

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

Securing Your Applications & Data Survival In An Evolving Threat Landscape

Alexander Krakhofer





► Cyberwar: The Web App Aspect

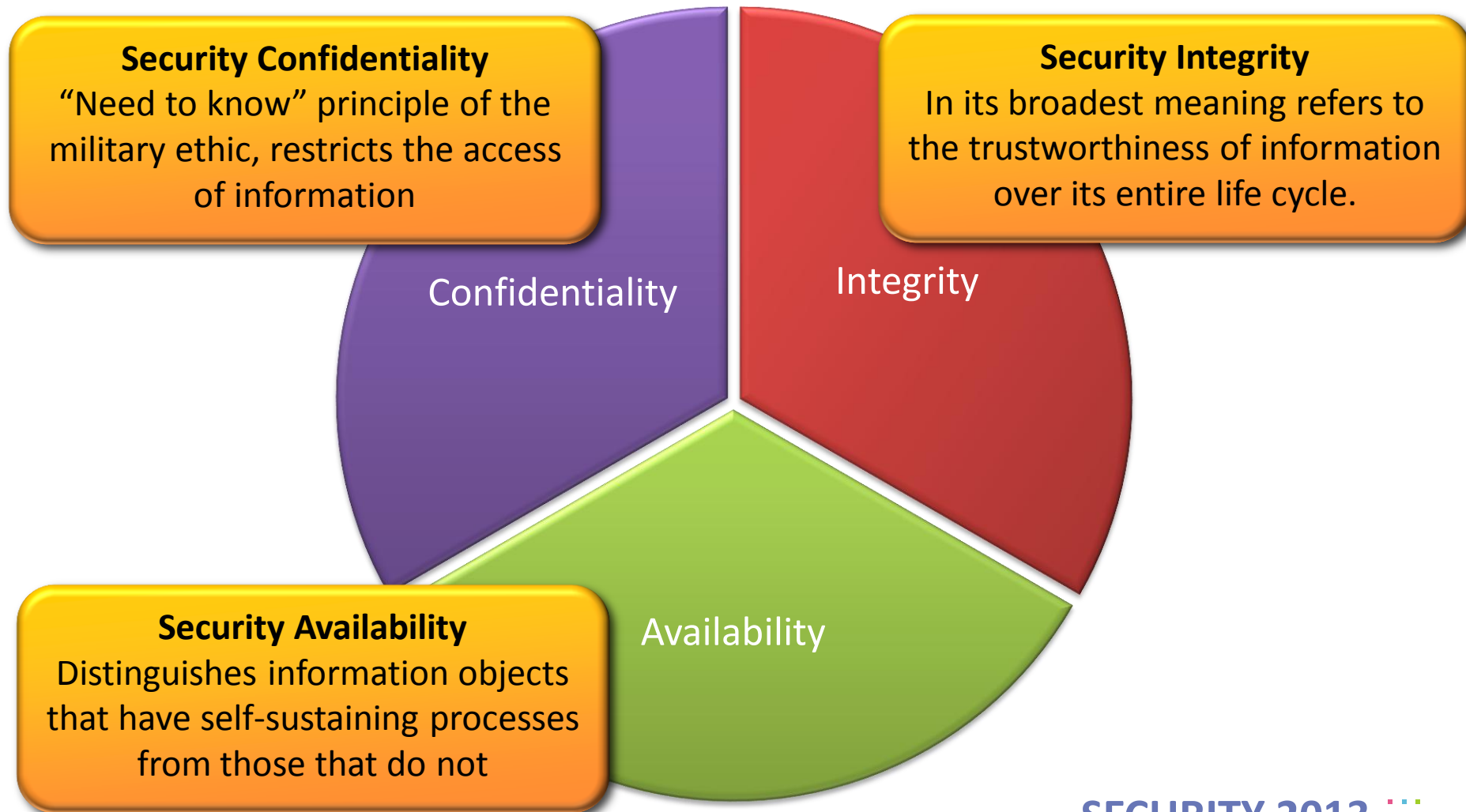
The Evolving Threat Landscape

Securing Tomorrow's Perimeter



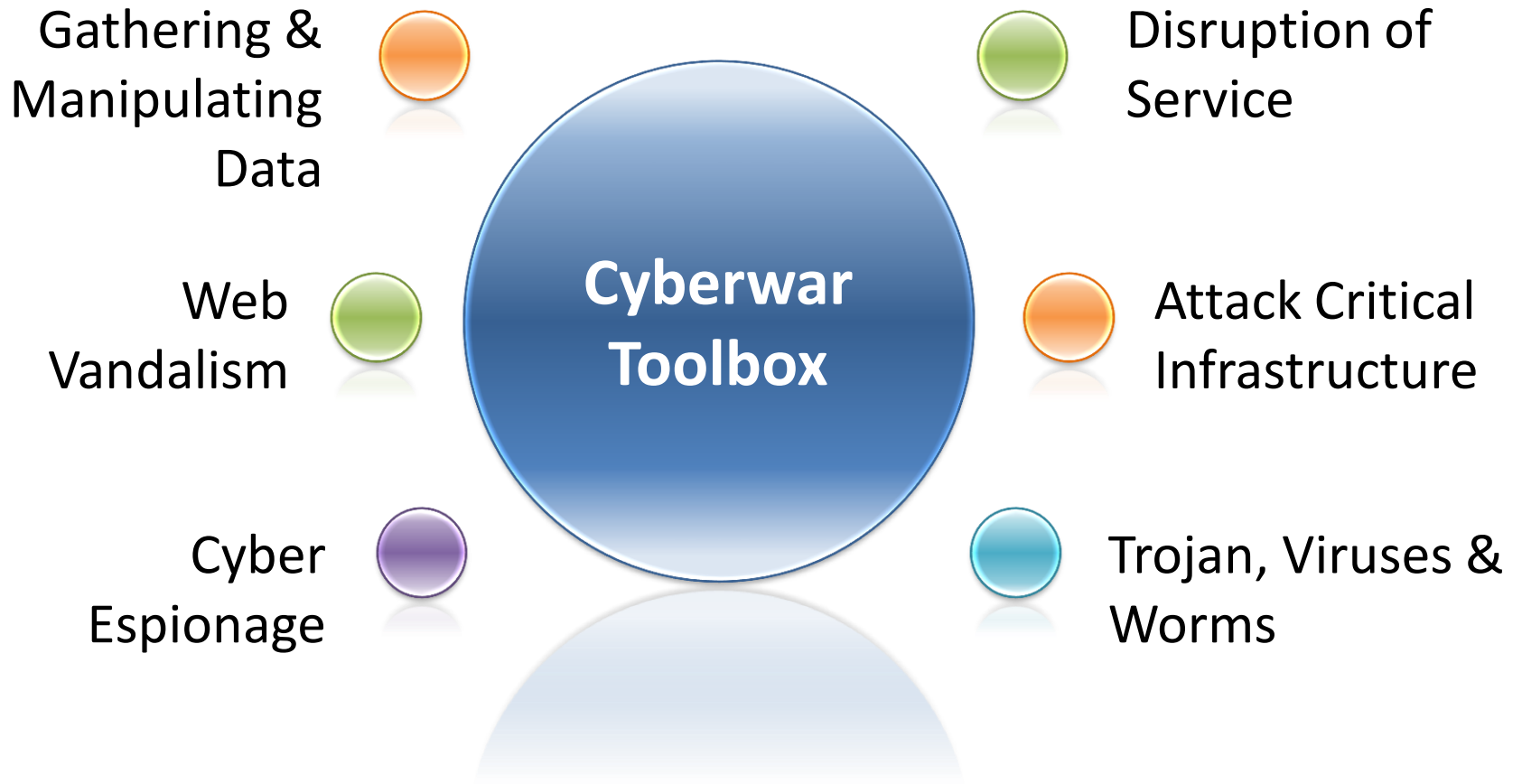


The Security Trinity



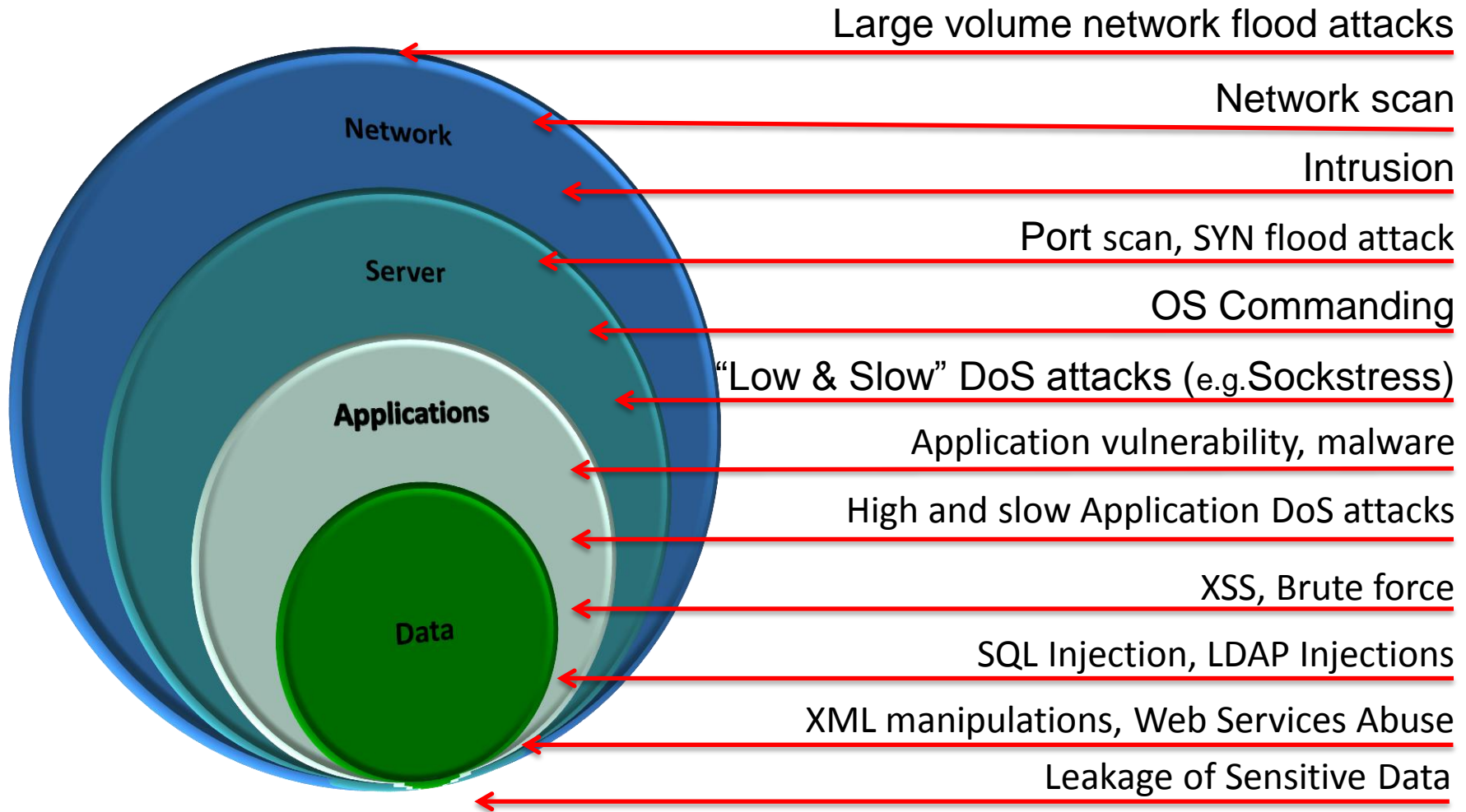


The Cyber Attack Vectors





Targeting Different Layers





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 cyberwar

The ongoing cyberwar between

capabilities
ilities to

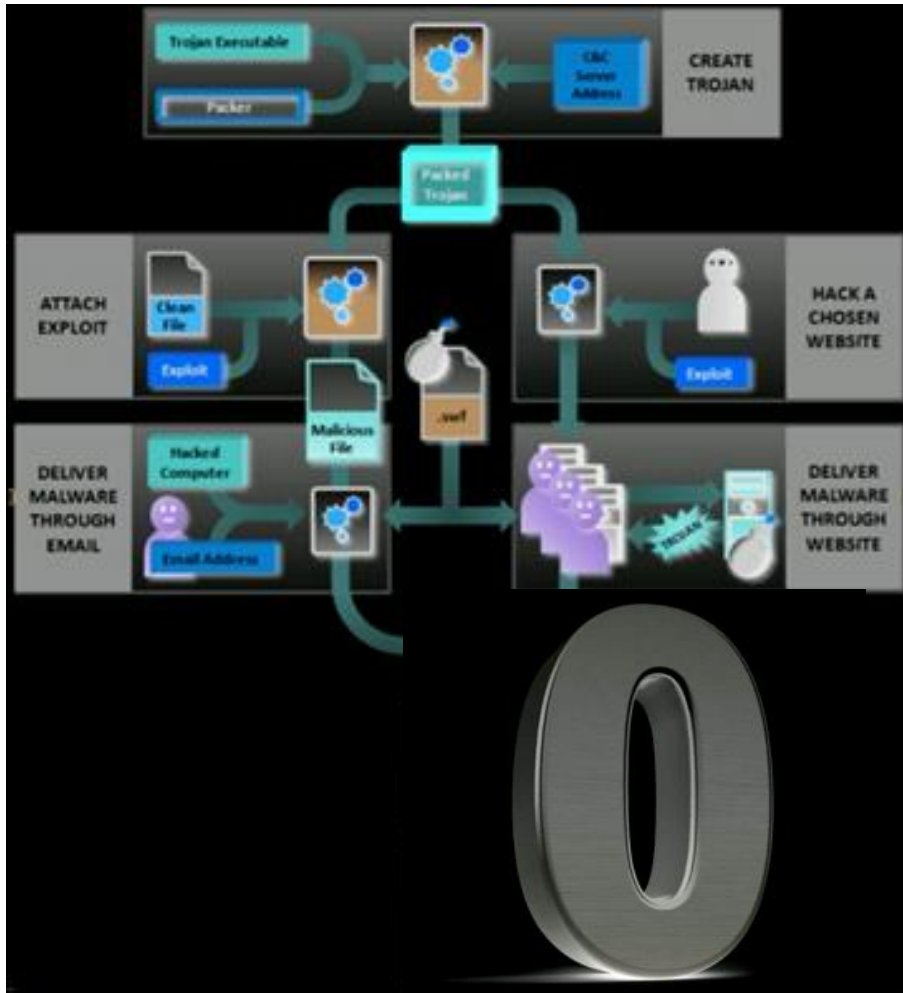
July 6, 2012

Pentagon Digs In on Cyberwar Front

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

can
hackers take

Cyberwar – The Web App Aspect

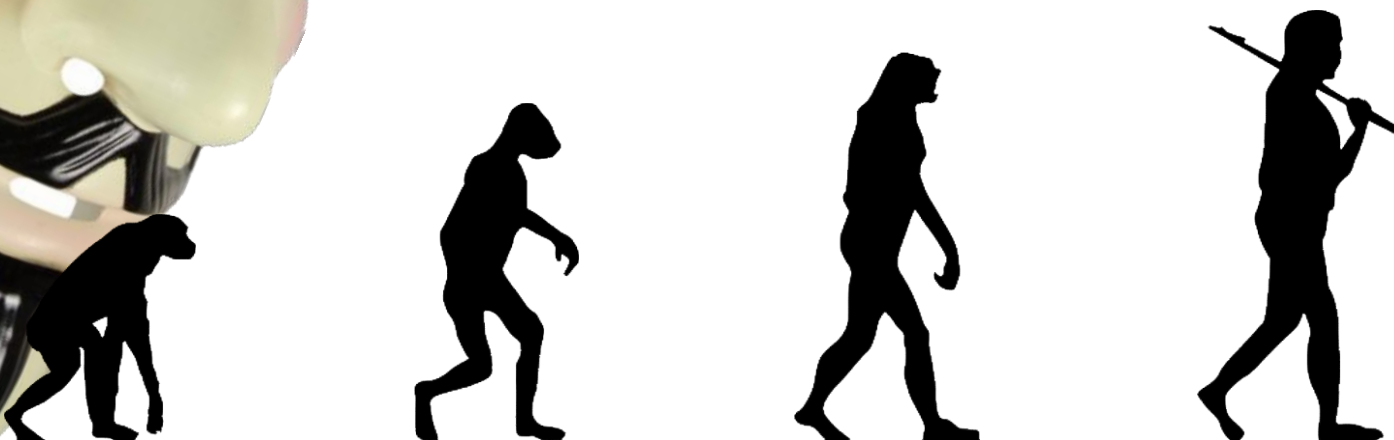




Cyberwar: The Web App Aspect

▶ The Evolving Threat Landscape

Securing Tomorrow's Perimeter



SECURITY 2

AGENDA

Web Apps are Easy to Exploit

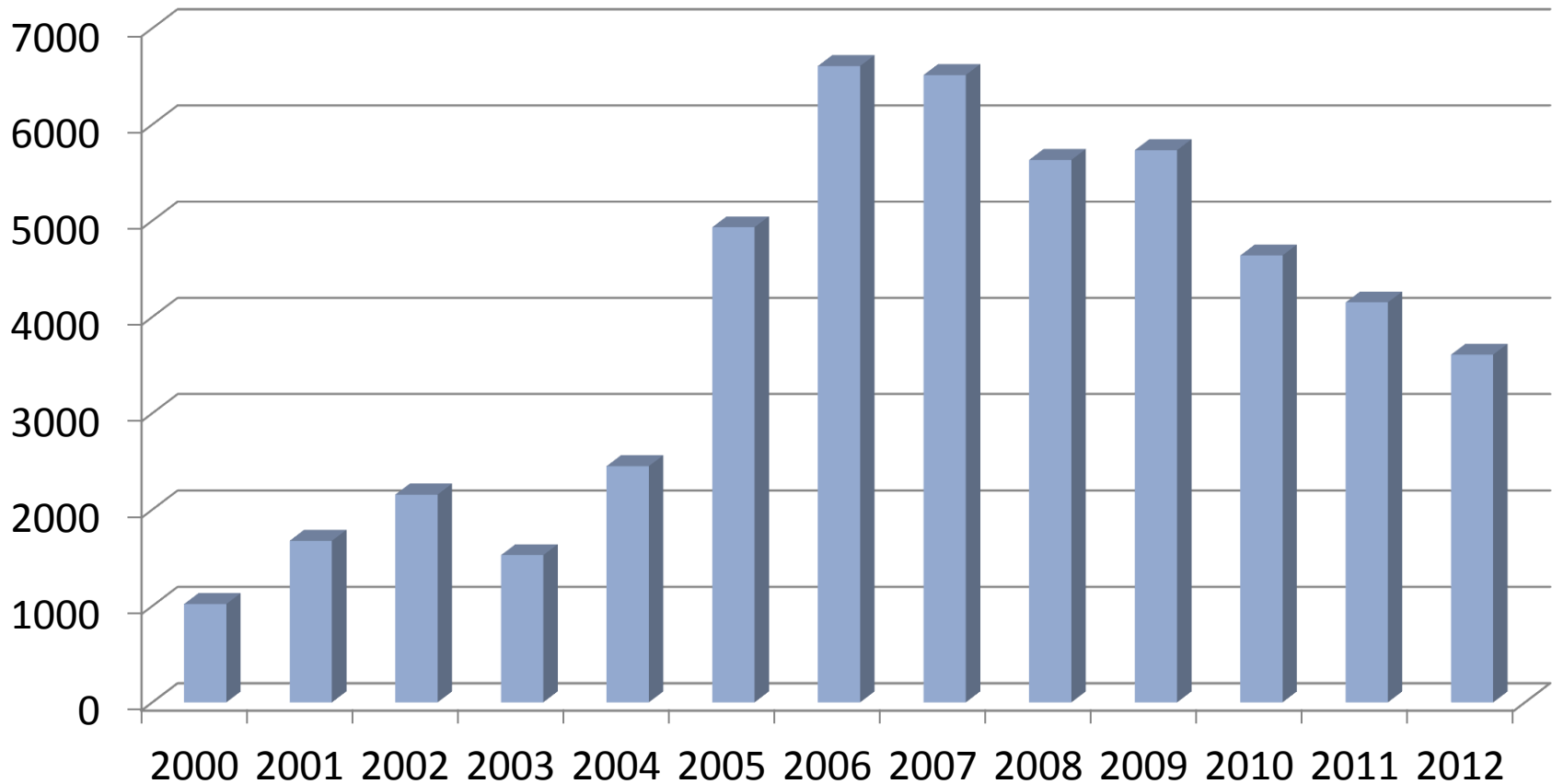
- Whole system open to attack
- Can target different layers
- Thousands of Web security vulnerabilities
- Minimal attention to security during development
- Traditional defences inadequate

**All they need is a
browser**



Thousands of Vulnerabilities Every Year

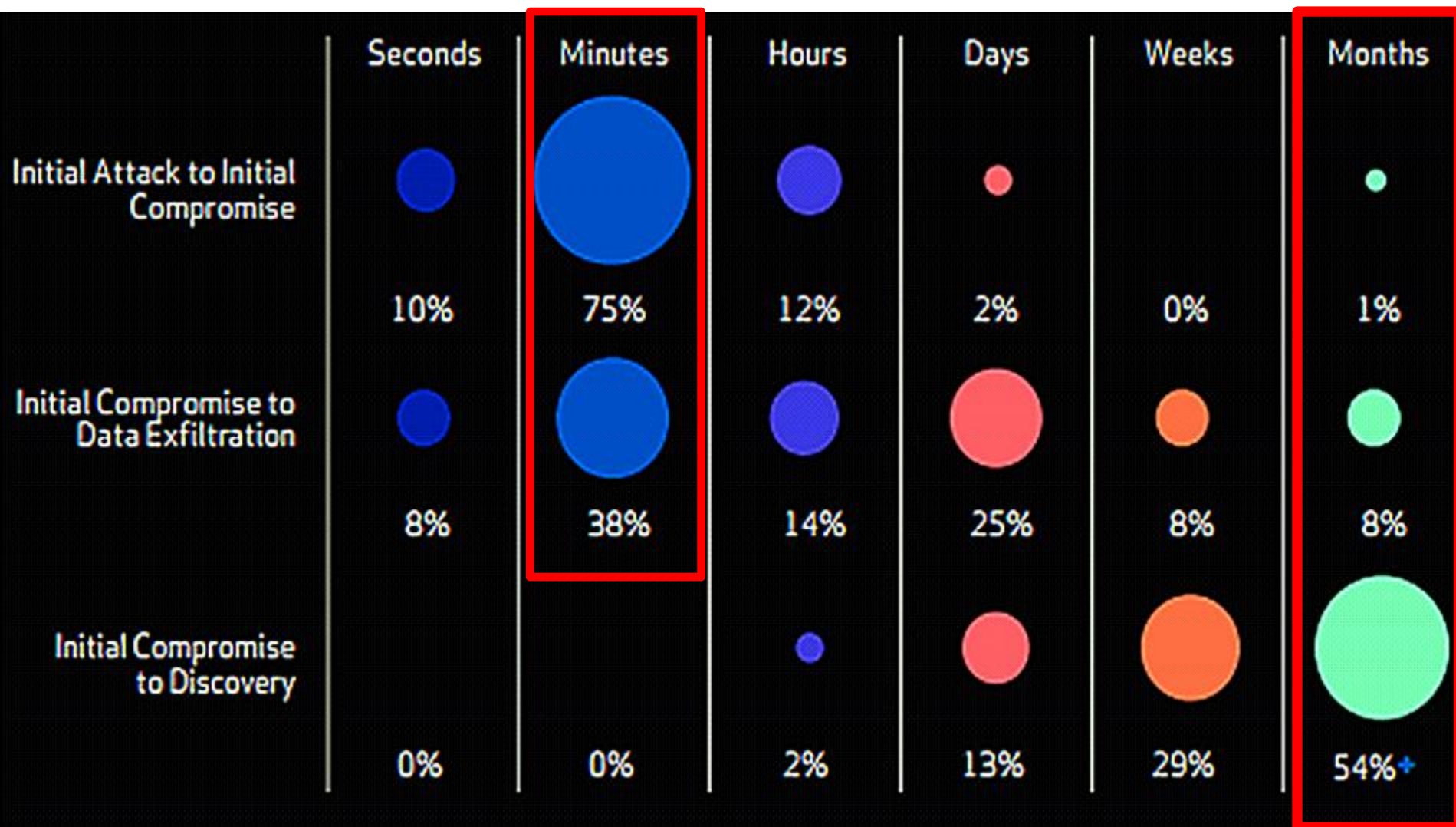
of Vulnerabilities



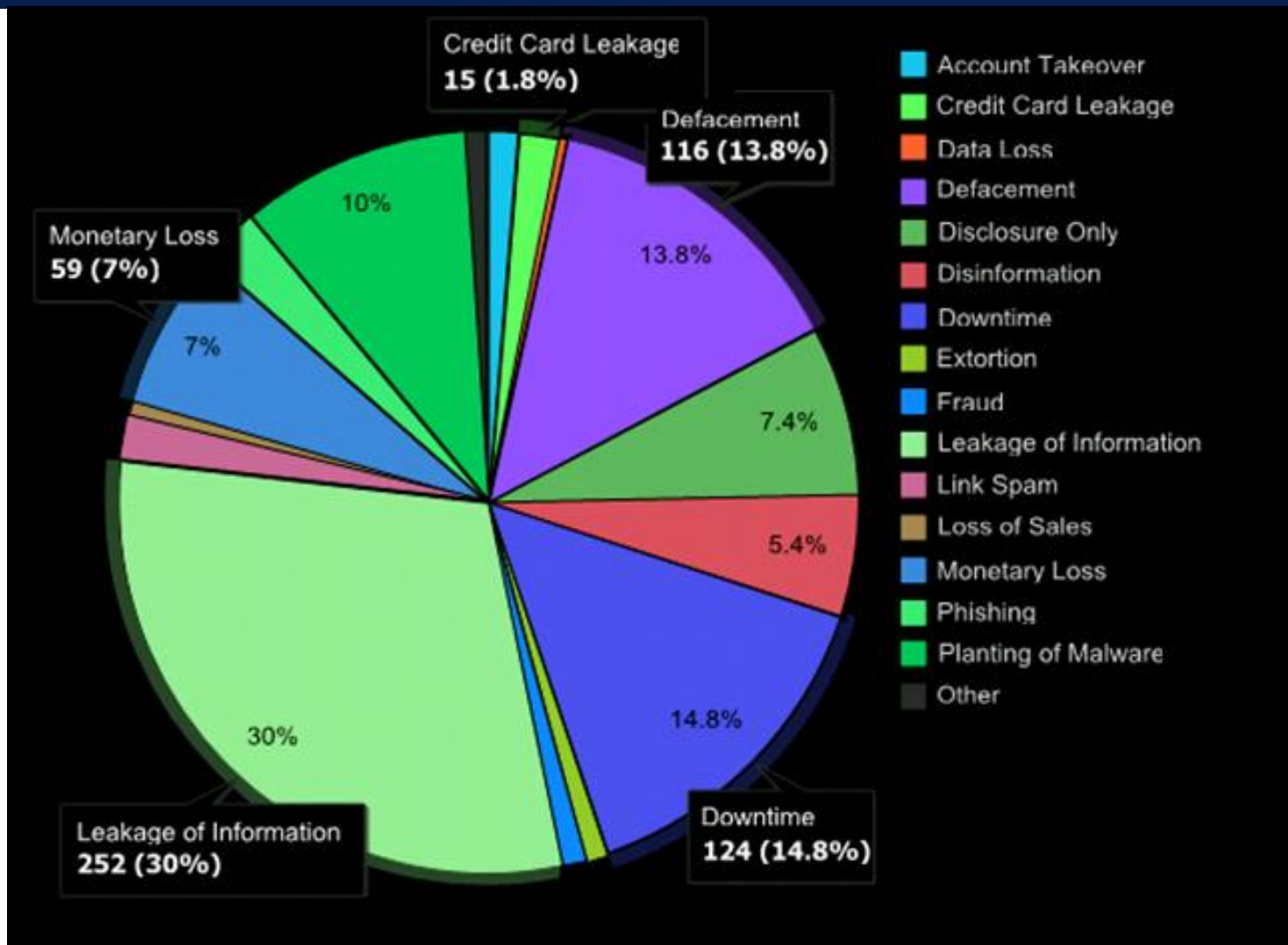
- Source: National Vulnerabilities Database



Minutes to Compromise, Months to Discover




Top Web Attack Impacts



■ Source: webappsec.org

Millions of Records Breached



Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

Home Why Privacy About Us Fact Sheets Latest Issues Speeches & Testimony Search

Who We Are


Privacy Rights Clearinghouse

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 Chronology of Data Breaches page?

- [Read our FAQ](#) about what we do, our data sources, state breach laws, and more.

Breach Subtotal

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

Records currently displayed:

Breach Types: HACK

Organization Types: BSO, BSH, BSR, EDU, GOV, MED, NGO

Years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012

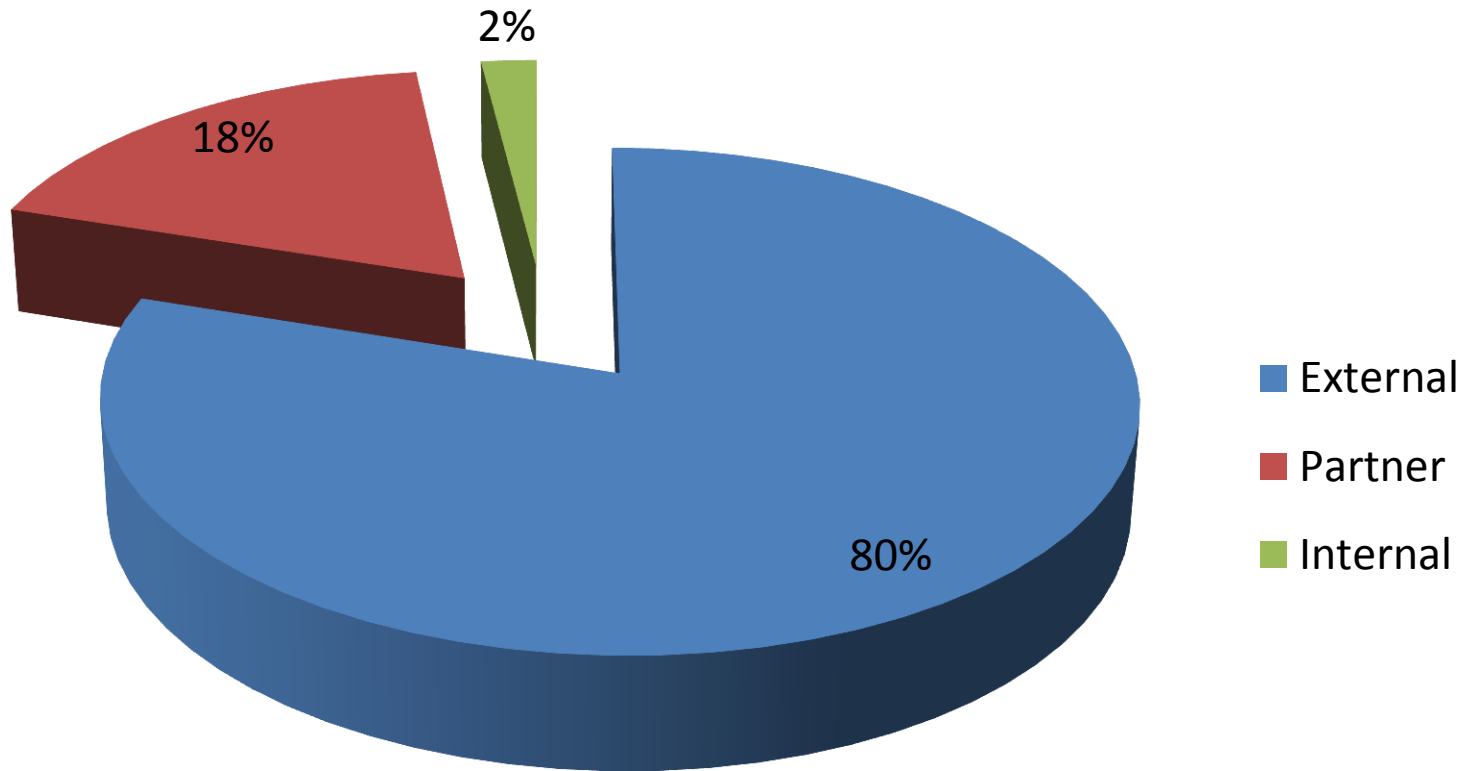
315,112,297 Records in our database from.

718 Breaches made public fitting this criteria

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



Source of Breach



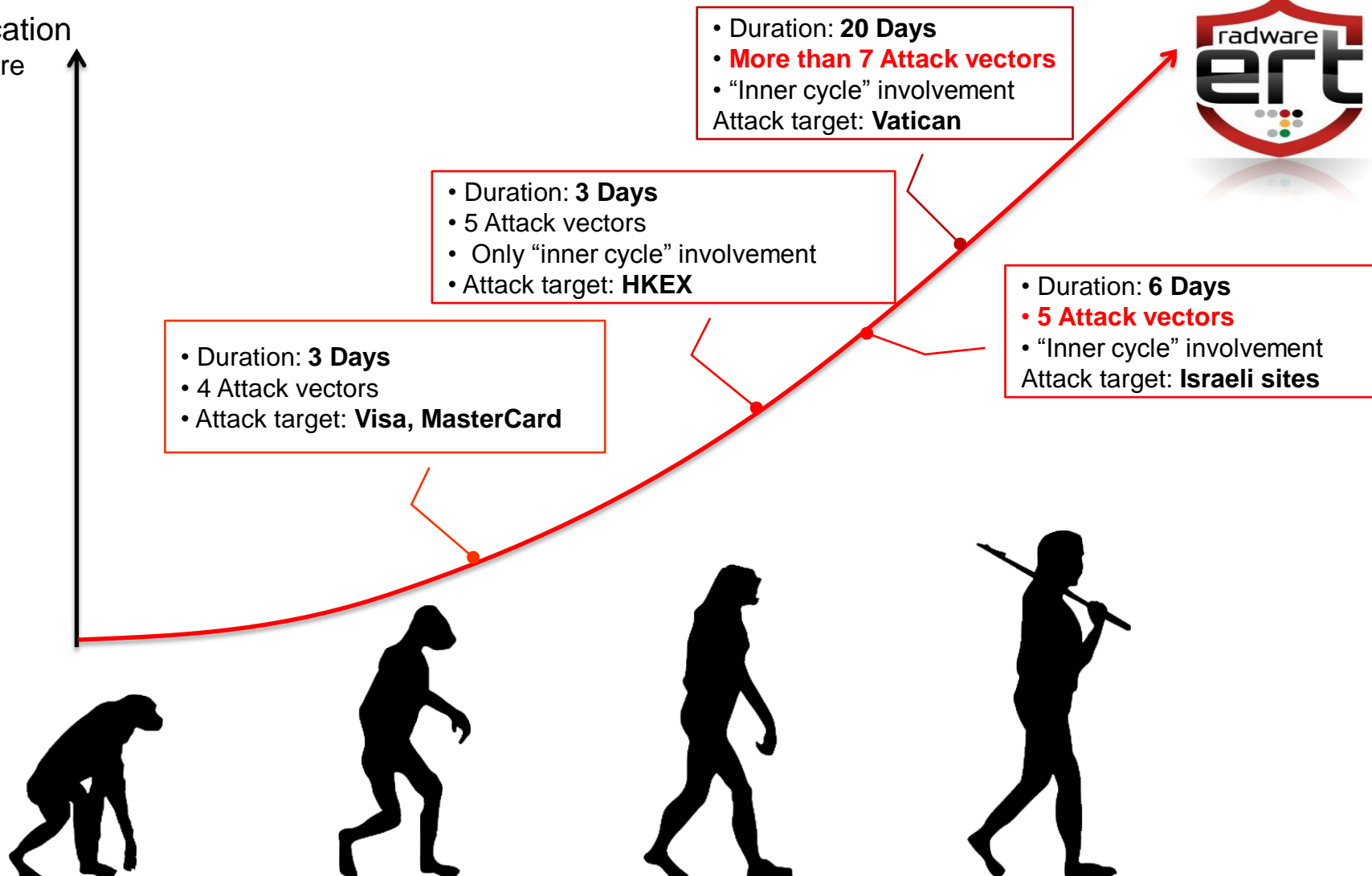
- Source: 7safe.com



Hacktivism - Becomes More Campaign Blend-APT Oriented



Sophistication
measure





The Impact

Confidentiality



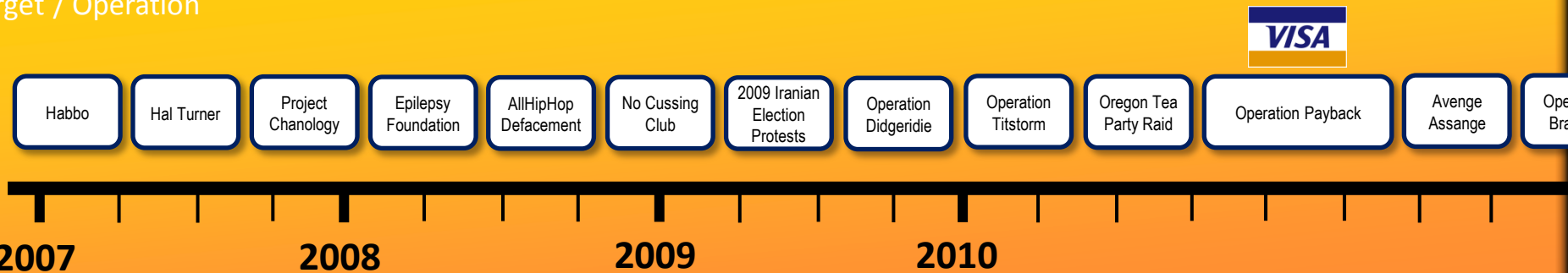
Integrity



Availability



Target / Operation





Cyberwar: The Web App Aspect

The Evolving Threat Landscape

▶ Securing Tomorrow's Perimeter

SECURITY 2

AGENDA

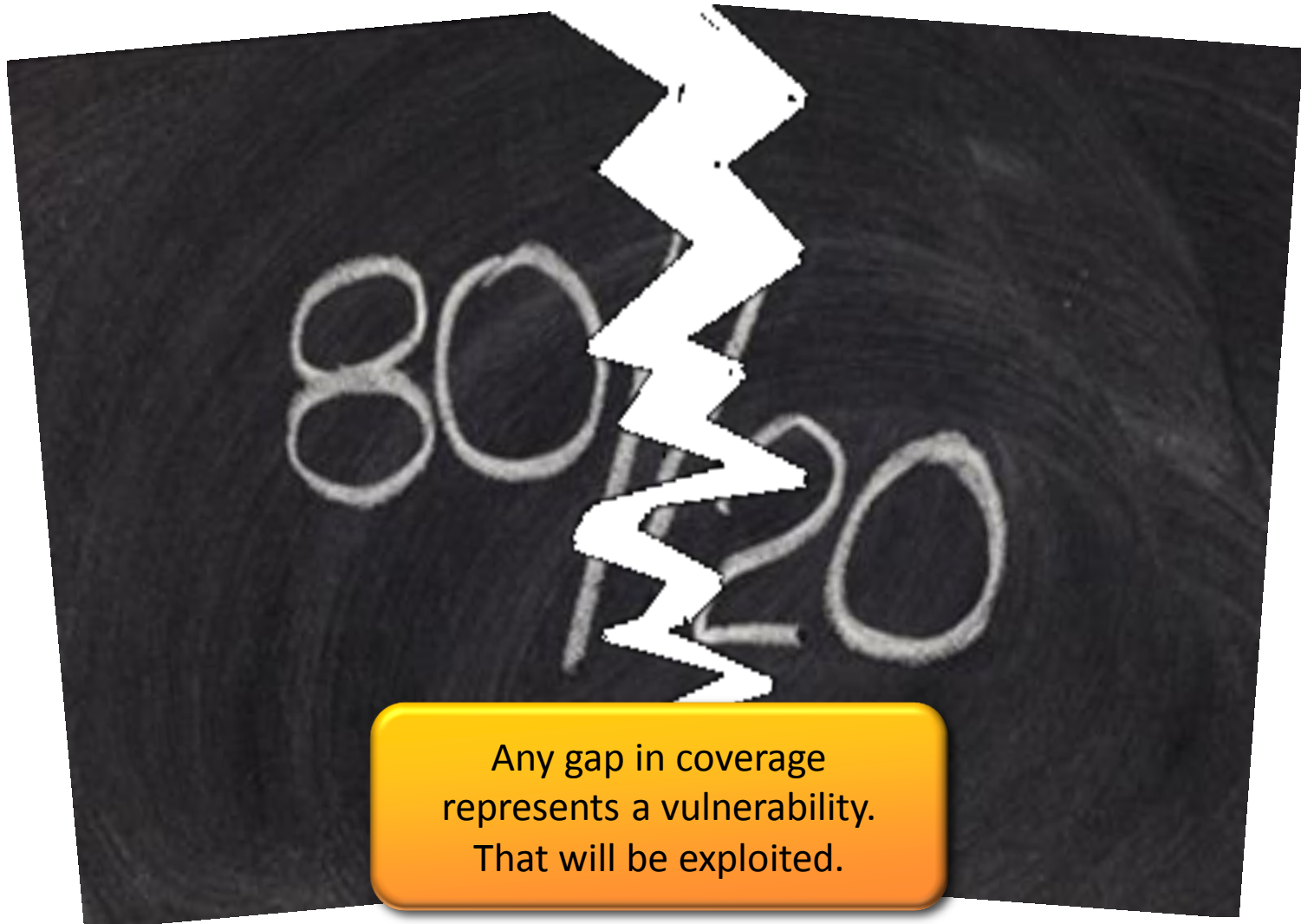


Perimeter Defense Planning





Perimeter Defense Planning





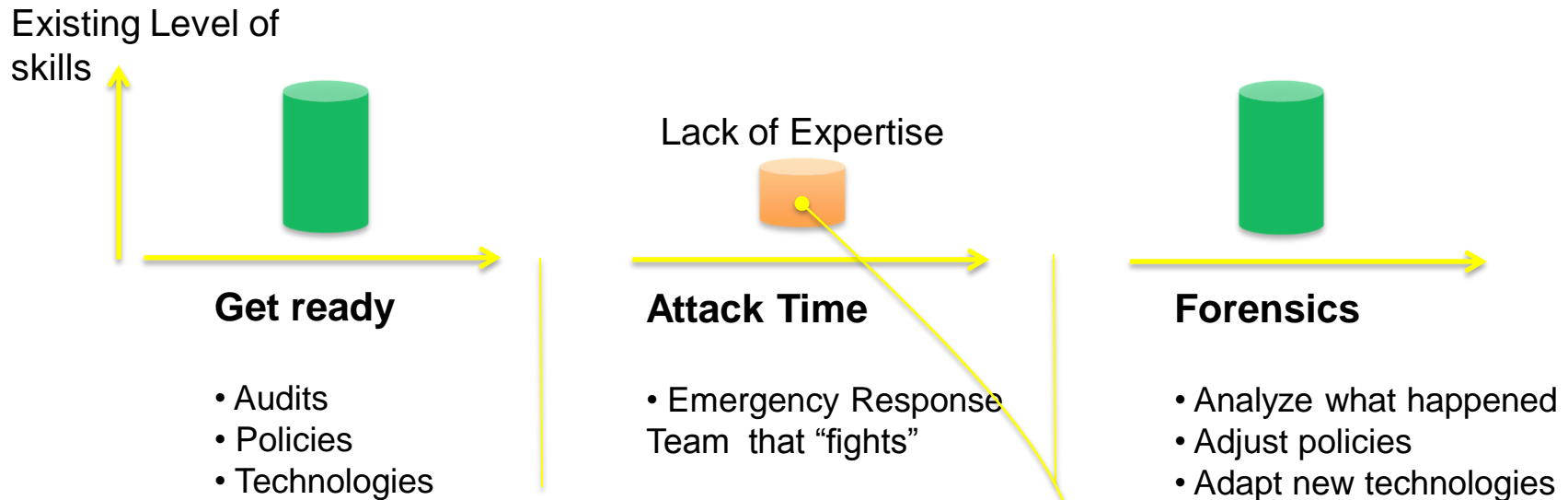
Perimeter Defense Planning



SECURITY 2013 



Emergency Response Teams & Cyber War Rooms



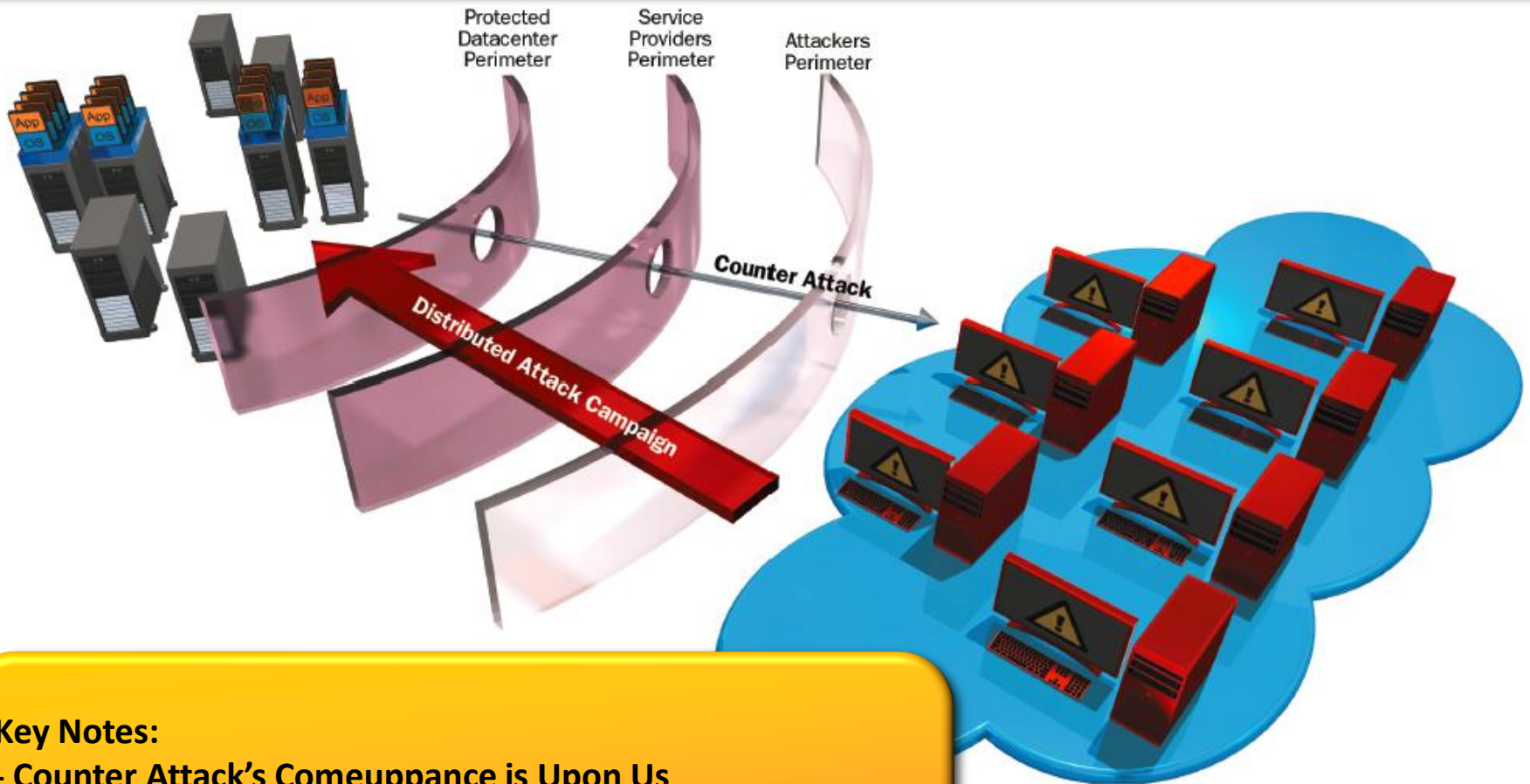
■ Required expertise during attack campaign

- Complex risk assessment
- Tracking and modifying protections against dynamically evolved attacks
- Real time intelligence
- Real time collaboration with other parties
- Counter attack methods and plans
- Preparation with cyber “war games”

Strategy



The Best Defense Is A...



Key Notes:

- Counter Attack's Comeuppance is Upon Us
- Key IR Assumptions are wrong – e.g. Law enforcement
- Attack Mitigation Talent is Low. Knowledge must increase.
- Corporate Policies are IR not ERT focused



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

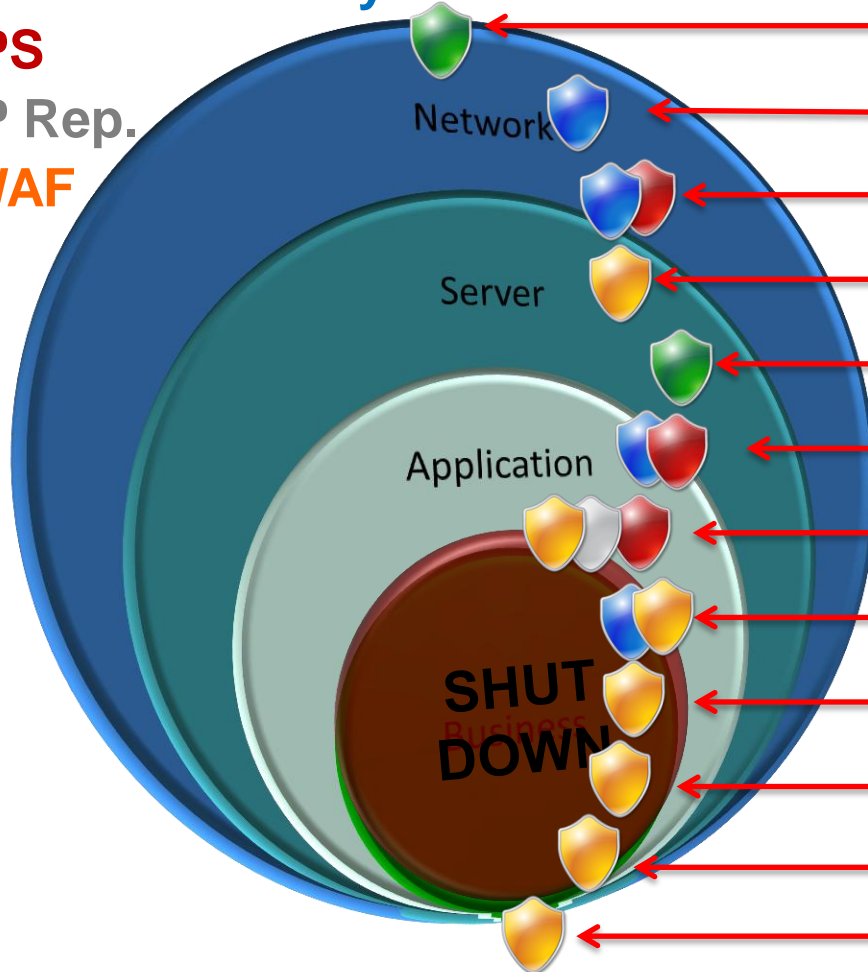
High and slow Application DoS attacks

XSS, Brute force

SQL Injection, LDAP Injections

XML manipulations, Web Services Abuse

Leakage of Sensitive Data





Conclusion

- Attackers deploy multi-vulnerability attack campaigns
 - Organizations deploy point security solutions
 - Attackers target for blind spots
- Companies need a solution that:
 - Can defend against emerging cyber attack campaigns
 - Has no blind spots in network & application security
- Customer success: best security solution for
 - Online business protection
 - Data center protection

<http://edition.cnn.com/video/#/video/bestoftv/2013/01/09/exp-tsr-todd-us-banks-hacked-iran.cnn?iref=allsearch>





What Changed in Security in 2012?

In 2012, we saw a new cyber security trend a consistent and steady increase in advanced and persistent DoS and DDoS attack campaigns. These campaigns have multiple attack vectors, are longer in duration and are more complex. Nowadays it's common to see attacks with four, five, or even ten attack vectors, lasting last three days, a week or even a month. This new trend of advanced and persistent threats creates big challenges and organizations are not prepared.

Organizations Are Bringing a Knife to a Gunfight!

Download Security report 2012 from

<http://www.radware.com/Resources/rcip.aspx?campaign=1630844> !

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Alexander Krakhofer



alexanderk@radware.com

