Maliciously monetizing AppSec “Features”

It’s all about the $money

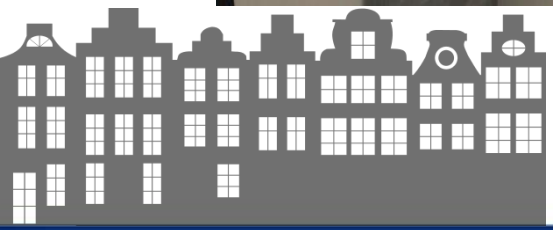
Or Katz – Principal Security Researcher Akamai

Ezra Caltum – Senior Security Researcher Akamai

OWASP AppSecEU 15

Amsterdam, The Netherlands

And Then the Red Phone Started Ringing…



OWASP AppSecEU 15
Amsterdam, The Netherlands

Looking Into the Data

Single HTTP Request

Open Redirect

What does it mean?

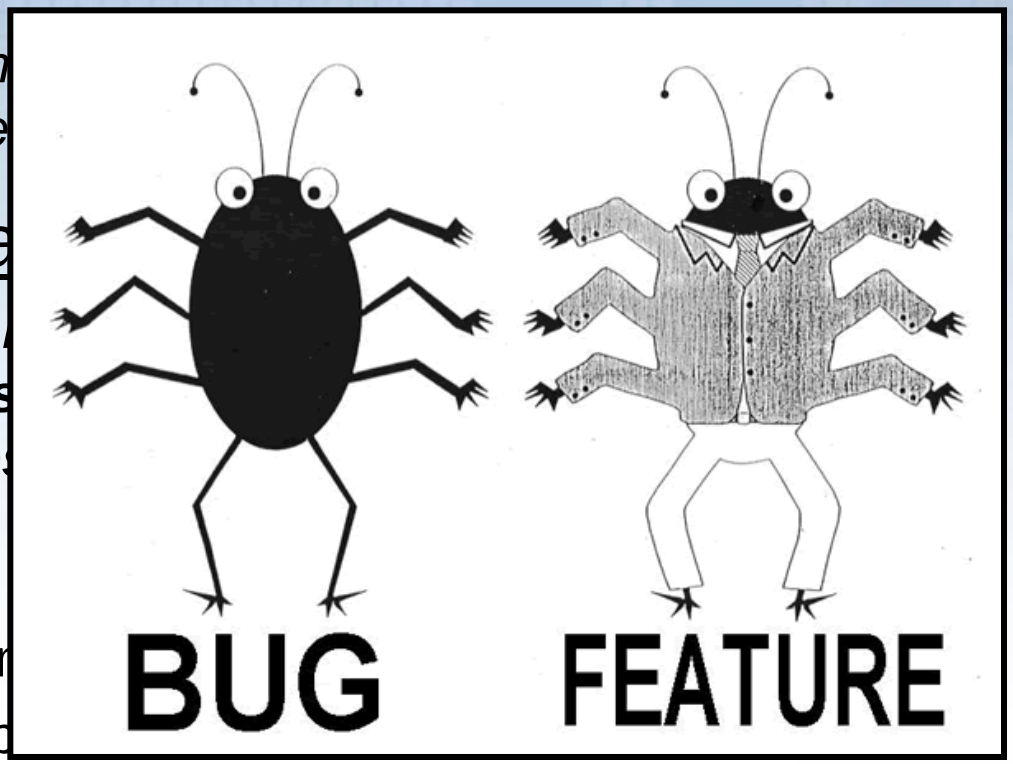
cwe.mitre.org: "A web application specifies a link to an external site

How it is being used ma

*OWASP Top 10: "Such redirects trick victims into **disclosing pass** Unsafe forwards may allow **acce***

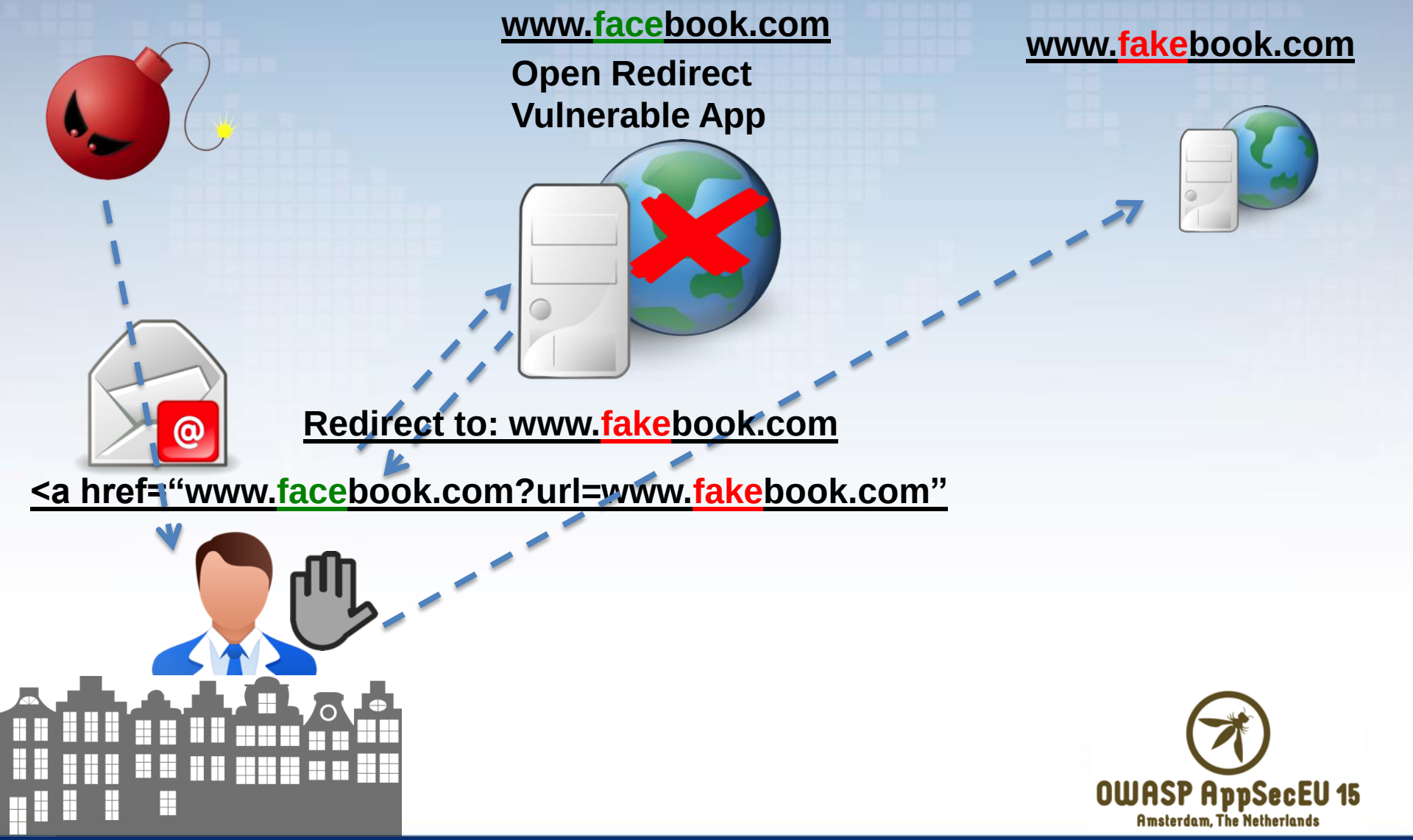
Severity/Impact?

- OWASP Top 10: A10, Impact r
- cwe.mitre.org likelihood of exp

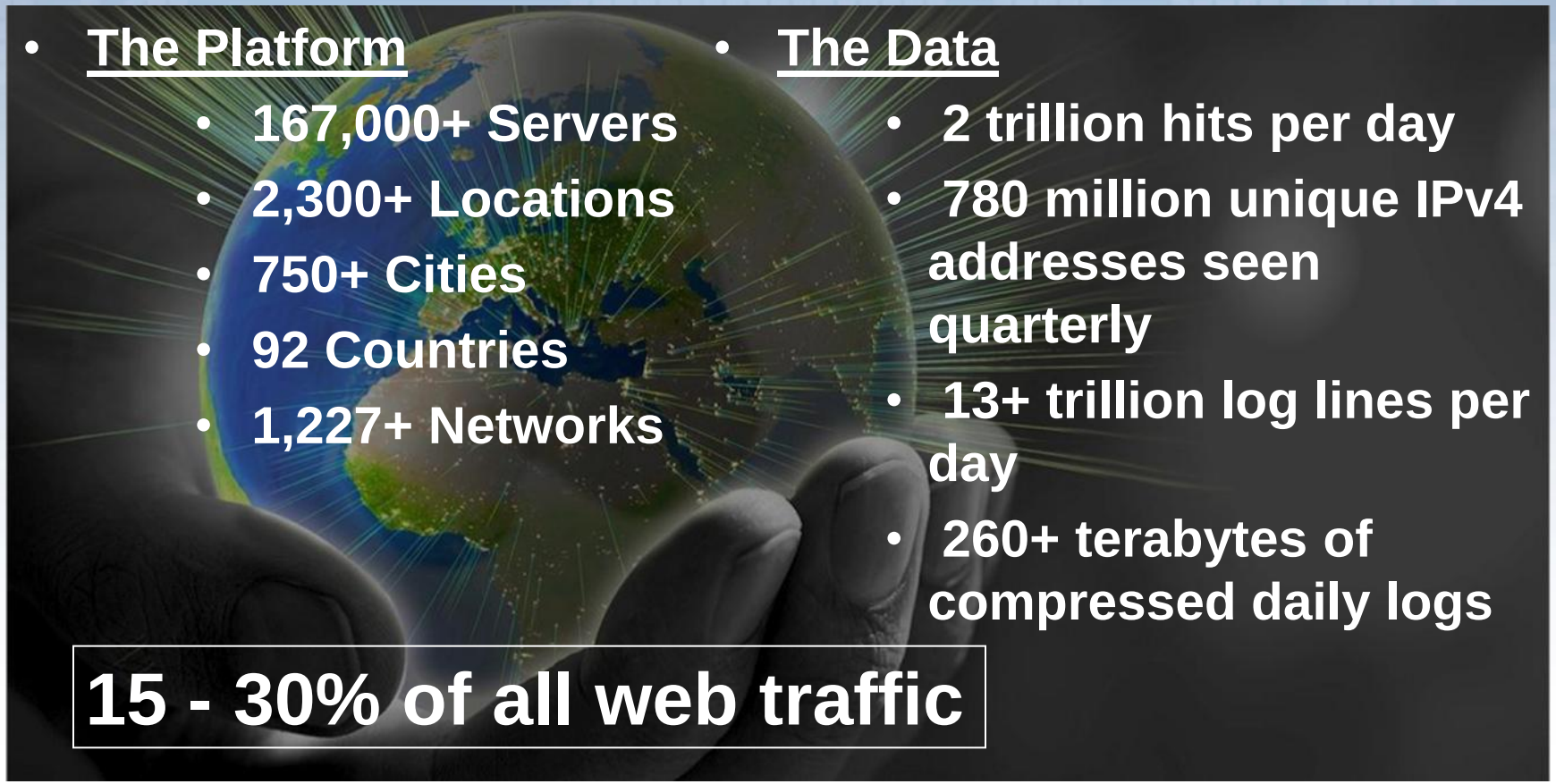


OWASP AppSecEU 15
Amsterdam, The Netherlands

Phishing with Open Redirect



The Akamai Intelligent Platform



- **The Platform**
  - 167,000+ Servers
  - 2,300+ Locations
  - 750+ Cities
  - 92 Countries
  - 1,227+ Networks
- **The Data**
  - 2 trillion hits per day
  - 780 million unique IPv4 addresses seen quarterly
  - 13+ trillion log lines per day
  - 260+ terabytes of compressed daily logs

15 - 30% of all web traffic

Step #1 - Attacker's Activity

Same attacker to vulnerable page

Redirection to **1732** different domains

OWASP AppSecEU 15
Amsterdam, The Netherlands

Step #2 – Attack Activity

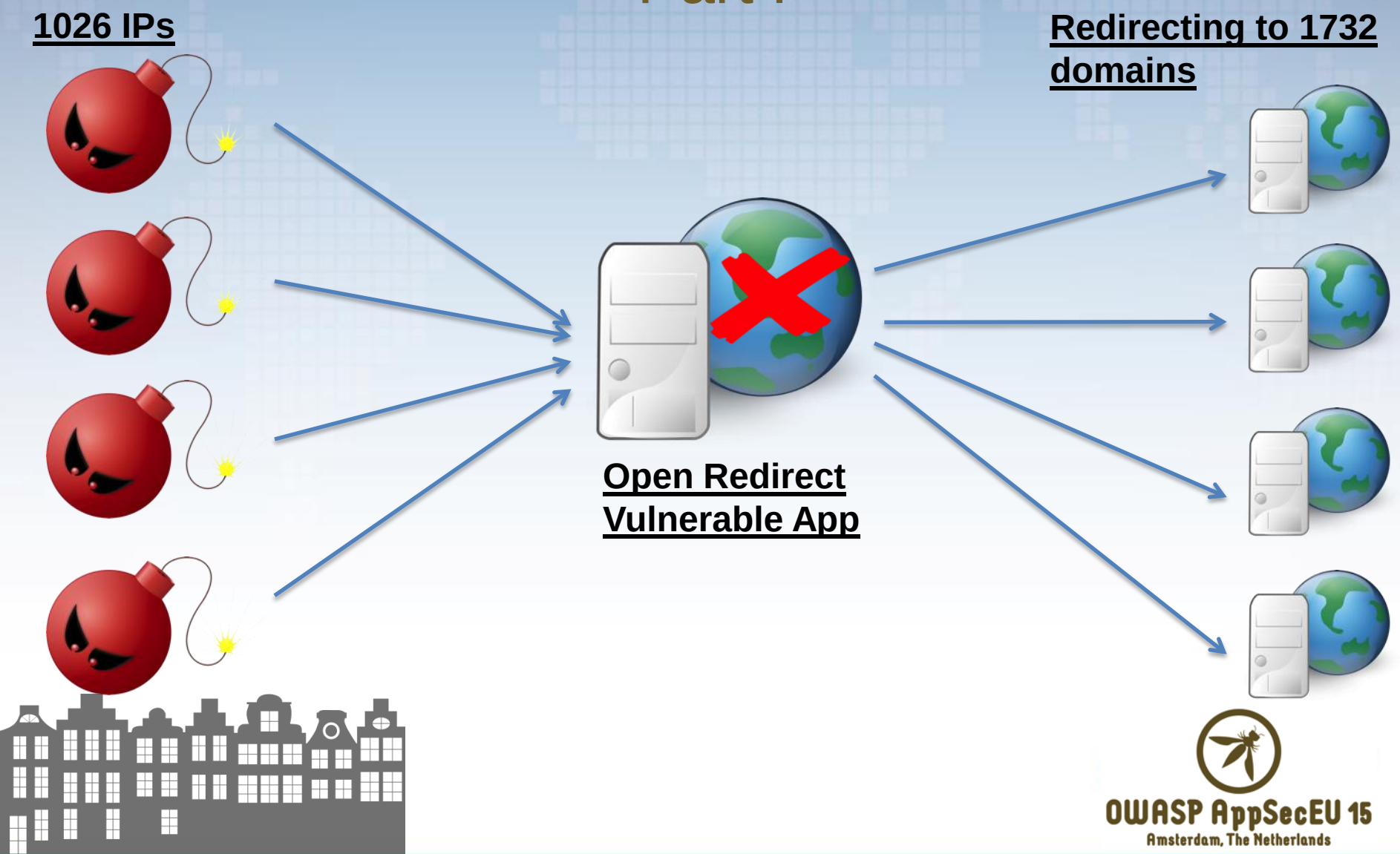
Excessive Access to vulnerable page

Originated from **1026** IP Addresses

OWASP AppSecEU 15
Amsterdam, The Netherlands

What Have We Seen So Far

Part I



Step #3 – Attackers' Activity

Same attackers web applications

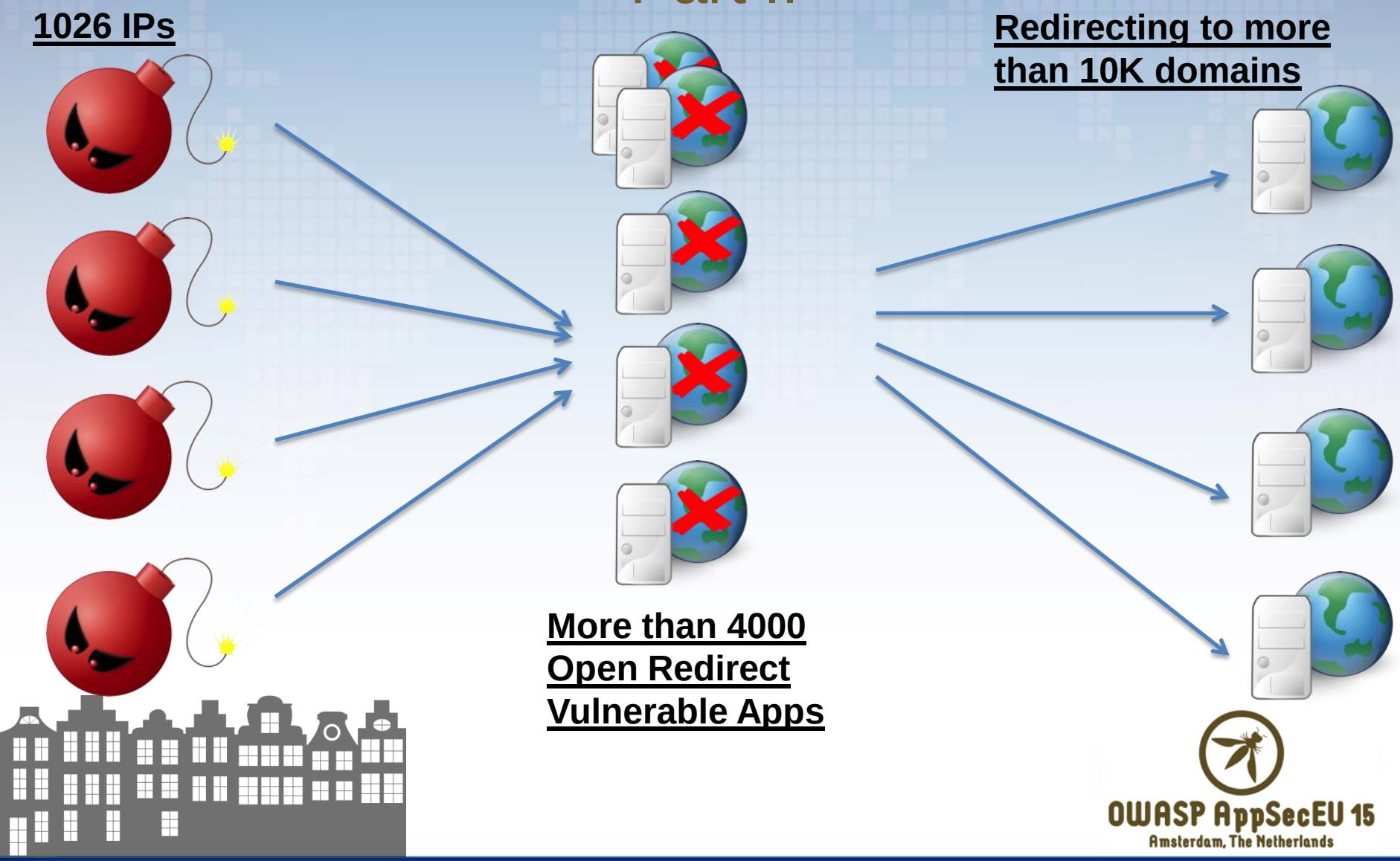
other

Abusing more than **4000** vulnerable applications

Redirecting to more than **10K** different domains

What Have We Seen So Far

Part II



Step #4 – Attackers' Common Denominator

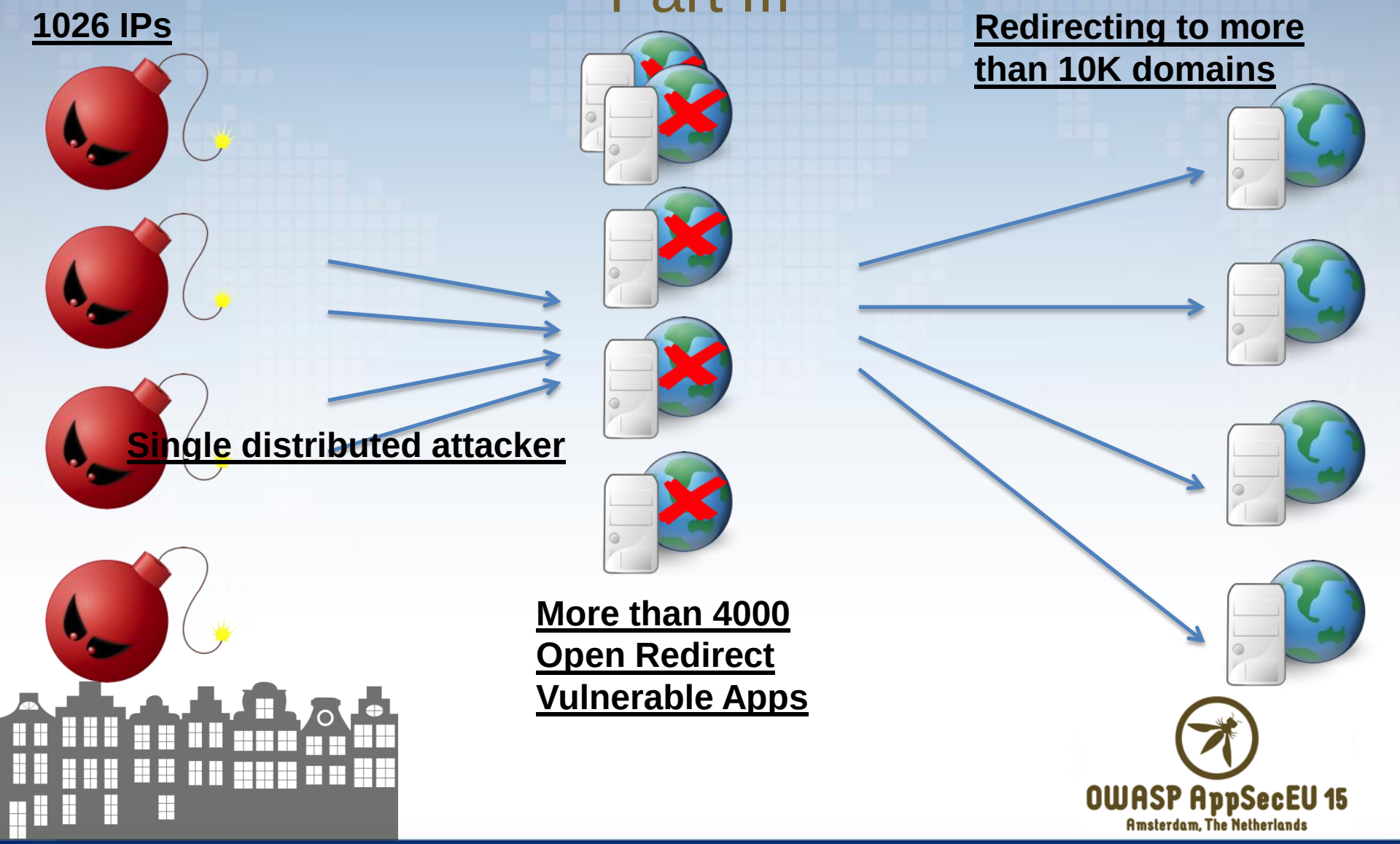
Same User-Agent header value

Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.16

1026 IP Addresses → Controlled by same attacker

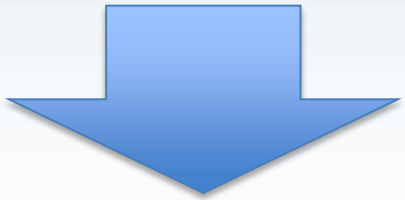
What Have We Seen So Far

Part III



Step #5 – Security Data Intelligence

- 10K domains – legitimate applications
- 1K IP address - ~40% are proxies
- 4K vulnerable apps – among them Fortune1000 companies



Part of Search Engine Optimization (SEO) attack

SEO Campaign – The Bigger Picture

www.HighRanked.com

www.LowRanked.com

Redirect to: www.LowRanked.com

OWASP AppSecEU 15
Amsterdam, The Netherlands

What We Get Out of This Story?

- Open redirect is being maliciously used beyond phishing and malware infection
- Cloud based threat intelligence is critical tool for detecting emerging threats
- Attacks scale when $money driven objectives are involved
- We need to:
  - know “How to” detect & defend against such attacks
  - look beyond OWASP Top 10

How To: Analytics

The logs will look like this:

- ::1 - - [10/May/2015:15:06:00 +0300] "GET /redirect.php?link=http://www.google.com HTTP/1.1" 200 412
- ::1 - - [10/May/2015:15:06:00 +0300] "GET /redirect.php?link=http://www.google.com HTTP/1.1" 200 412
- ::1 - - [10/May/2015:15:00:23 +0300] "GET /redirect.php?link=http://www.ShadyDomain.net/act/info.php?a%5B%5D=%3Ca+href%3Dhttp%3A%2F%2Flowscore.com%%3C%2Fa%3E HTTP/1.1" 200 461
- ::1 - - [10/May/2015:15:06:00 +0300] "GET /redirect.php?link=http://www.google.com HTTP/1.1" 200 412
- ::1 - - [10/May/2015:15:00:38 +0300] "GET /redirect.php?link=http://www.StrangeDomain.com
- /?a%5B%5D=%3Ca+href%3Dhttp%3A%2F%2Flowscore.com%2F HTTP/1.1" 200 399
- ::1 - - [10/May/2015:15:06:00 +0300] "GET /redirect.php?link=http://www.google.com HTTP/1.1" 200 412

How To: Read The Traces

Template based signature - Identify external URL parameters in your application.

Egrep ‘(..{0,10})\?=https?://[^s]/[a-zA-Z0-9.]+’ access.log

How To: Read the traces

Parameter Name	Number of unique domains
link=	8000
url=	2000
A=	0
Amount=	0
Help=	0

How To: Read The Traces

Order by accessed domains(Sort | uniq –c) - Identify your usual links, domains related to your industry and common websites.

How to: Read the traces

Domain	Counter
http://www.yourdomain.com	10000
http://www.google.com	800
http://www.strangedomain1.com	10
http://www.strangedomain2.com	5

How To: Read The Traces

Common Indicator (signature based)- A Indicator of Compromise (IoC) is the word “info.php?a[]”, due to a known SEO technique abusing it.

Grep ‘info.php?a%5b%5d’

How To: Analytics

The logs will look like this:

::1 - - [10/May/2015:15:00:23 +0300] "GET /redirect.php?link=http://www.strangedomain.com/act/

info.php?a%5B%5D

=%3Ca+href%3Dhttp%3A%2F%2Flowscore.com%2F HTTP/1.1" 200 461

How to: Read the Traces

- **Template based signature**
- **Order by accessed domains**
- **Common Indicator (signature based)**

How to: Execute Defensive Coding

- Quoting OWASP:
  - "Force[illegible]redirects to first go [illegible]ugh a page notifying use[illegible] going off of your site, a[illegible]ve them click a [illegible] confirm."
- Use a whitelist approach of valid redirect domains.
- As this is an SEO technique, disable open the access to redirect pages for robots.

OWASP AppSecEU 15
Amsterdam, The Netherlands

How to: Execute Defensive Coding

- Save a list of redirected domains, monitor accordingly and create a blacklist approach.
- Ensure that there are no XSS, nor HTML injections in your website.

Beyond OWASP Top 10

Few Examples:

1. Web Scraping
2. Shady Redirection/Fake products
3. DDOS Ransom

1- Web Scraping

WikiPedia: "*Web scraping (web harvesting or web data extraction) is a computer software technique of extracting information from websites.*"

In Other words, someone is harvesting application's **feature** for **financial** reasons.

Web Scraping

Web Scraper

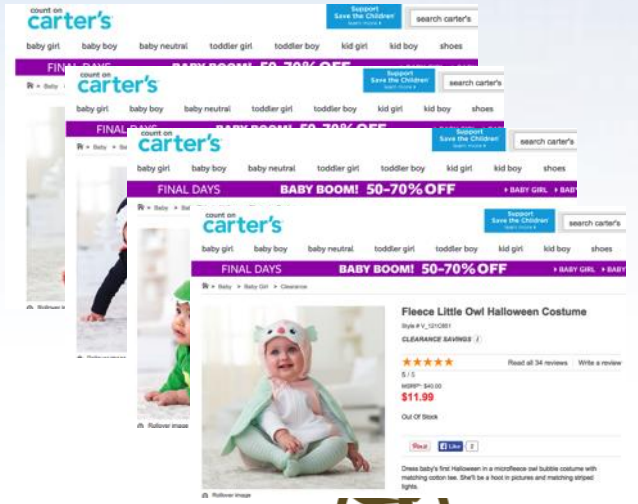
Targeted Application

GET /Catalog.php?pageId=1111

GET /Catalog.php?pageId=1112

GET /Catalog.php?pageId=1113

GET /Catalog.php?pageId=1114

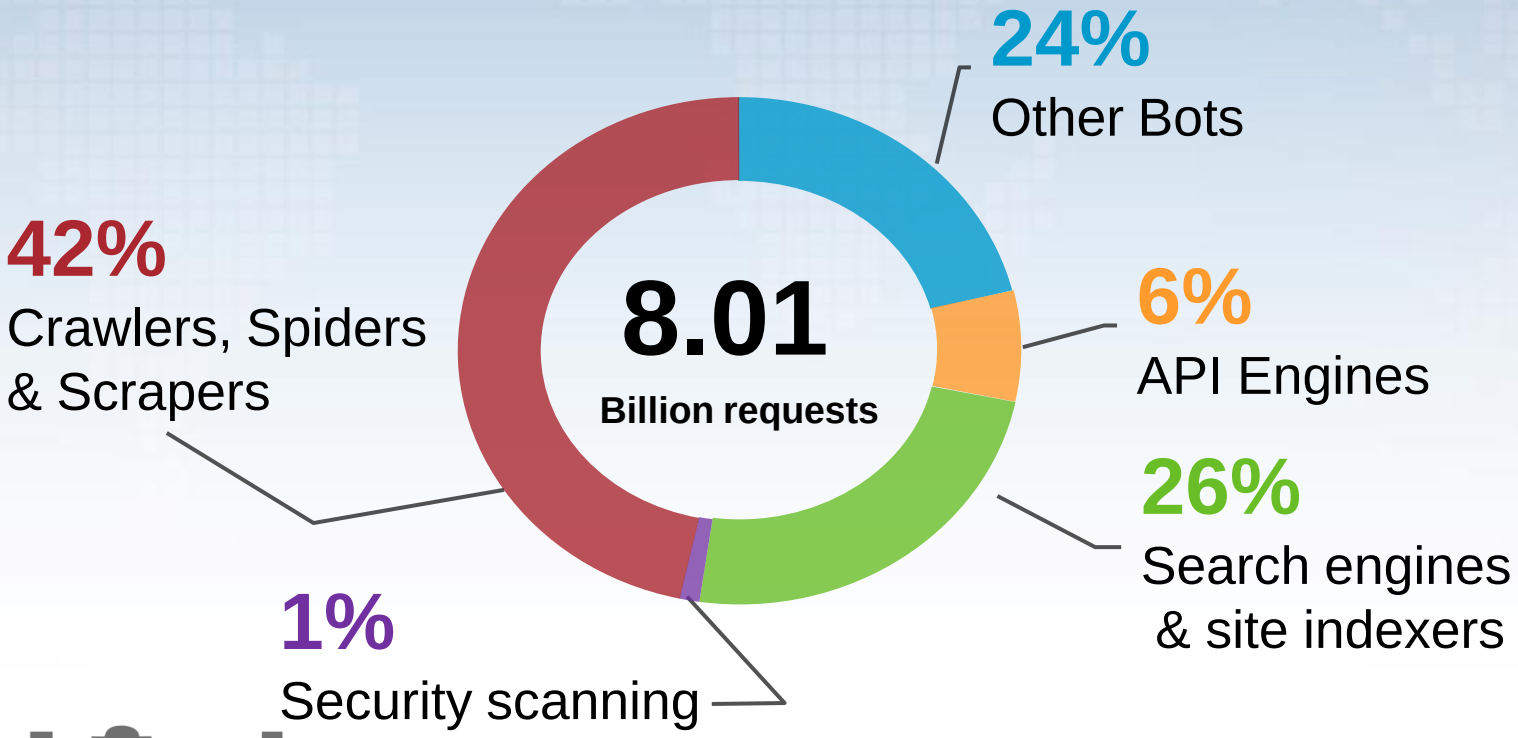


OWASP AppSecEU 15
Amsterdam, The Netherlands

Web Scraping In The Wild

Analyzing 24 hours of data, 85,475,034,620 requests

Out of it 9.4% are Bots → 8.01 Billion



OWASP AppSecEU 15
Amsterdam, The Netherlands

How Web Scraping Attack Scale

- Attackers are using headless browser to evade detection (scapy, PhantomJS)
- Using Proxies and Botnet to obfuscate Identity and to load-balance traffic
- Utilize attacks by scraping industry segments

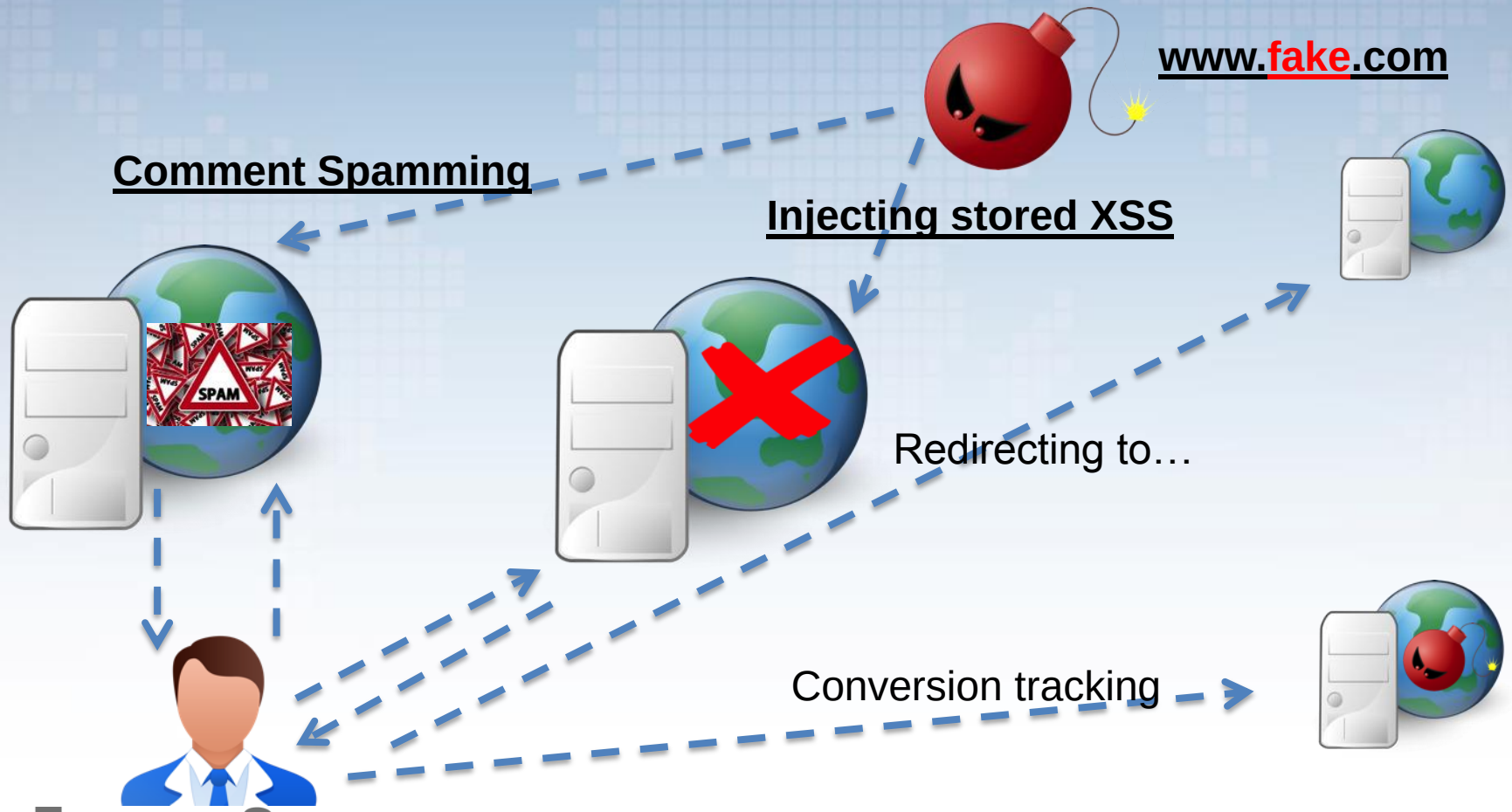
2- Shady Redirection

A phishing attack in which attacker will be redirected to a fake products shop.

What is so special?

- Attack vector that combines several attack techniques such as: stored XSS, comment spamming
- “Conversion” tracking

Phishing with Open Redirect



3- DDOS Ransom

"I have a DDoS army ready to attack. Pay $300 in 24 hours or I will crash your website again. Good day!"

Not paying

You will be DDOS'ed

Paying

become a victim for life (paying protection $money)

OWASP AppSecEU 15
Amsterdam, The Netherlands

Summary

- Yep, It is all about the $money
- When attackers objective is money driven attack scale
- Known attacking techniques are being used for new attacking vectors
- Known attacking techniques are being re-branded and monetized
- Call for action – moving beyond OWASP Top 10

Q&A

Ezra Caltum - @*aCaltum*

Or Katz - @*or_katz*