



Network & Application Availability in an Evolving Threat Environment



Howard Teicher
VP, Public Sector, Radware

Delaware Cyber Workshop
February 2013



Anatomy of an Attack

The Evolving Threat Landscape

Securing Tomorrow's Perimeter

AGENDA

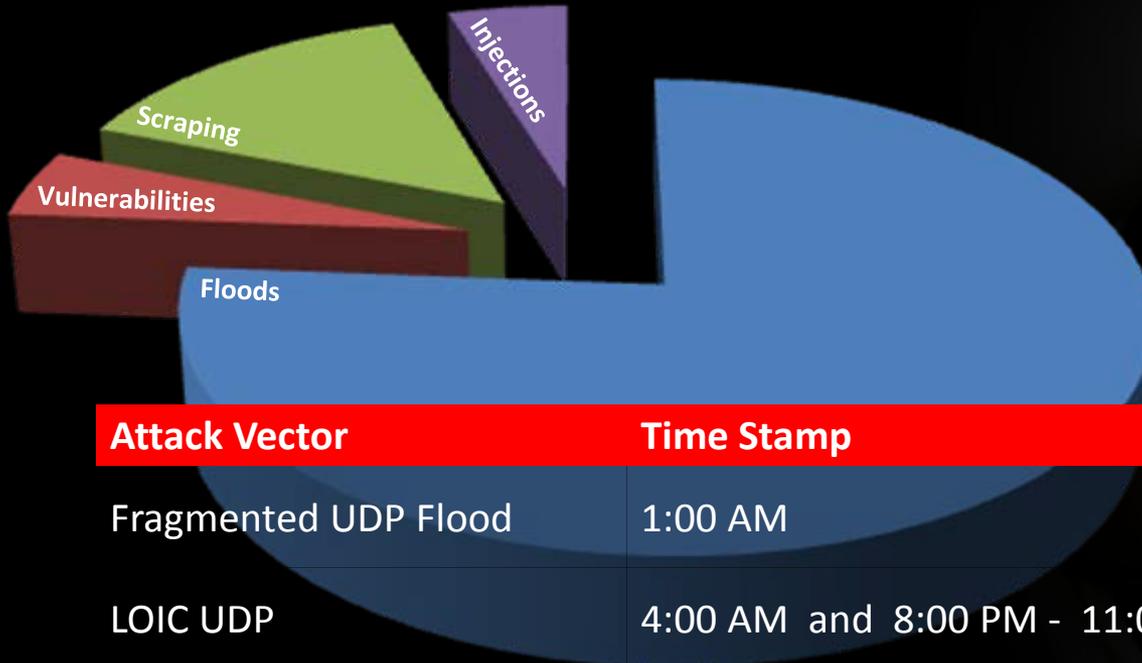


► Anatomy of an Attack

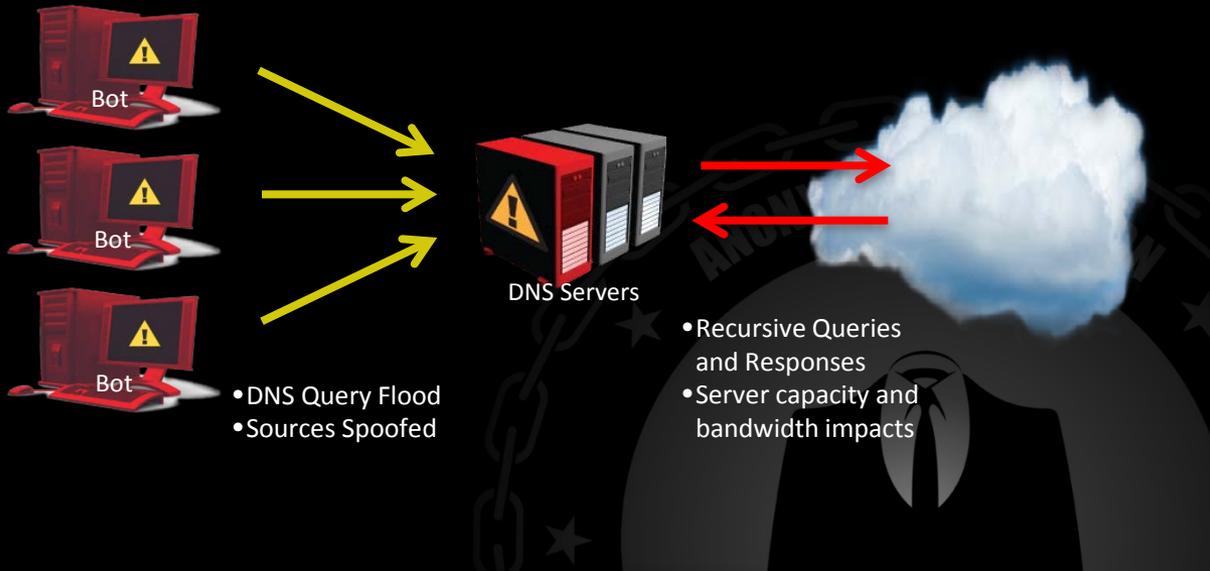
The Evolving Threat Landscape

Securing Tomorrow's Perimeter

AGENDA



Attack Vector	Time Stamp	Attack Peak
Fragmented UDP Flood	1:00 AM	95 Mbps 10K PPS
LOIC UDP	4:00 AM and 8:00 PM - 11:00 PM	50 Mbps 5K PPS
TCP SYN Flood	1:40 PM	13.6 Mbps 24K PPS
R.U.D.Y	4:00 PM	2.1 Mbps 0.7K PPS
LOIC TCP	11:00 PM - 3:30 AM	500 Kbps 0.2K PPS
Mobile LOIC	6:00 PM- 8:30 PM	86 Kbps 13 PPS
#RefRef	9:45 PM	Few packets



- 1M DNS Queries per second for random domains which the servers were not authoritative
- Servers initiated recursive queries, but consumed an impossible amount of recursive service resources

Time Stamp	Standard Query
8:56 PM	...
8:56 PM	vihuqot.info
8:56 PM	vowebuc.info
8:56 PM	qeguwaq.info
8:56 PM	kevycyd.info
8:56 PM	gohakow.info
8:56 PM	cicevut.info
8:56 PM	wexyral.info
8:56 PM	hacakoz.info
8:56 PM	lyrevyn.info
8:56 PM	tucidyp.info
8:56 PM	xugevyj.info
8:56 PM	sivajob.info
8:56 PM	lygolan.info
8:56 PM	ryhodyl.info
8:56 PM	jejycex.info
8:56 PM	...

Security Confidentiality,

a mainstream adaptation of the “need to know” principle of the military ethic, restricts the access of information to those systems, processes and recipients from which the content was intended to be exposed.

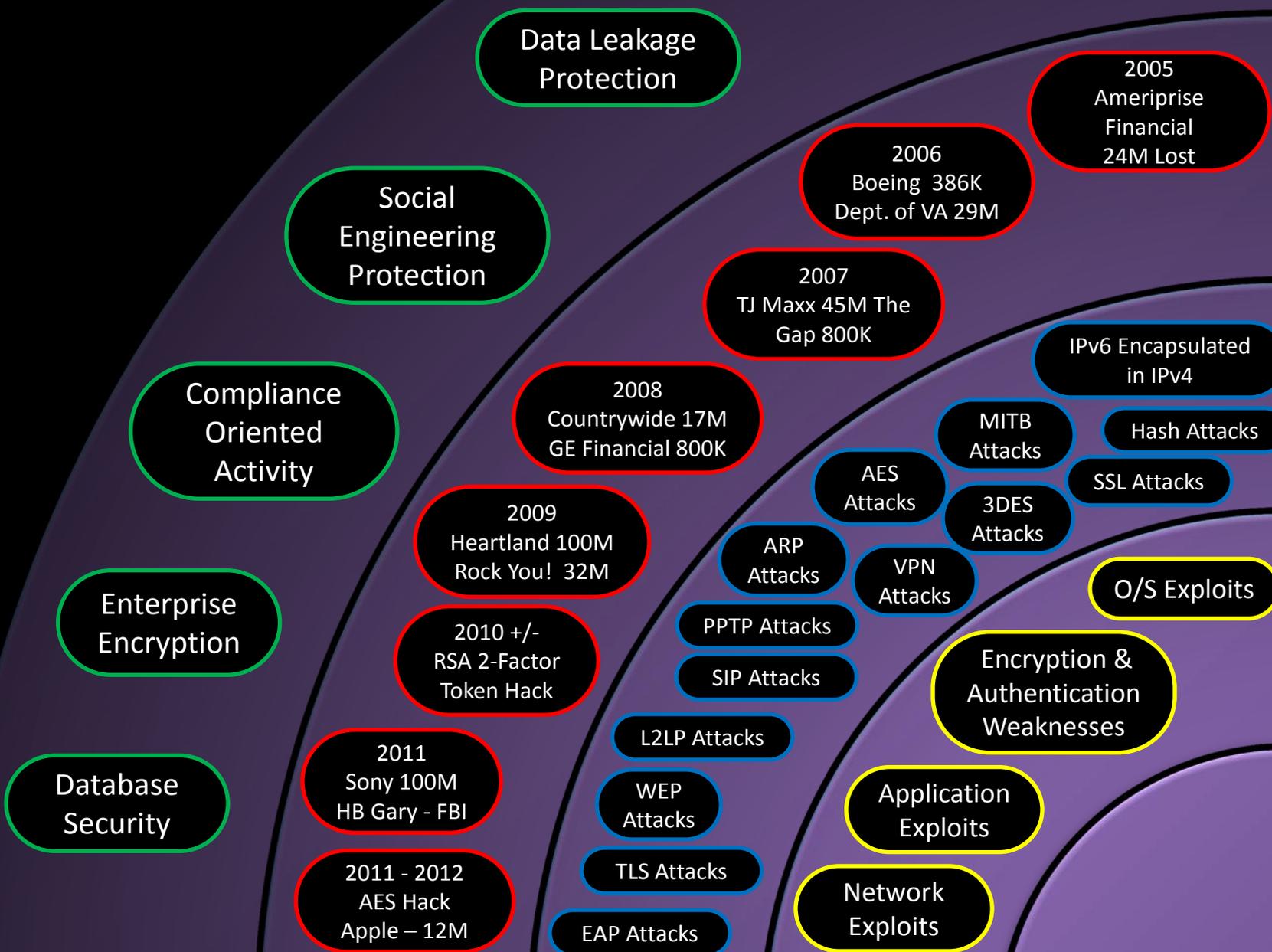
Security Integrity

in its broadest meaning refers to the trustworthiness of information over its entire life cycle.

Security Availability

is a characteristic that distinguishes information objects that have signaling and self-sustaining processes from those that do not, either because such functions have ceased (outage, an attack), or else because they lack such functions .





Defenses

Examples

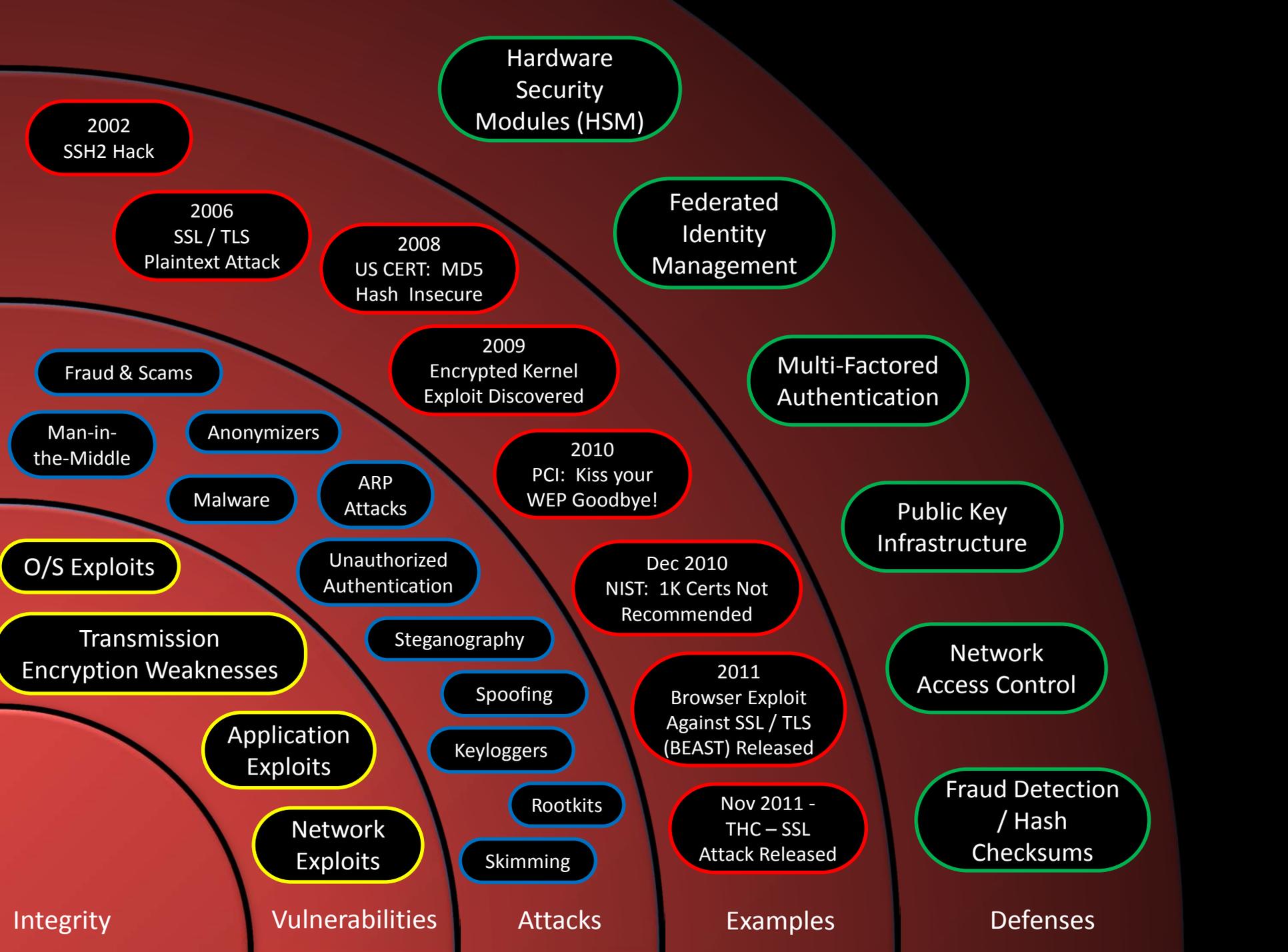
Attacks

Vulnerabilities

Confidentiality







Hardware Security Modules (HSM)

2002 SSH2 Hack

2006 SSL / TLS Plaintext Attack

2008 US CERT: MD5 Hash Insecure

Federated Identity Management

2009 Encrypted Kernel Exploit Discovered

Multi-Factored Authentication

Fraud & Scams

2010 PCI: Kiss your WEP Goodbye!

Public Key Infrastructure

Man-in-the-Middle

Anonymizers

Malware

ARP Attacks

Dec 2010 NIST: 1K Certs Not Recommended

Network Access Control

O/S Exploits

Unauthorized Authentication

Steganography

Transmission Encryption Weaknesses

Spoofing

Application Exploits

Keyloggers

Rootkits

2011 Browser Exploit Against SSL / TLS (BEAST) Released

Fraud Detection / Hash Checksums

Network Exploits

Skimming

Nov 2011 - THC - SSL Attack Released

Integrity

Vulnerabilities

Attacks

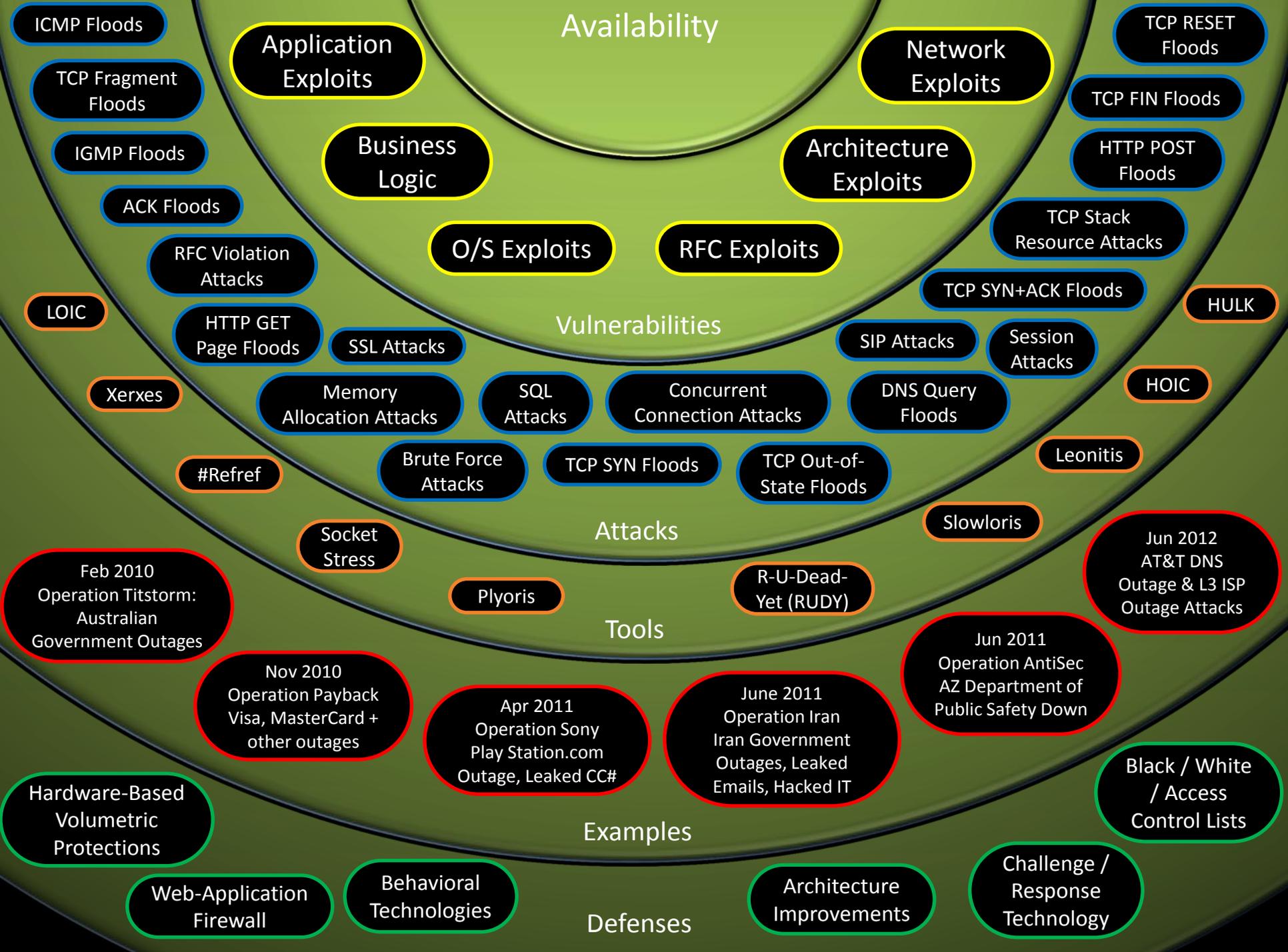
Examples

Defenses

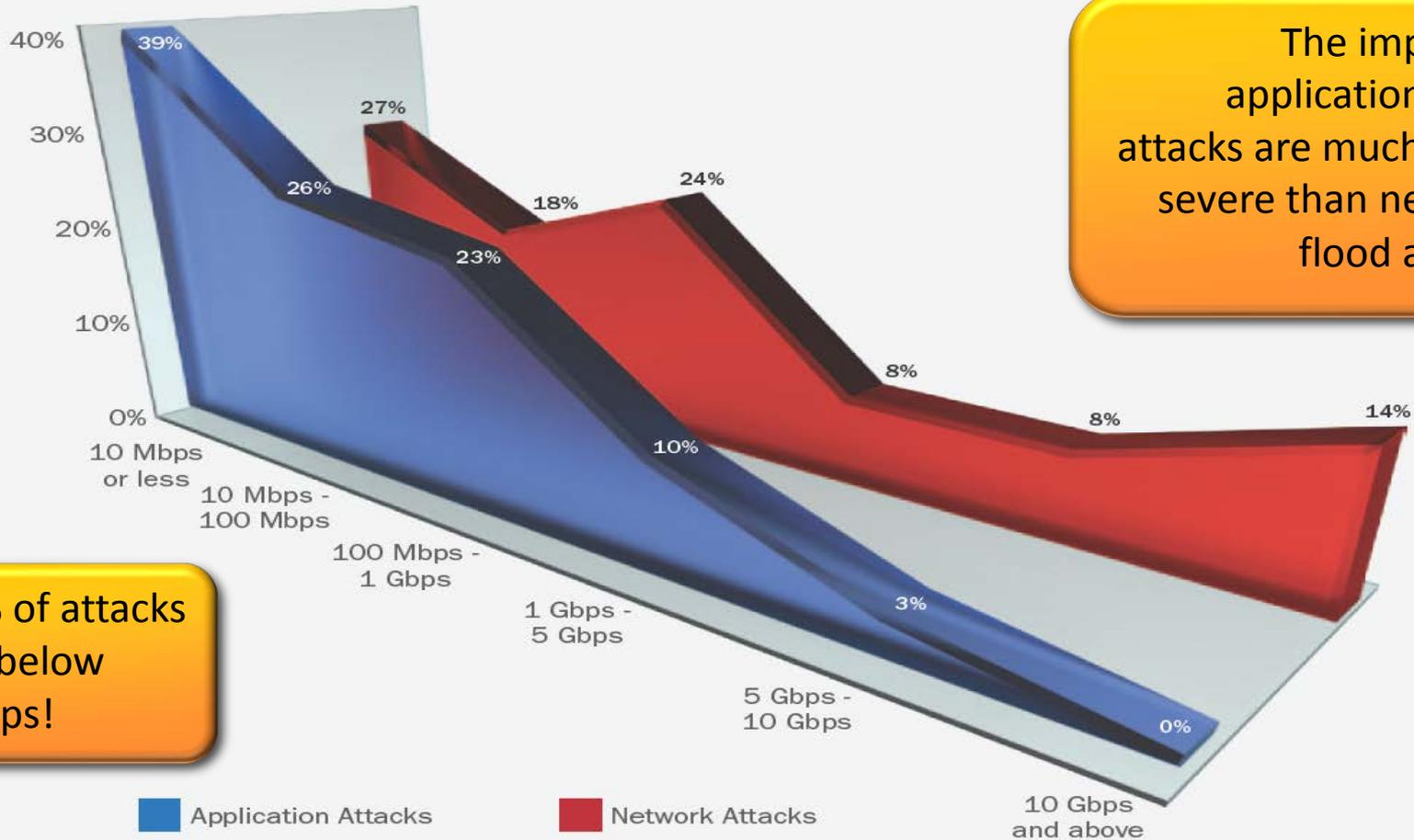


The Security Trinity



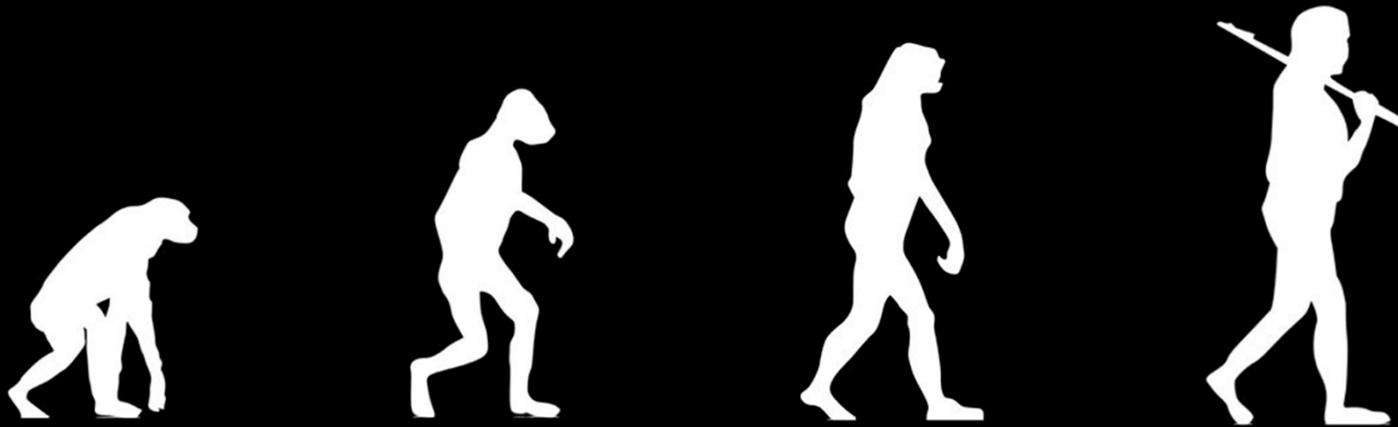


The impact of application flood attacks are much more severe than network flood attacks



76% of attacks are below 1Gbps!

▶ The Evolving Threat Landscape





More Attacks. More Often.



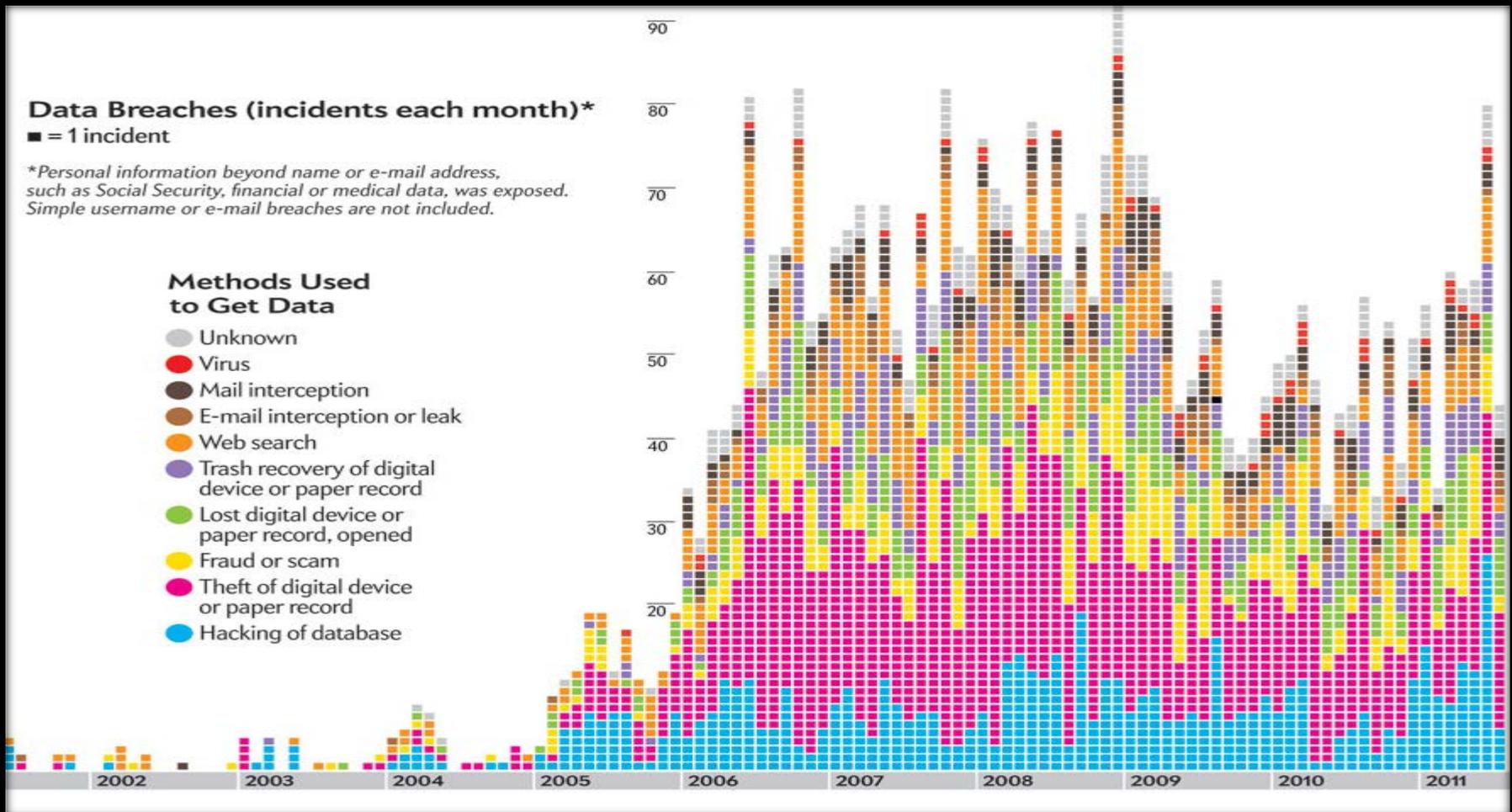
Data Breaches (incidents each month)*

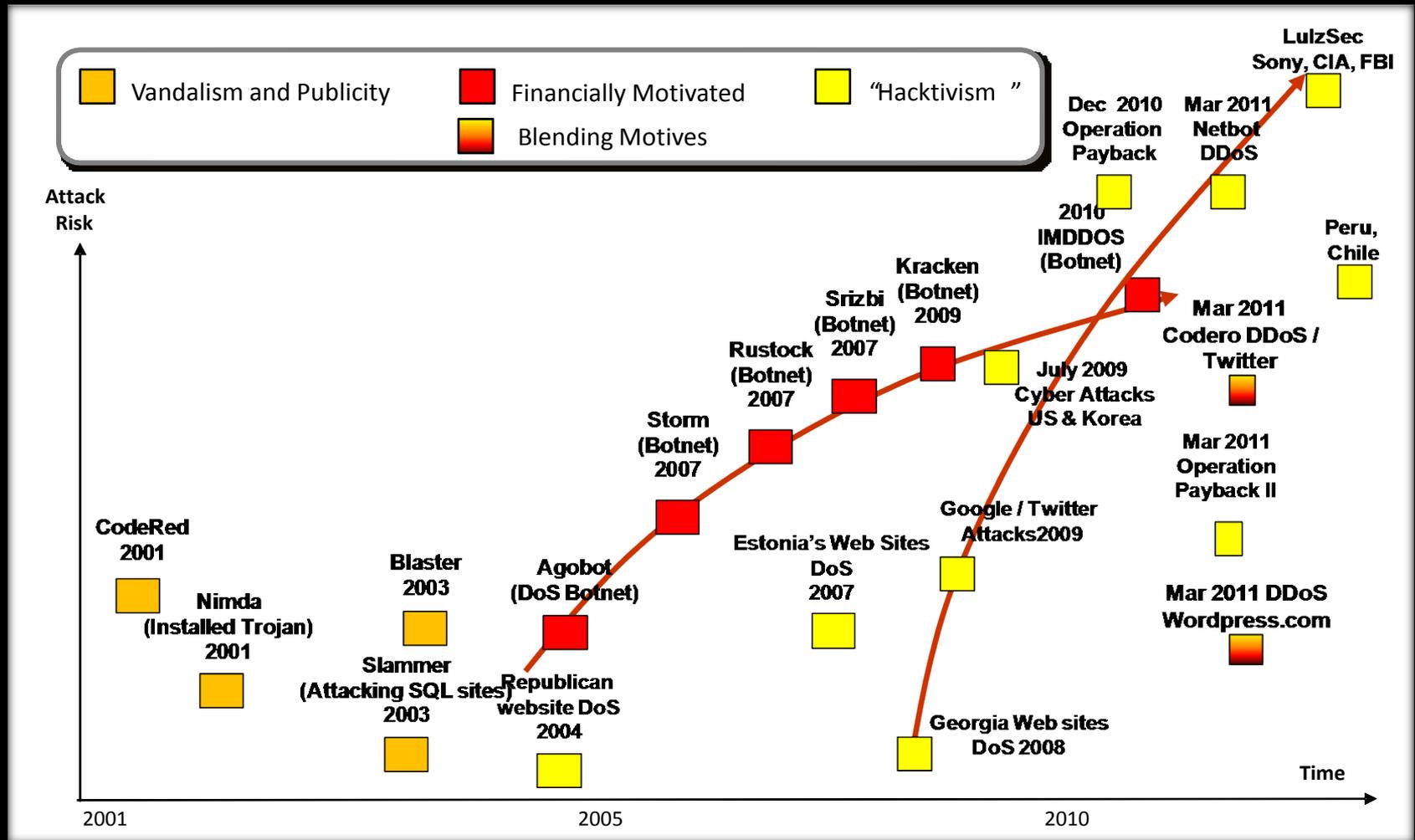
■ = 1 incident

*Personal information beyond name or e-mail address, such as Social Security, financial or medical data, was exposed. Simple username or e-mail breaches are not included.

Methods Used to Get Data

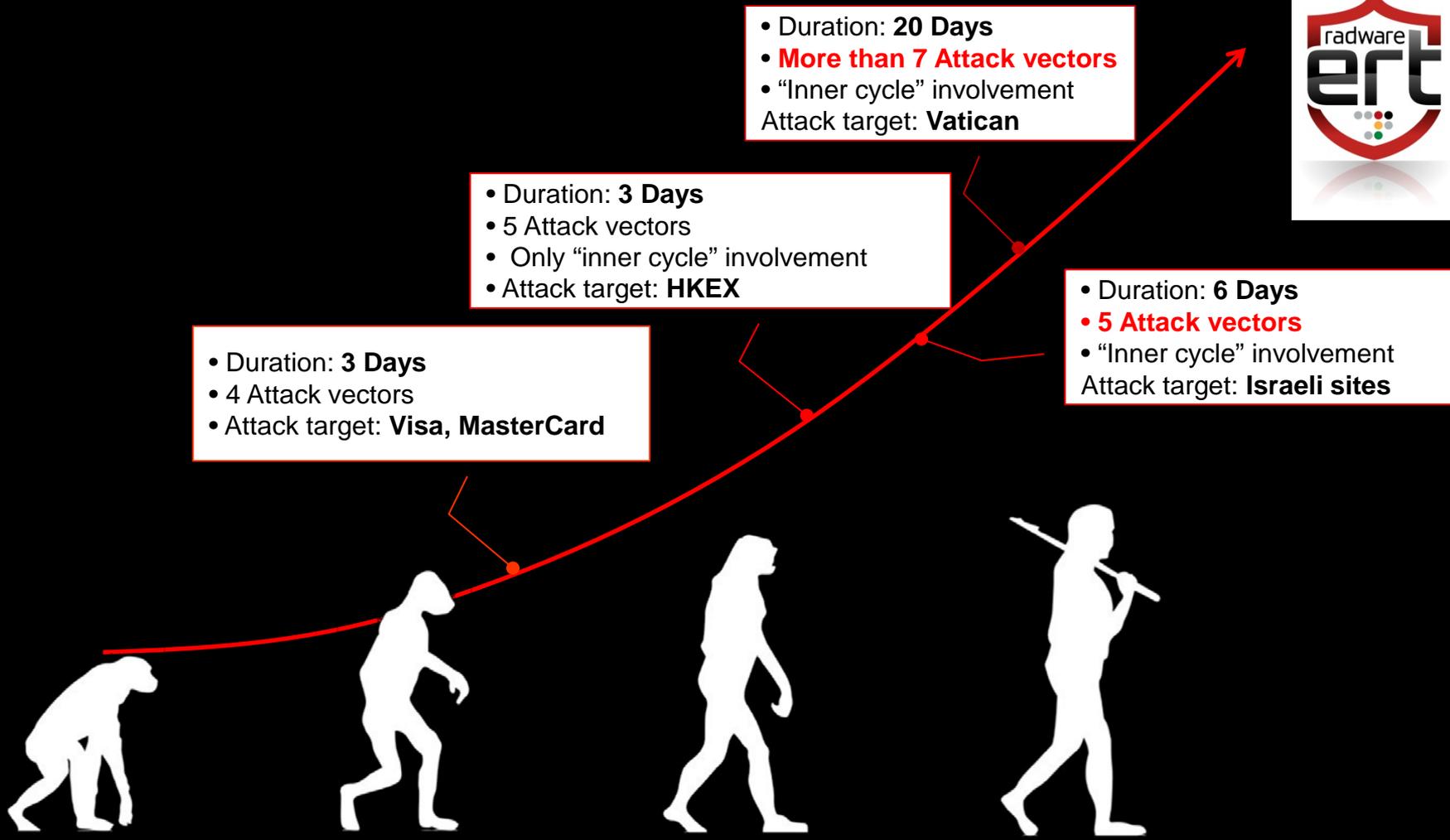
- Unknown
- Virus
- Mail interception
- E-mail interception or leak
- Web search
- Trash recovery of digital device or paper record
- Lost digital device or paper record, opened
- Fraud or scam
- Theft of digital device or paper record
- Hacking of database





- **Complex:** More than seven different attack vectors at once
- **Blending:** both network and application attacks
- **Targeteering:** Select the most appropriate target, attack tools,
- **Resourcing:** Advertise, invite, coerce anyone capable ...
- **Testing:** Perform short “proof-firing” prior to the attack
- **Timeline:** Establish the most painful time period for his victim







Network	Application Flood	Low & Slow	Vulnerability Based
UDP Floods	Dynamic HTTP	RUDY	Intrusion Attempts
SYN Floods	HTTPS Floods	Slowloris	SQL Injection
Fragmented Floods		Pyloris	#refref
FIN + ACK			xerex

Confidentiality



Integrity



Availability



Target / Operation

Habbo

Hal Turner

Project Chanology

Epilepsy Foundation

AllHipHop Defacement

No Cussing Club

2009 Iranian Election Protests

Operation Didgeridie

Operation Titstorm

Oregon Tea Party Raid


Operation Payback

Avenge Assange

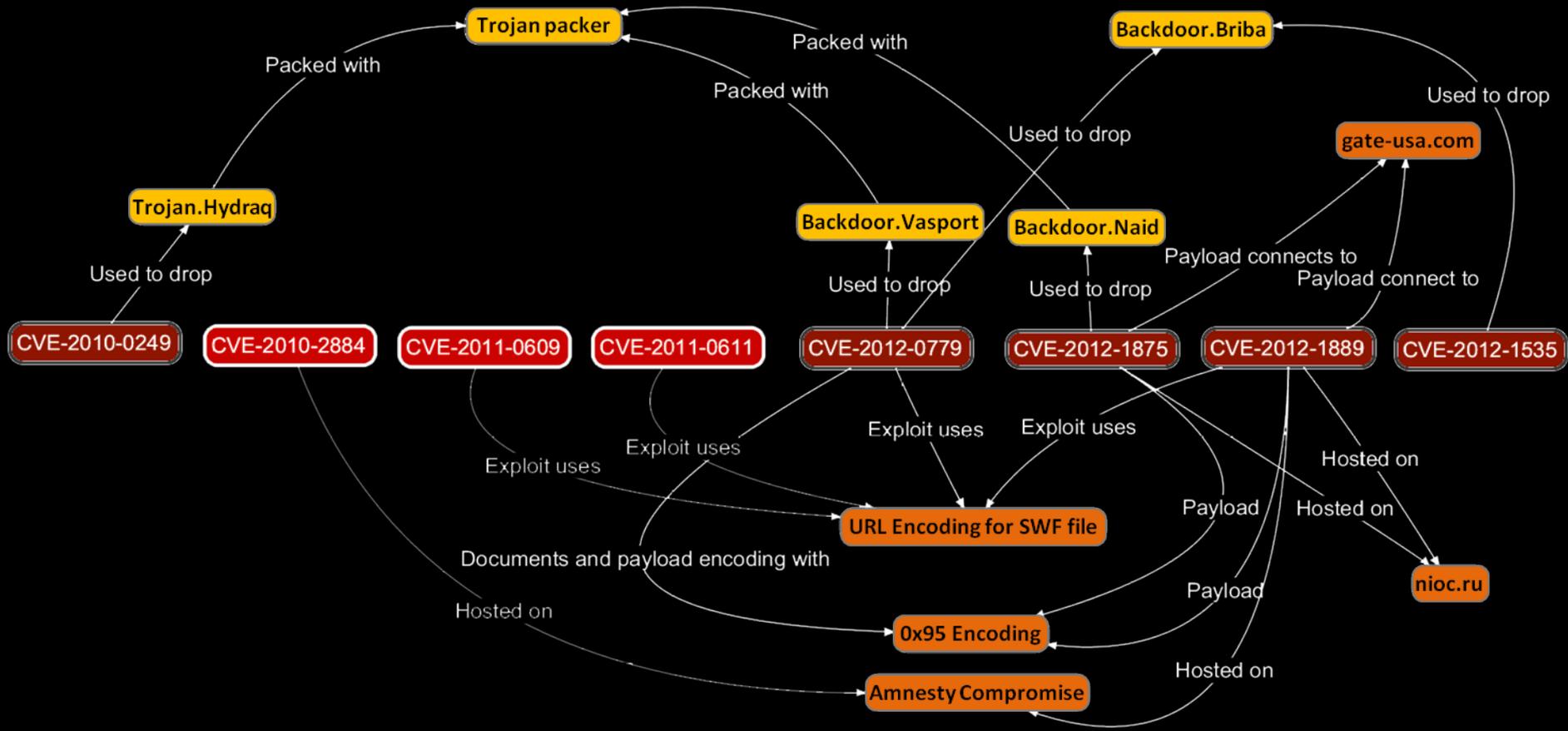
Ope
Bra

2007

2008

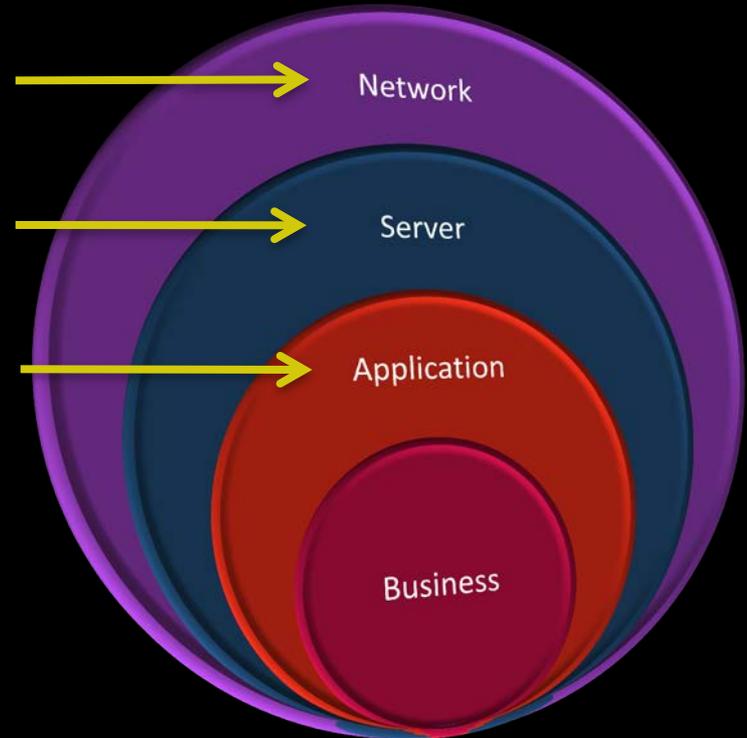
2009

2010

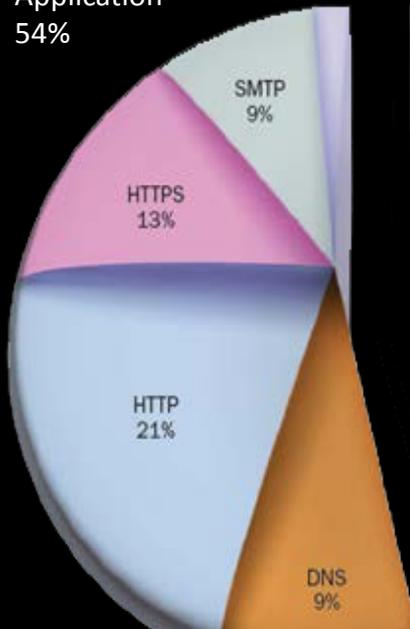


Network & Application Attacks Coexist

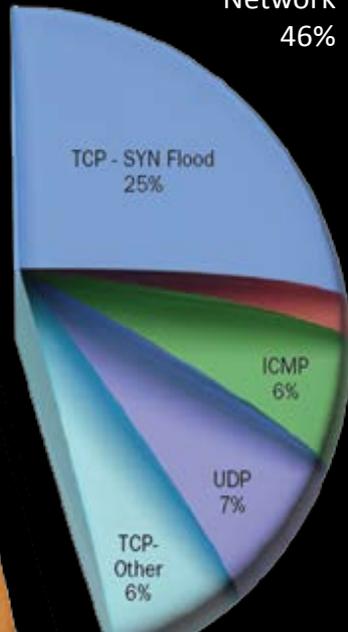
- *Volumetric network level*
- *Application level , Encrypted*
- *Low & Slow*
- *Directed Application DoS*
- *Intrusions*
- *Web attacks (injections, XSS,...)*



Application
54%



Network
46%





Defense Blind Spot Map

Protection Purpose	Firewall	IPS	WAF	Router ACLs	Next Gen FW	Anti-DoS Appliance (CPE)	DLP	Cloud Anti-DoS
Data-At-Rest Protections (Confidentiality)	Red	Orange	Red	Red	Red	Red	Green	Red
Data-At-Endpoint (Confidentiality)	Red	Orange	Red	Red	Red	Red	Green	Red
Data-In-Transit (Confidentiality)	Orange	Orange	Green	Orange	Orange	Green	Green	Red
Network Infrastructure Protection (Integrity)	Green	Red	Red	Orange	Green	Orange	Red	Red
Application Infrastructure Protection (Integrity)	Red	Red	Green	Red	Orange	Orange	Red	Orange
Volumetric Attacks (Availability)	Red	Red	Orange	Orange	Red	Green	Red	Green
Non-Volumetric Resource Attacks (Availability)	Red	Orange	Red	Red	Red	Green	Red	Red

Table 6. Defense Approaches by Attack Type

DoS Defense Component	Vulnerability Exploitation	Network Flood	Infrastructure Exhaustion	Target Exhaustion
Network devices	No	No	Some	Some
Overprovisioning	No	Yes, bandwidth	Yes, infrastructure	Yes, servers and applications
Firewall and network equipment	No	No	Some	Some
NIPS or WAF security appliances	Yes	No	No, usually part of the problem	No, NIPS resource may be exhausted before the target's
Anti-DoS box (stand-alone)	No	No	Yes	Yes
ISP-side tools	No	Yes	Rarely	Rarely
Anti-DoS appliances (ISP-connected)	No	Yes	Yes	Yes
Anti-DoS specialty provider	No	Yes	Yes	Yes
CDN	No	Yes	Yes	Somewhat — limited to common issues

Table 6. Defense Approaches by Attack Type

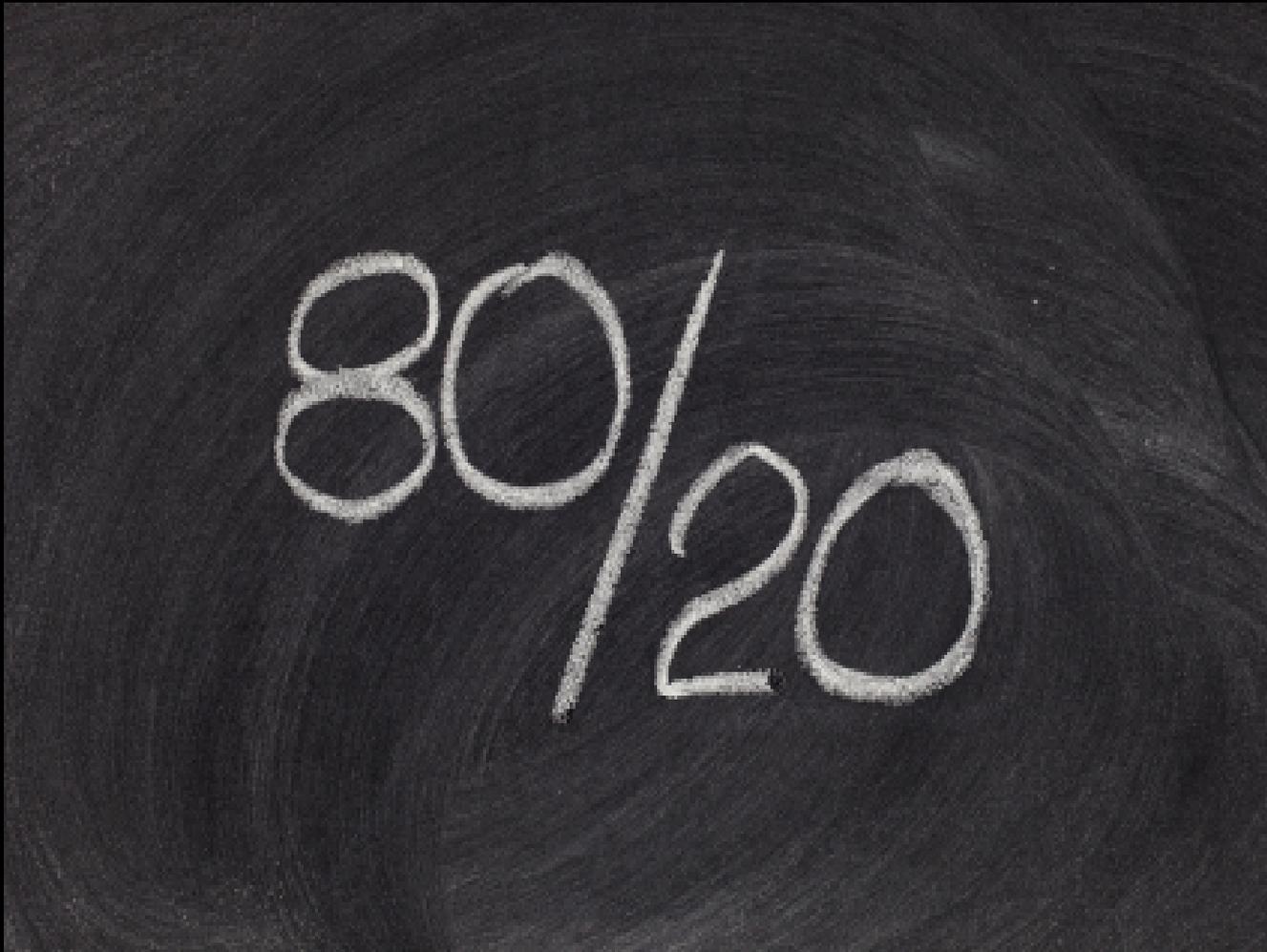
DoS Defense Component	Vulnerability Exploitation	Network Flood	Infrastructure Exhaustion	Target Exhaustion
Network devices	No 	No 	Some 	Some 
Overprovisioning	No 	Yes, bandwidth 	Yes, infrastructure 	Yes, server and application 
Firewall and network equipment	No 	No 	Some 	Some 
NIPS or WAF security appliances	Yes 	No 	No, usually part of the problem 	No, NIPS resource may be exhausted before the target's 
Anti-DoS box (stand-alone)	No 	No 	Yes 	Yes 
ISP-side tools	No 	Yes 	Rarely 	Rarely 
Anti-DoS appliances (ISP-connected)	No 	Yes 	Yes 	Yes 
Anti-DoS specialty provider	No 	Yes 	Yes 	Yes 
CDN	No 	Yes 	Yes 	Somewhat limited to common issues 

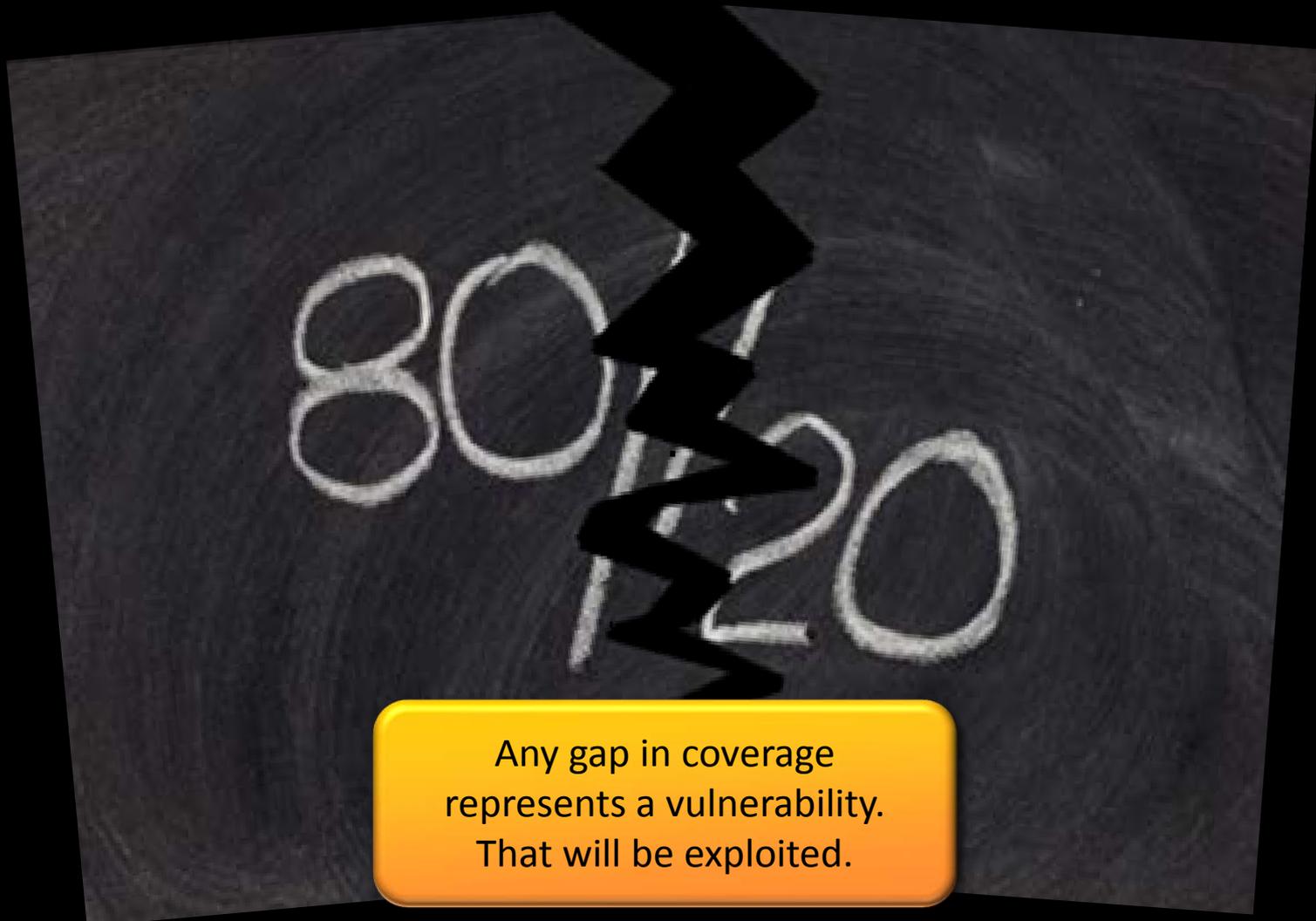


▶ Securing Tomorrow's Perimeter

AGENDA

- 100% Architecture Protection. Varied Deployment Models.
- Understand the behavior beyond protocol and content
- It's an eco-system....collaboration is key
- Emergency response & triage: Practice cyber war rooms
- Integrate offense into your security strategies.



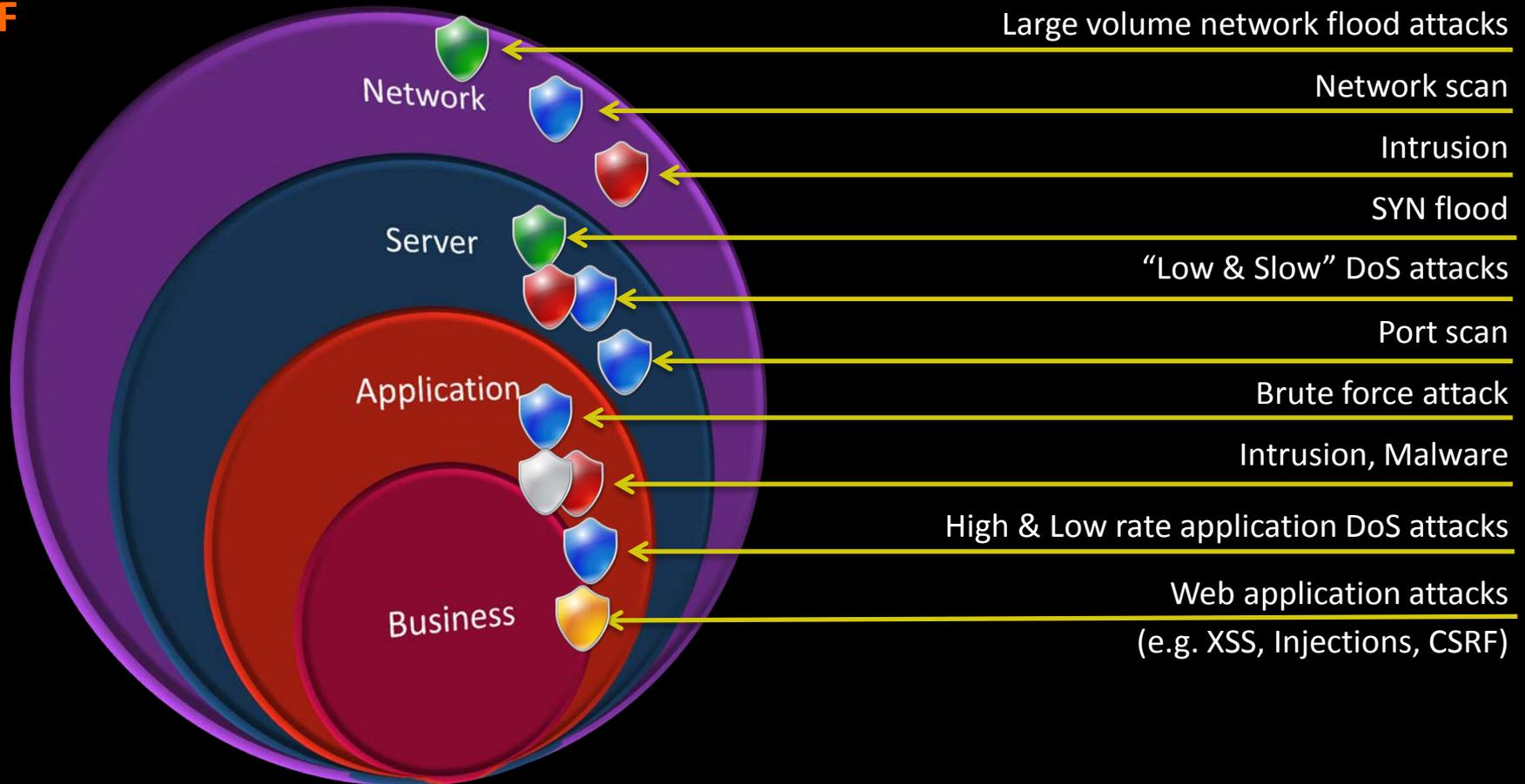


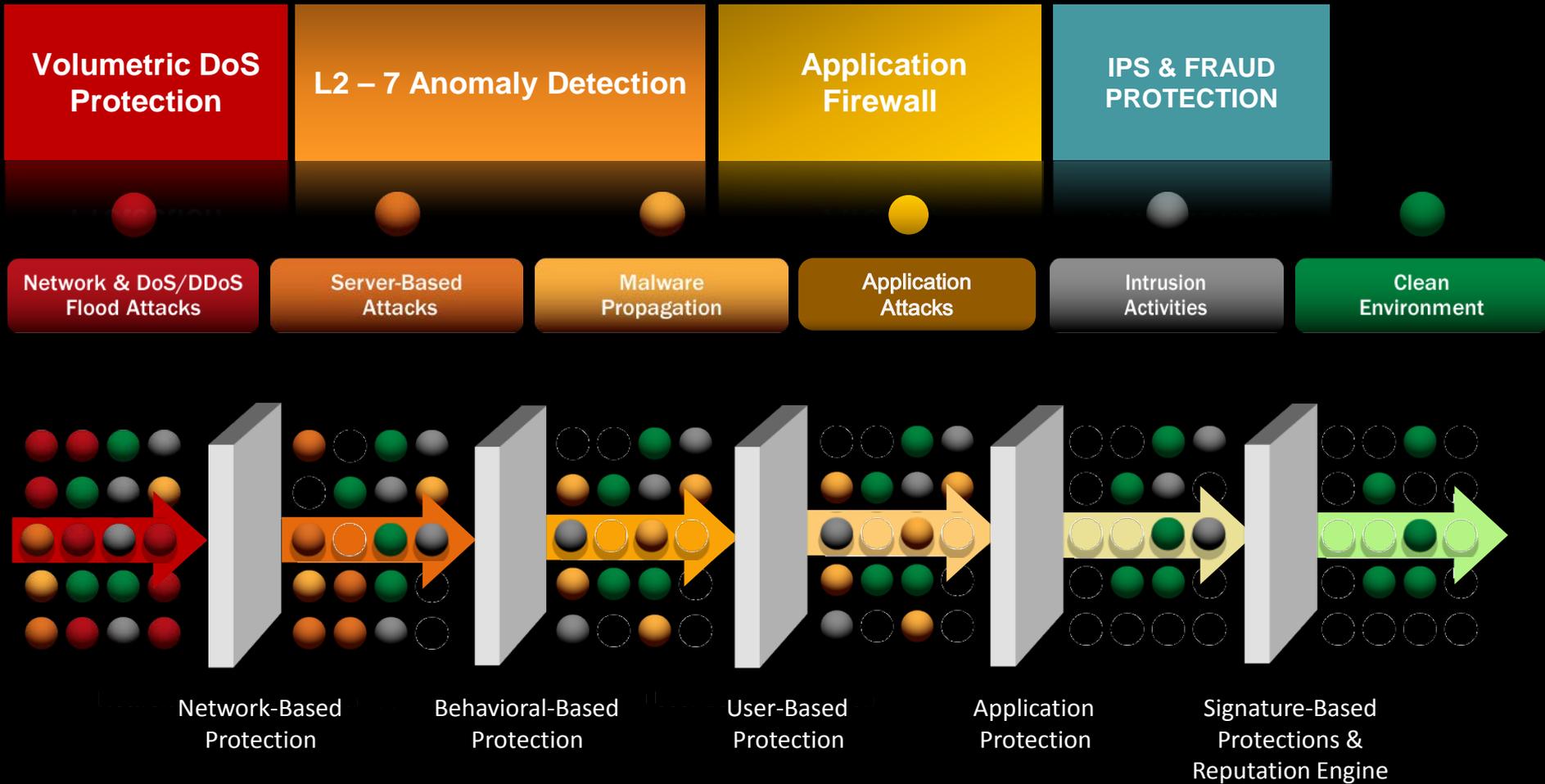


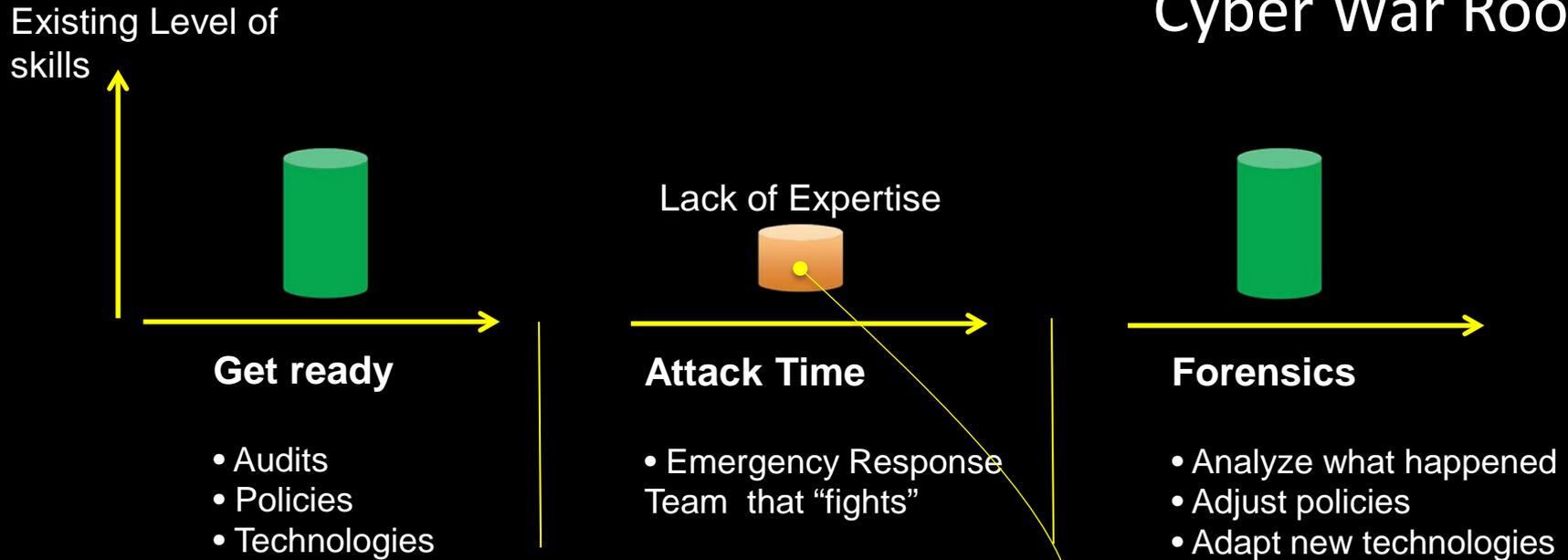
Perimeter Defense Planning



DoS Protection
Behavioral Analysis
IPS
IP Reputation
WAF



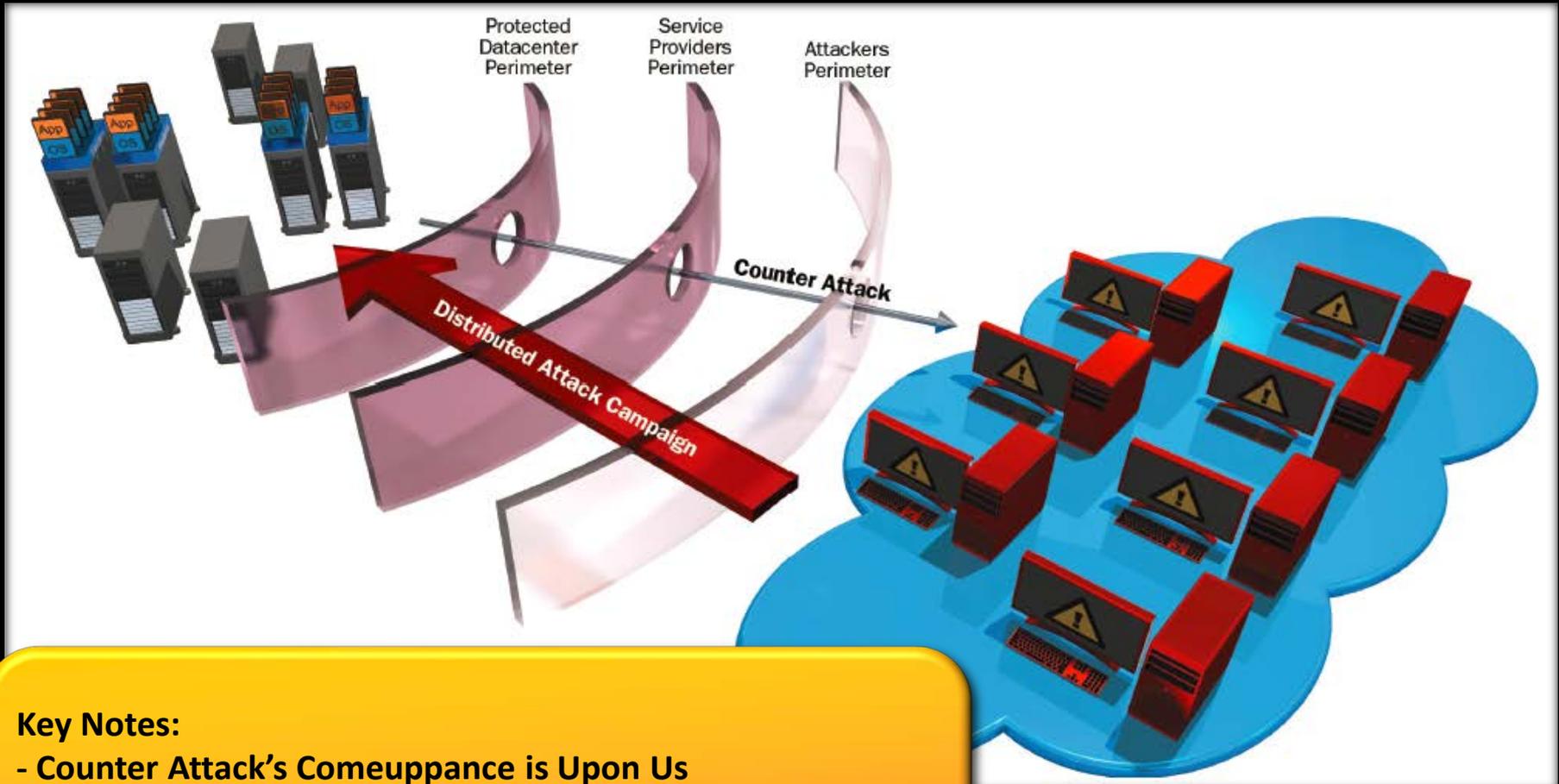




- **Required expertise during attack campaign**

- 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

**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



Anatomy of an Attack

The Evolving Threat Landscape

Securing Tomorrow's Perimeter

AGENDA

- 1. Assess DDoS vulnerabilities**
- 2. Look beyond large attacks**
- 3. Plan ahead – Can't stop attacks without a game plan**
- 4. Secure potential bottlenecks – Which of YOUR devices will fail first?**
- 5. Watch what's happening on the network – Do you have signals?**
- 6. Be aware of all threat surfaces - including mobile phones**
- 7. Beware of application-layer attacks - Not just DDoS anymore**
- 8. Watch for blended attacks**
- 9. Partner up with companies that know how to counter attack**



O'REILLY
Answers Clever hacks. Creative ideas.
Innovative solutions.

[Home](#)[Shop](#)[Radar: News & Commentary](#)[Answers](#)[Safari Books Online](#)[Conferences](#)[School of Tech](#)Trending Topics: [mobile](#) | [ios](#) | [core data](#) | [scratch](#) | [web](#) | [ipad](#) | [php](#) | [WebGL](#) | [More...](#)

DDoS school server?

**Asked by misterfox**

Posted Dec 02 2011 06:35 PM

1930 Views

I am attempting to figure out how to effectively DDoS my high school's server (the server hosting the internet connection to every computer in the school). I have LOIC and a few friends who will join me with LOIC, but I'm not so sure about the target. The IP address of the server is- 10.88.0.13:1347

I understand the first 4 numbers, but the :1347 at the end is confusing me. What is that? do I need it to effectively target LOIC?

NOTE- I'm doing this as a senior prank for 1 day, Please don't tell me not to do this. If you don't have any useful info, don't answer my question!

Tags: [LOIC](#) [DDoS](#) [server](#) [school](#) [hacking](#) [IP](#) [address](#)



Thank You

Howard Teicher
VP, Public Sector
Radware, Inc.
howardt@radware.com

