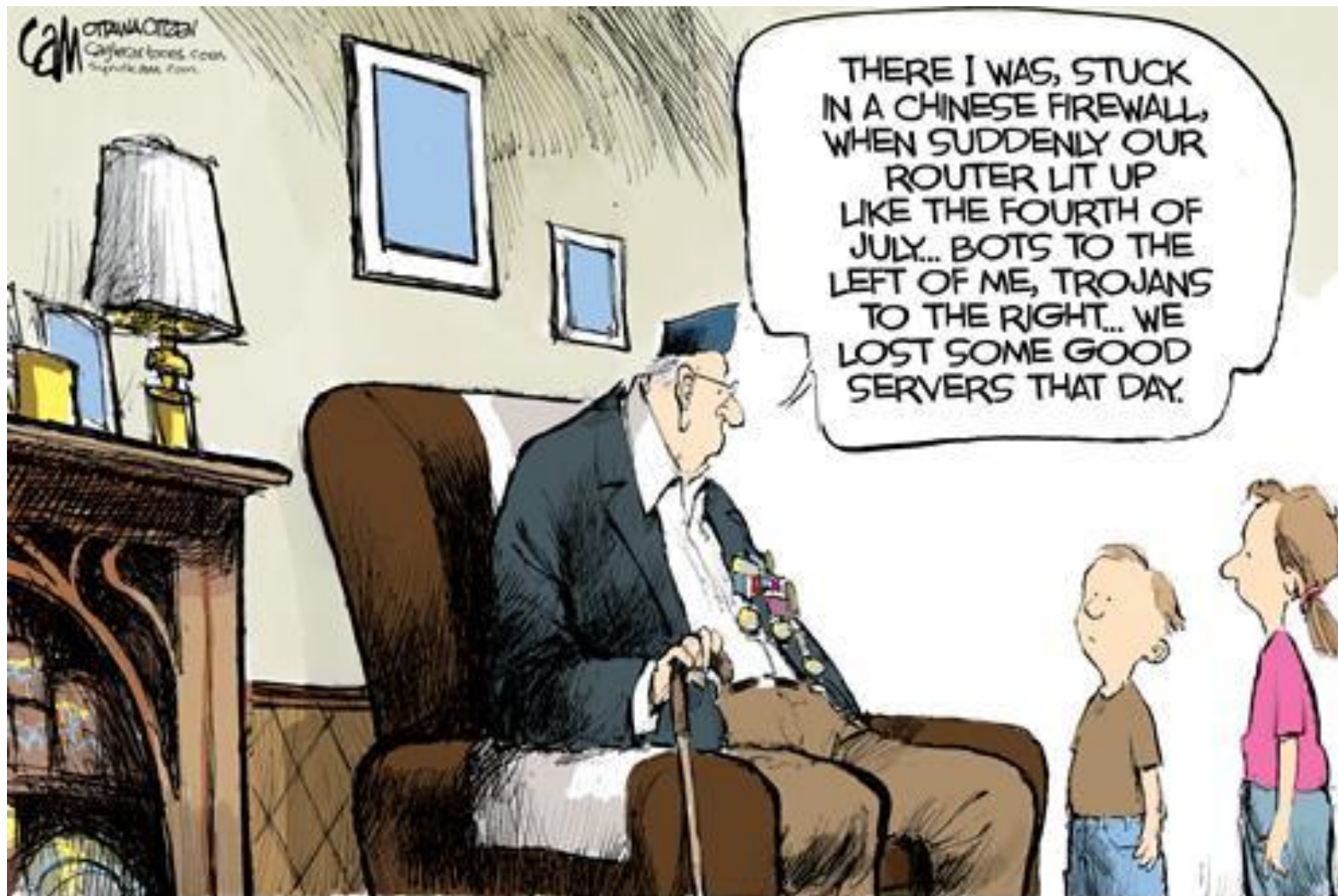


Rise of Hacktivism and The Overhaul of Perimeter Defense

August 2011

*Carl W. Herberger
V.P., Security Solutions*



The Rise of Hacktivism

Recent Perimeter Defense Breakdowns

New Learned Lessons

The Evolving Perimeter

- **Dawn of Hacktivism**
 - **Definition & Key Attributes**
 - **Family Tree of Main Players**
 - **2009-2011 Have Seen a Dramatic Rise in “Hacktivism**
- **Recent Breakdown of Perimeter Defenses**
 - **Two Main Effective Tools: DDoS & SQL Injection**
 - **Disintegration of General IT Risk Models**
- **2011 Establish Numerous Lessons: High Level & Technical Level**
 - **Definitive Proof that Security Perimeter Point Solutions Are Ineffective**
 - **Few Models have Passed Successfully Battled Hacktivists**
 - **Worst Case Security Models Work!!! Risk-Adjusted Models Do Not.**
- **New Perimeter Security 10 Must Haves:**
 - **More Alerting Coverage – More Deployed Perimeter Platforms**
 - **Tighter Integration – Instantly Normalize & Correlated Data**
 - **Prioritization of Threats for Mitigation**

The Rise of Hacktivism



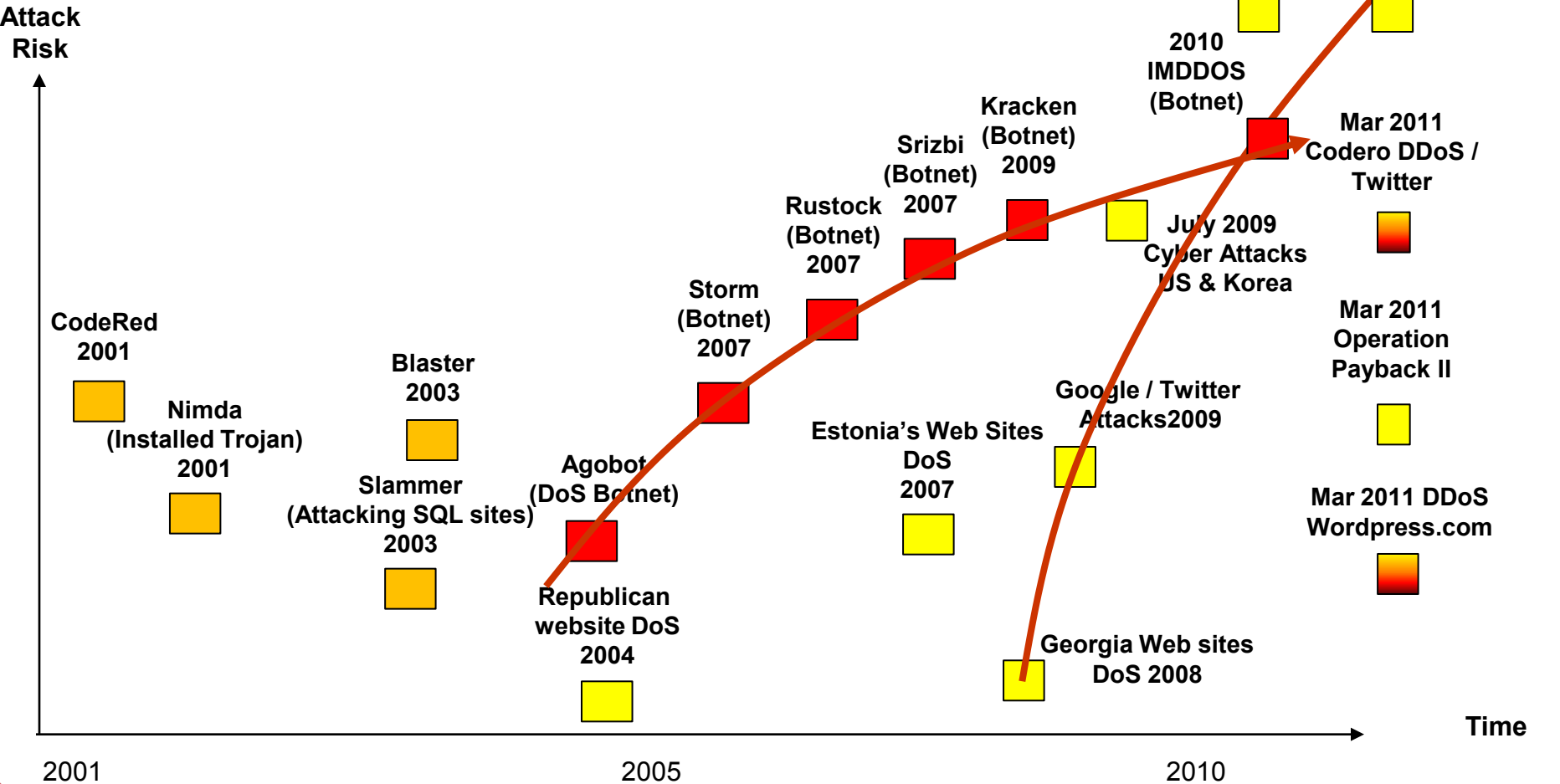
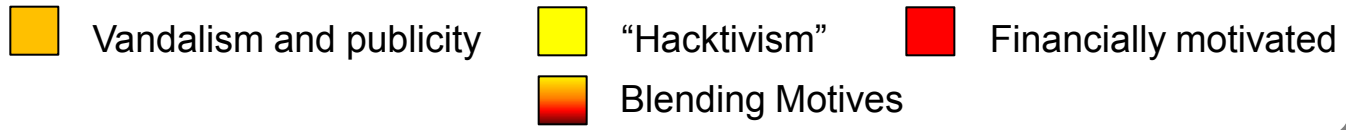
Hacktivism: political activism using computer networks: the activity of breaking into and sabotaging a computer system via the Internet as a political protest

A meme is an *idea, behavior or style that spreads from person to person within a culture*. While genes transmit biological information, memes are said to transmit ideas and belief information.

Vulnerability: A bug or feature of a system that exposes it to possible attack, a flaw in the system's security. A weakness.

Ubiquity: The state or capacity of being everywhere, esp. at the same time; omnipresence

Vulnerability: A state of seemingly infinite or pervasive weakness and vulnerability of a system that exposes it to possible attack.



"Hacktivist for Good"

- Claims to be ex-military
- Originally performed DoS attacks on Jihadist sites
 - Uses the internally developed (& legendary) Xerxes tool
 - Bringing them down for brief periods, such as 30 minutes
 - Announces his attacks on Twitter, discusses them on a blog and live on irc.2600.net



th3j35t3r Jester

www.almedad.net - TANGO DOWN. Temporarily. For the online radicalization of young muslims in US and Europe.

12 Dec

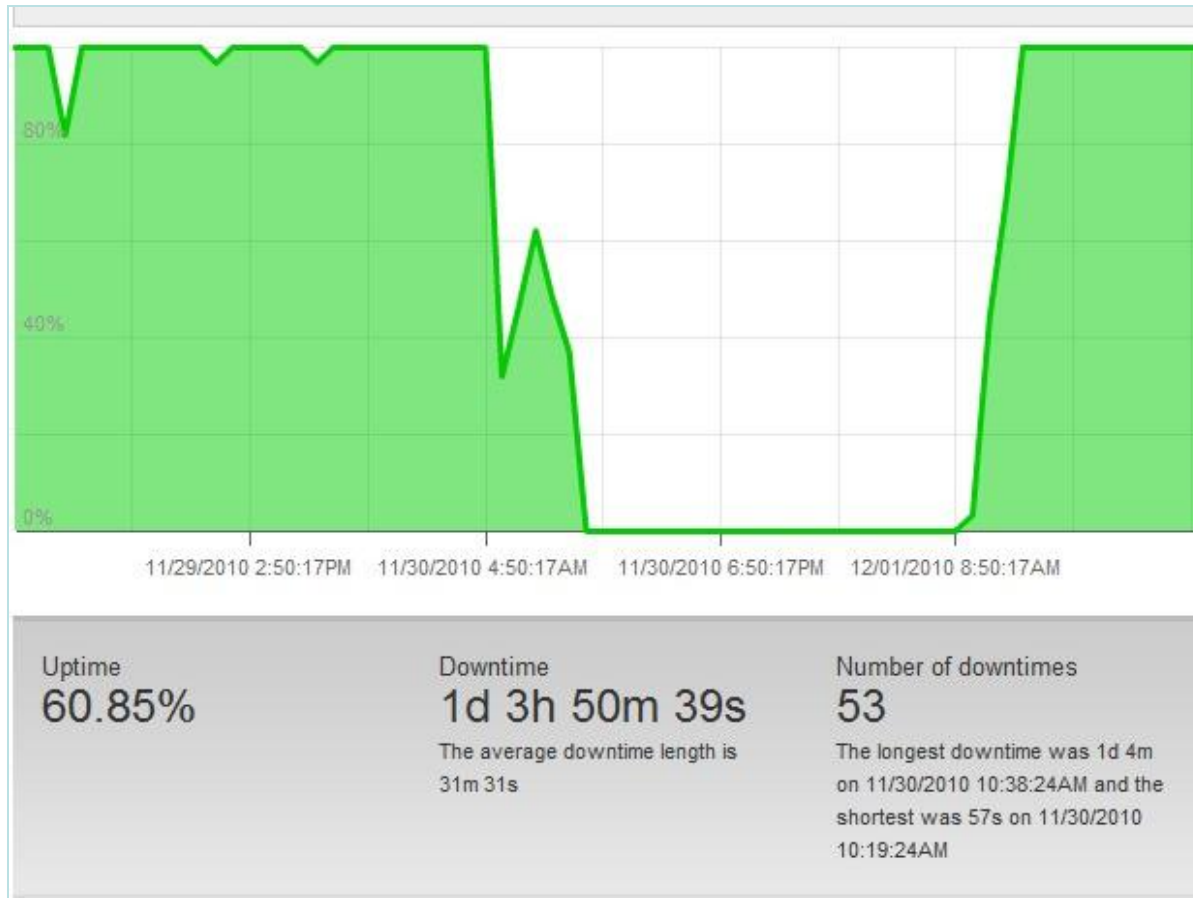


th3j35t3r Jester

www.ansar1.info - TANGO DOWN. Temporarily. For online incitement to cause young muslims to carry out acts of violent jihad.

12 Dec

Wikileaks Outage



- One attacker, no botnet

- After his Wikileaks attack
 - He battled Anonymous
 - He claims to have trojaned a tool the Anons downloaded
 - He claims to pwn Anon insiders now
 - He battles LulzSec and recently claimed to „out“ their members forcing a disband



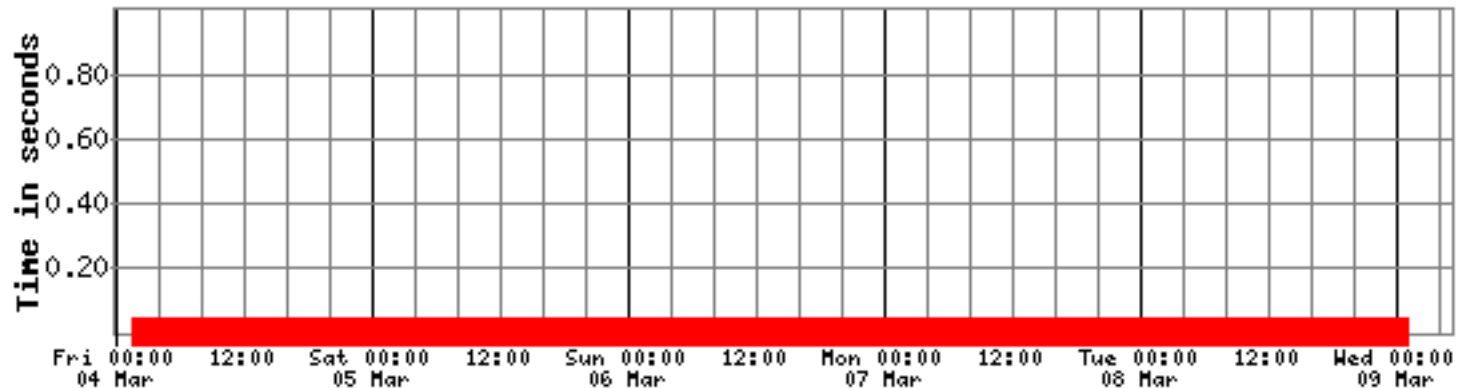
Performance Charts and Statistics for www.godhatesfags.comTotal time

Examine

Total time for www.godhatesfags.com from Pennsylvania/INetU-2

Display steps: 15.00 minutes

Last sample 9-Mar-2011 01:00:00 GMT

Total time from Pennsylvania/INetU-2 to www.godhatesfags.com

Failures

(c) www.netcraft.com

- 4 sites held down for 8 weeks
- From a single 3G cell phone
 - <http://tinyurl.com/4vggluu>



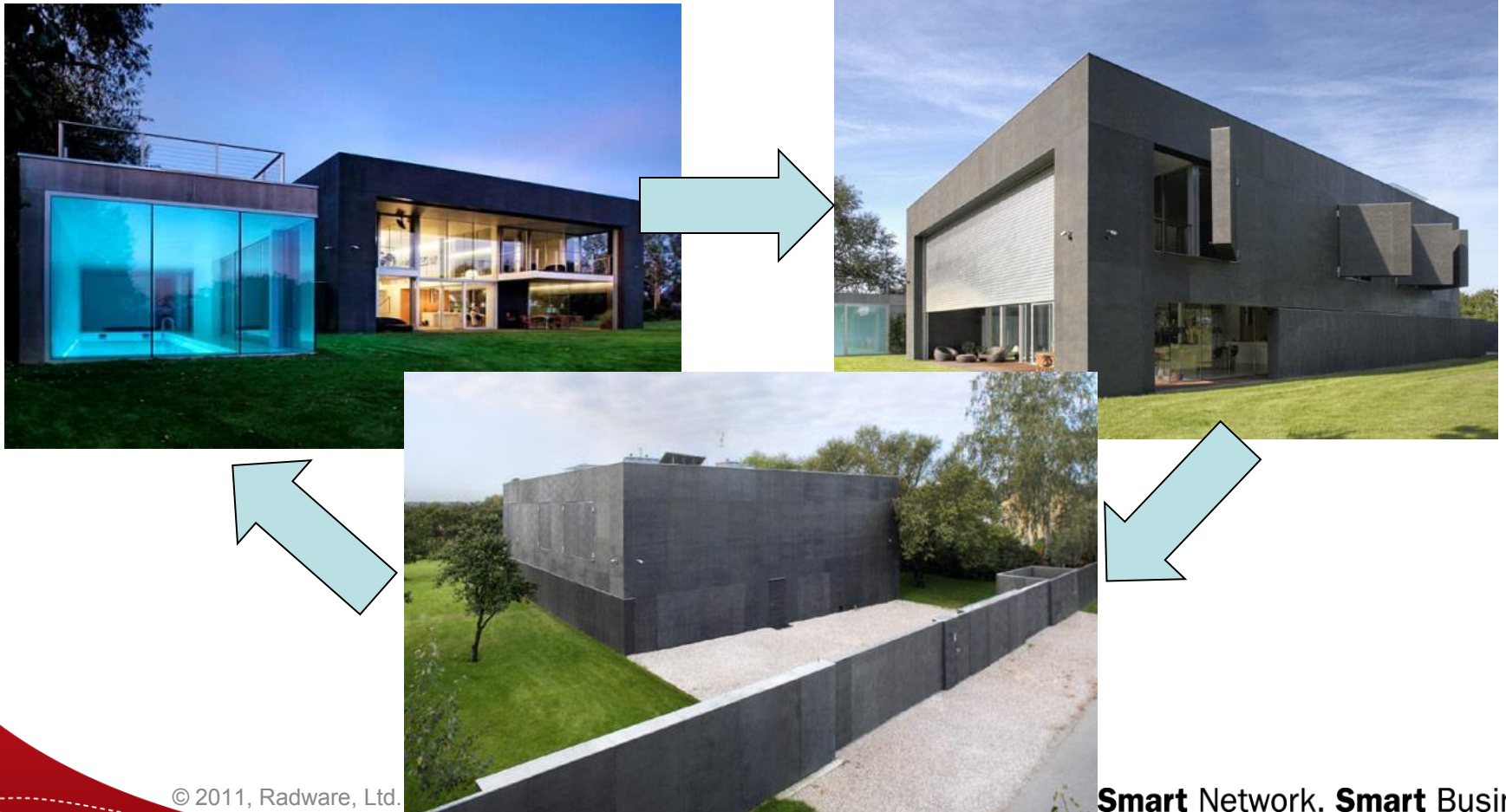
The Rise of Hacktivism

Recent Perimeter Defense Breakdowns

New Learned Lessons

The Evolving Perimeter

Recent Breakdown Of Perimeter Defenses



1. Many Cases, Inadequate Attack Coverage

- **Inadequate DoS Coverage (e.g. Layer 7)**
- **Inadequate Application-Layer Security**
- **Isolated Security Point-Solutions**

2. Incapable to Handle Multi-Vulnerability Attack Campaigns

- **Difficulty or Inability to triage threats**
- **Difficulty or Inability to handle attack tools**
- **Difficulty in Inability to maintain business while fighting threats**

The Rise of Hacktivism

Recent Perimeter Defense Breakdowns

New Learned Lessons

The Evolving Perimeter

Inadequate Perimeter Attack Coverage

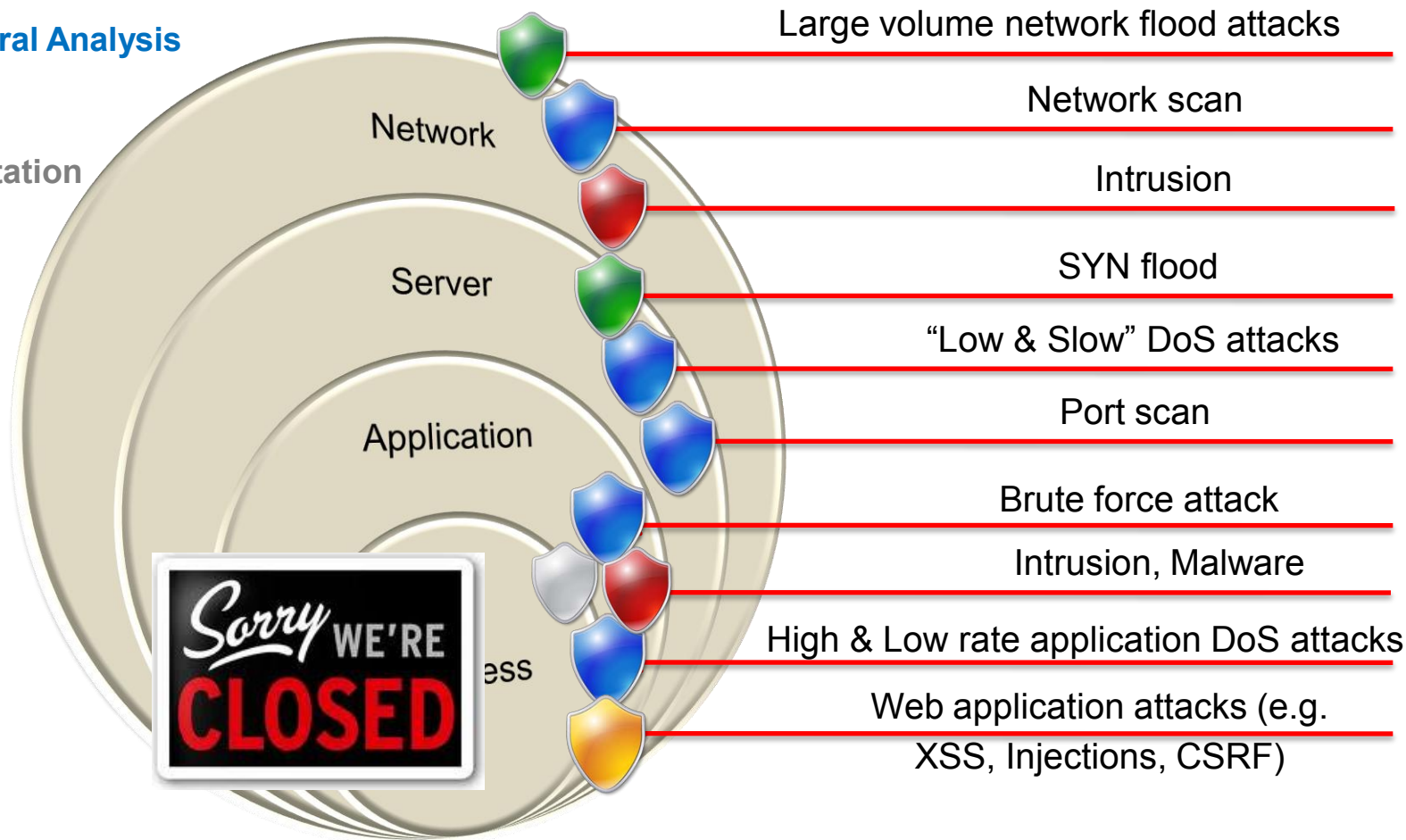
DoS Protection

Behavioral Analysis

IPS

IP Reputation

WAF



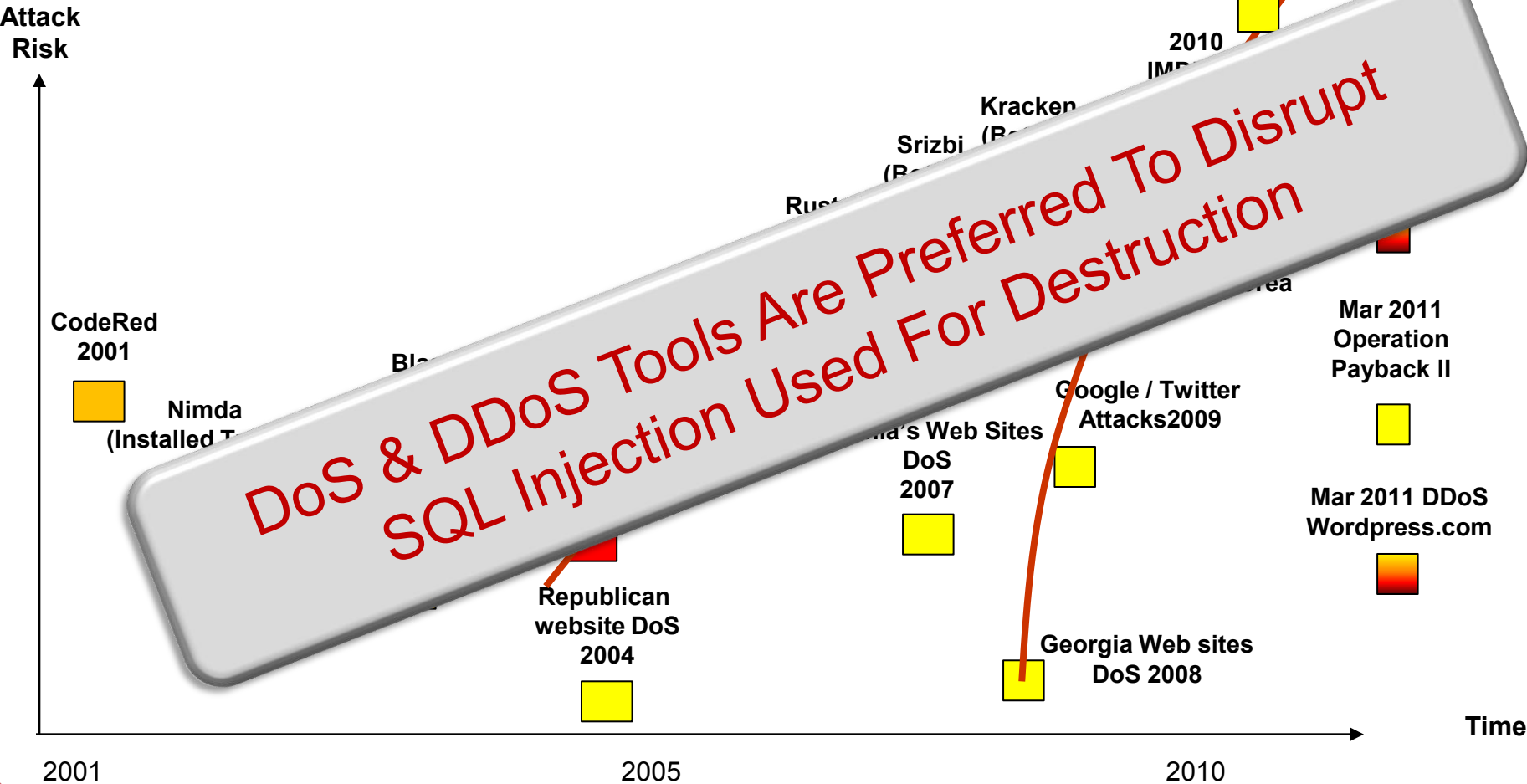
Inadequate Perimeter Attack Coverage: Example One: DDoS

- Vandalism and publicity
- "Hacktivism"
- Financially motivated
- Blending Motives

LulzSec
Sony, CIA, FBI,
Orange County

Dec 2010
Operation
Payback

Mar 2011
Netbot
DDoS



July 2009 - Low & Slow Attacks - Slowloris

July 2009 - MyDoom - Over 50,000 Zombies

August 2009 - Twitter/Cyxymu DDoS

Sept 2010 - IMDDOS - Commercial Botnet

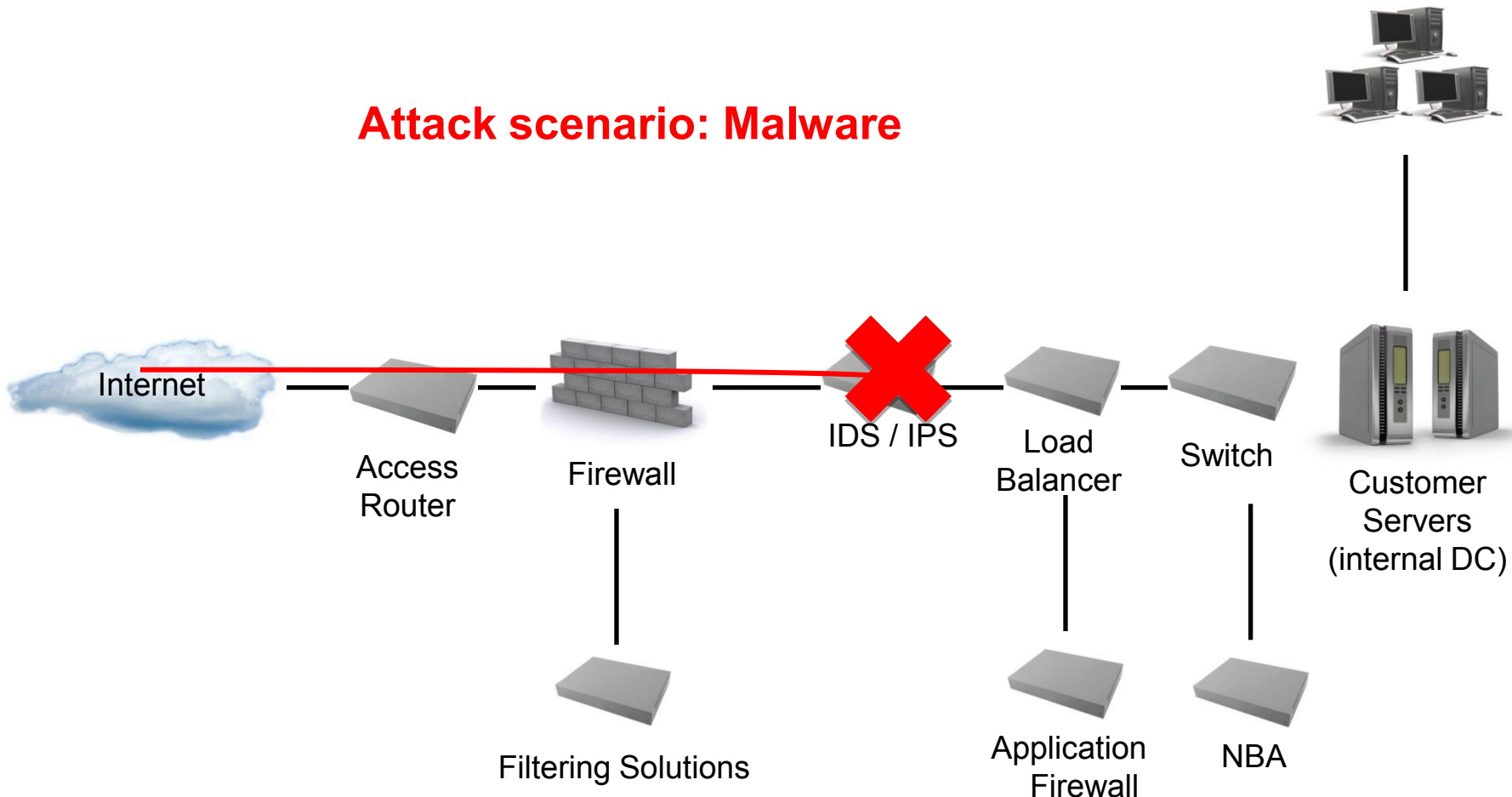
DEC 2010 - Operation Payback
(Nearly All DoS / DDoS Was Tried)

March 2011 - Operation Payback II, Codero, Netbot DDoS & Wordpress.com DDoS!!!

April 2011 - Operation Sony DDoS

TCP SYN	OPERATION	
TCP SYN+ACK		
Malware / Botnets		
TCP FIN		
TCP RESET		
TCP ACK		
TCP ACK+PSH		
TCP Fragment		
UDP		PAYBACK
ICMP		
IGMP		
HTTP Flood		
Brute Force		
HTTP Connection Floods		

Attack scenario: Malware



Attack scenario: 8M PPS SYN Flood Firewall can not be the first line of



“The rising tide of distributed denial of service attacks (DDoS) is being made much worse by a tendency to mis-deploy firewalls and intrusion prevention systems (IPS) in front of servers”

“During 2010, nearly half of all respondents had experienced a failure of their firewall or IPS due to DDoS, something that could have been avoided”

– Arbor Networks Survey of 111 Global Service Providers,
Comments Published by John E. Dunn, Feb 01, 2010 Tech World

Post-Mortem Analysis

Operation Payback Network DDoS attacks:

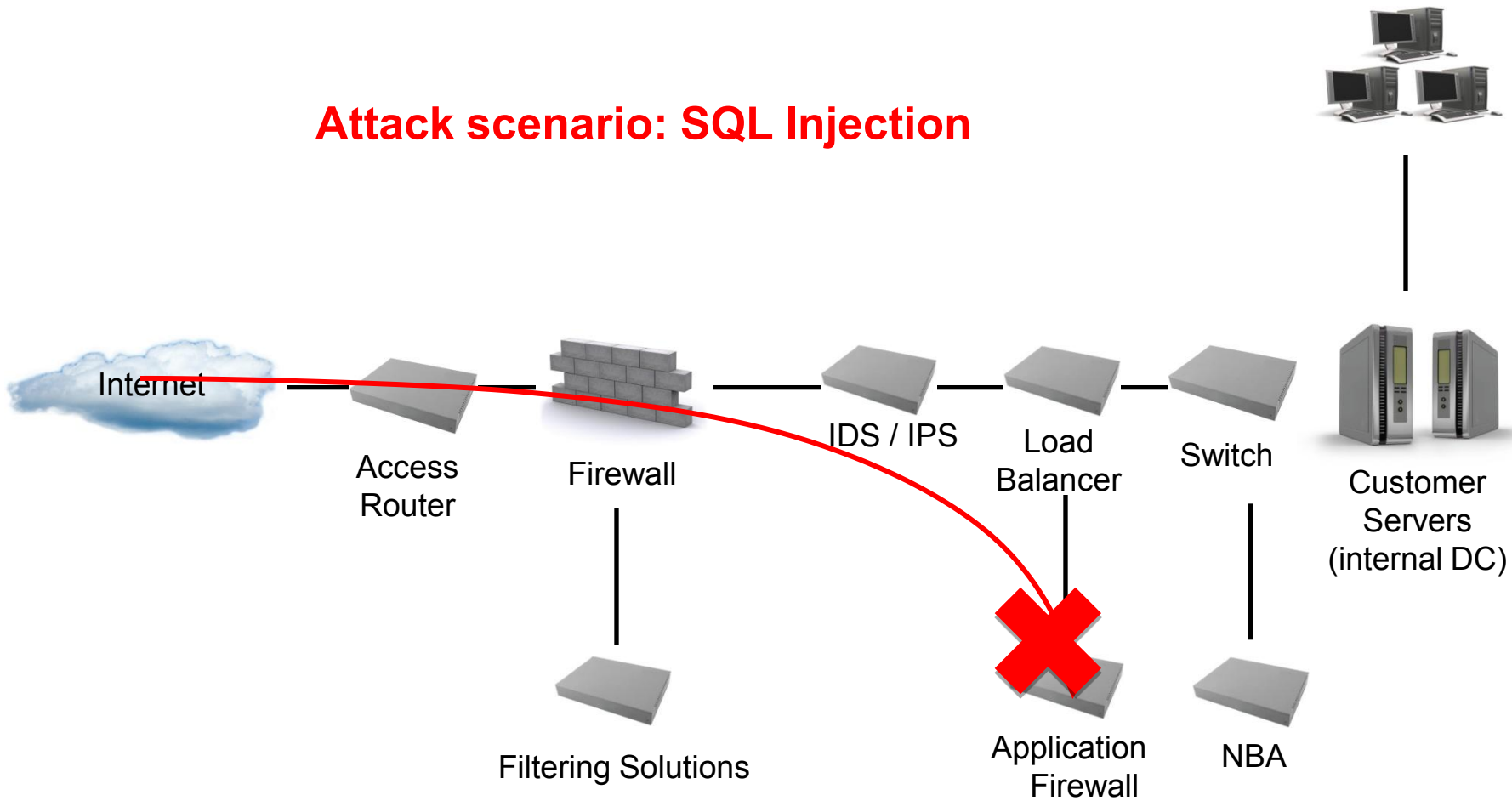
- High PPS attacks: extremely high SYN flood and UDP flood attack rates (up to 8M packets-per-second) hit victim sites.**
- Oversized UDP frames in an intent to consume bandwidth**
- Fragmented and corrupted UDP frames in an intent to consume more resources on application delivery equipment**
- Connection flood attacks: attacks that target the server TCP stack resources;**

Operation Payback Application DDoS attacks:

- HTTP page request floods targeting crafted URLs**
- HTTP data floods**
- Crafted Layer7 TCP attacks such as SlowLoris**

Inadequate Perimeter Attack Coverage: Example Two: SQL Injection

Attack scenario: SQL Injection



What Perimeter Defenses Broke Down?

- ❑ **IPS & Firewalls Deployment / Architecture Problems:** High rate attacks – Security tools themselves crashed under the load and improper placement
- ❑ **Network & Telecom Oriented Rate-Limiting Protections:** Low and slow DoS/DDoS attacks - Easily go under the radar of traditional security solution (if you define low rate thresholds you raise the false positive ratio and the opposite)
- ❑ **Application-Level Protection w/o NBA:** Today's application DDoS attacks are well integrated into legitimate forms of business delivery models - wreaking havoc with distinguishing the difference between legitimate and illegitimate traffic

Attacks

High PPS attacks

Oversized UDP frames

Fragmented and corrupted
UDP frames

Connection flood attacks

HTTP page flood attacks

Slowloris

Impacts

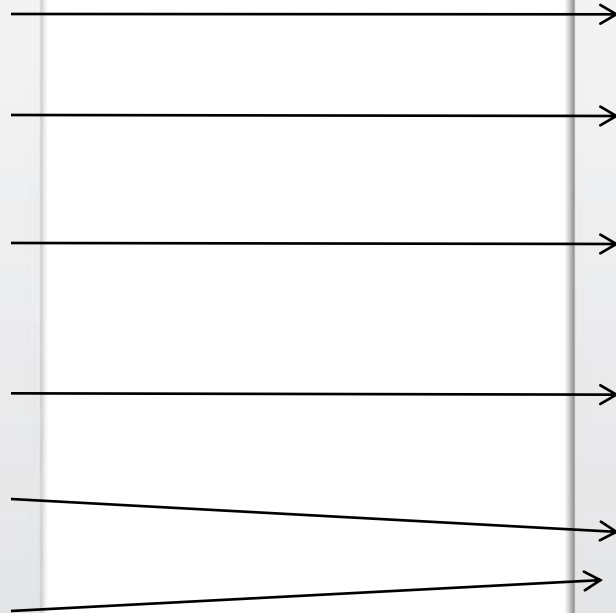
Equipment Bottlenecks

Consume network
bandwidth

Consume resources –
Memory / Processing

Consume TCP stack
resources - Processing

Consume server resources
– Memory / Processing



(Multi-Vulnerability) Is Difficult

Attack Types

High PPS attacks

Oversized UDP frames

Fragmented and corrupted
UDP frames

Protection

→ Anti-DoS / DDoS

→ IPS – In front of Firewall

→ NBA – In front of Firewall

→ IPS – In front of Firewall

No single protection tool can handle today's attack campaign threats

New Lessons Learned

Rise of Hacktivism

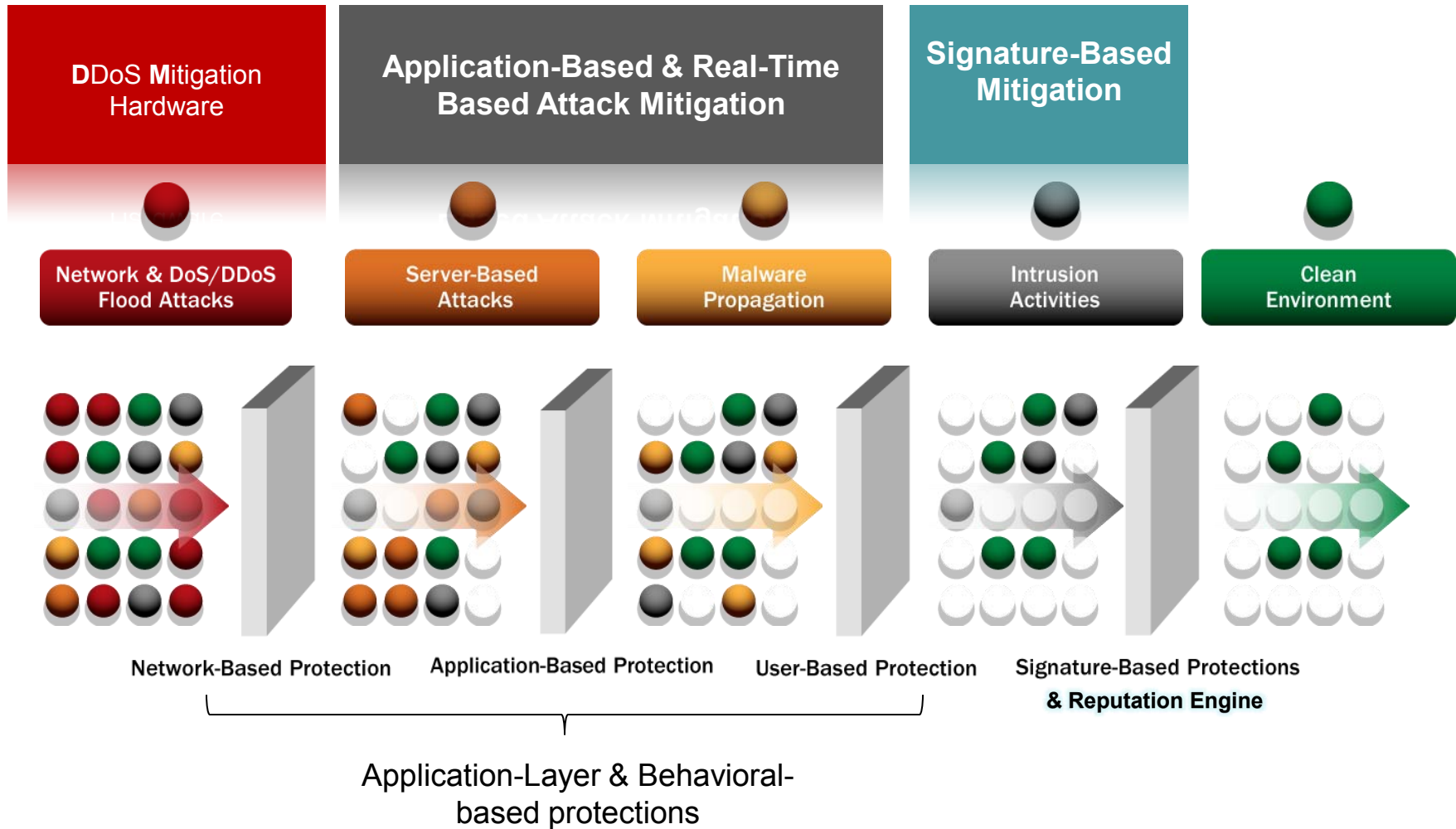
- ❑ **Cyber-retaliation: DDoS – has become a new tool for angry mobs or overzealous activists**
- ❑ **Use of social media networks for quick distribution of malicious tools and target lists**
- ❑ **Previously unqualified attackers/profiles (no signature profiles available) volunteer in attacks**
- ❑ **Bundled, multi-layered DDoS / SQL attack structures**
- ❑ **Multi-Vector: Unquantifiable scalability (any attacker from anywhere)**
- ❑ **Enterprise Risk Assessments prove Useless**
- ❑ **Defending Tools rises against Defending single vulnerabilities (LOIC vs. http-get rqst vul), defeding Stuxnet vs. Microsoft Patch Issue, etc**



**You plan for a
gap in coverage
and the gap = an
exploit.**

**New Model =
Worst Case
Scenario
Planning**

Adequation Attack Mitigation Security Architecture



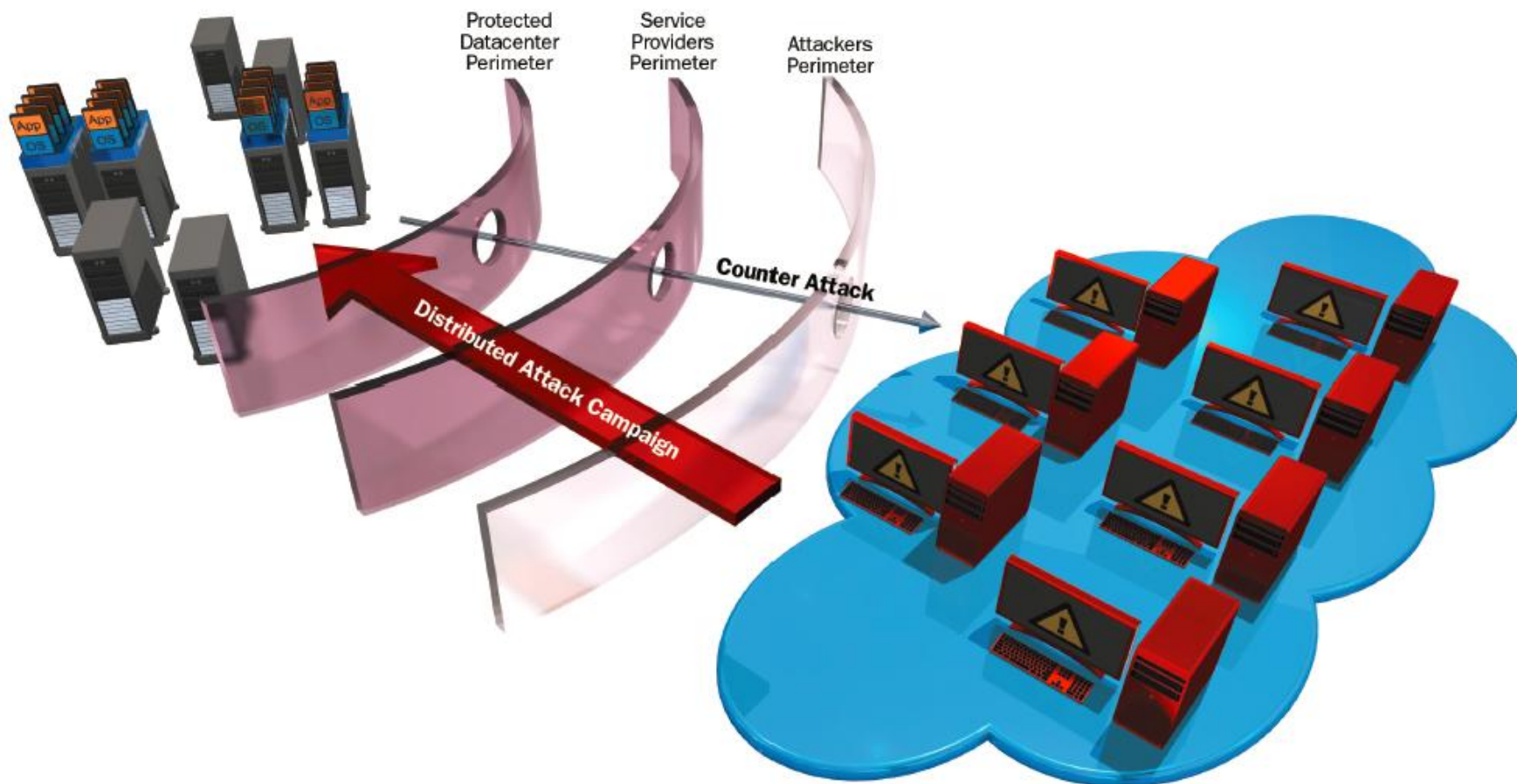
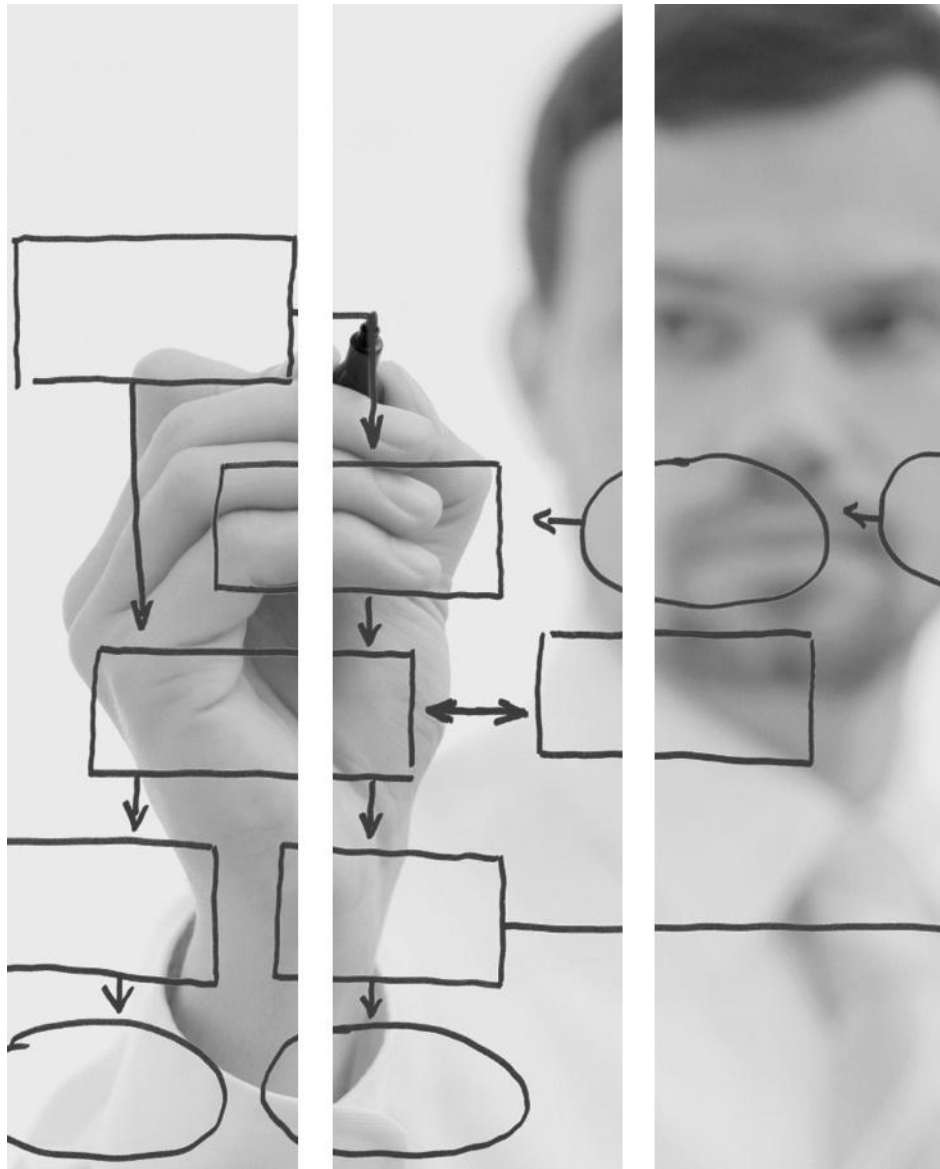


Figure 1: Breaching network perimeters with a counter attack operation

- Characteristics of Successful Perimeter Security Models:
 - Availability is as important as Confidentiality
 - Assume worst case in all situations
 - Not compliance driven
 - Think in terms of „lack of coverage“ not in vulnerability assessments – big difference
 - Defense Model built around „Tools“ and „Technique“ - - Not single Vulnerabilities

- **Dawn of Hacktivism**
 - **Definition & Key Attributes**
 - **Family Tree of Main Players**
 - **2009-2011 Have Seen a Dramatic Rise in “Hacktivism**
- **Recent Breakdown of Perimeter Defenses**
 - **Two Main Effective Tools: DDoS & SQL Injection**
 - **Disintegration of General IT Risk Models**
- **2011 Establish Numerous Lessons: High Level & Technical Level**
 - **Definitive Proof that Security Perimeter Point Solutions Are Ineffective**
 - **Few Models have Passed Successfully Battled Hacktivists**
 - **Worst Case Security Models Work!!! Risk-Adjusted Models Do Not.**
- **New Perimeter Security 10 Must Haves:**
 - **More Alerting Coverage – More Deployed Perimeter Platforms**
 - **Tighter Integration – Instantly Normalize & Correlated Data**
 - **Prioritization of Threats for Mitigation**



Thank You

Carl W. Herberger
V.P., Security Solutions
610.529.6229

Carl.Herberger@Radware.com

Smart Network. Smart Business.

© 2011, Radware, Ltd.