FORTINET®

Web application and cloud security: Learning through mistakes

Timo Lohenoja, CISSP

Systems Engineer, Fortinet

timo@fortinet.com

First law of software quality

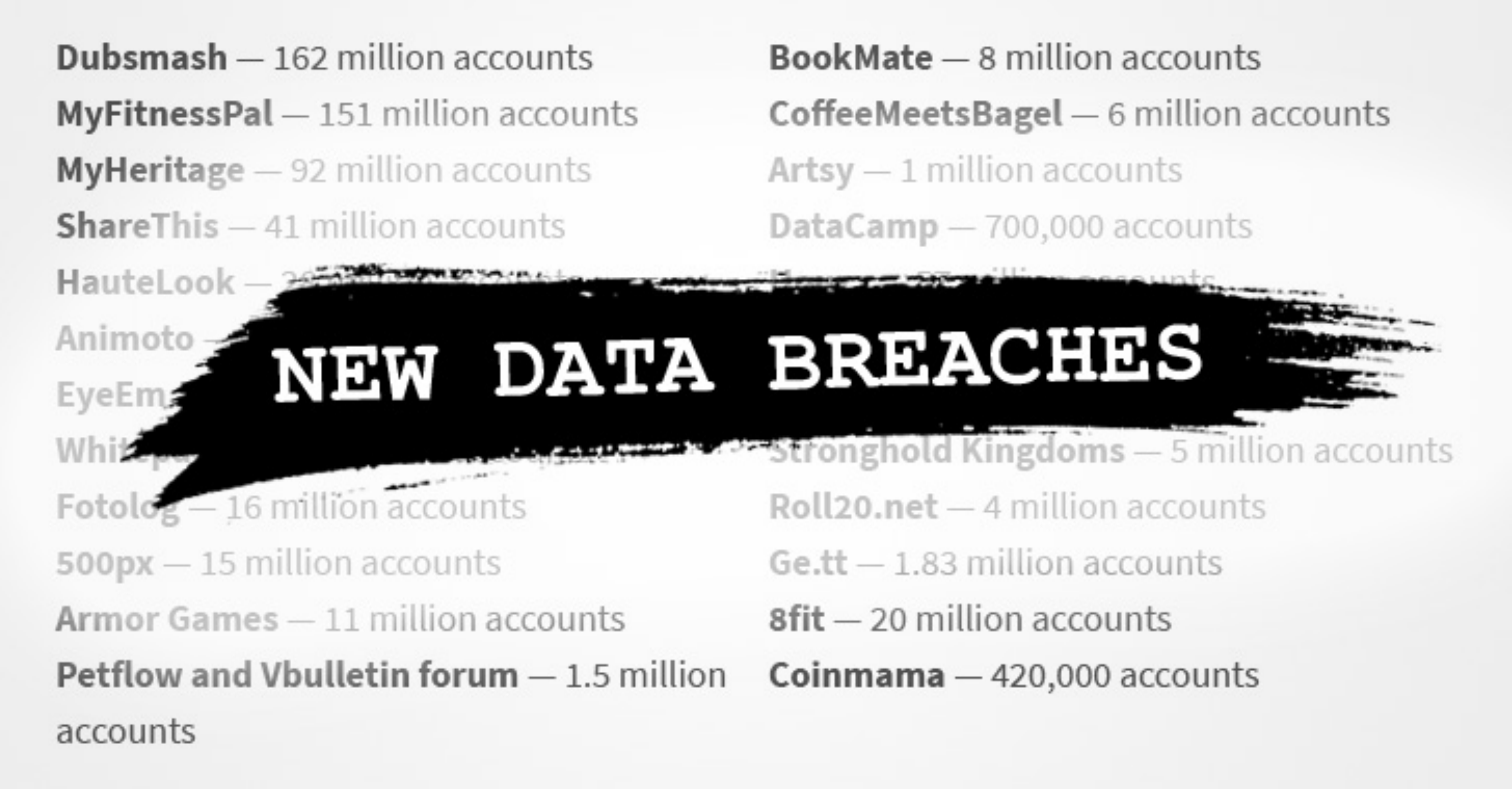
$$\text{errors} = (\text{more code})^2$$

$$E = mc^2$$

Moral: Some errors always come back

Hacker Breaches Dozens of Sites, Puts 127 Million New Records Up for Sale

February 15, 2019



NEW DATA BREACHES

Dubsmash — 162 million accounts

MyFitnessPal — 151 million accounts

MyHeritage — 92 million accounts

ShareThis — 41 million accounts

HauteLook —

Animoto —

EyeEm

Whi

Fotolog — 16 million accounts

500px — 15 million accounts

Armor Games — 11 million accounts

Petflow and Vbulletin forum — 1.5 million accounts

BookMate — 8 million accounts

CoffeeMeetsBagel — 6 million accounts

Artsy — 1 million accounts

DataCamp — 700,000 accounts

Stronghold Kingdoms — 5 million accounts

Roll20.net — 4 million accounts

Ge.tt — 1.83 million accounts

8fit — 20 million accounts

Coinmama — 420,000 accounts

Hacker Breaches Dozens of Sites, Puts 127 Million New Records Up for Sale

February 15, 2019 *(Previous Breach was 620 million accounts)*

Package 1- Databases From 16 Compromised Websites On Sale

- Dubsmash — 162 million accounts
- MyFitnessPal — 151 million accounts
- MyHeritage — 92 million accounts
- ShareThis — 41 million accounts
- HauteLook — 28 million accounts
- Animoto — 25 million accounts
- EyeEm — 22 million accounts
- 8fit — 20 million accounts
- Whitepages — 18 million accounts
- Fotolog — 16 million accounts
- 500px — 15 million accounts
- Armor Games — 11 million accounts
- BookMate — 8 million accounts
- CoffeeMeetsBagel — 6 million accounts
- Artsy — 1 million accounts
- DataCamp — 700,000 accounts

Package 2 - Hacked Databases From 8 More Websites On Sale

- Houzz — 57 million accounts
- YouNow — 40 million accounts
- Ixigo — 18 million accounts
- Stronghold Kingdoms — 5 million accounts
- Roll20.net — 4 million accounts
- Ge.tt — 1.83 million accounts
- Petflow and Vbulletin forum — 1.5 million accounts
- Coinmama (Cryptocurrency Exchange) — 420,000 accounts

Dream Market

Hacker Breaches Dozens of Sites, Puts 127 Million New Records Up for Sale

February 15, 2019

Confirmed leaks by targets (8/24):

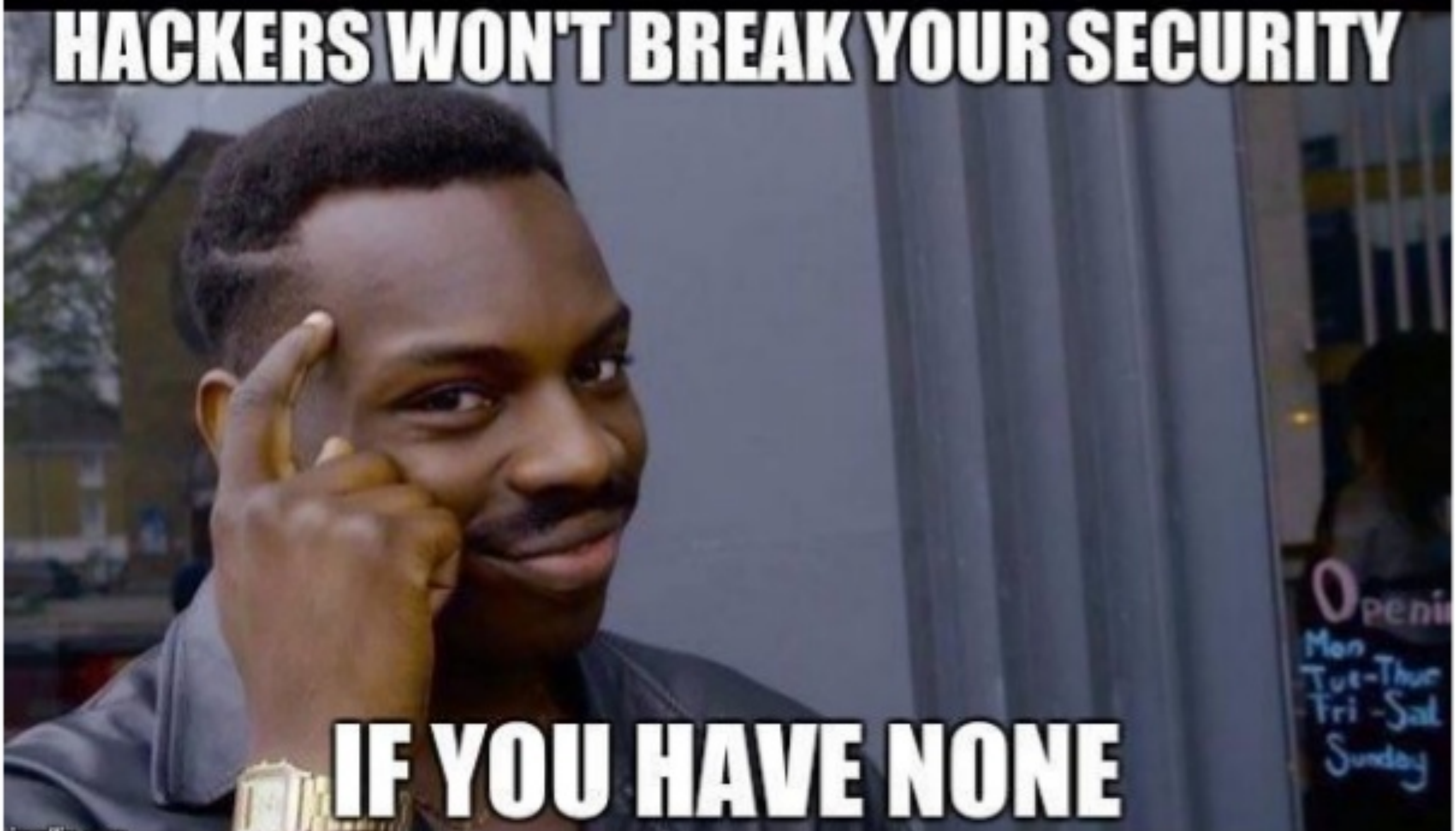
- Houzz
- 500px
- Artsy
- DataCamp
- CoffeeMeetsBagel
- MyFitnessPal
- MyHeritage
- Animoto

Total: 347,7 Million accounts

What was stolen:

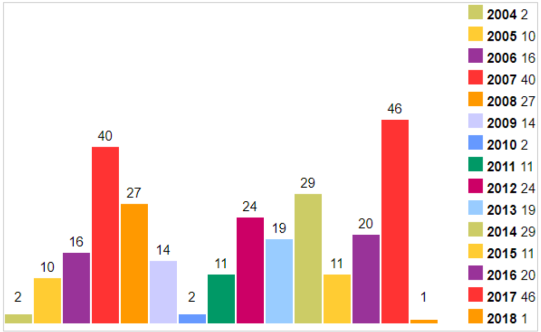
- Username
- Password
- Date of Birth
- Gender
- Home Addres
- Phone number
- Credit Card Numbers

Closed 30th of April 2019


HACKERS WON'T BREAK YOUR SECURITY
IF YOU HAVE NONE
Openi
Mon
Tue-Thur
Fri-Sat
Sunday

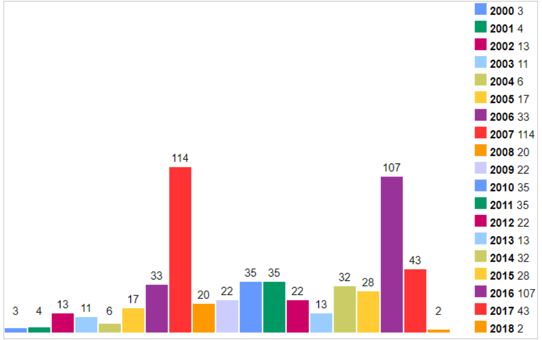
Wordpress

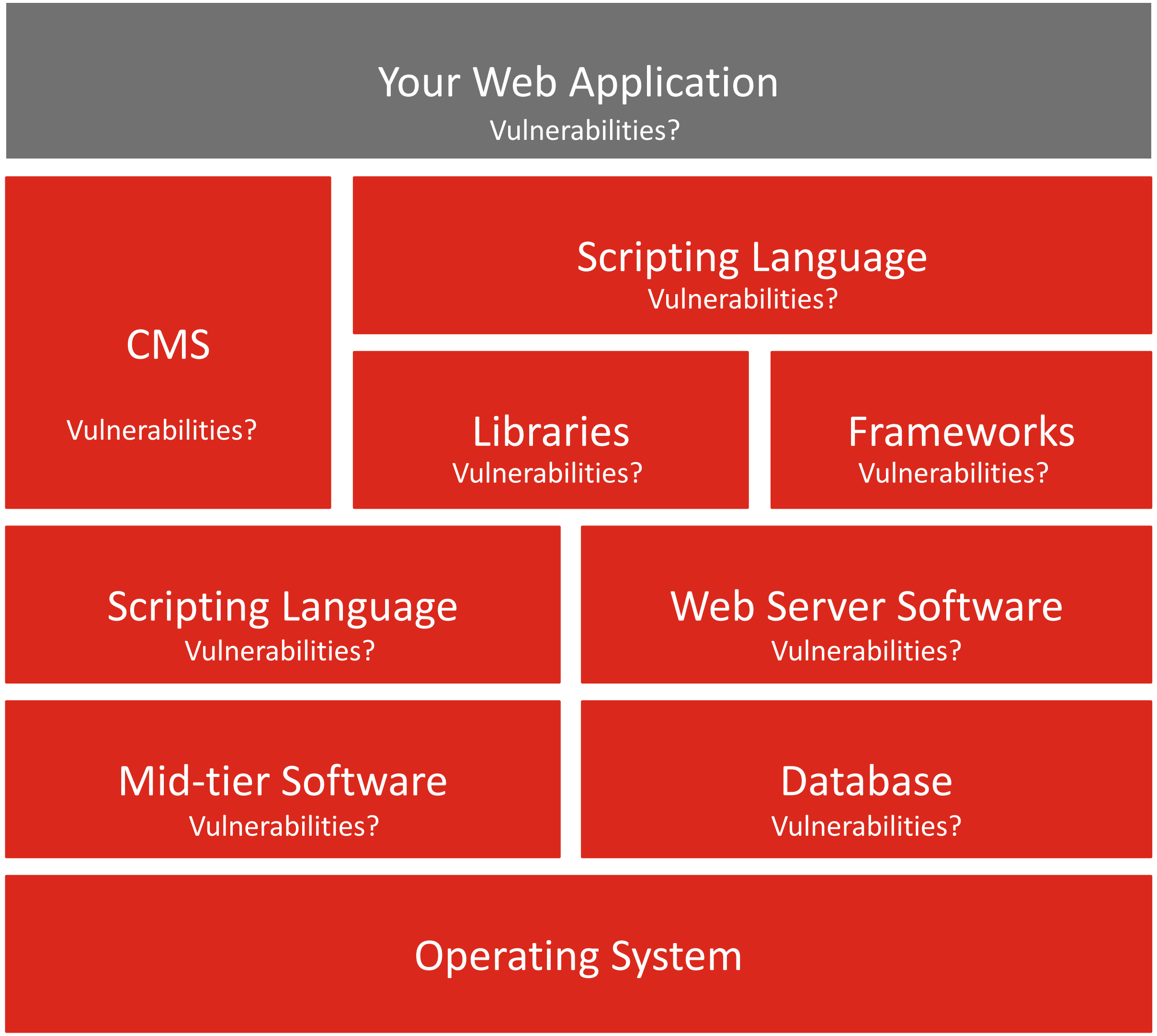
Vulnerabilities By Year



PHP

Vulnerabilities By Year





Your Web Application
Vulnerabilities?

CMS
Vulnerabilities?

Scripting Language
Vulnerabilities?

Libraries
Vulnerabilities?

Frameworks
Vulnerabilities?

Scripting Language
Vulnerabilities?

Web Server Software
Vulnerabilities?

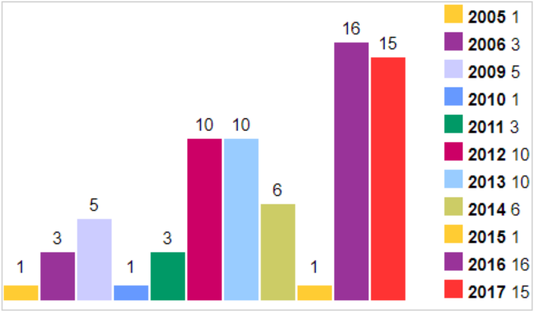
Mid-tier Software
Vulnerabilities?

Database
Vulnerabilities?

Operating System

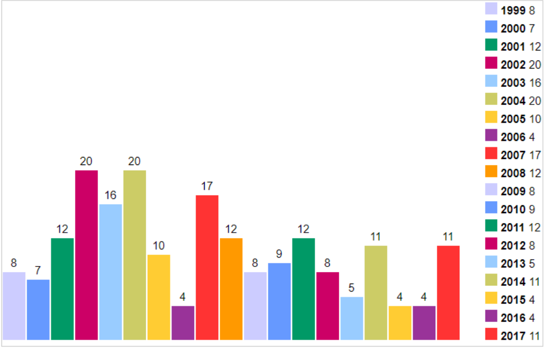
Apache Struts

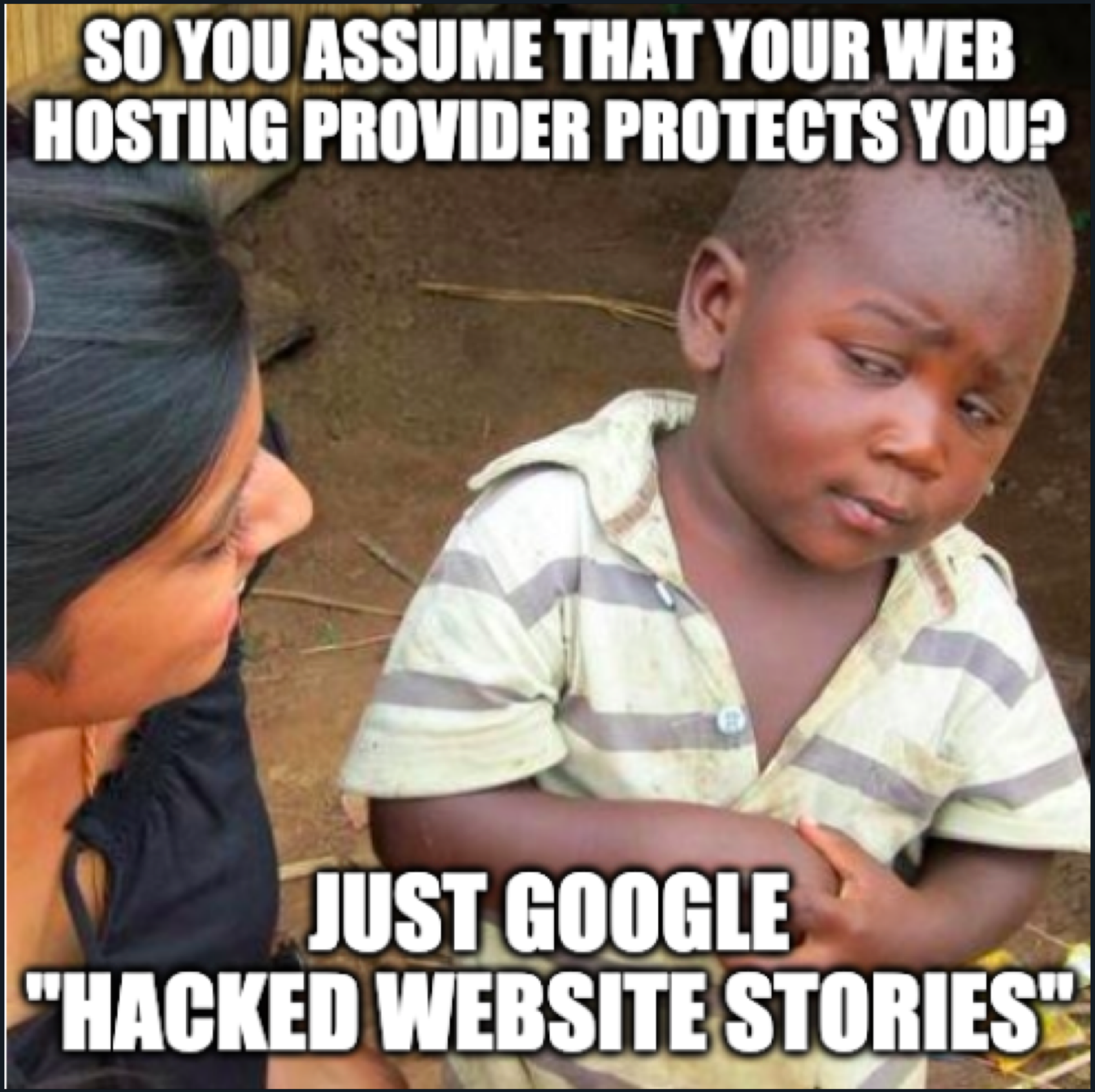
Vulnerabilities By Year



Apache Web Server

Vulnerabilities By Year




SO YOU ASSUME THAT YOUR WEB HOSTING PROVIDER PROTECTS YOU?
JUST GOOGLE "HACKED WEBSITE STORIES"

2017 OWASP

TOP 10

APPLICATION SECURITY RISKS

A1
INJECTION

A2
BROKEN AUTHENTICATION

A3
SENSITIVE DATA EXPOSURE

A4
XML EXTERNAL ENTITIES (XXE)

A5
BROKEN ACCESS CONTROL

A6
SECURITY MISCONFIGURATION

A7
CROSS-SITE SCRIPTING (XSS)

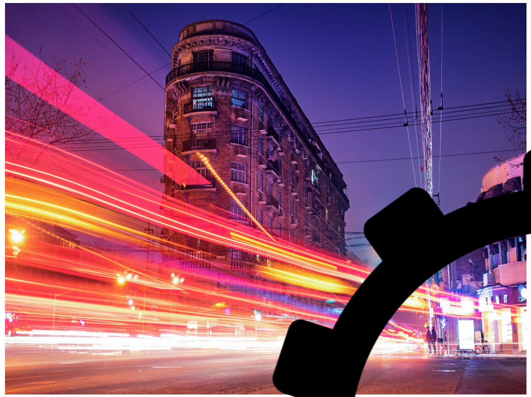
A8
INSECURE DESERIALIZATION

A9
USING COMPONENTS WITH KNOWN VULNERABILITIES

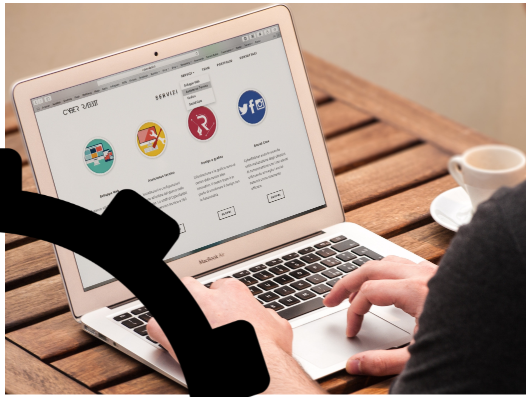
A10
INSUFFICIENT LOGGING & MONITORING

Why Web Applications?

Abundant Tools



Rapid Deployment



Common User Experience

User Engagement

APIs are also part of the mix . . .

Mobile

Middleware

Web Applications Accelerate Business

DevOps
Sec

Web Application Security

Internet-facing applications increase your attack surface

Regulatory requirements apply to some of your most sensitive data

The threat landscape continues to evolve

Protection for the Layer 7 Perimeter

Web Protection

API Protection

Bot Protection

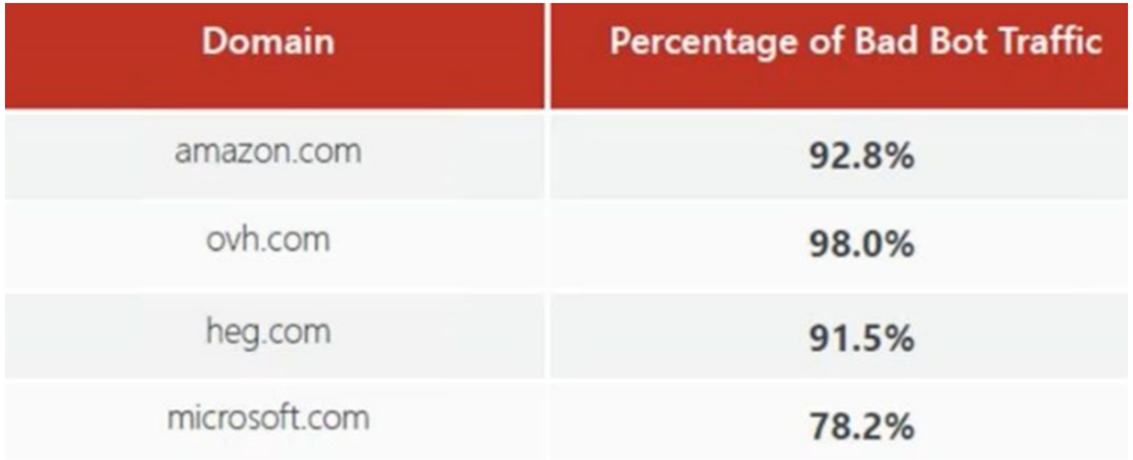
The Challenge of Bots

Bots are applications that run automated tasks over the internet

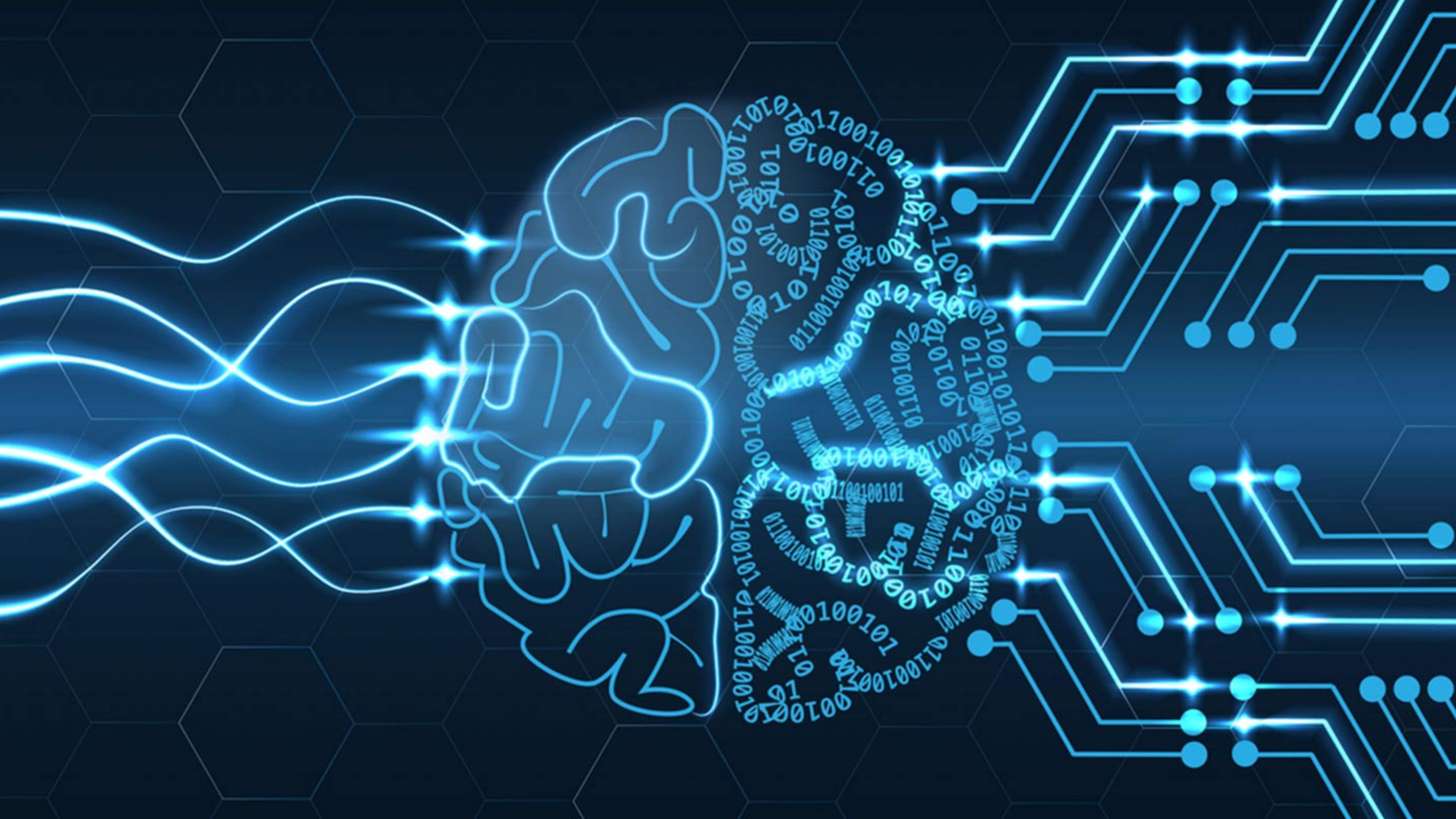
- Good bots:
  - search engines
  - virtual assistants
  - chatbots
- Bad bots:
  - web scraping
  - competitive data mining
  - personal and financial data harvesting
  - account takeover
  - digital ad fraud
  - transaction fraud

Bot Mitigation – Detection Techniques

- Sender and Request reputation – IP Reputation
- Signatures
- Traffic thresholds
- Business Logic analysis

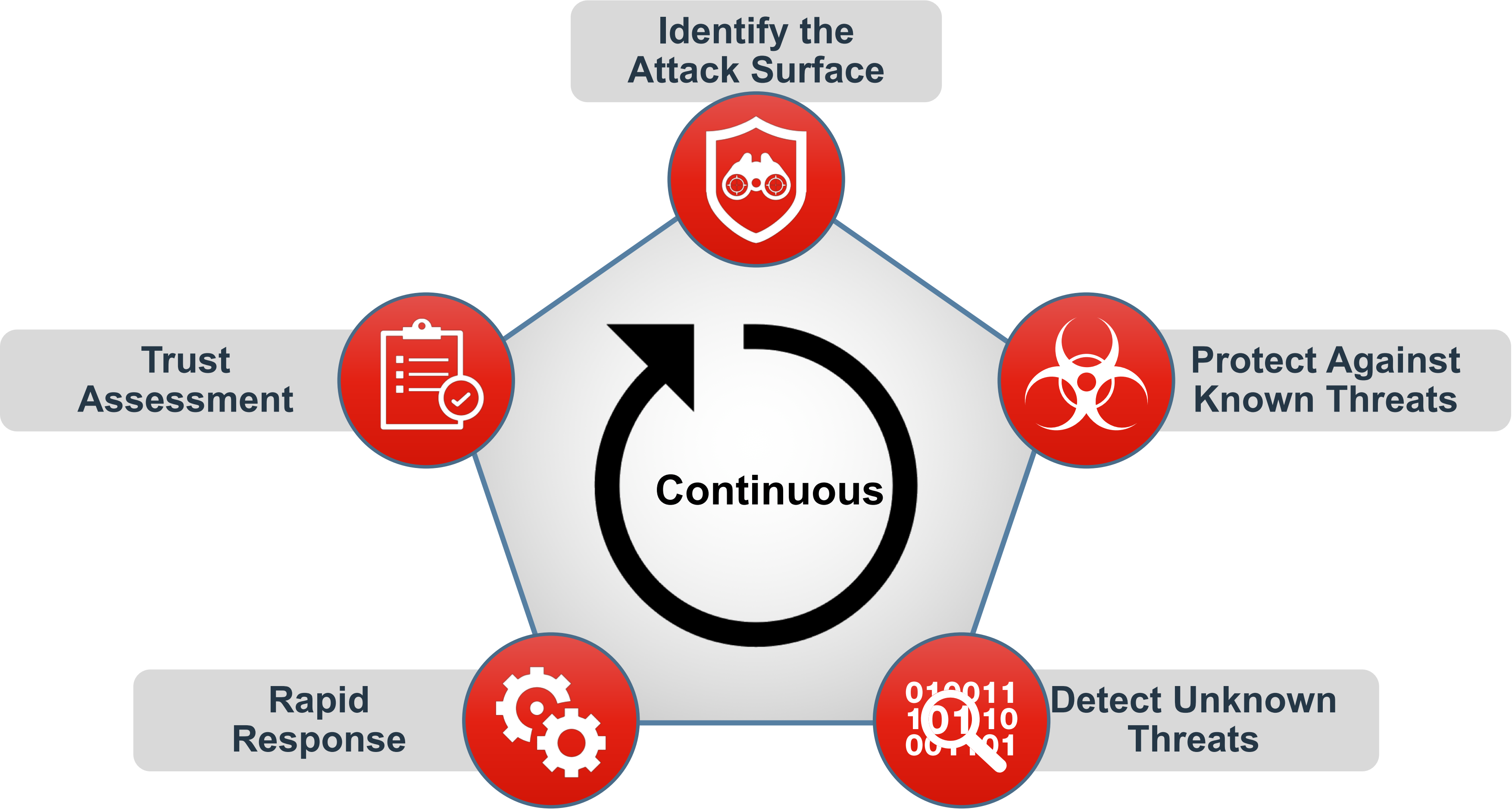


Domain	Percentage of Bad Bot Traffic
amazon.com	92.8%
ovh.com	98.0%
heg.com	91.5%
microsoft.com	78.2%



Security Framework for Digital Security

NIST Model



Identify the Attack Surface

Protect Against Known Threats

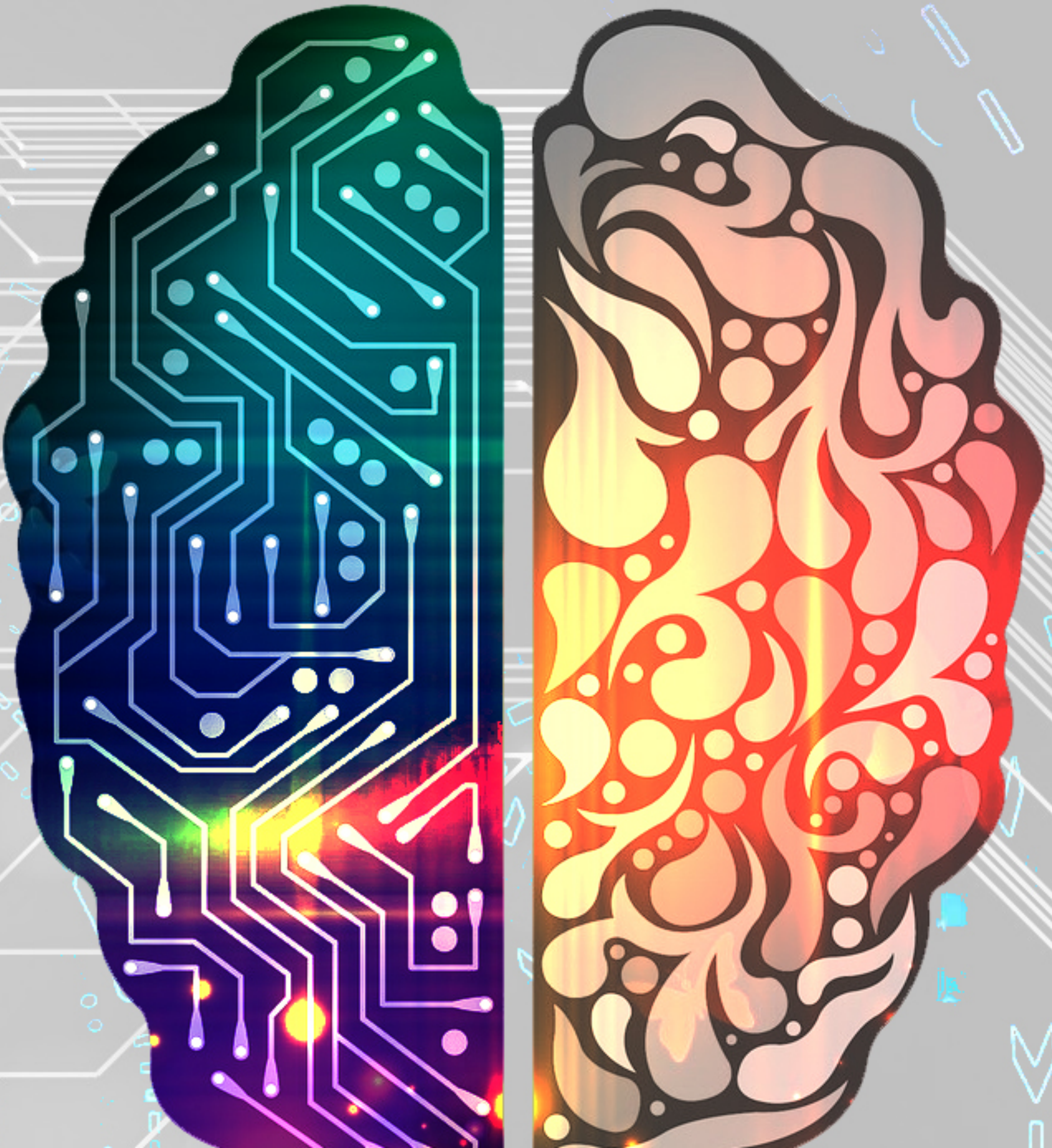
Detect Unknown Threats

Rapid Response

Trust Assessment

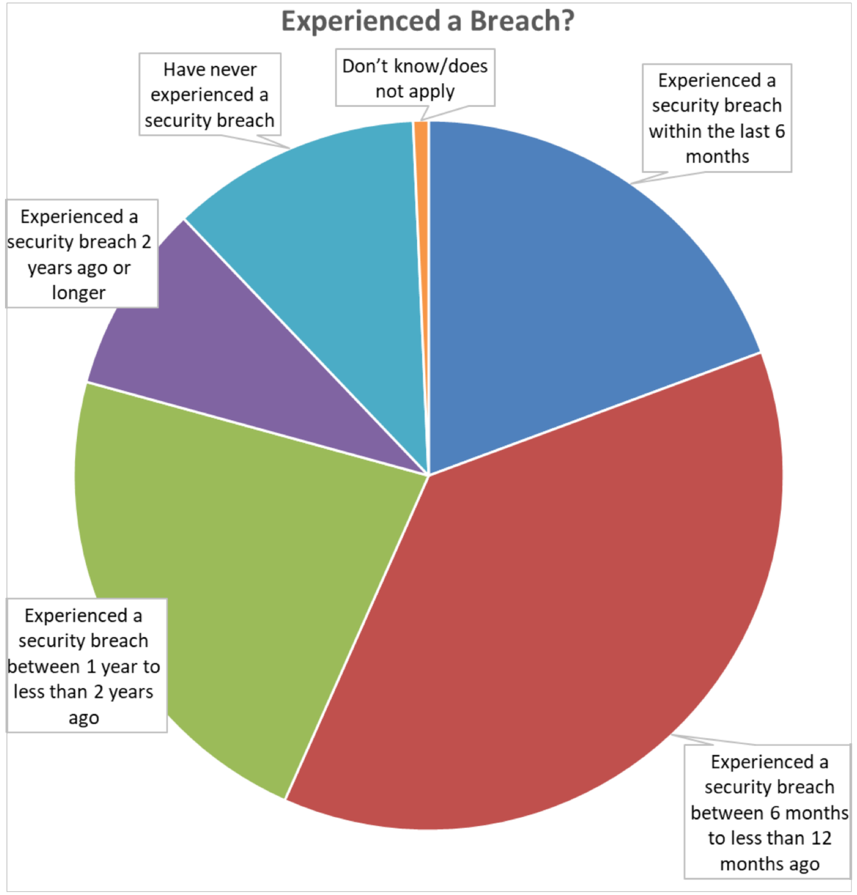
Continuous

MACHINE
LEARNING



Market Situation for Cybersecurity

- Almost 90% have experienced a breach
- >50% in last year



Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

DIGITAL TRANSFORMATION INTRODUCES

NEW ATTACK SURFACES

CLOUD MANAGEMENT API

CLOUD INTERCONNECT

CONTAINER ENVIRONMENTS

ORCHESTRATION SYSTEMS

THE RISE OF BOTS AND ATTACK FRAMEWORKS

MULTI-LAYERED ATTACK STRATEGIES

ATTACKS HIDDEN IN ENCRYPTED TRAFFIC

ENDLESS STREAM OF ZERO-DAY VULNERABILITIES

DIGITAL TRANSFORMATION INTRODUCES

NEW THREATS

CLOUD COMPUTING LEADS TO
NEW SECURITY CHALLENGES

CROSS PLATFORM VISIBILITY

COMPLEXITY DRIVEN HUMAN ERROR

REGULATORY COMPLIANCE

EXPLOSION OF DATA

COMPLEXITY DRIVEN HUMAN ERROR

Through 2023, at least 99% of cloud security failures will be the customer’s fault.

Gartner, Oct. 2018

The Shared Responsibility Model

On-Prem	Public Cloud	SaaS
🟩 Platform Control	🟩 Platform Control	🟩 Platform Control
🟩 Visibility	🟩 Visibility	🟩 Visibility
🟩 Access Control	🟩 Access Control	⬛ Access Control
🟩 Data	🟩 Data	⬛ Data
🟩 Applications	🟩 Applications	⬛ Applications
🟩 Libraries/Containers	🟩 Libraries/Containers	⬛ Libraries/Containers
🟩 Operating Systems	🟩 Operating Systems	⬛ Operating Systems
🟩 Hypervisor	⬛ Hypervisor	⬛ Hypervisor
🟩 Networking	⬛ Networking	⬛ Networking
🟩 Physical Security	⬛ Physical Security	⬛ Physical Security

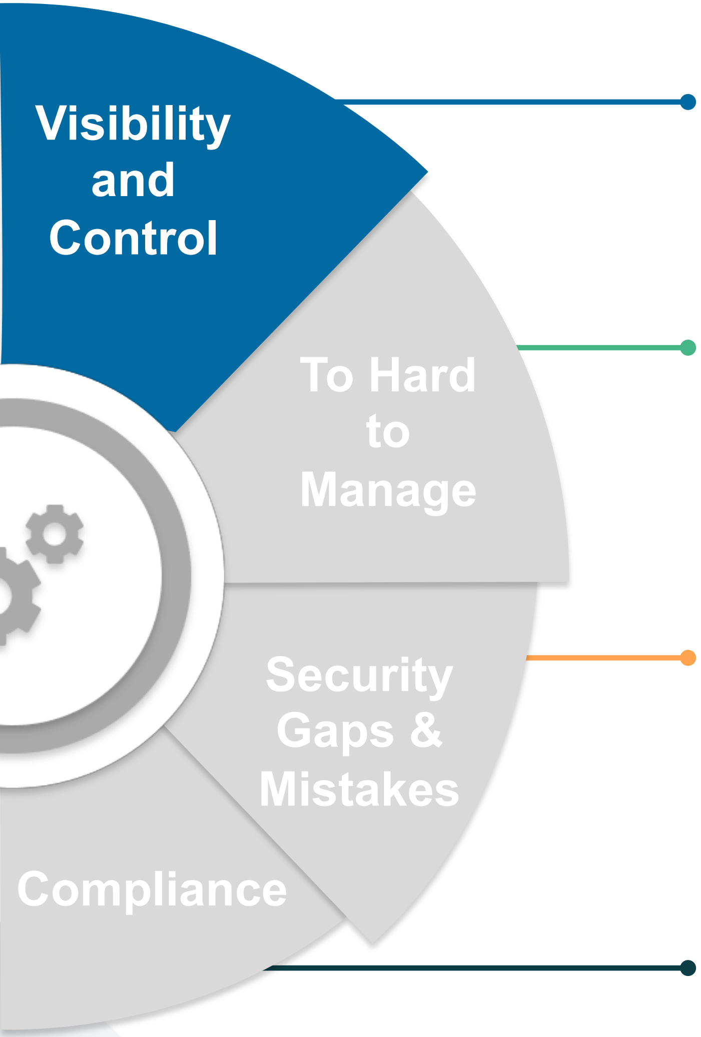
Shared Responsibility Model

- Customer responsibility varies with the consumption model
- Highlights the need for management across clouds and data centers
- Best with native integration in cloud security system

🟩 Customer Responsibility

⬛ Cloud Provider Responsibility

Challenges Created by Multi/Hybrid Clouds



Visibility and Control

- No central view of security events
- No real-time resource inventory or network topology
- Large number of privileged users with limited governance

To Hard to Manage

- Too many point solutions for different clouds and data centers
- Lack of cloud context and event correlation
- Hard to force consistent policies

Security Gaps & Mistakes

- Shared security model can be confusing
- Hard to identify configuration errors

Compliance

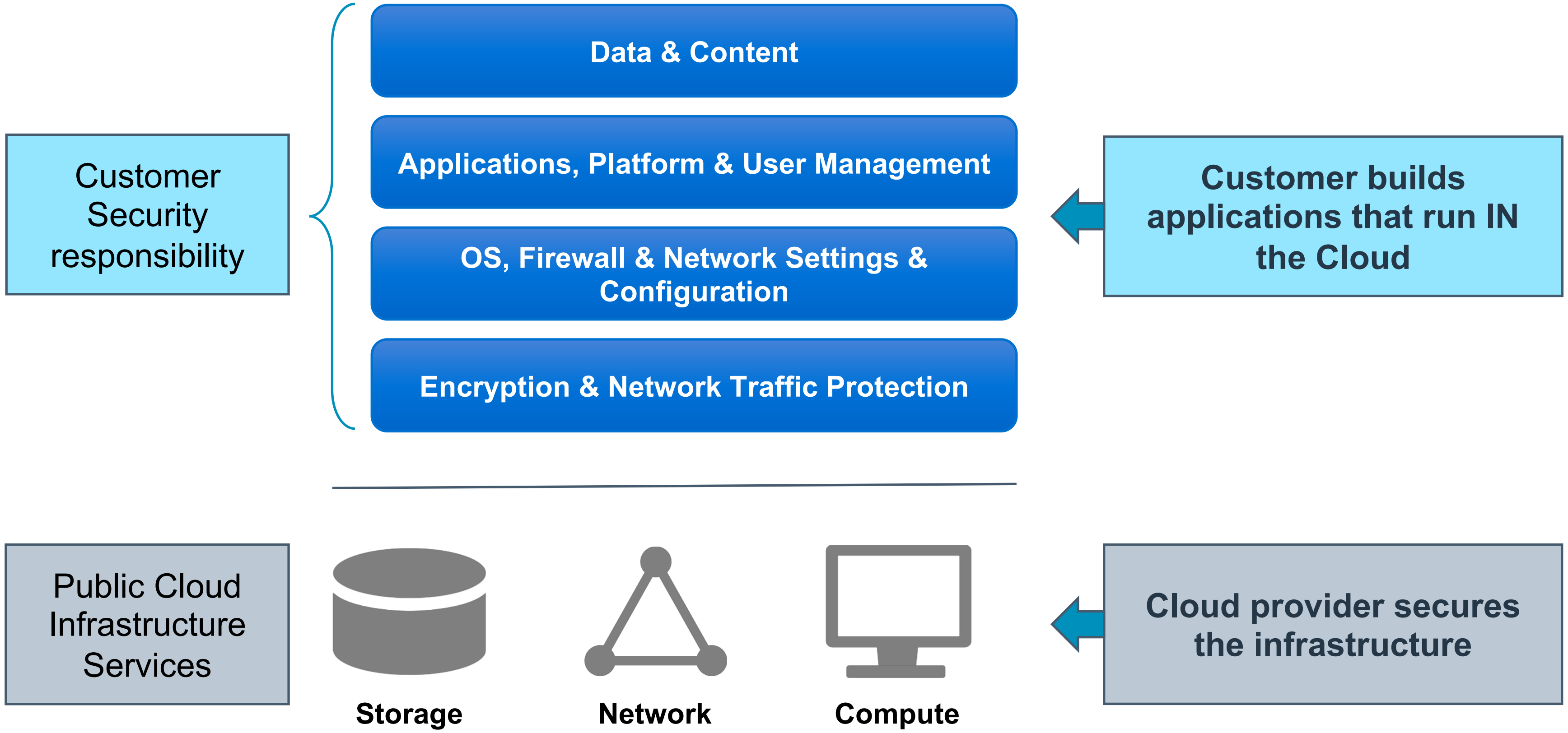
- Hundreds of cloud services added daily
- Hard to prove compliance to auditors

Shared Responsibility

The majority of the cloud security responsibility is on the user — not the provider

95%

Cloud security failures through 2020 where the customer is at fault[1]



Customer Security responsibility

Data & Content

Applications, Platform & User Management

OS, Firewall & Network Settings & Configuration

Encryption & Network Traffic Protection

Customer builds applications that run IN the Cloud

Public Cloud Infrastructure Services

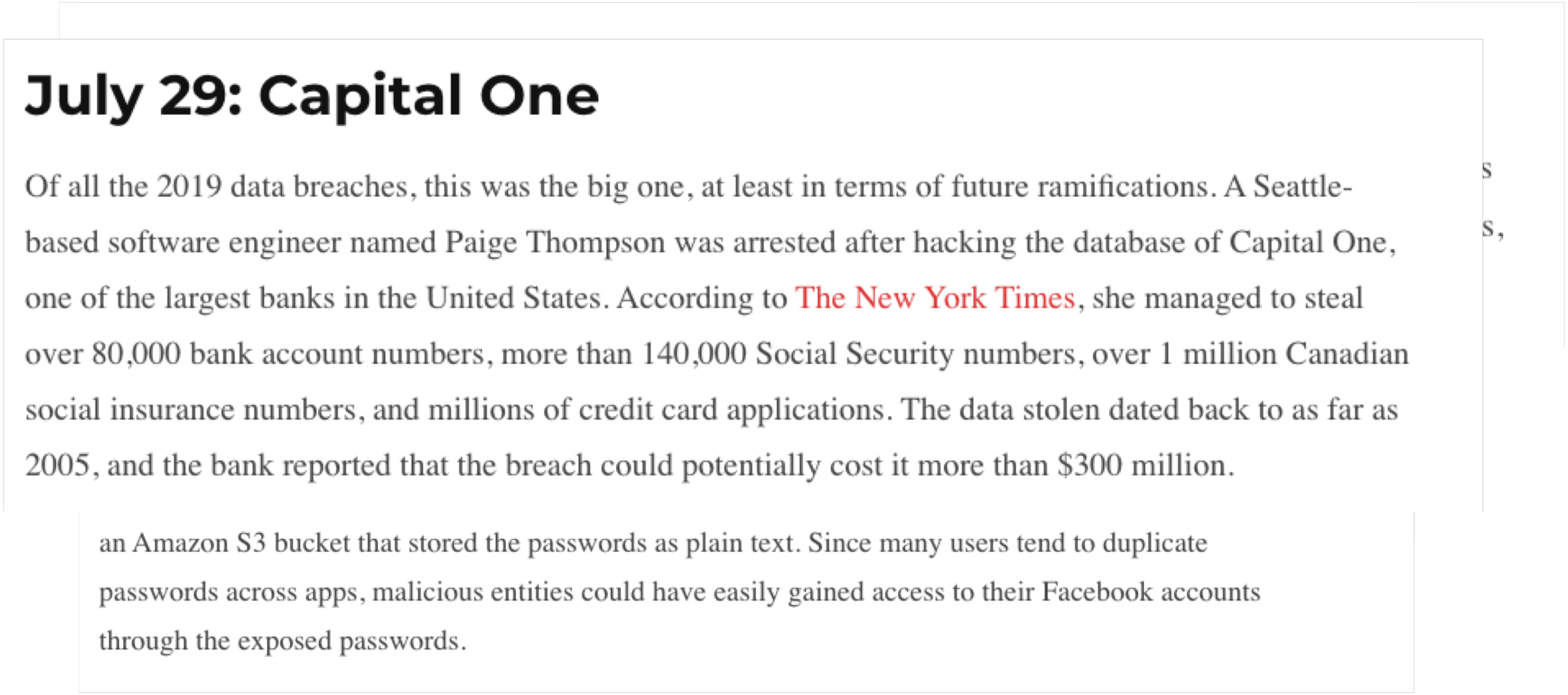
Storage

Network

Compute

Cloud provider secures the infrastructure

Web Application Breaches - 2019



July 29: Capital One

Of all the 2019 data breaches, this was the big one, at least in terms of future ramifications. A Seattle-based software engineer named Paige Thompson was arrested after hacking the database of Capital One, one of the largest banks in the United States. According to The New York Times, she managed to steal over 80,000 bank account numbers, more than 140,000 Social Security numbers, over 1 million Canadian social insurance numbers, and millions of credit card applications. The data stolen dated back to as far as 2005, and the bank reported that the breach could potentially cost it more than $300 million.

s

s,

an Amazon S3 bucket that stored the passwords as plain text. Since many users tend to duplicate passwords across apps, malicious entities could have easily gained access to their Facebook accounts through the exposed passwords.

FORTINET®

Timo Lohenoja, CISSP

Systems Engineer, Fortinet

timo@fortinet.com