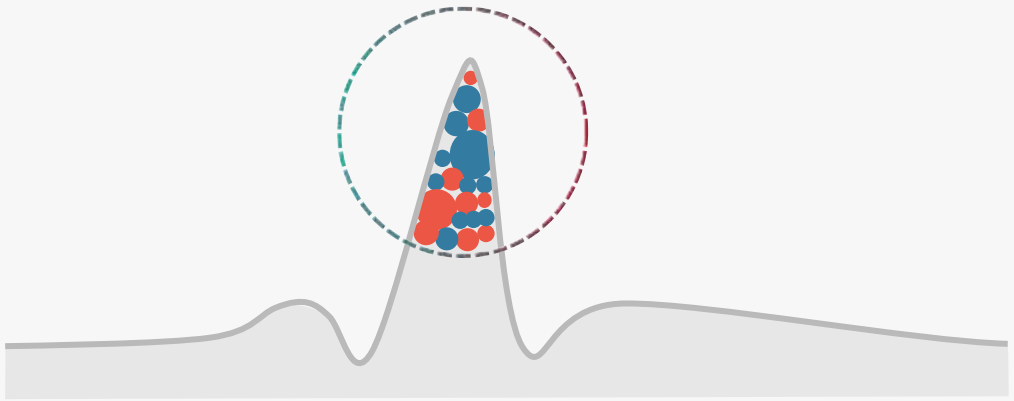

DDoS

# Efektivní ochrana

*Analýza legitimního provozu -> Behaviorální analýza -> Dynamická signatura*

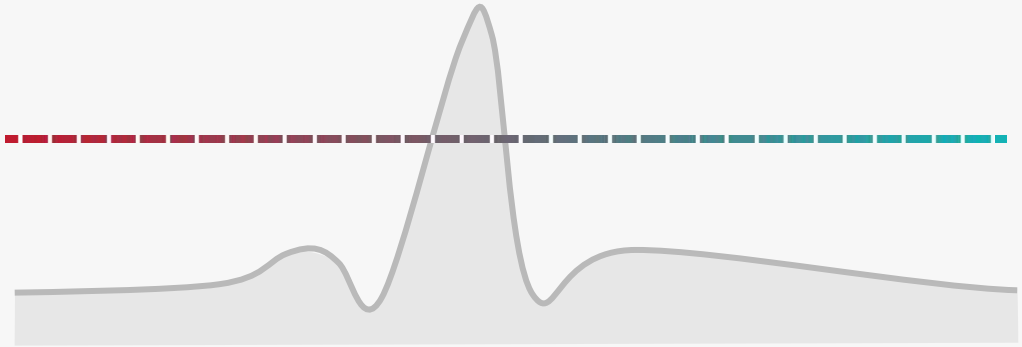
## Radware

Behaviorální analýza



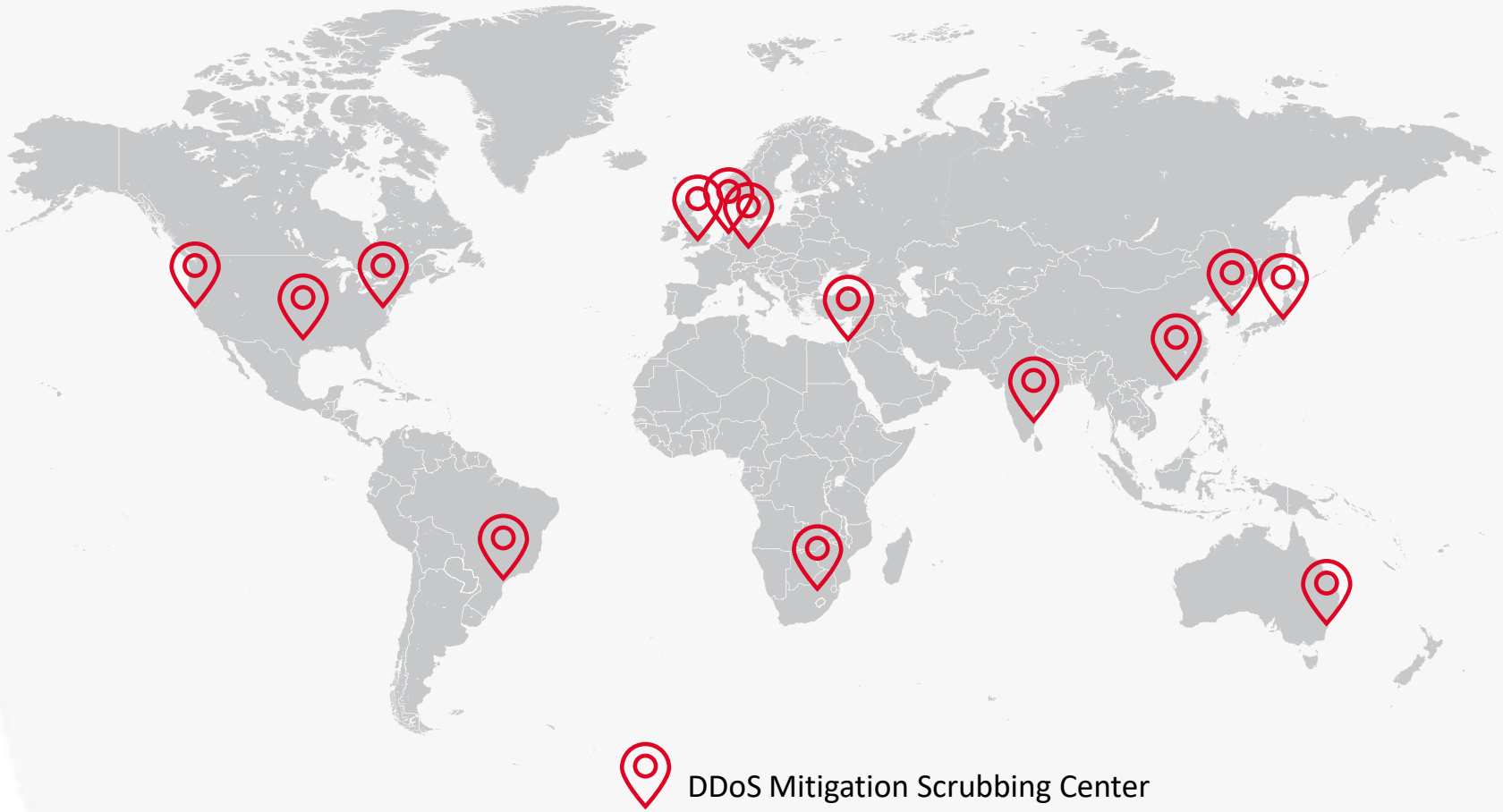
## Standardní přístup

Statická konfigurace



Snadné nasazení, automatická detekce a mitigace

# DDoS - globální infrastruktura



DDoS Mitigation Scrubbing Center

**22** scrubbinových center

**15 Tbps** kapacity

# Jednoznačné SLA

## TIME TO DETECT

Jak rychle je útok detekován

## TIME TO ALERT

Jak rychle je zákaznik informován

## TIME TO DIVERSION

Jak rychle dojde k přesměrování

## TIME TO MITIGATE

Jak rychle je útok čištěn

## CONSISTENCY OF MITIGATION

Efektivita mitigace


## SERVICE AVAILABILITY

Dostupnost


Web DDoS

# Kombinovaný útok mitigovaný RADWARE

| Czech Republic | | | | |
|---|---|---|---|---|
| www.zakaznik.cz | | | | |
| ab.xx.xxx.xy | http-GET | port:443 | ssl:True | path:/novinky?do[dataList]=1&paging.pageNo=$_2 |
| ab.xx.xxx.xy | http-POST | port:443 | ssl:True | path:/web/karta-overeni.html |
| ab.xx.xxx.xy | http-GET | port:443 | ssl:True | path:/hledat?searchString=$_1 |
| ab.xx.xxx.xy | http-POST | port:443 | ssl:True | path:/web/widget.html |
| | | widget_zakazniknewsletterregirwidget2_email=$_1%&widget_zakazniknewsleterwidget2_confirm=0&widget_zakazniknewsletterregisterwidget2_do%5Bregister%5D=&_w=163d69299119af2b501f4e88abf2bb9f1fb2151058233736823bc8bdc2da98cb52840e43ab4e2feab5d2ca016bd44e8a7fa5cbc55f82ae8726265c3166ff7b95 | | |
| ab.xx.xxx.xy | tcp-syn | port:443 | ssl:True | path: |
| ab.xx.xxx.xy | tcp-syn | port:80 | ssl:False | path: |
| ab.xx.xxx.xy | nginx_loris- | port:443 | ssl:True | path: |

**L7 DDoS**
**Botnet**
**DDoS**
**Low&Slow**

# WebDDoS “chirurgická přesnost“

Mitigation

Total Requests
Received 7,323,560,508
Dropped 7,322,893,004

Average Values
Requests per Second 839,857 RPS

Maximum Values
Requests per Second 1,892,054 RPS

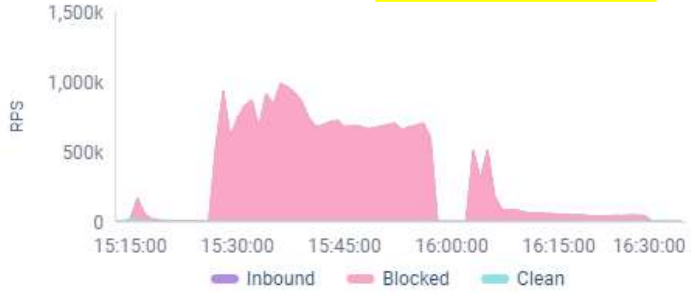

Mitigation

Total Requests
Received 1,546,214,661
Dropped 1,544,249,607

Average Values
Requests per Second 333,235 RPS

Maximum Values
Requests per Second 1,289,856 RPS

Requests Rate
Detection Manual
Attack Start Value 92,937 RPS




Mitigation

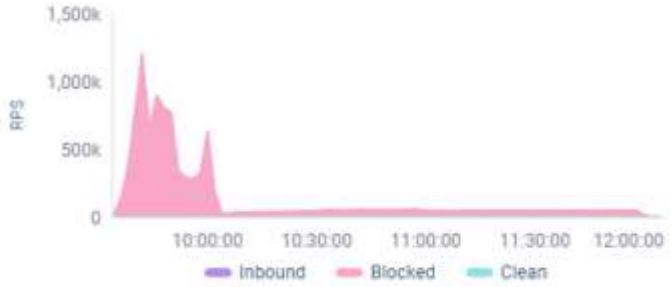
Total Requests
Received 1,240,818,185
Dropped 1,240,530,161

Average Values
Requests per Second 138,022 RPS

Maximum Values
Requests per Second 1,776,723 RPS

Detection

Requests Rate
Detection Manual
Attack Start Value 4,140 RPS



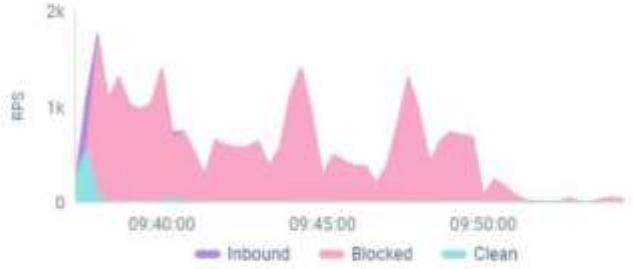

Mitigation

Total Requests
Received 575,899
Dropped 561,448

Average Values
Requests per Second 559 RPS

Maximum Values
Requests per Second 2,031 RPS

Requests Rate
Detection Manual
Attack Start Value 755 RPS

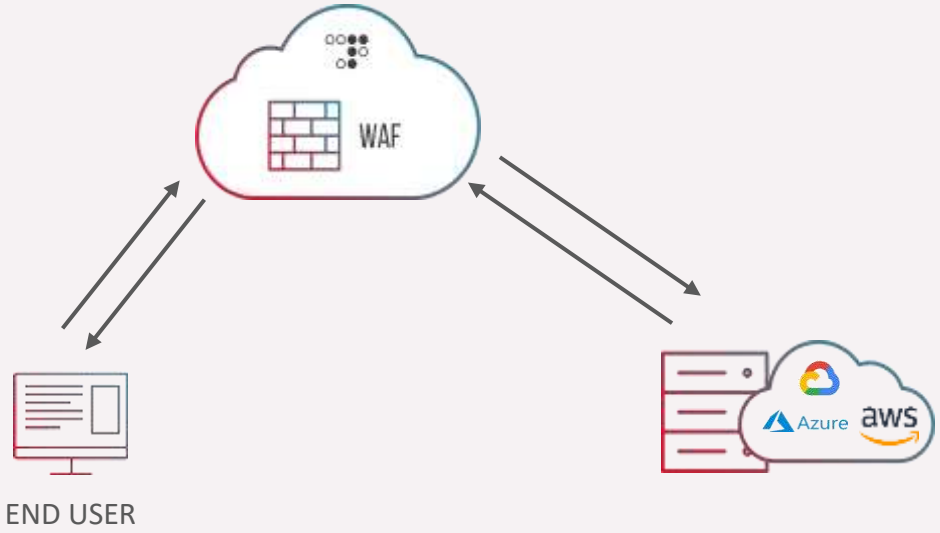


# Možnosti nasazení

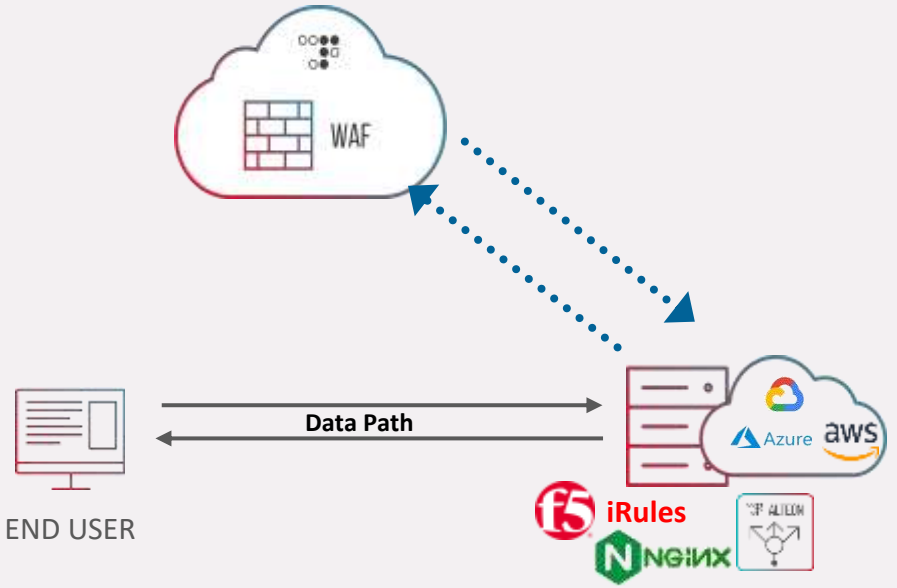
# S přesměrováním nebo bez?

## SecurePath™

### DNS přesměrování




### Plugin



# Certifikace a audity

- **BSI qualified** **DDoS Protection Vendor Listing**
- **ISO 22301** Business Continuity Management System
- **ISO 27001** Information Security Management Systems
- **ISO 27017** **Information Security for Cloud Services**
- **ISO 27018** **Information Security Protection of 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-DSSv4** Payment Card Industry Data Security Standard
- **HIPAA** Health Insurance Portability and Accountability Act
- **US SSAE16** SOC-1 Type II, SOC-2 Type II
- **DORA** **Digital Operational Resilience Act**
- **NIS2** **Network and Information Systems Directive 2022/0383**

# RADWARE WAFaaS

Radware CWAF nabízí:

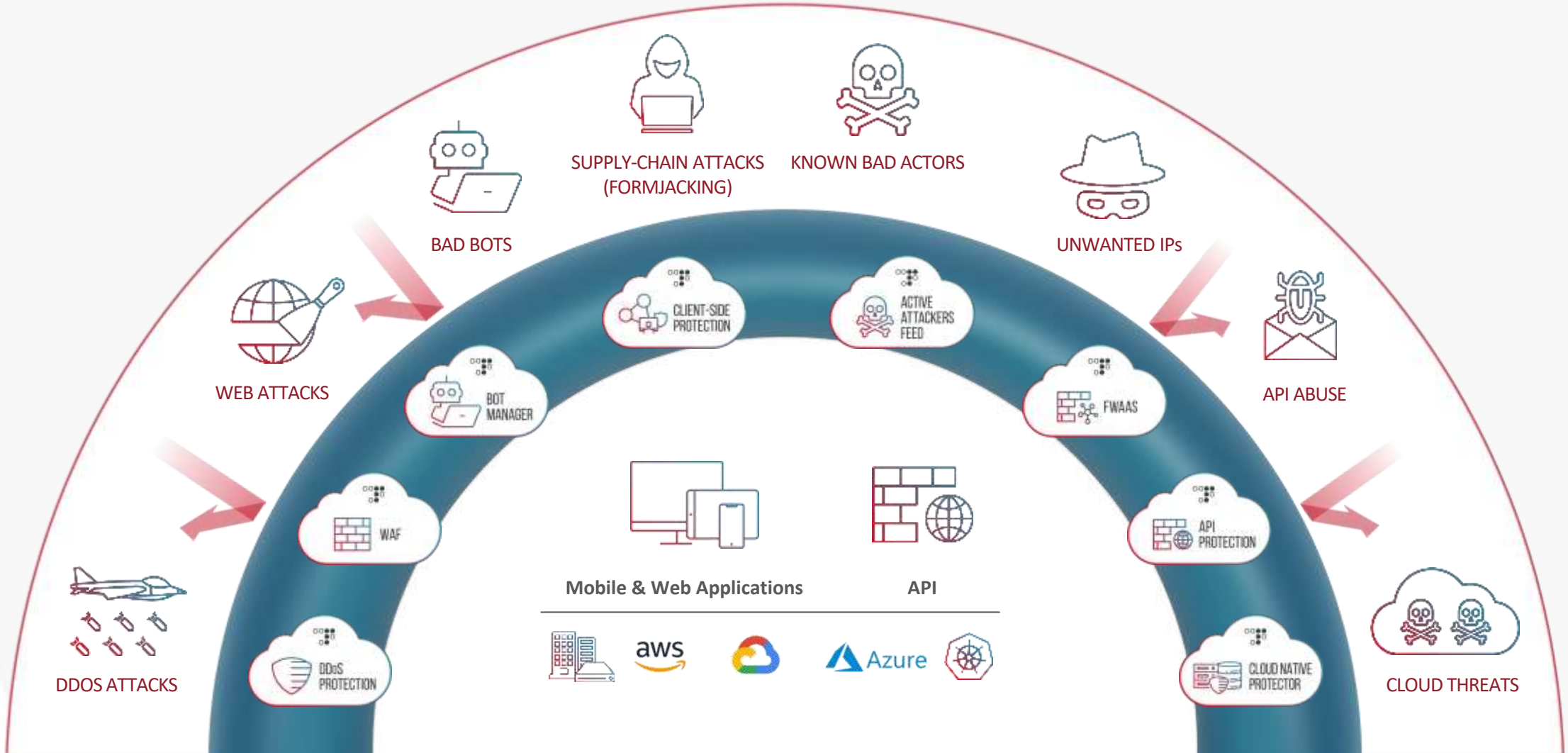
- Manage service/SLA
- DDoS
- BOT Management
- IP reputace signatury
- CDN
- Jednotný portál (MSSP)

**Služba:**

- **Technologie**
- **Know-how (Emergency response tým 24x7, 200+)**
- **Best practices (certifikace, audity)**
- **SLA + support**
- **Response time 30 minut (10 minut pro prémiovou službu)**

# Radware 360° ochrana

Ochrana webu, ochrana prohlížeče a všeho „mezi tím“



# Kompletní ochrana

**Learning**


**OWASP Top 10**

**+**

**Zero-Day**

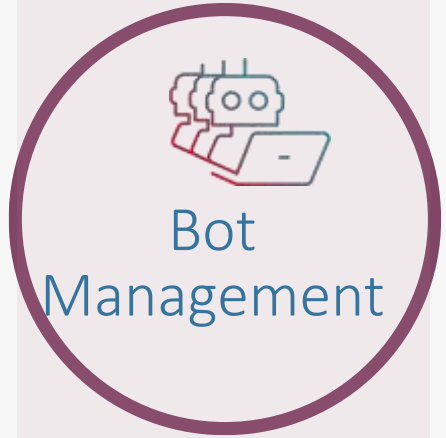
**JS + ML**


**“Dodavatelský řetězec“**

**Learning**


**Ochrana API**

**Machine learning**




**Ochrana před boty**

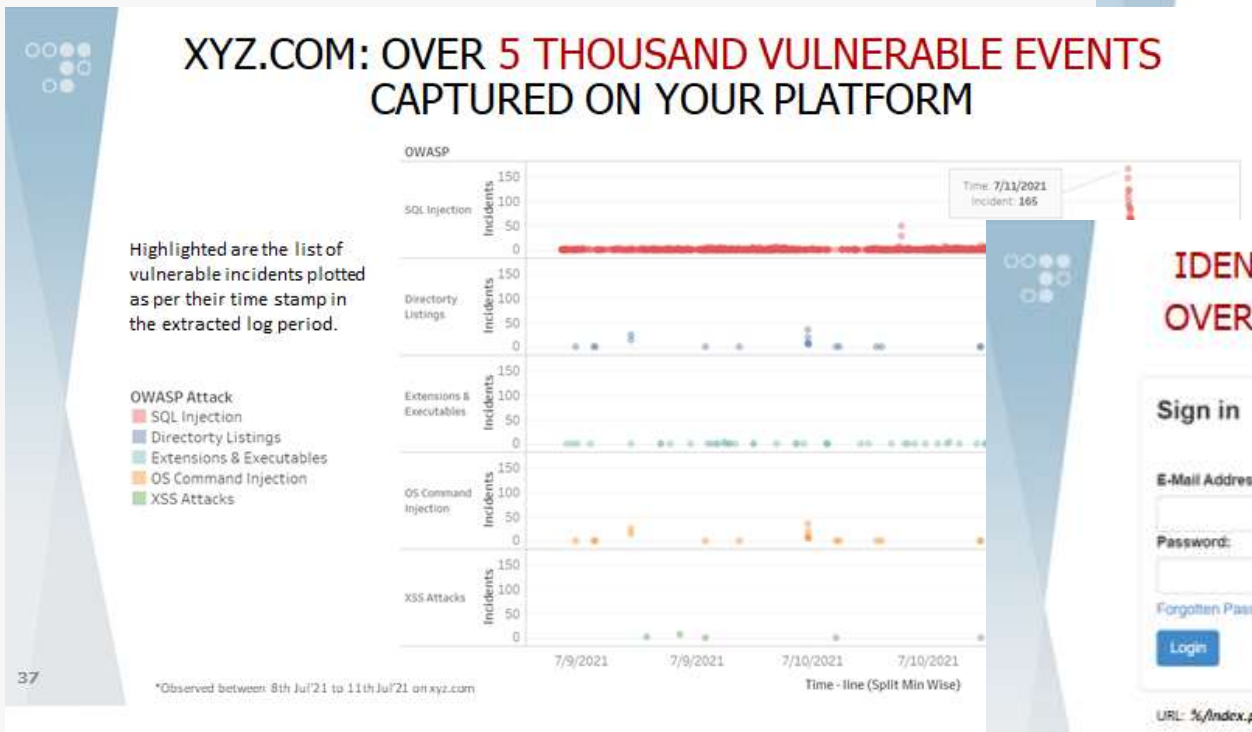
**Behavioral**

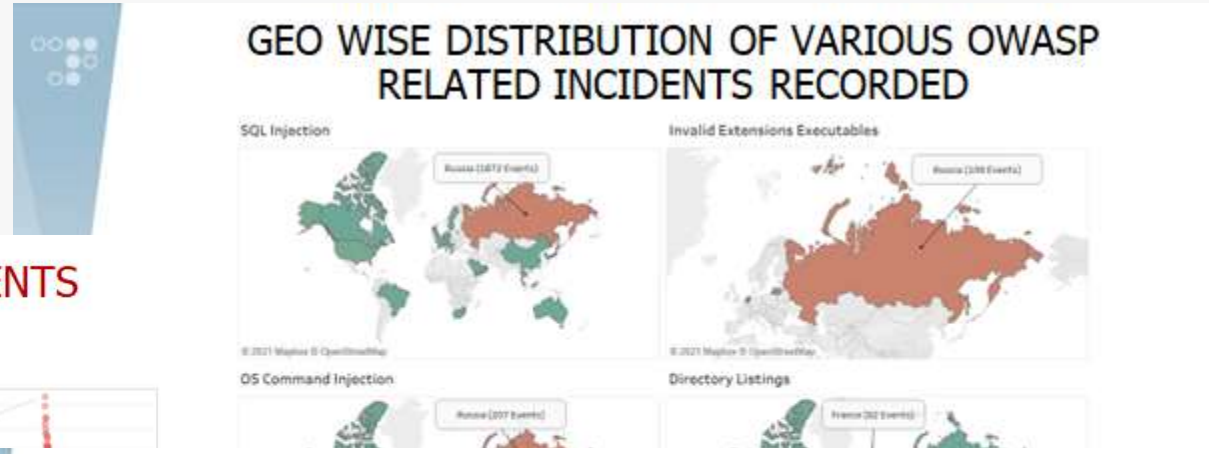

**DDoS ochrana**

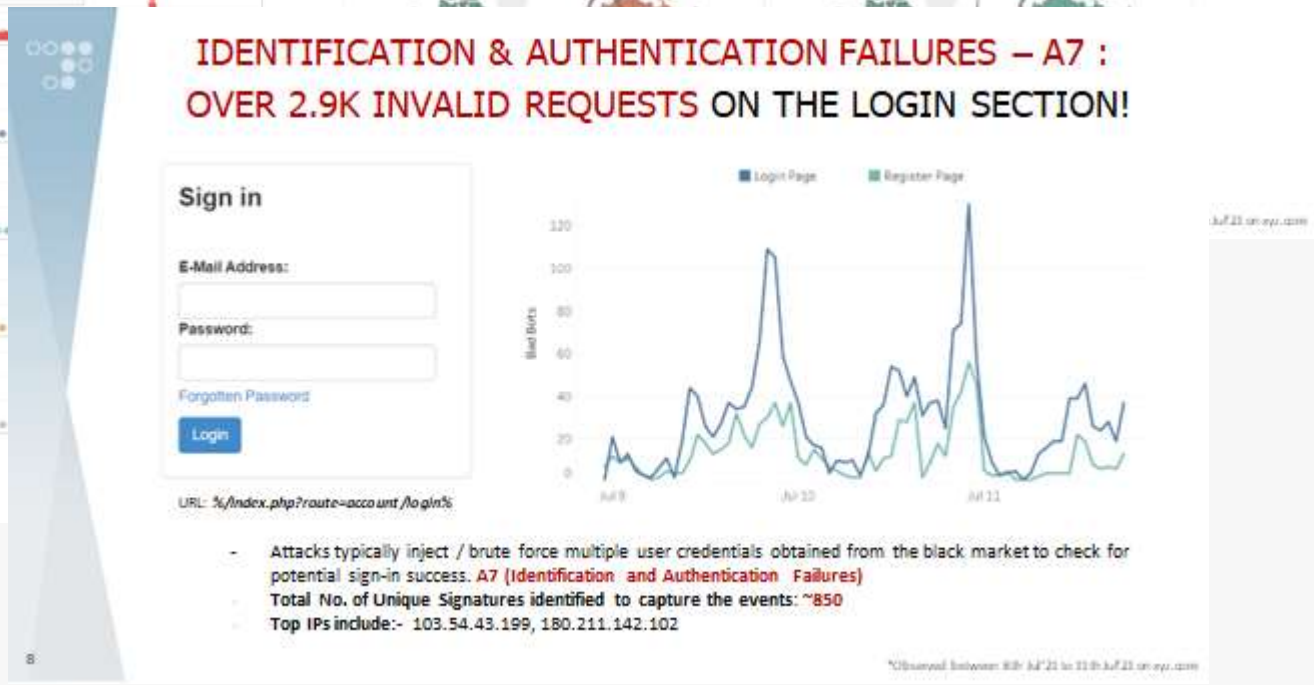
**Web DDoS**

Source blocking (Threat Scoring, AI)

# Vás se to netýka?




**Analýza webových logů zdarma!!!**