radware

Securing your Applications & Data
With
Web Application Firewalls

Dennis K. Usle

Sr. Security Architect, Radware

July 2013

radware

AGENDA

Cyberwar: The Web App Aspect

Web Application Security Challenge

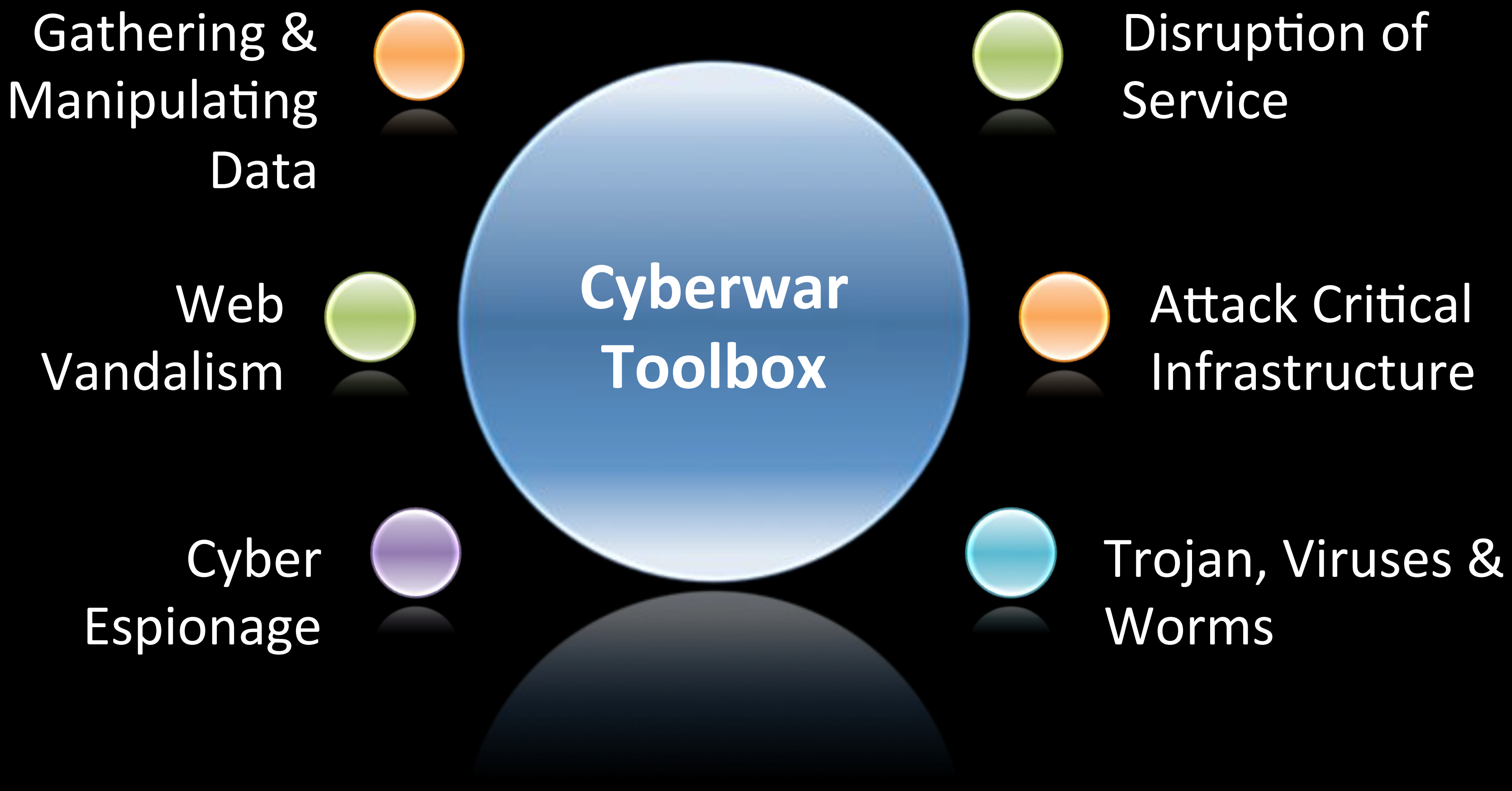
Countermeasure: WAF

Selection Considerations

radware

Cyber War:
The Web Application Aspect

rootkit phishing malware worm trojan virus
phishing malware worm trojan virus spam hack
malware worm trojan virus spam hackers
worm trojan virus spam hackers spyware
trojan virus spam hackers spyware security
virus spam hackers spyware security rootkit
spam hackers spyware security rootkit phis



Cyberwar Toolbox

Gathering & Manipulating Data

Web Vandalism

Cyber Espionage

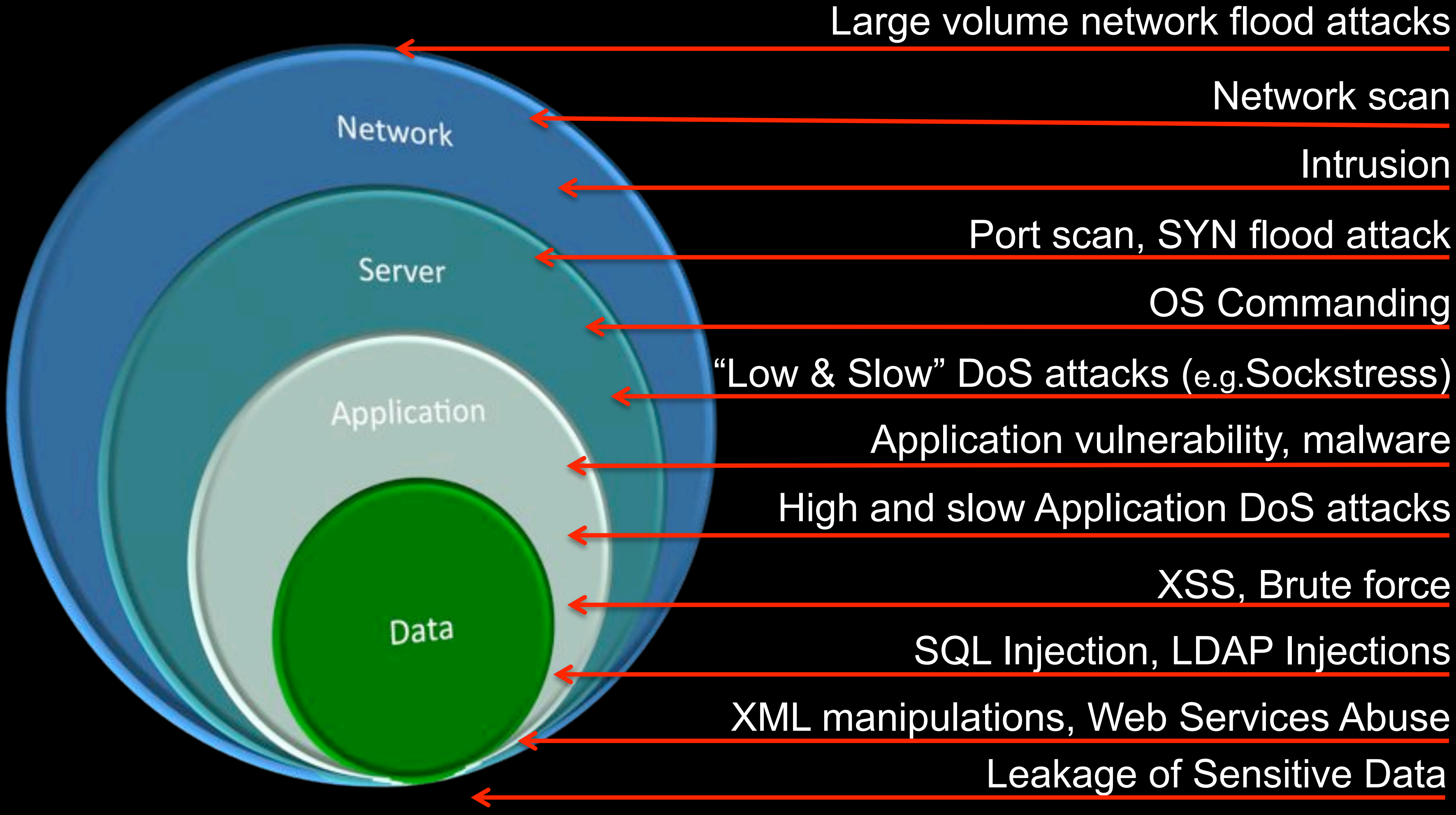
Disruption of Service

Attack Critical Infrastructure

Trojan, Viruses & Worms

radware

Targeting Different Layers



Large volume network flood attacks

Network scan

Intrusion

Port scan, SYN flood attack

OS Commanding

“Low & Slow” DoS attacks (e.g.Sockstress)

Application vulnerability, malware

High and slow Application DoS attacks

XSS, Brute force

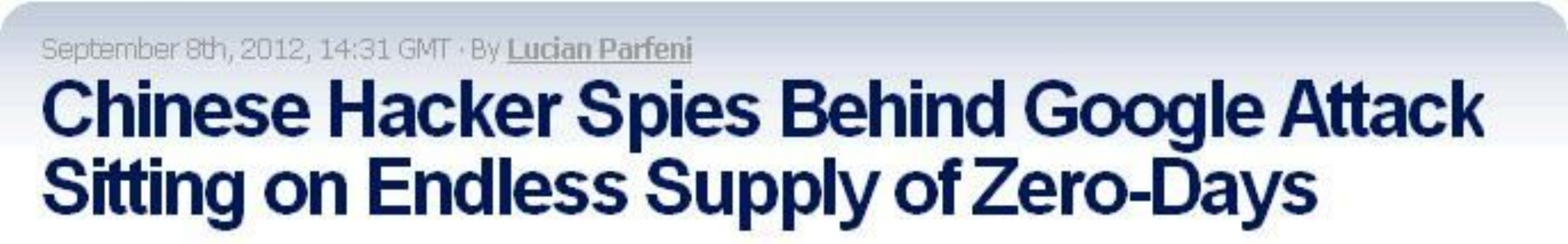
SQL Injection, LDAP Injections

XML manipulations, Web Services Abuse

Leakage of Sensitive Data

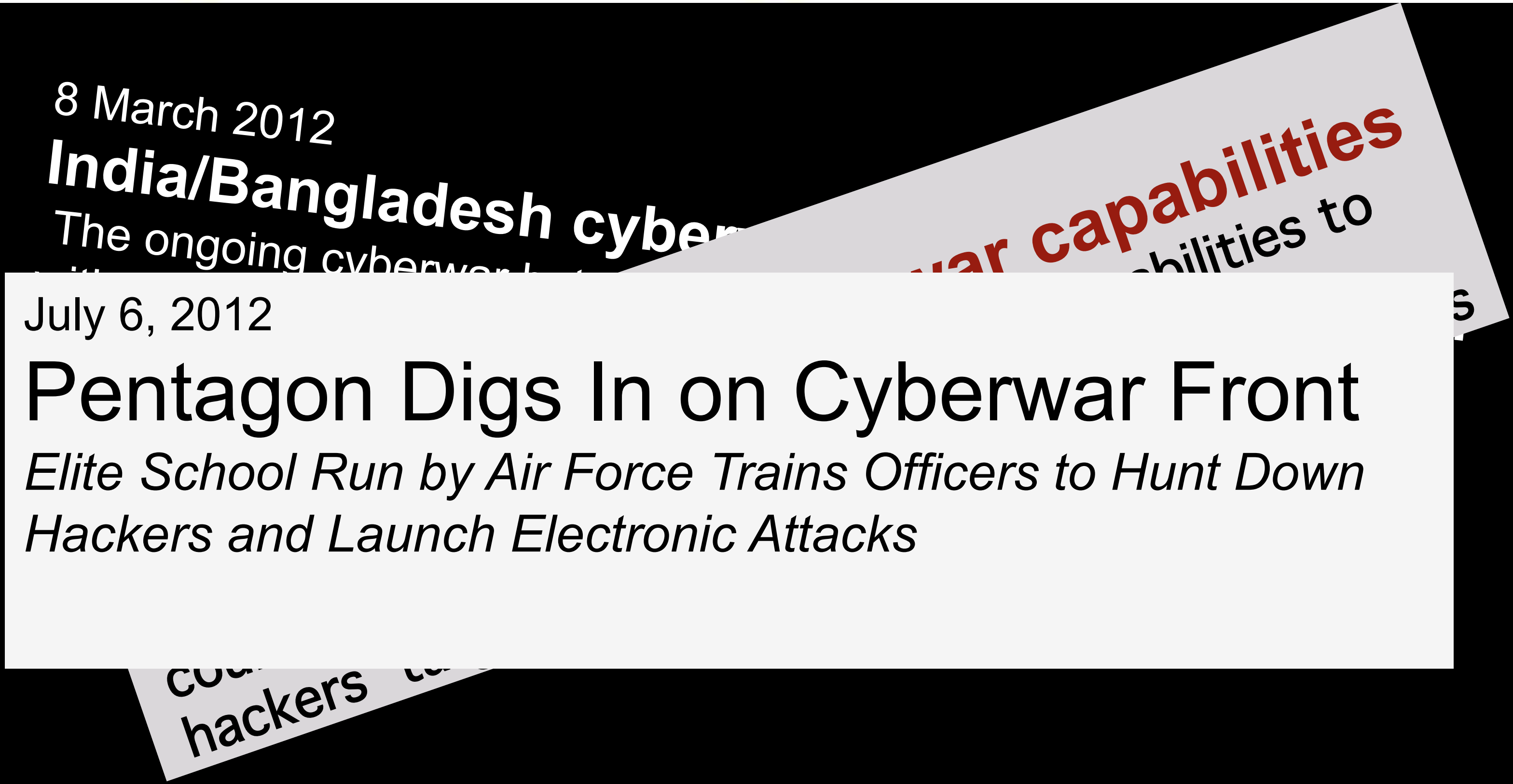
McAfee, 2007,
The Internet security report

Approximately **120 countries** have been developing ways to use **the Internet as a weapon** and target financial markets, government computer systems and utilities.



September 8th, 2012, 14:31 GMT · By Lucian Parfeni

Chinese Hacker Spies Behind Google Attack Sitting on Endless Supply of Zero-Days



8 March 2012

India/Bangladesh cyber

The ongoing cyberwar bet

war capabilities

bilities to

s

cou

hackers ta

July 6, 2012

Pentagon Digs In on Cyberwar Front

Elite School Run by Air Force Trains Officers to Hunt Down Hackers and Launch Electronic Attacks

radware

Cyberwar – The Web App Aspect

CREATE TROJAN
ATTACK EXPLOIT
HACK A CHOSEN WEBSITE
DELIVER MALWARE THROUGH EMAIL
DELIVER MALWARE THROUGH WEBSITE

radware

Web Applications Security Challenge

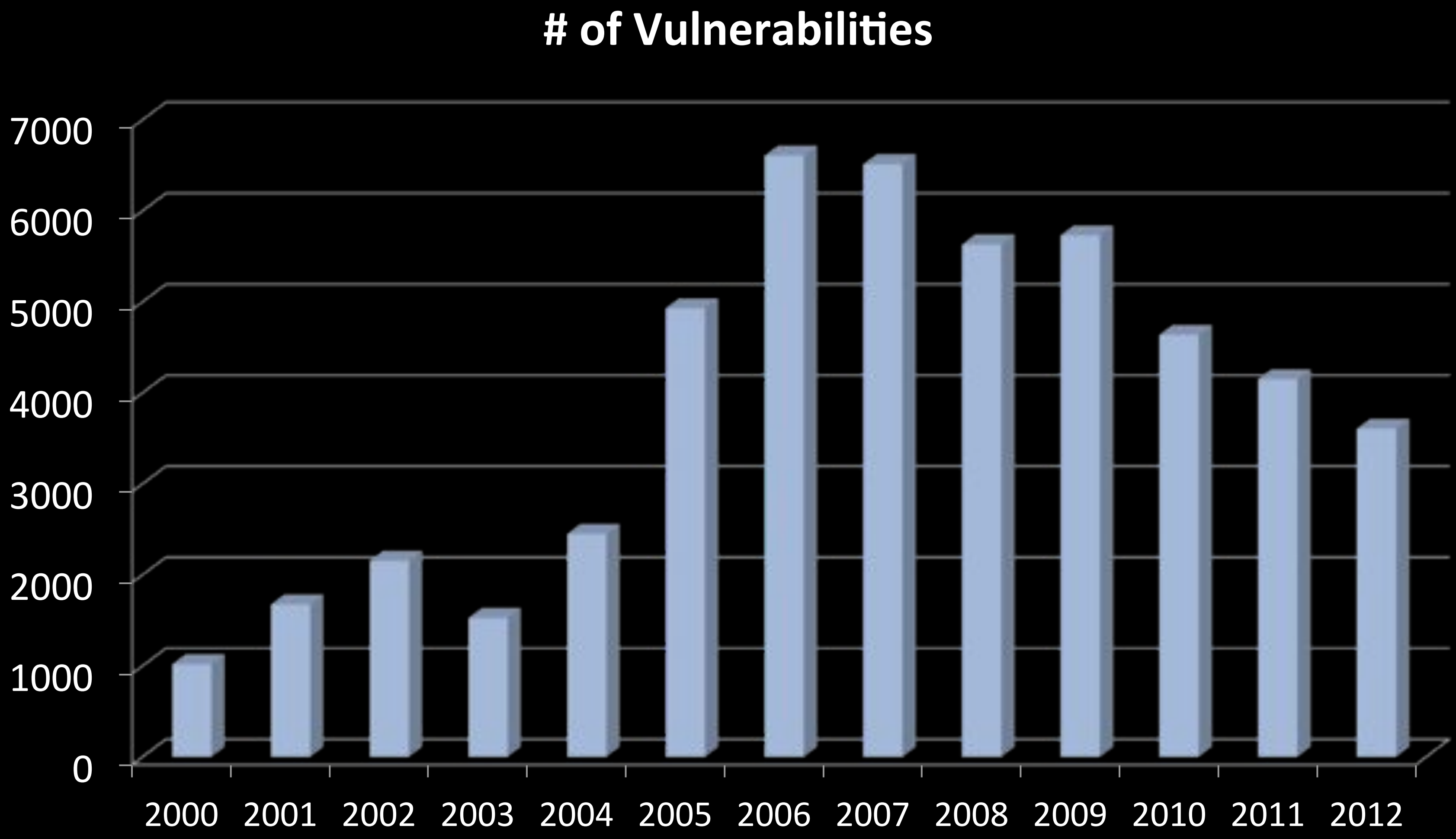
radware

Web Apps are Easy to Exploit

- Whole system open to attack
- Can target different layers
- Thousands of Web security vulnerabilities
- Minimal attention to security during development
- Traditional defences inadequate

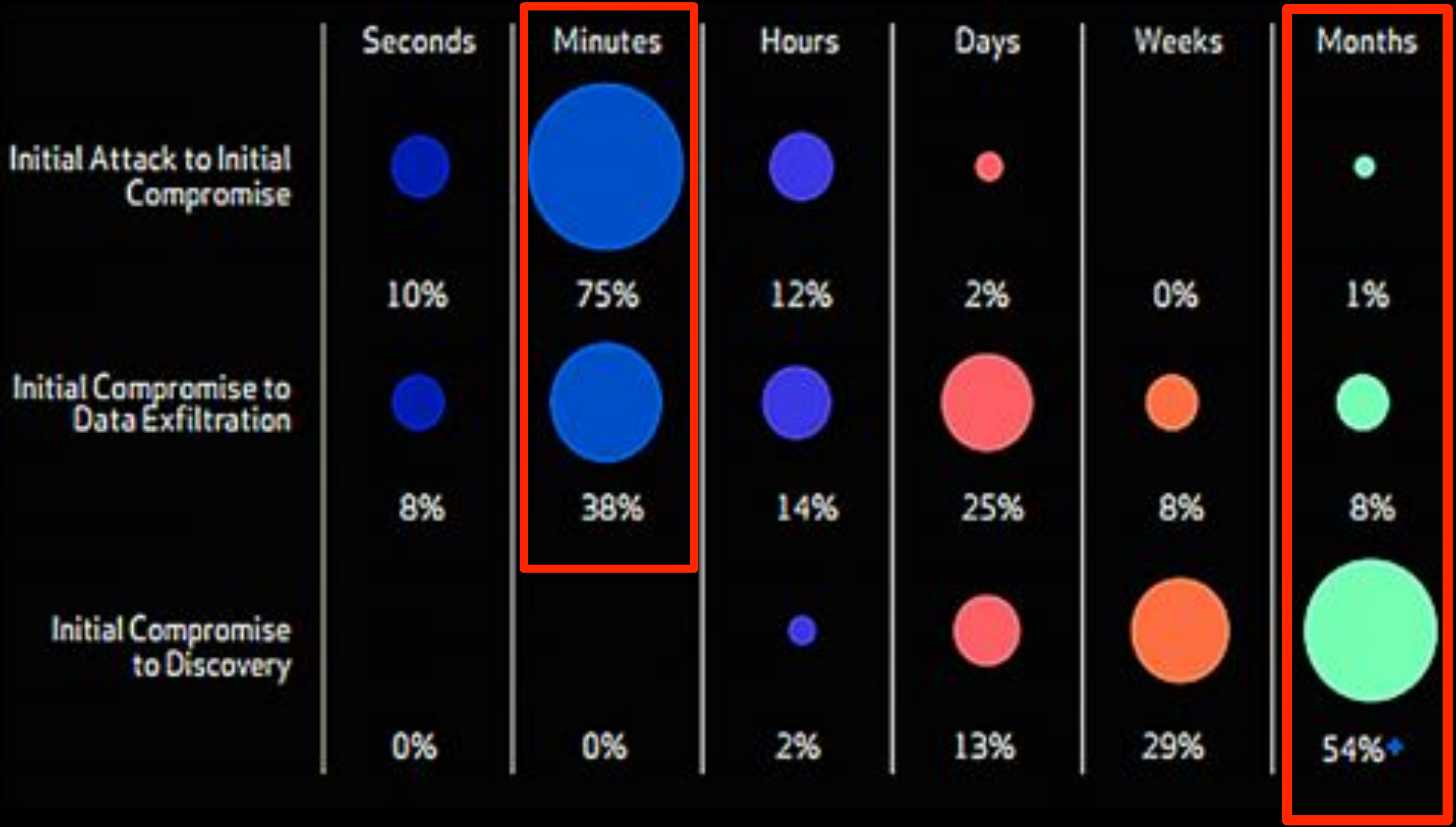
All they need is a browser

Thousands of Vulnerabilities Every Year



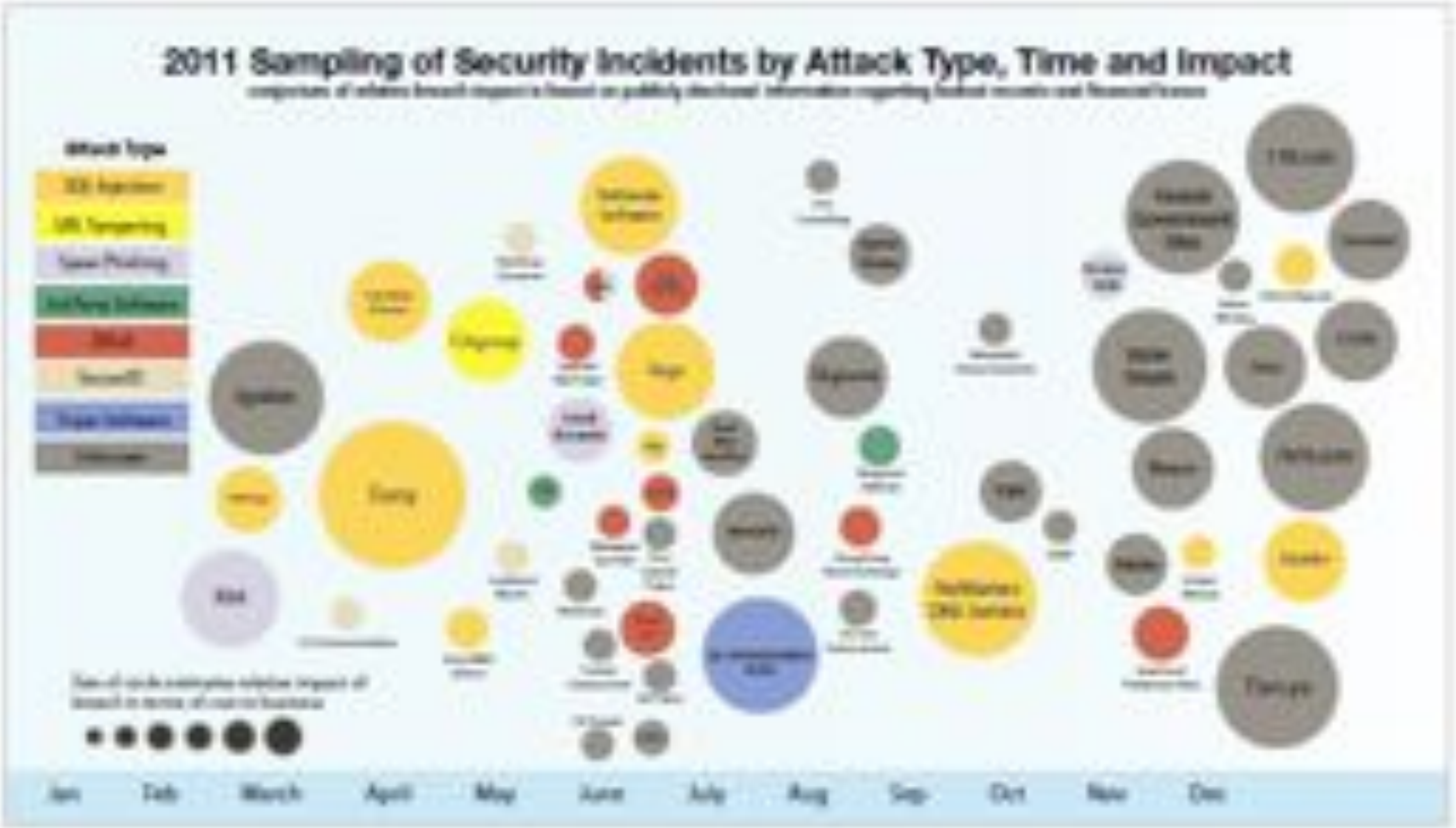
- Source: National Vulnerabilities Database

Minutes to Compromise, Months to Discover

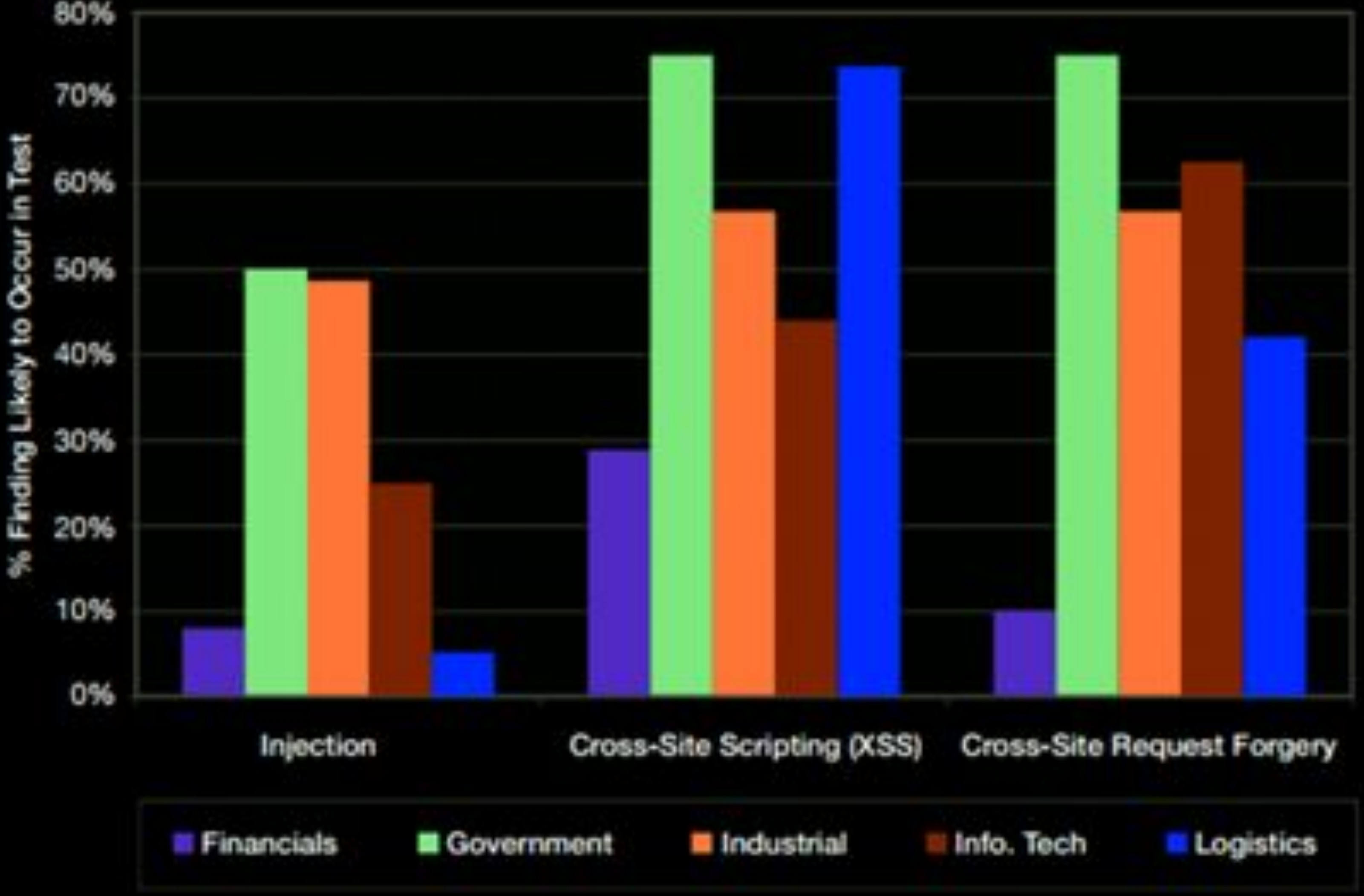


	Seconds	Minutes	Hours	Days	Weeks	Months
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%

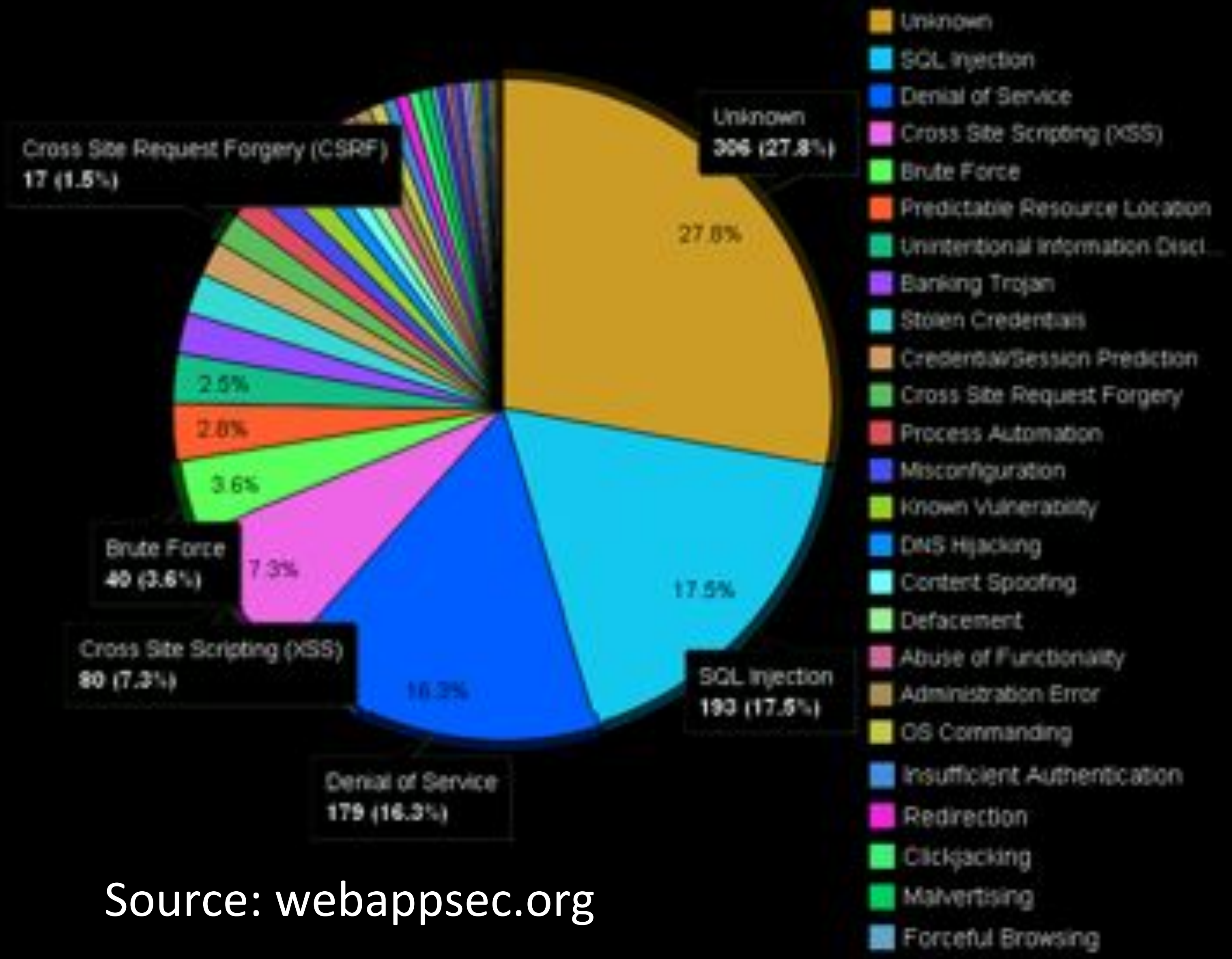
SQL Injections are Dominant



Trends for Web App Vulnerability Types



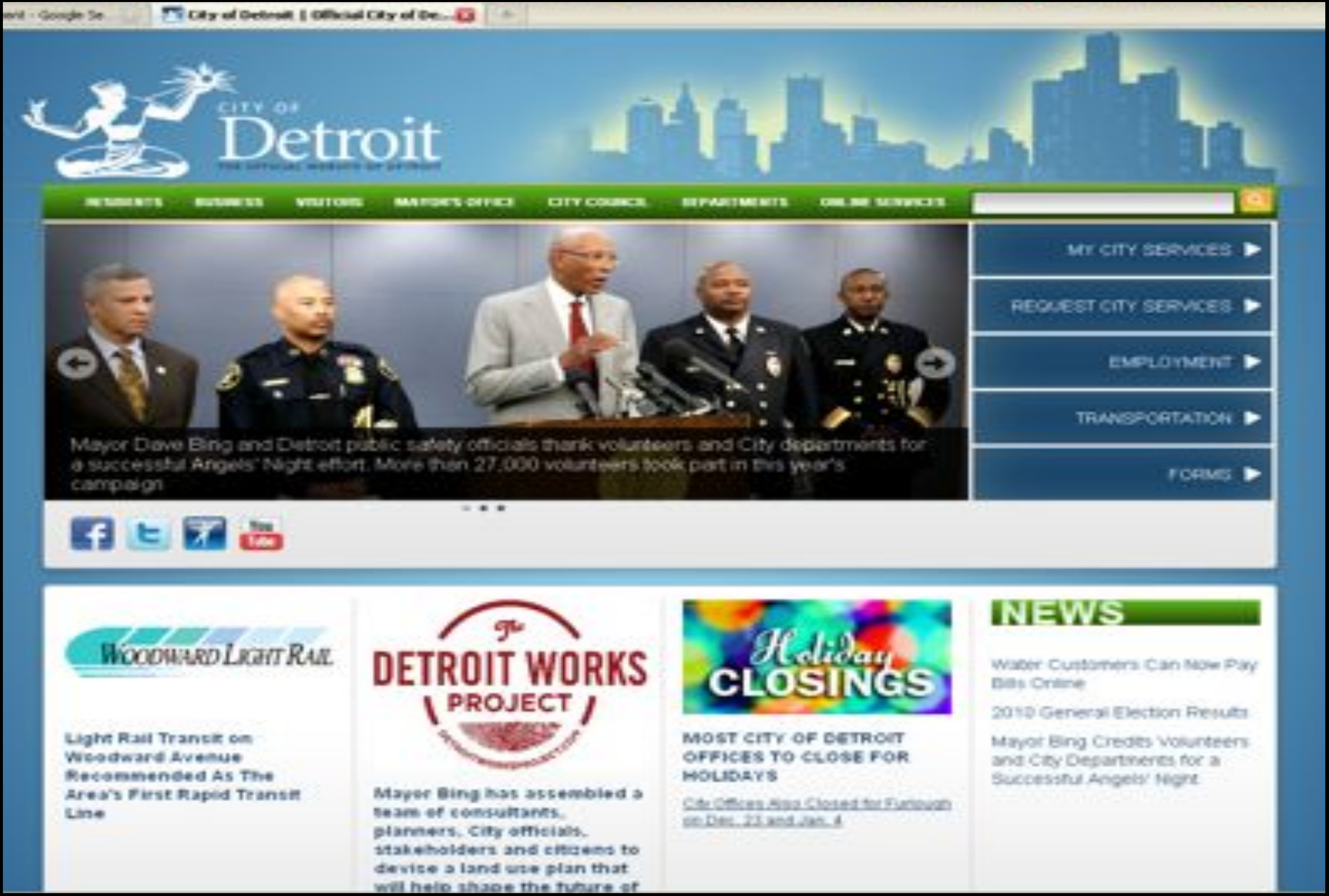
Top Attack Methods



Source: webappsec.org

Demo

Web Site Defacements (before)



City of Detroit | Official City of De...

CITY OF Detroit

THE OFFICIAL WEBSITE OF DETROIT

RESIDENTS BUSINESS VISITORS MAYOR'S OFFICE CITY COUNCIL DEPARTMENTS ONLINE SERVICES

MY CITY SERVICES ▶

REQUEST CITY SERVICES ▶

EMPLOYMENT ▶

TRANSPORTATION ▶

FORMS ▶

Mayor Dave Bing and Detroit public safety officials thank volunteers and City departments for a successful Angels' Night effort. More than 27,000 volunteers took part in this year's campaign

WOODWARD LIGHT RAIL

Light Rail Transit on Woodward Avenue Recommended As The Area's First Rapid Transit Line

The DETROIT WORKS PROJECT

Mayor Bing has assembled a team of consultants, planners, City officials, stakeholders and citizens to devise a land use plan that will help shape the future of

Holiday CLOSINGS

MOST CITY OF DETROIT OFFICES TO CLOSE FOR HOLIDAYS

City Offices Also Closed for Furlough on Dec. 23 and Jan. 4

NEWS

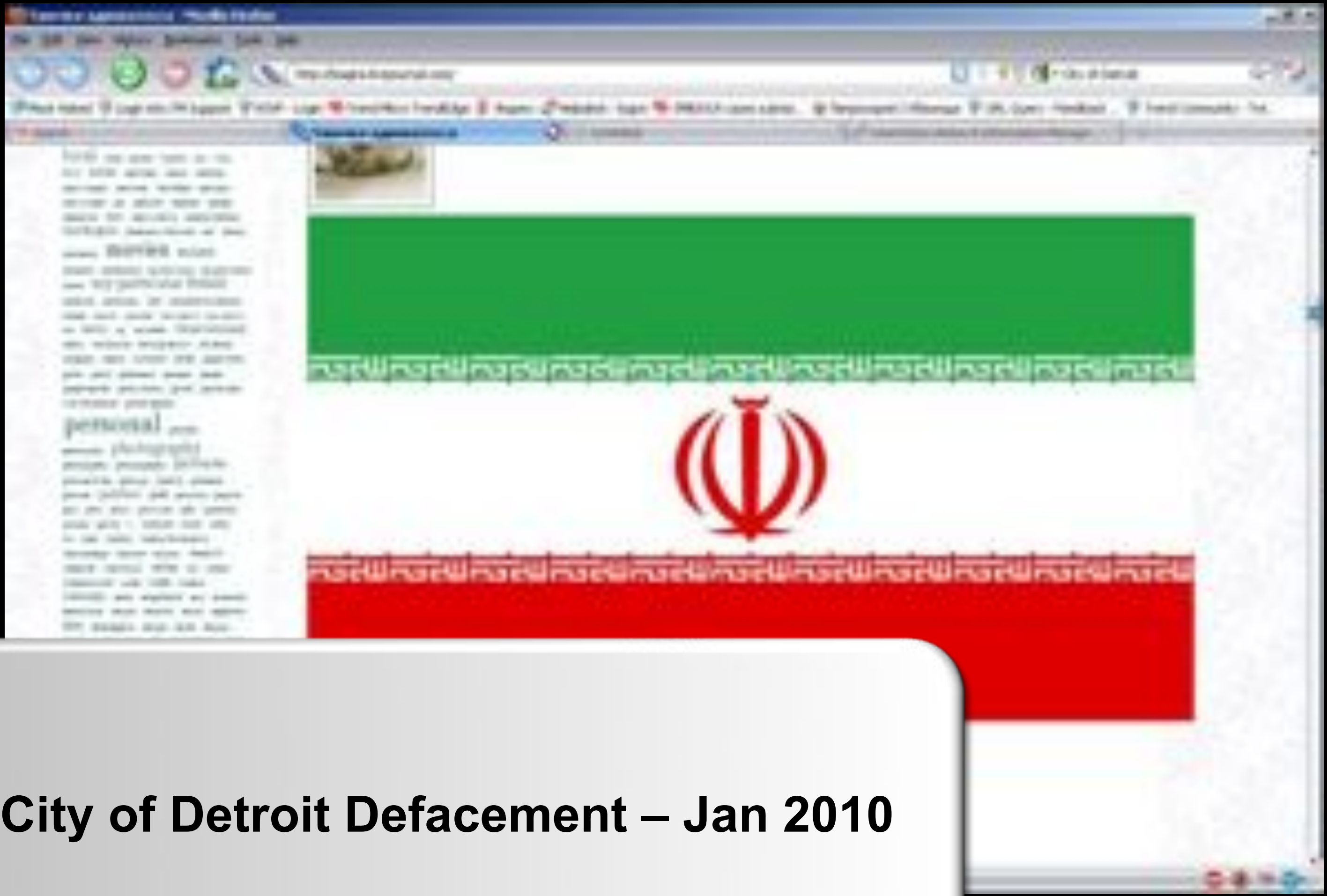
Water Customers Can Now Pay Bills Online

2010 General Election Results

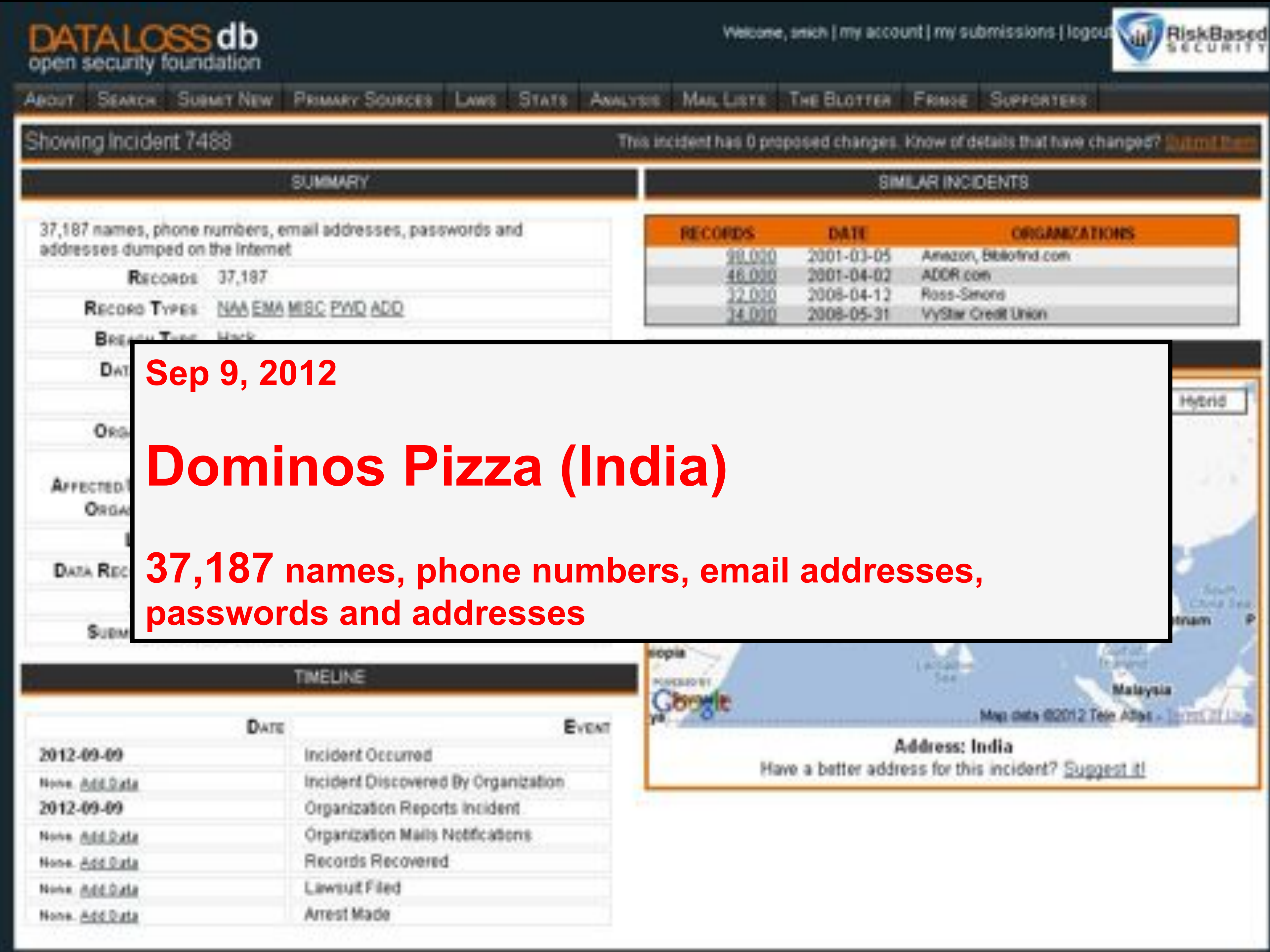
Mayor Bing Credits Volunteers and City Departments for a Successful Angels' Night

Slide 17

Web Site Defacement (after)



City of Detroit Defacement – Jan 2010



Showing Incident 7488

This incident has 0 proposed changes. Know of details that have changed? Submit them

SUMMARY

37,187 names, phone numbers, email addresses, passwords and addresses dumped on the Internet

Records	37,187
Record Types	NAA EMA MISC PWD ADD
Breach Type	Hack

SIMILAR INCIDENTS

RECORDS	DATE	ORGANIZATIONS
98,000	2001-03-05	Amazon, Bibliofind.com
46,000	2001-04-02	ADDR.com
32,000	2008-04-12	Ross-Simons
34,000	2008-05-31	VyStar Credit Union

TIMELINE

Date	Event
2012-09-09	Incident Occurred
None. Add Data	Incident Discovered By Organization
2012-09-09	Organization Reports Incident
None. Add Data	Organization Mails Notifications
None. Add Data	Records Recovered
None. Add Data	Lawsuit Filed
None. Add Data	Arrest Made

Address: India

Have a better address for this incident? Suggest it!

Sep 9, 2012

Dominos Pizza (India)

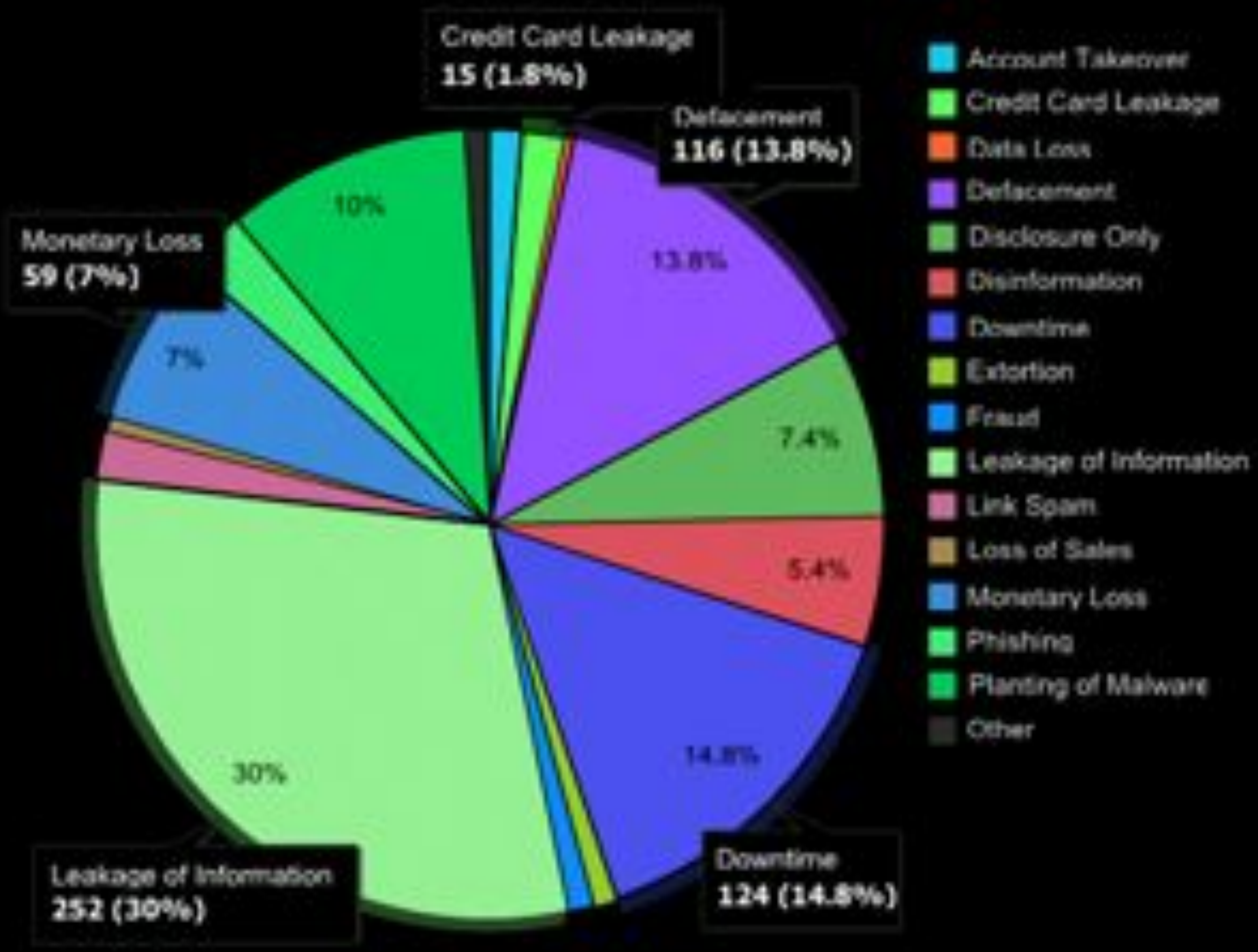
37,187 names, phone numbers, email addresses, passwords and addresses

Data Security Breaches

Online Dating Site Breached

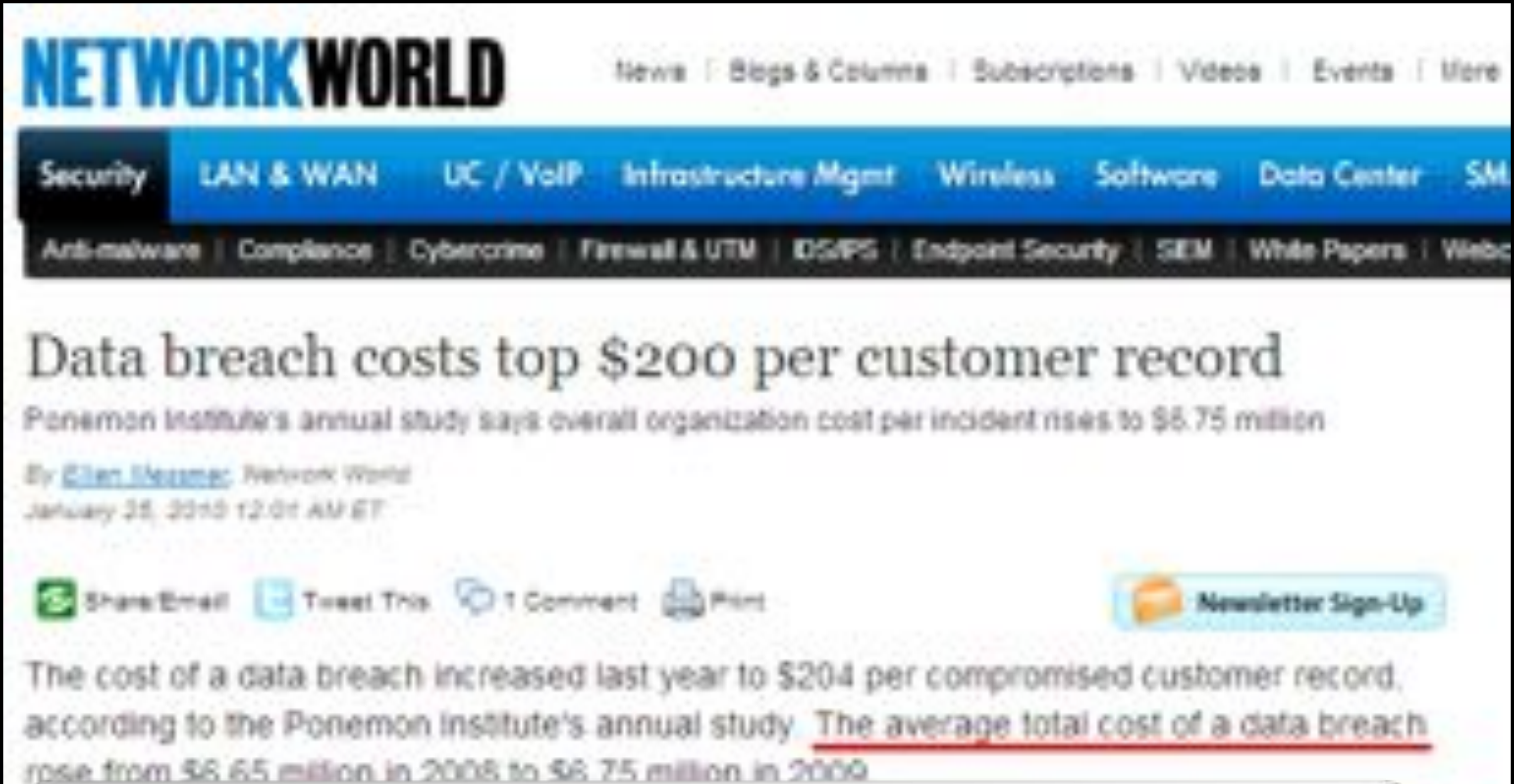
Jan 31, 2011:
“Online dating Web site **PlentyOfFish.com** has been hacked, exposing the **personal information and passwords** associated with almost **30 million accounts“**

Top Web Attack Impacts



- Source: webappsec.org

Lost Record Cost Rises



NETWORKWORLD
News | Blogs & Columns | Subscriptions | Videos | Events | More
Security | LAN & WAN | UC / VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SM
Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SEM | White Papers | Webc
Share/Email | Tweet This | 1 Comment | Print
Newsletter Sign-Up

Data breach costs top $200 per customer record

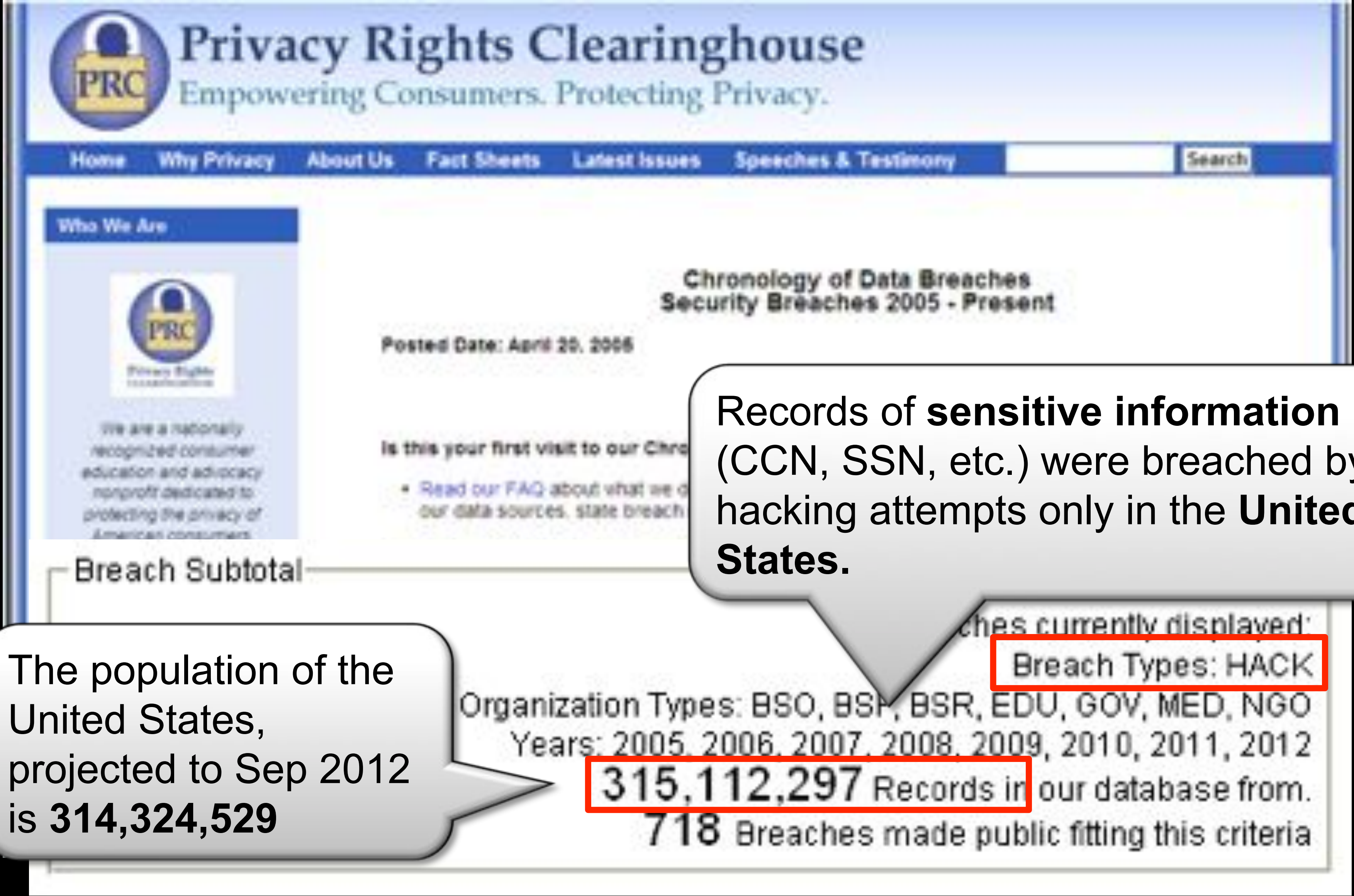
Ponemon Institute's annual study says overall organization cost per incident rises to $6.75 million

By Ellen Messmer, Network World
January 25, 2010 12:01 AM ET

The cost of a data breach increased last year to $204 per compromised customer record, according to the Ponemon Institute's annual study. The average total cost of a data breach rose from $6.65 million in 2008 to $6.75 million in 2009.

The average total cost of a data breach rose to **$6.75 million** in 2009

Millions of Records Breached



Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

We are a nationally recognized consumer education and advocacy nonprofit dedicated to protecting the privacy of American consumers

Chronology of Data Breaches
Security Breaches 2005 - Present

Posted Date: April 20, 2005

Is this your first visit to our Chro

- Read our FAQ about what we d
our data sources, state breach

Breach Subtotal

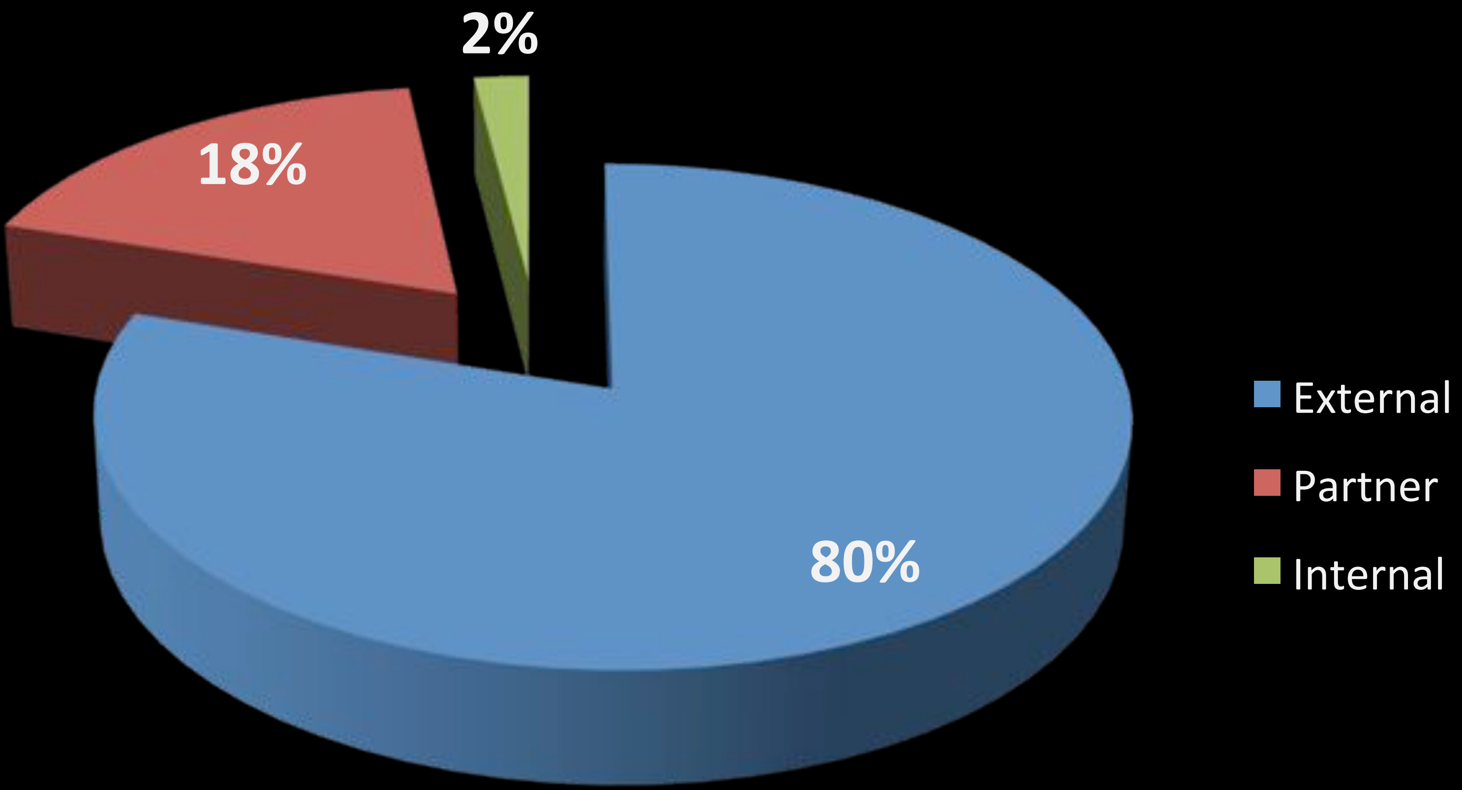
ches currently displayed:
Breach Types: HACK
Organization Types: BSO, BSP, BSR, EDU, GOV, MED, NGO
Years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012
315,112,297 Records in our database from.
718 Breaches made public fitting this criteria

Records of **sensitive information** (CCN, SSN, etc.) were breached by hacking attempts only in the **United States.**

The population of the United States, projected to Sep 2012 is **314,324,529**

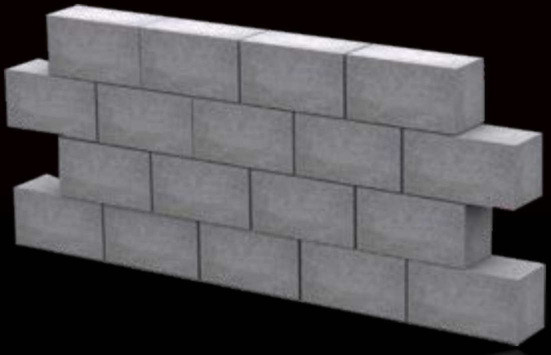
radware

Source of Breach



- Source: 7safe.com

Countermeasures: Web Application Firewall



radware

Mapping Security Protection Tools

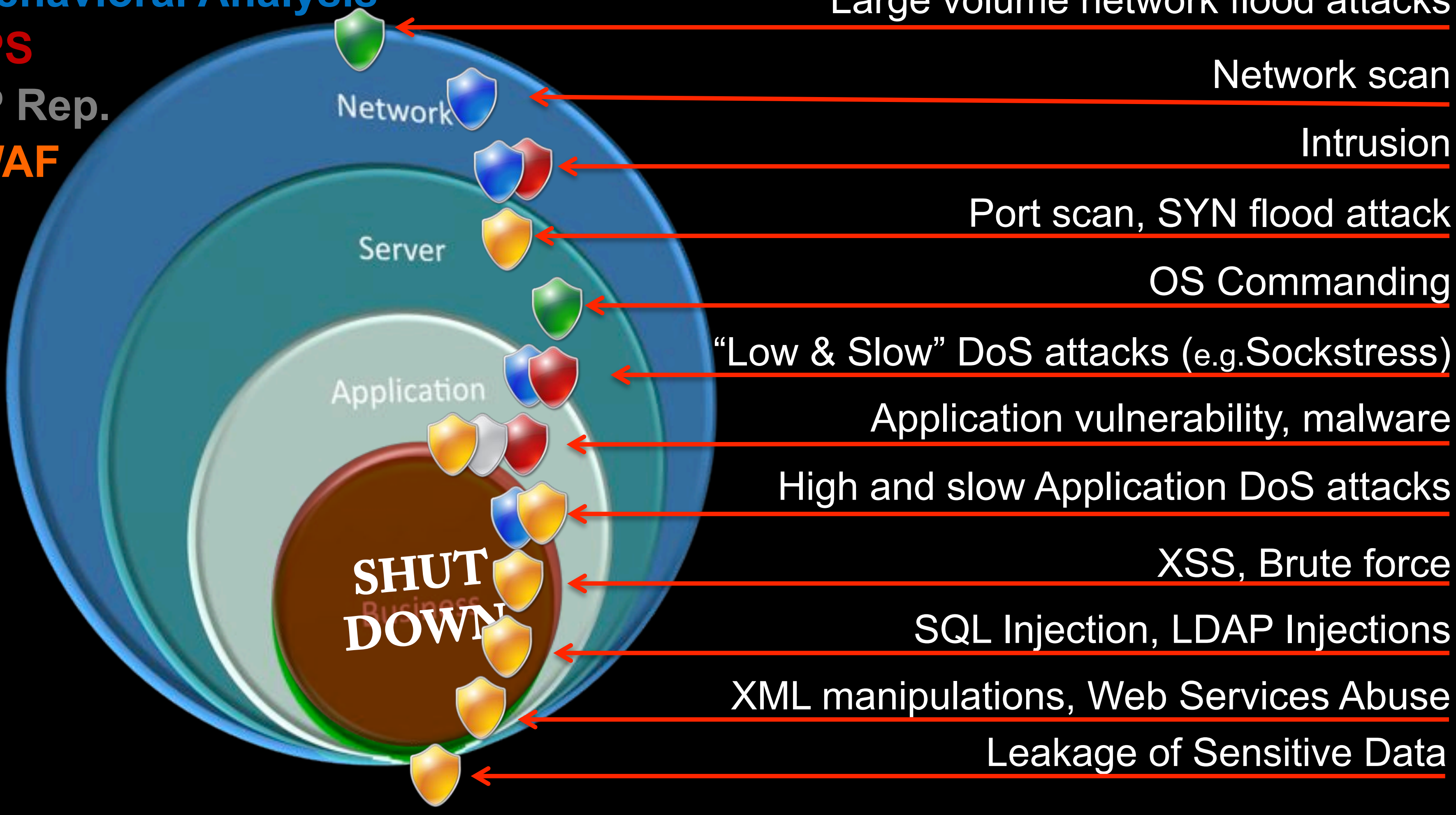
DoS Protection

Behavioral Analysis

IPS

IP Rep.

WAF



Large volume network flood attacks

Network scan

Intrusion

Port scan, SYN flood attack

OS Commanding

“Low & Slow” DoS attacks (e.g.Sockstress)

Application vulnerability, malware

High and slow Application DoS attacks

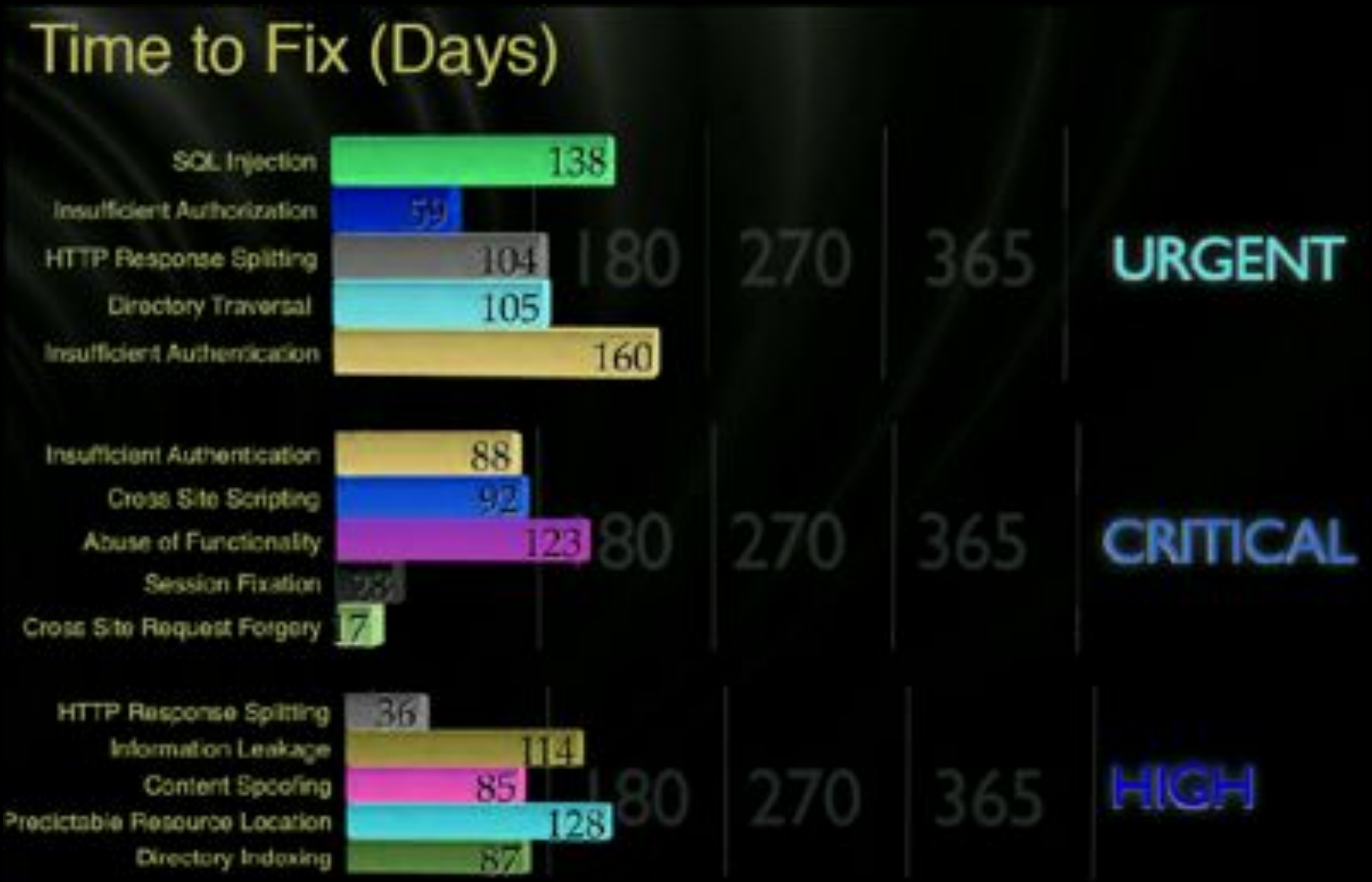
XSS, Brute force

SQL Injection, LDAP Injections

XML manipulations, Web Services Abuse

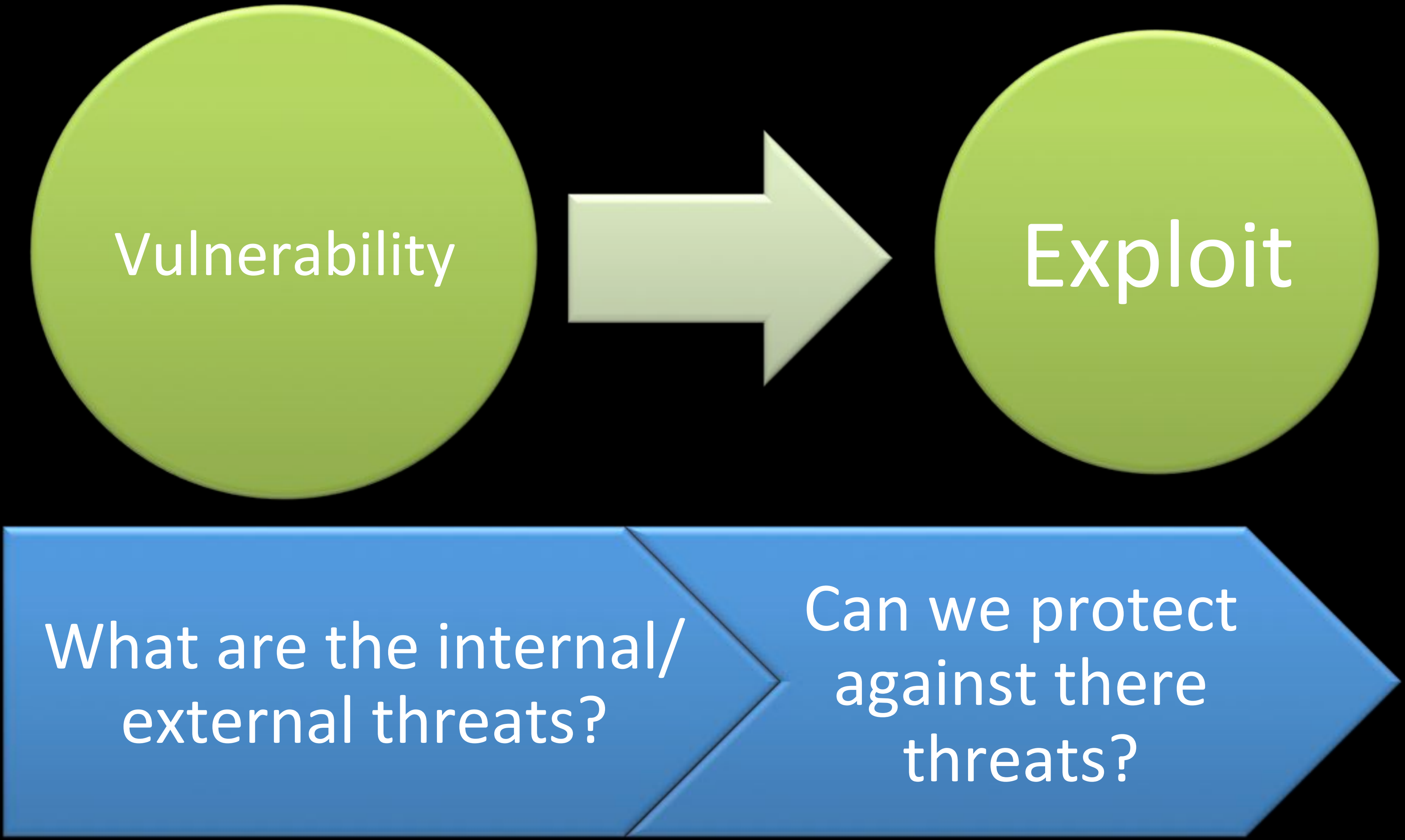
Leakage of Sensitive Data

Cost Effective, Time to Security



Source: WhiteHat Security

Security Intelligence Timeline



Vulnerability

Exploit

What are the internal/ external threats?

Can we protect against there threats?

Why WAF

Time to Security

Centralized Security

Protect 3rd Party Modules

No App Modification

Security While App Changes

Application Visibility

Cost Effective

WAF Selection Considerations

radware

Mapping Your Requirements - Essential

- Zero Day vs. Know attacks
- False Negative vs. False Positive
- Time to Security
- Auto Policy Generation
- Performance / Scalability

Mapping Your Requirements - Advanced

- Cost of Ownership
- Changes to Existing Environment
- Inline vs. out-of-path
- Reverse Proxy vs. Bridge
- Level of Protection

radware Standard Web Application Protection

Data Leak Prevention

- Credit card number (CCN) / Social Security (SSN)
- Regular Expression

Terminate TCP, Normalize, HTTP RFC

- Evasions
- HTTP response splitting (HRS)

Signature & Rule Protection

- Cross site scripting (XSS)
- SQL injection, LDAP injection, OS commanding

radware Advanced Web Application Protection

Parameters Inspection	• Buffer overflow (BO) • Zero-day attacks
User Behavior	• Cross site request forgery • Cookie poisoning, session hijacking
Layer 7 ACL	• Folder / file level access control • White listing or black listing
XML & Web Services	• XML Validity and schema enforcement
Role Based Policy	• Authentication • User Tracking

Priorities make things happen

Summary

Smart Network. Smart Business.

radware

AGENDA

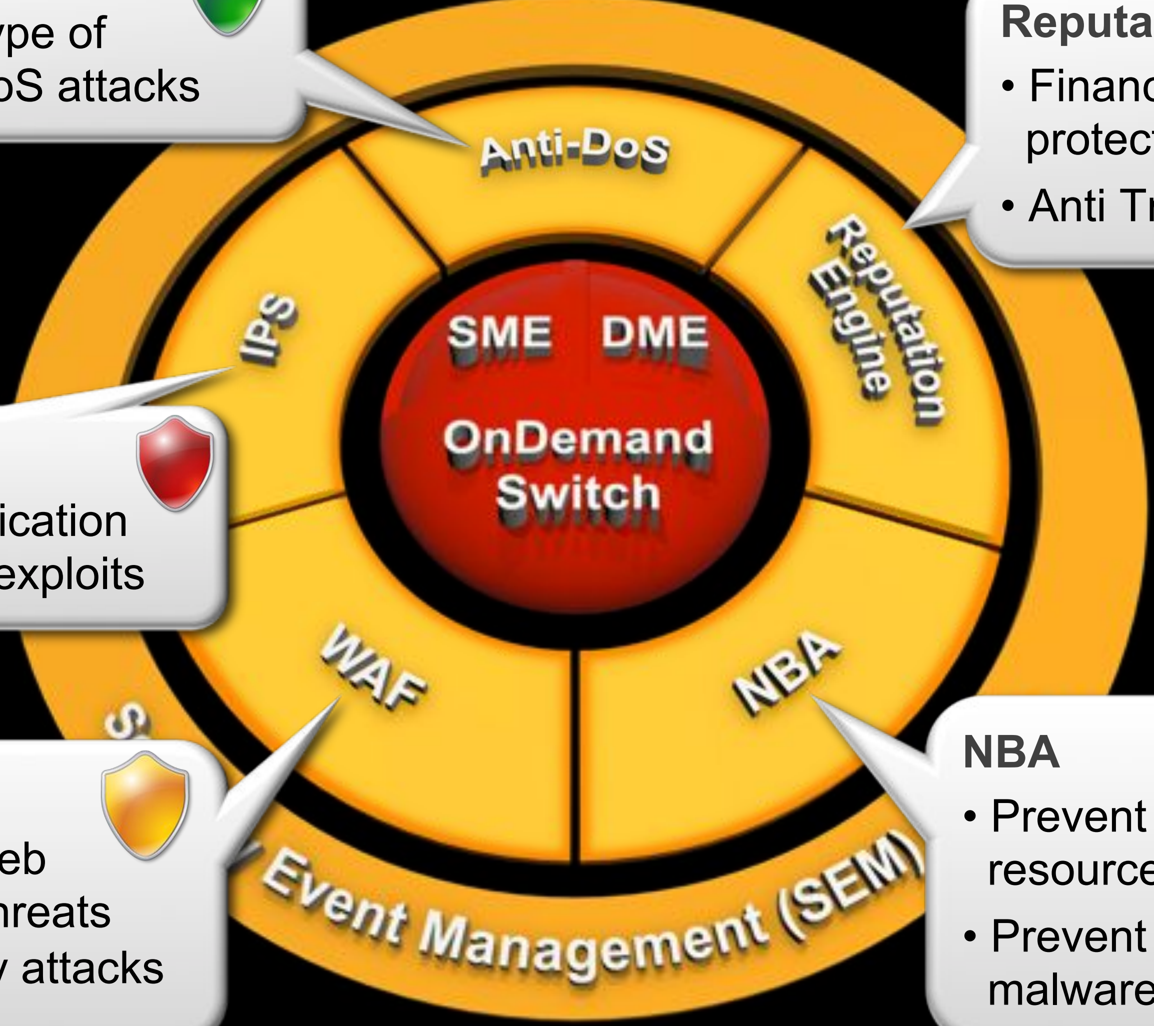
Cyberwar: The Web App Aspect

Web Application Security Challenge

Countermeasure: WAF

Selection Considerations

radware



DoS Protection

- Prevent all type of network DDoS attacks

Reputation Engine

- Financial fraud protection
- Anti Trojan & Phishing

IPS

- Prevent application vulnerability exploits

WAF

- Mitigating Web application threats and zero-day attacks

NBA

- Prevent application resource misuse
- Prevent zero-minute malware

radware

Thank You

Reputation Engine
IPS
WAF
AMS
NBA
Anti-DoS
Security Event & Information Management