Ochrana a zabezpečený přístup k citlivým datům

Filip Kolář
F5 Networks
Web App Attacks are the #1 Source of Data Breaches

"Web Application Attacks remains the most prevalent"

"Use of stolen credentials against web applications was the dominant hacking tactic"
<table>
<thead>
<tr>
<th>OWASP Top 10 - 2013</th>
<th>OWASP Top 10 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 – Broken Authentication and Session Management</td>
<td>A2:2017-Broken Authentication</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>A3:2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A6 – Sensitive Data Exposure</td>
<td>A6:2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
<td>A8:2017-Insecure Deserialization [NEW, Community]</td>
</tr>
<tr>
<td>A9 – Using Components with Known Vulnerabilities</td>
<td>A9:2017-Using Components with Known Vulnerabilities</td>
</tr>
</tbody>
</table>
Attacker Demands Ransom After Series of DDoS Attacks on Poker Site

Source: Verizon 2017 Data Breach Investigations Report
THE APPLICATION IS THE GATEWAY TO DATA

Understand the application
Jaký je nejvhodnější nástroj pro ochranu aplikací?

<table>
<thead>
<tr>
<th>known web worms</th>
<th>Network / Next Gen Firewall</th>
<th>IPS</th>
<th>Web Application FW</th>
</tr>
</thead>
<tbody>
<tr>
<td>limited</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>unknown web worms</td>
<td>X</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>known web vulnerabilities</td>
<td>Limited</td>
<td>Partial</td>
<td>✓</td>
</tr>
<tr>
<td>unknown web vulnerabilities</td>
<td>X</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>illegal access to web-server files</td>
<td>limited</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>forceful browsing</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>file/directory enumerations</td>
<td>X</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>buffer overflow</td>
<td>limited</td>
<td>limited</td>
<td>✓</td>
</tr>
<tr>
<td>cross-site scripting</td>
<td>limited</td>
<td>limited</td>
<td>✓</td>
</tr>
<tr>
<td>sql/os injection</td>
<td>X</td>
<td>limited</td>
<td>✓</td>
</tr>
<tr>
<td>cookie poisoning</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>hidden-field manipulation</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>parameter tampering</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>layer 7 dos attacks</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>brute force login attacks</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>app. security and acceleration</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
F5 Networks Positioned as a Leader in 2017 Gartner Magic Quadrant for Web Application Firewalls*

F5 is highest in execution within the Leaders Quadrant.

* Gartner, Magic Quadrant for Web Application Firewalls, Jeremy D’Hoinne, Adam Hils, Claudio Neiva, 7 August 2017
Bots, Bots, and More Bots

50% of Internet traffic is automated

77% of 2016 web application breaches involved the use of bots

98.6M bots observed

Source: Internet Security Threat Report, Symantec, April 2017
Bots

A common source of many threat vectors

Client-Side Attacks
- Malware
- Ransomware
- Man-in-the-browser
- Session hijacking
- Cross-site request forgery
- Cross-site scripting

App Infrastructure Attacks
- Man-in-the-middle
- Key disclosure
- Eavesdropping
- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Protocol abuse
- Dictionary attacks

DDoS Attacks
- SYN, UDP, and HTTP floods
- SSL renegotiation
- DNS amplification
- Heavy URL

Web Application Attacks
- API attacks
- Cross-site scripting
- Injection
- Cross-site request forgery
- Malware
- Abuse of functionality
- Man-in-the-middle
- Credential theft
- Credential stuffing
- Phishing
- Certificate spoofing
- Protocol abuse

© 2018 F5 Networks
Proactive Bot Defense

**PROBLEM**
Malicious bots

**SOLUTION**
Web Application Firewall (WAF)
Behavioural analysis to identify malicious bots
Evolution of DDoS Attacks

**Volumetric take-downs**
Consume bandwidth of target

**Network layer attack**
Consume connection state tables

**Application layer**
Consume application resources

Source: How DDoS attacks evolved in the past 20 years, BetaNews
DDoS for Hire
Low sophistication, high accessibility

- **Accessible**
  Booters/stressers easy to find

- **Lucrative**
  Profit margins of up to 95%

- **Effective**
  Many DDoS victims pay up

Source: Securelist, Kaspersky Lab, March 2017
L7 Behavioral DDOS Protection: an advanced, phased approach

Multiple Layers of Protection

- Rate Limit to Protect the Server
- Detect and Block Bots and Bad Actors
- Create and Enforce Dynamic Signatures
- Analyze Application Stress and Continually Tune Mitigations.

Start of Attack
Identify Attackers
Advanced Attacks
Persistent Attacks

Even basic attacks can take an unprotected server down quickly.

Persistent attackers will adjust tools, targets, sources and attack volume to defeat static DOS defenses.
Malware Trends

In the first quarter of 2017, a new specimen of malware emerged every 4.2 seconds.

1 in every 131 emails included malware in 2016.

Over half (51%) of all breaches in 2016 involved some form of malware.

Sources:
1) Malware trends 2017, G DATA Software
2) Symantec Internet Security Threat Report, April 2017
3) WannaCry Update, Rapid7 Blog, May 2017
Credential Theft Using Malware (DataSafe)

**PROBLEM**
Malware

**SOLUTION**
App-layer encryption

---

**Form Data**
username: bobsmith
_password: 084bd66fd2011800f864091ce1f352a3bb449d3bf0ae139dfb1be08997b87ebb54cc
b09078646101bd40842d83983d99cb554c3fd538188840a1a57ea16736391c46a00cbfcde83071
4cb6652893b5c449fcd69a55c83dbee2a0c0db832141ed0fc04bea70aa97ee1b7377ff004ba
submit: 33
submit: 27
submit: Submit
CLIENT

- Cross-site request forgery
- Cross-site scripting
- Man-in-the-browser
- Session hijacking
- Malware

DNS

- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Dictionary attacks
- DDoS

NETWORK

- Eavesdropping
- Protocol abuse
- Man-in-the-middle

APP SERVICES

- API attacks
- Injection
- Malware
- Cross-site scripting
- DDoS

ACCESS

- Credential theft
- Credential stuffing
- Session hijacking
- Brute force
- Phishing

TLS

- Key disclosure
- Protocol abuse
- Session hijacking
- Certificate spoofing

© 2018 F5 Networks
How Credential Stuffing Works

- Healthcare Data
- Credit Card Data
- Financial Data
- Passport Data
- Intellectual Property
Zabezpečený, zjednodušený přístup k Vašim aplikacím nehledě na to, kde jsou provozovány

**Challenges**

- Complex and varied app access
- Protect assets from fraudulent access
- Password fatigue
- Concerns with user credentials in the cloud

**Multi-Cloud Benefits**

- Prevent data exfiltration from unauthorized users of cloud apps
- Simplify app access and password fatigue for end users regardless of location
- Reduce time-consuming and error-prone access policy management across clouds/SaaS
“IoT Devices are the Latest Minions in Cyber Weaponry Toolkits”

“Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps Attack on OVH”

“IoT Threats: A First Step into a Much Larger World of Mayhem”

Search by topic, type, tag, and author.

Visit Us at F5Labs.com