# WAF'sup
# How to properly use a WAF to mitigate layer 7 attacks.

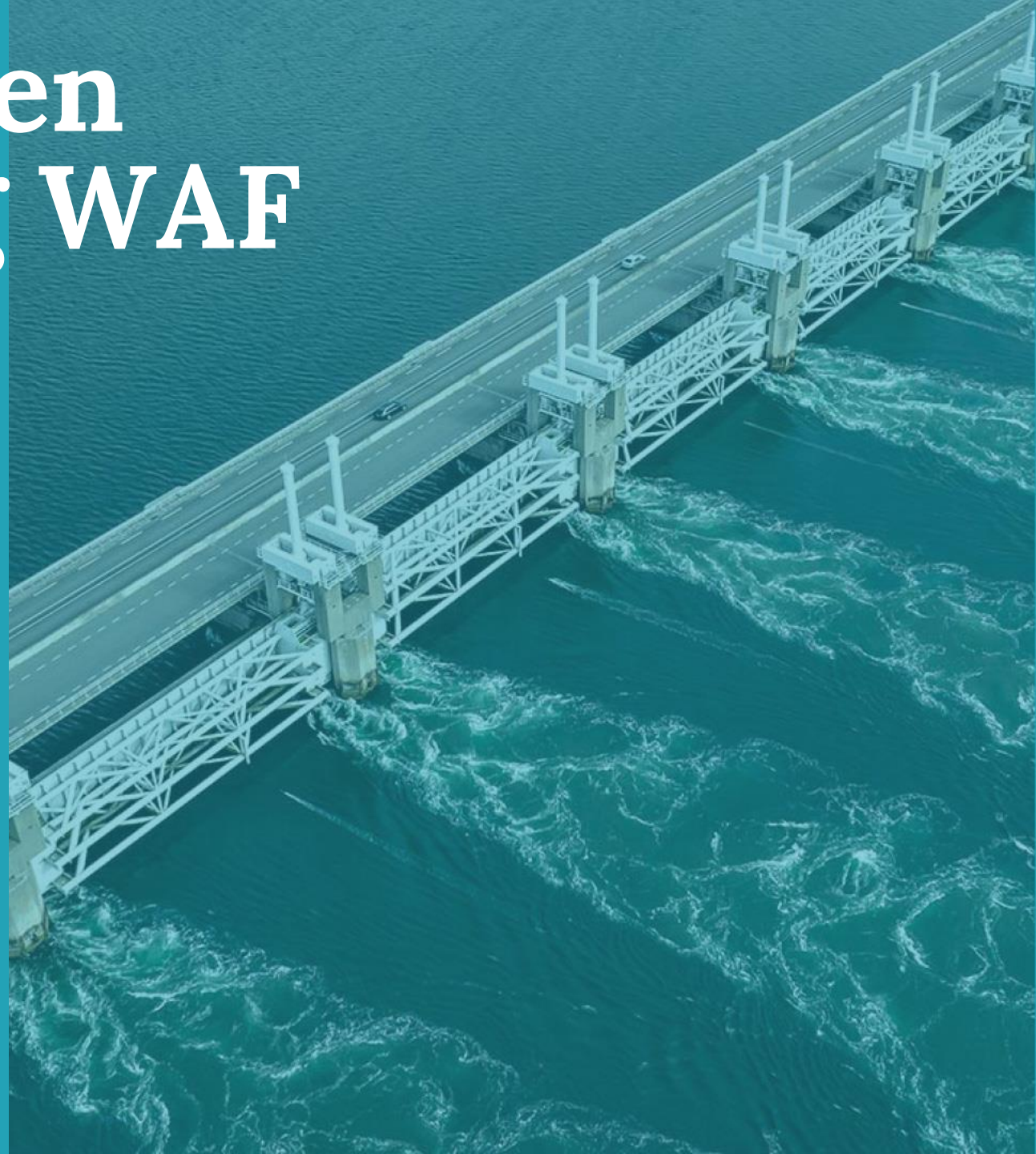
Johan Lamprecht

Security Engineer - NaWas

**NBIP** • 05 December 2025

# Strategies when implementing WAF

1. Static Rule examples
2. Bot Protections
3. Observability
4. Analysis approaches



# Why do WAFs fail during L7 Attacks

1. Over focus on OWASP CVE-style signatures
2. Lack of visibility lead to bad decisions
3. Analysis paralysis identifying the needle in a haystack of attack requests

# Static Rule examples

## Block unexpected signatures

**path normalization**

/access/../phpmyadmin → /phpmyadmin

/./phpmyadmin → /phpmyadmin

//phpmyadmin → /phpMyAdmin

Patterns to be blocked: ".." "./" "//"

# Static Rule examples

## Block unexpected signatures

**Unexpected source networks**

Regions from which you expect no legitimate traffic like out-of-scope geographies)

Cloud Providers or Datacenters

# Static Rule examples

## Block unexpected signatures

**Proxied requests**

Requests containing headers such as:

"X-Forwarded-For" "True-Client-IP" "X-Real-IP" "CF-Connecting-IP" "Via"

# Static Rule examples

## IP Reputation block lists

**Example lists**

Spamhaus: Botnet Controller List (BCL)

and Do Not Route or Peer (DROP)

FireHol: level1

CrowdSec Security Engine

# Static Rule examples

## Rate limiting rules

Strictly limit single sources emitting known signatures

limit single IPs exceeding 20 requests/min towards “/”

# Static Rule examples

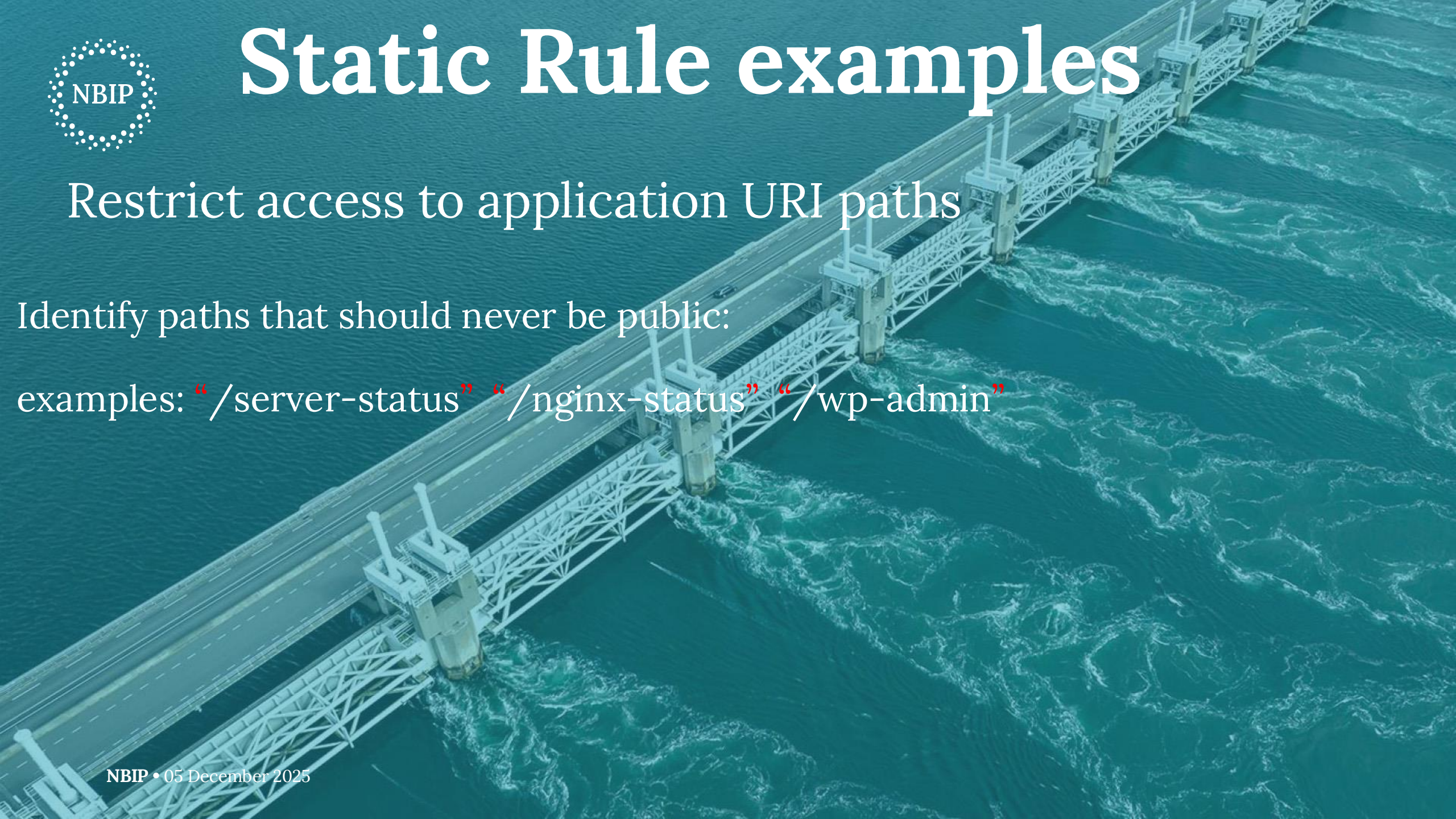
## Rate limiting rules

Tier of global rate limits

limit any source IP exceeding 20 requests/min - in COUNT mode

limit any source IP exceeding 200 requests/min - in COUNT mode

limit any source IP exceeding 2000 requests/min - in BLOCK

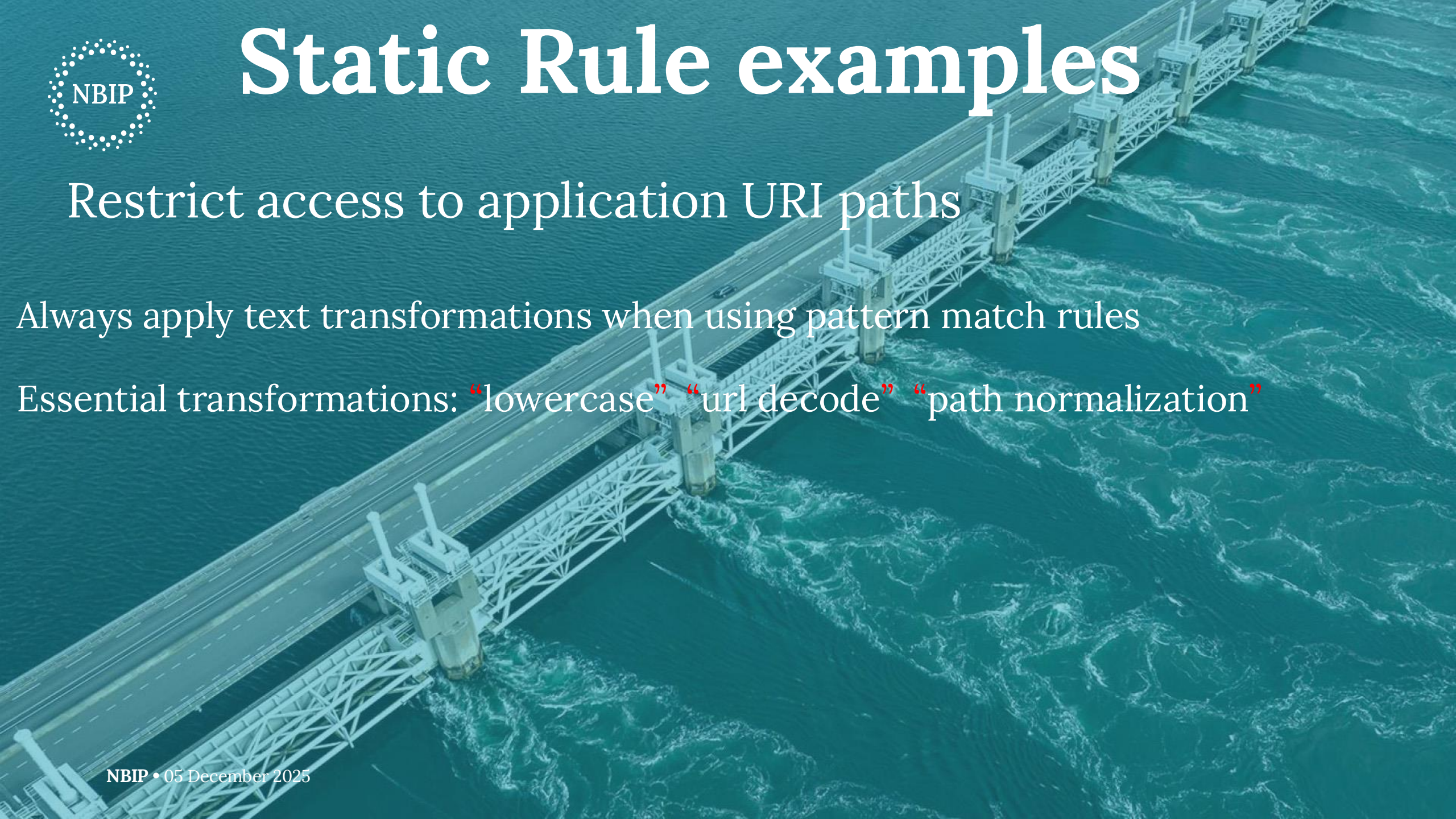


# Static Rule examples

## Restrict access to application URI paths

Identify paths that should never be public:

examples: “/server-status” “/nginx-status” “/wp-admin”



# Static Rule examples

## Restrict access to application URI paths

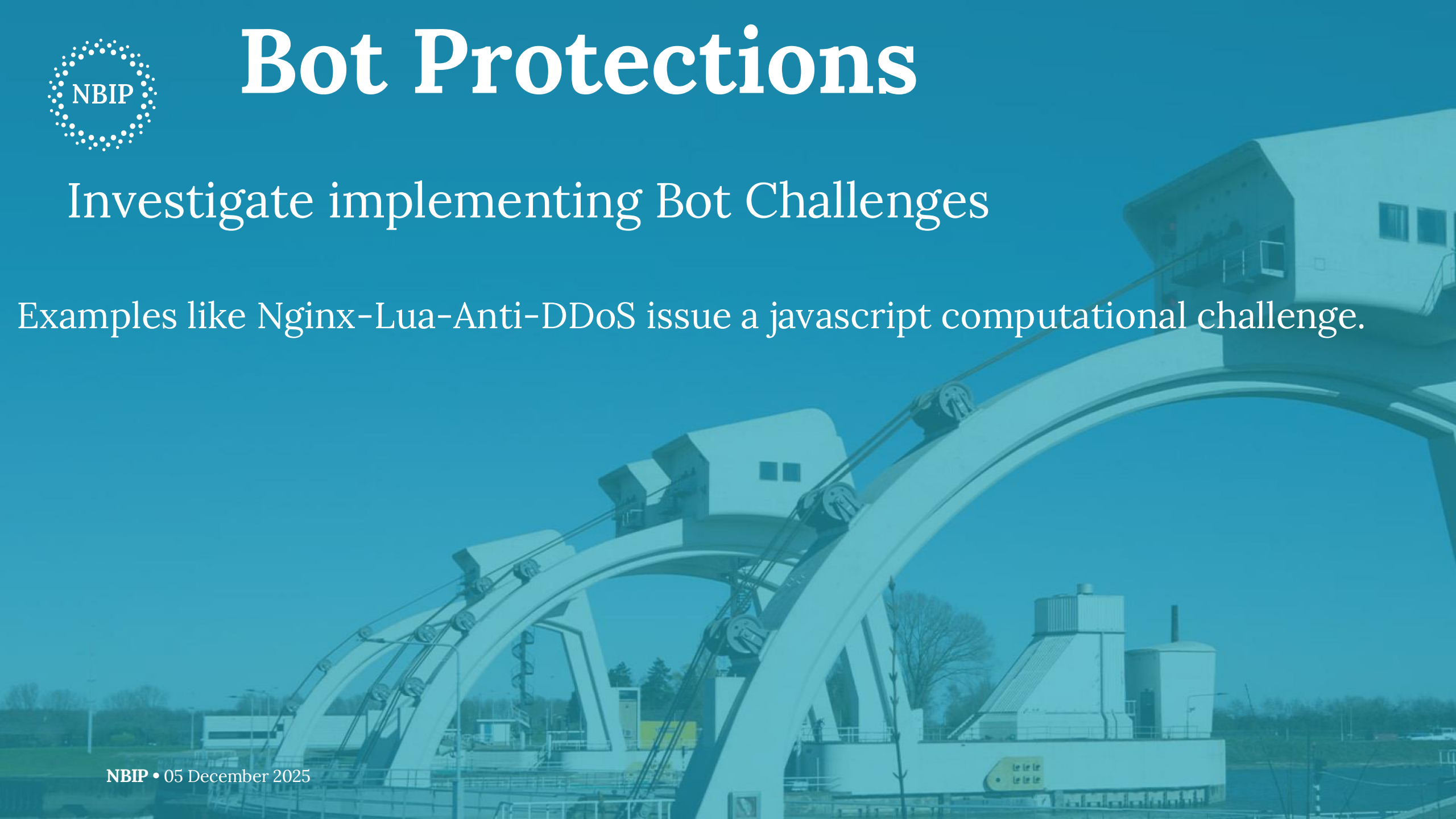
Always apply text transformations when using pattern match rules

Essential transformations: “lowercase” “url decode” “path normalization”

# Bot Protections

## Investigate implementing Bot Challenges

Examples like Nginx-Lua-Anti-DDoS issue a javascript computational challenge.



# Observability

## Essential metrics

Total requests/min

Blocked/Allowed/Counted requests/min

Requests by Rule/min

4xx and 5xx response codes/min

# Observability

## Alarms

Configure alarms for unexpected threshold breaches with notifications that actively engage support operators to investigate impact.

# Observability

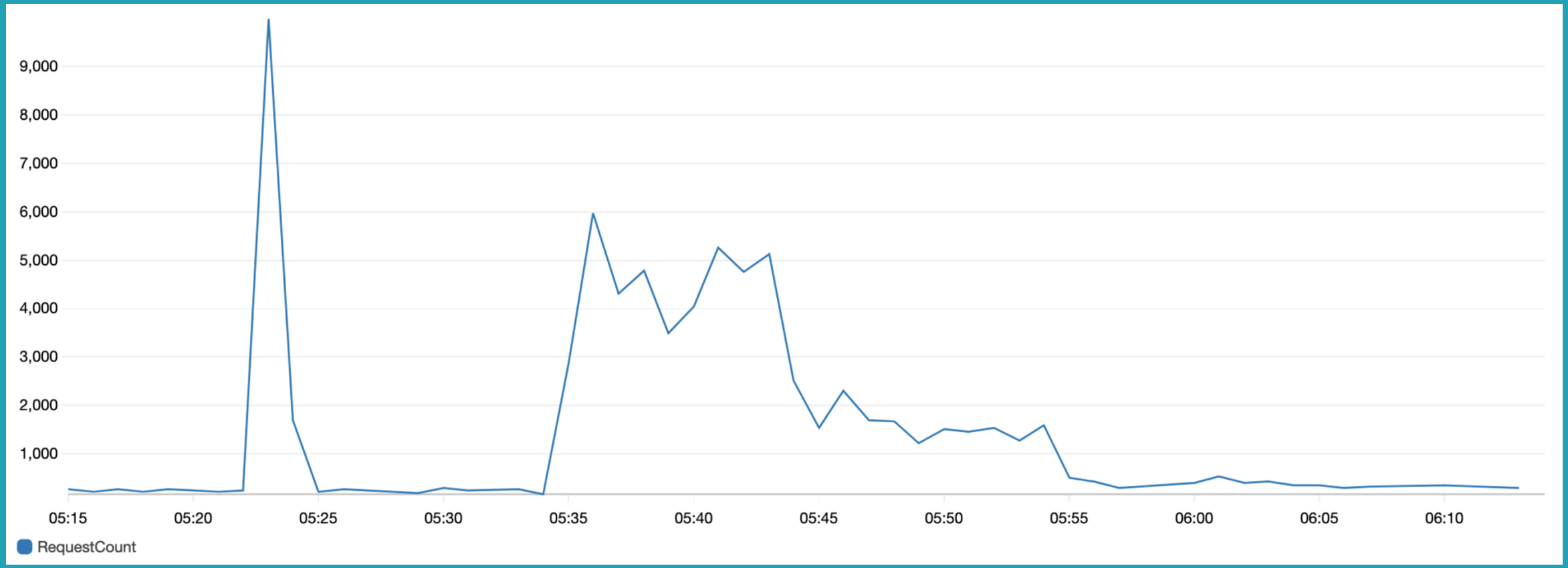
## Logs

Logging full request parameters and additional metadata is invaluable during attack investigations.

Parameters to log: source IP (source ASN), URI path, query string, Method, all headers, header order, JA3/JA4/client hello TLS fingerprint

# Analysis Approaches

## Identify event start and a good baseline comparison



# Analysis Approaches

## Query for top talker parameters across both timeframes

| uri | baseline_count | event_count |
|---|---|---|
| / | 30900 | 6348397 |
| /versions.json | 64319 | 63998 |
| /service-worker.js | 29437 | 29202 |
| /webmanifest.json | 16061 | 15799 |
| /pwa-round-icon-192x192.png | 14966 | 14814 |
| /oembed | 13625 | 14056 |
| /offline.html | 9965 | 9762 |
| /discover | 5752 | 5981 |
| /stream | 5893 | 5828 |

# Analysis Approaches

## Query for top talker parameters across both timeframes

| header_user_agent | baseline_count | event_count |
|---|---|---|
| L43s9ejCDYRk | 0 | 787762 |
| w6iz7Rl68jex | 0 | 767266 |
| v6O27jVekWTa | 0 | 754957 |
| D9PpQTkhyFHg | 0 | 744824 |
| OGPRT2KUO5Oo | 0 | 719036 |
| roWWjEYZF7uR | 0 | 699417 |
| umwUzdoEMaOq | 0 | 493739 |
| eMgTlyMgfaqr | 0 | 269206 |
| bp4WIOkcjJpv | 0 | 259707 |
| 6nnM3BsA3SC1 | 0 | 248239 |
| Opera/9.80 (Windows NT 6.1 x64; U; en) Presto/2.7.62 Version/11.00 | 0 | 74500 |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0) Gecko/20100101 Firefox/24.0 | 0 | 73540 |
| Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/53 | 0 | 72643 |
| Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; FunWebProducts) | 0 | 72606 |
| Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:16.0.1) Gecko/20121011 Firefox/21.0.1 | 0 | 70509 |
| Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; ko-kr) AppleWebKit/533.20.25 (KHTML, like Gecko) V | 0 | 65197 |
| Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 | 0 | 60555 |
| Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0. | 58700 | 58231 |
| Mozilla/5.0 (compatible; MSIE 10.6; Windows NT 6.1; Trident/5.0; InfoPath.2; SLCC1; .NET CLR 3.0.4506 | 0 | 56497 |
| Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) C | 28674 | 33879 |

# Analysis Approaches

## Query for top talker parameters across both timeframes

| header_accept | baseline_count | event_count |
|---|---|---|
| text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8,text/plain;q=0.8 | 0 | 1499781 |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 | 6023 | 1277542 |
| text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,en;q=0.7 | 0 | 787762 |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8,application/ld+json;q=0.9 | 0 | 767266 |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 | 149 | 742147 |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8,application/xml-dtd;q=0.9 | 0 | 719036 |
| text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 | 48743 | 302554 |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 | 1636 | 270939 |
| */* | 135460 | 137696 |
| application/json, text/javascript, */*; q=0.01 | 66112 | 65418 |
| text/html,application/xhtml+xml,application/signed-exchange;v=b3,application/xml;q=0.9,*/*;q=0.8 | 32422 | 37872 |

# Analysis Approaches

## Query for top talker parameters across both timeframes

| header_accept_language | baseline_count | event_count |
|---|---|---|
| en-US,en;q=0.9 | 69202 | 1396375 |
| zh-CN | 0 | 959124 |
| da, en-gb;q=0.8, en;q=0.7 | 0 | 787762 |
| utf-8, iso-8859-1;q=0.5, *;q=0.1 | 0 | 767266 |
| en-ZA | 0 | 744824 |
| fr-CH, fr;q=0.9, en;q=0.8, de;q=0.7, *;q=0.5 | 0 | 719036 |
| he-IL,he;q=0.9,en-US;q=0.8,en;q=0.7 | 269 | 517700 |
| zh-TW | 0 | 493747 |
| __MISSING__ | 159383 | 151983 |
| en-US,en;q=0.5 | 27845 | 28211 |
| en-US | 18007 | 19477 |
| en-GB,en-US;q=0.9,en;q=0.8 | 7678 | 7393 |

# Analysis Approaches

Query for top talker parameters across both timeframes

Identify clear signatures to mitigate attack

# Analysis Approaches

Query by identified signatures to reveal offending source IPs

Implement additional IP based mitigation


# Analysis Approaches

## Behavioural traffic observations of source IPs

| extensions | extension_count | uri | method | uri_count |
|---|---|---|---|---|
| .json | 80512 | / | GET | 6340490 |
| .js | 29220 | /versions.json | GET | 63998 |
| .png | 17771 | /service-worker.js | GET | 29202 |
| .html | 9799 | /webmanifest.json | GET | 15799 |
| .ico | 2214 | /pwa-round-icon-192x192.png | GET | 14814 |
| .xml | 1533 | /oembed | GET | 13818 |
| .txt | 446 | /offline.html | GET | 9762 |
| .php | 97 | / | HEAD | 7908 |

## Block IPs with unexpected ratios

# Key Takeaways

DDoS flood protection is possible with basic rules

Observability enables sound decision making

Analysis is the engine for developing high confidence mitigations


# WAF's Up!

Now attackers must work harder to evade your mitigations

# NBIP WAF POC

# Thank you

# Q & A