

# 21<sup>st</sup> Century Banking

## New Risks Management and Security Challenges

Presented by Warren Sookdar CIO

First Citizens

# San Francisco

- ❑ **San Francisco is a major city in California**
- ❑ **Estimated population 825,863**
- ❑ **Leading financial and cultural centre of Northern California.**
- ❑ **Banks (Bank of San Francisco, Sterling Bank & Trust, Wells Fargo Bank)**
- ❑ **Credit Unions (San Francisco Federal Credit Union, Provident Credit Union)**

# Location of Trinidad



# Trinidad and Tobago

- ❑ **Trinidad and Tobago is a country in the northern edge of South America**
- ❑ **Island covers an area 5,128 square km**
- ❑ **Largest economy in the Caribbean**
- ❑ **Indigenous Banks (First Citizens, Republic Bank, Intercommercial Bank)**
- ❑ **Currency TTD**

# Similar Services between banking in both countries

- Personal Banking**
- Business / Commercial Banking**
- Internet Banking**
- Voice / Mobile Banking**
- Lending Services**
- Investments**
- Websites**



## Similarities and Risks

- Global reach – No boundaries in the Virtual world**
- Physical Structure is irrelevant, website takes precedence**
- Company's website opens up the Organization to the world**
- Exploitation of data and network vulnerabilities**
- Cybercrime and Cyberwarfare**
- Reputational Risk**

# Impact of Malware

- Steals your personal information and address book (identity theft and keystroke-logging)
- Floods your browser with pop-up advertising
- Spams your inbox with advertising email
- Slows down your connection
- Hijacks browser and redirects you to an advertising or a phishing site
- Uses your computer as a secret server to broadcast pornography files.

# Distributed Denial of Service (DDoS)

- Disables Network / Cripples your organization.**
- Preventing legitimate network traffic**
- Impact**
- MODES OF ATTACK**
- PREVENTION and RESPONSE**



# Cyber Warfare

Are we in  
DENIAL?

**That will never happen to me**  
**I have nothing to hide**  
**We're too small to be a target**  
**Why me, when they could hit some  
bigger company**

Are we facing  
REALITY?

**Unfettered access to cyber weapons  
systems (computers and Internet access)**  
**Immense armies (botnets that can be  
captured or rented)**  
**Capacity for attacks to strike at our  
nation's most strategic vulnerabilities**

# Social Media

- Newest security threats - “free Apps”- What malicious content is being installed unto your network?**
- Exchanging information with third parties – Social Hackers are now “Social Engineers”!**
- Confidentiality and Sensitivity of information - Is company’s data still “secret”**
- Organization's policy Social media/ networking – stringent or relax?**

# A typical hacked Website

★ IRANIAN CYBER ARMY ★

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

IRANIAN.CYBER.ARMY@GMAIL.COM



# Hacktivism

## A combination of Politics, Internet & Hacking

Hacktivism combines three major groups

- ❑ **Anonymous** - the most publicized component of the movement
- ❑ **Cyberoccupiers** - the real activists.
- ❑ **Cyberwarriors** - patriots who group together as “cyberarmies”

# Phishing

- Is your Bank a Target?**
- How your Customer is Targeted**
- Phishing Attempts** – Link manipulation, Popup requests
- How Phishing Scams are Evolving**
- Pharming** – manipulating the HOSTS file
- Smishing** - phishing through SMS
- Vishing** - phishing through VOIP



# Phishing email

Subject: Bank of America Alert: Unauthorized Access was Detected

Date: May 27, 2012

Dear Valued Customer,

We have recently detected an unusual activity on your account.

Bank of America has placed a hold on your account until this issue will be resolved.

To ensure that your online banking service is not interrupted, please confirm your information exactly as it appears on your account , by following the link below:

[CLICK HERE](#)

We are sorry for any inconvenience that this might have caused.

© Bank of America 2012

Bank of America Alert is working 24/7 to ensure the protection of your account.

# DNS Hijacking

## What are the Dangers of DNS Hijacking?

Pharming, Phishing

## Hacktivists Turn to DNS Hijacking

## World's stealthiest rootkit pushes DNS hijacking trojan

## DNS Hijacking – Rerouting, Man in the middle

## Risk to your Organization

# Customer Threats

## Is a customer a Threat?

- Costly Customers**
- How effective is the Organization's Customer awareness program?**
- Image and Reputation of your Organization on Social Media**
- Do we really know our customer**

# Employees

- Insiders cause most high-impact security incidents successful attacks
- Employee recruitment / termination
- Rotation of duties/job rotation
- Thumb drives now a big security threat – information entering, storing and leaving the Organization.

**Are your Organization's policies enforced?**

## Who are the victims?

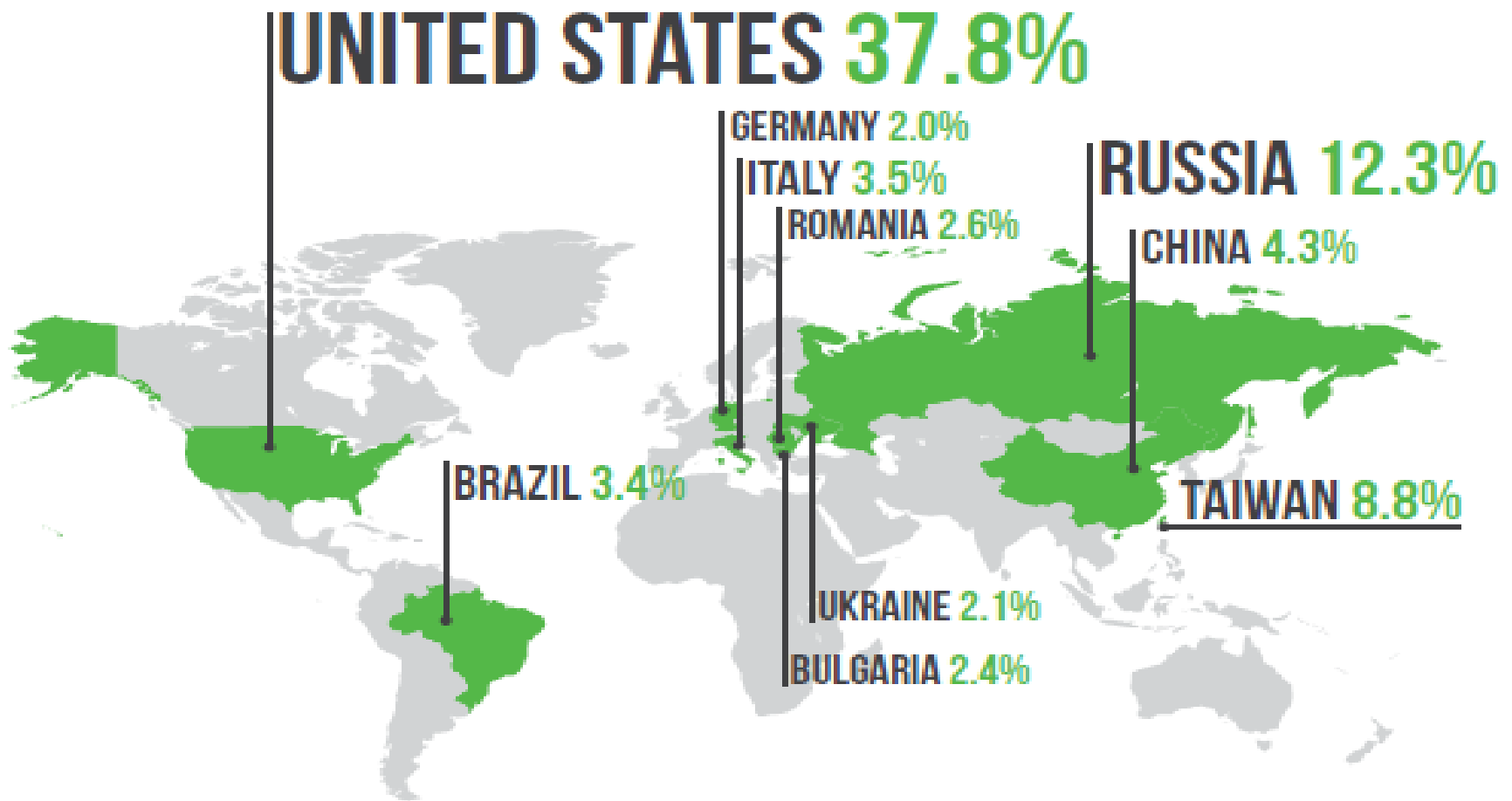
- ❑ **44%** breaches affected financial organizations
- ❑ **32%** breaches occurred in retail environments and restaurants
- ❑ **15%** network intrusions involved manufacturing, transportation, and utilities
- ❑ **9%** network intrusions hit information and professional services firms



## How do breaches occur?

- ❑ **54%** used some form of hacking
- ❑ **23%** of network intrusions exploited weak or stolen credentials
- ❑ **16%** incorporated malware
- ❑ **7%** leveraged social tactics

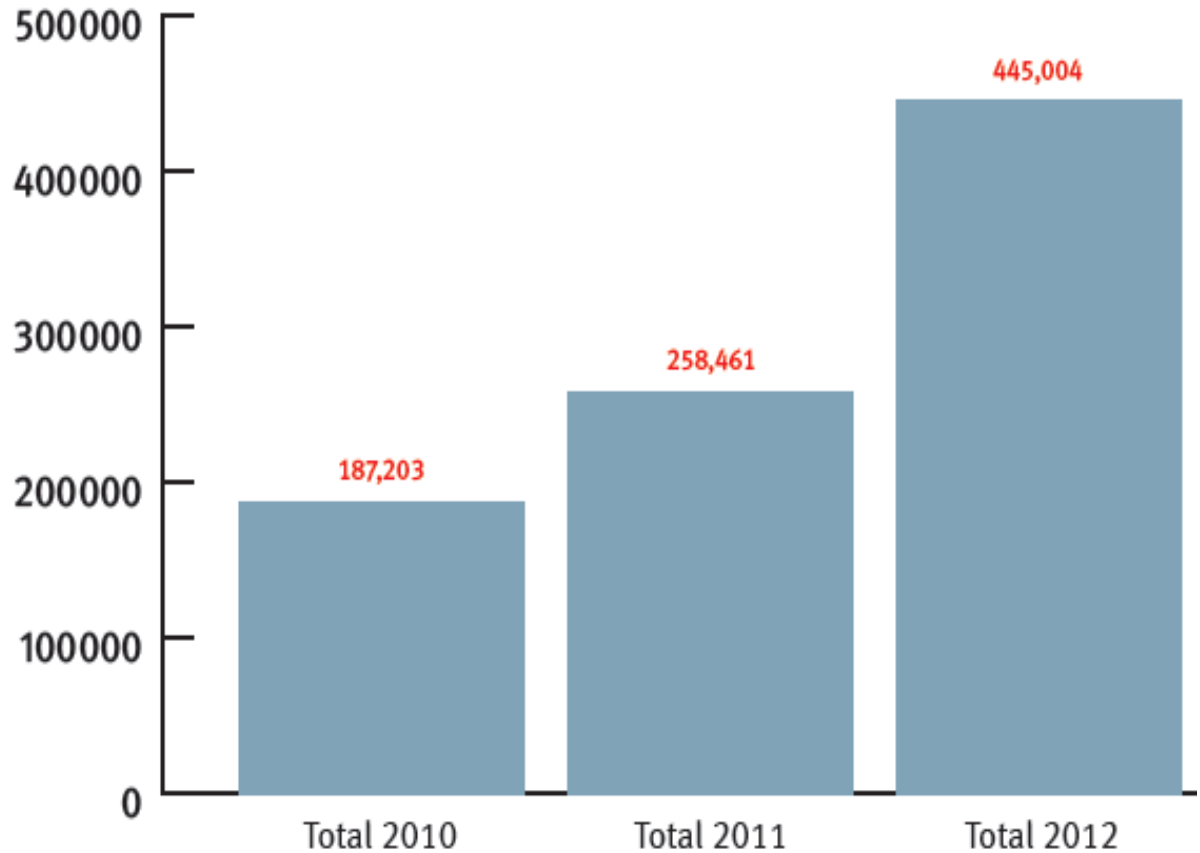
# Top 10 countries account for roughly 79% of network-based attacks



# Phishing Attacks increase

## Phishing Attacks per Year

Total number of phishing attacks detected by the RSA Anti-Fraud Command Center (AFCC) yearly.



# Network Attacks

## Free tool to perform DDOS attack

Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.25

Manual Mode (Do it yourself) IRC Mode (HiveMind) IRC server: [empty] Port: 6667 Channel: #loic Disconnected.

1. Select your target

URL:  Lock on

IP:  Lock on

3. Ready? IMMA CHARGIN MAH LAZER

Selected target

**192.168.1.7**

2. Attack options

TCP / UDP message:

HTTP Subsite:   Append random chars to the subsite / message

Method: HTTP Port: 80 Threads: 20 Timeout: 9001  Wait for reply  Use Gzip (HTTP)

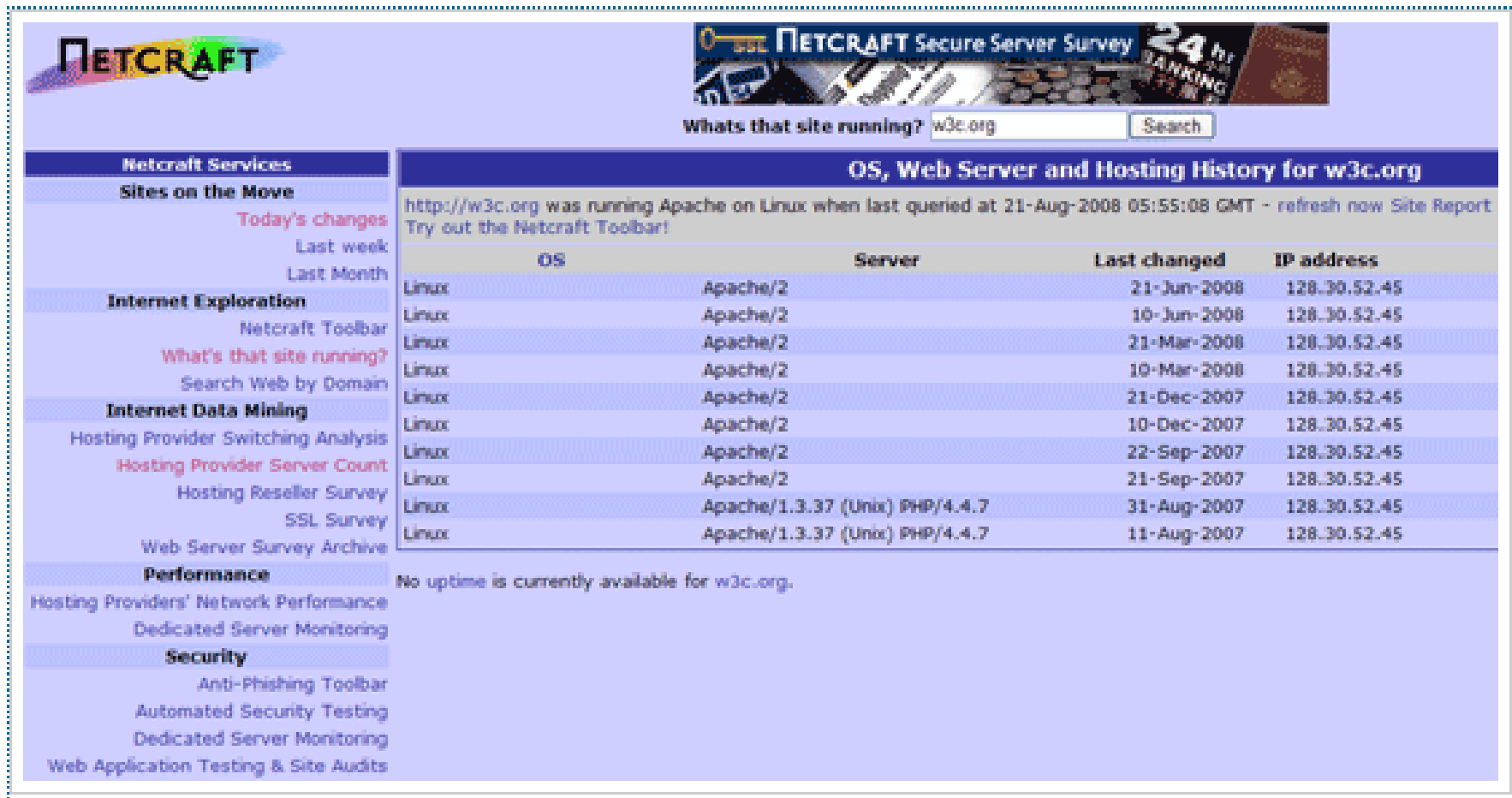
Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
20	0	0	0	64540	64540	386

github.com/NewEraCracker/LOIC

# Free tool to determine what OS a company is running

## Netcraft



The screenshot shows the Netcraft website interface. At the top, there is a search bar with the text "What's that site running? w3c.org" and a "Search" button. Below the search bar, the main content area displays the title "OS, Web Server and Hosting History for w3c.org" and a message: "http://w3c.org was running Apache on Linux when last queried at 21-Aug-2008 05:55:08 GMT - refresh now Site Report Try out the Netcraft Toolbar!".

OS	Server	Last changed	IP address
Linux	Apache/2	21-Jun-2008	128.30.52.45
Linux	Apache/2	10-Jun-2008	128.30.52.45
Linux	Apache/2	21-Mar-2008	128.30.52.45
Linux	Apache/2	10-Mar-2008	128.30.52.45
Linux	Apache/2	21-Dec-2007	128.30.52.45
Linux	Apache/2	10-Dec-2007	128.30.52.45
Linux	Apache/2	22-Sep-2007	128.30.52.45
Linux	Apache/2	21-Sep-2007	128.30.52.45
Linux	Apache/1.3.37 (Unix) PHP/4.4.7	31-Aug-2007	128.30.52.45
Linux	Apache/1.3.37 (Unix) PHP/4.4.7	11-Aug-2007	128.30.52.45

Below the table, a message states: "No uptime is currently available for w3c.org." The left sidebar contains various navigation links such as "Netcraft Services", "Sites on the Move", "Internet Exploration", "Internet Data Mining", "Performance", and "Security".



# What is your Organization doing to prevent?

- Phishing Scams**
- Network attacks**
- Viruses / Malware**
- Customer exploit**
- Internal attack by Employees**

## **What can we do?**

- ❑ Updated Risk Assessment for the Organization**
- ❑ Continuous Review / Update the Information Security Policy**
- ❑ Strengthen and Enhance existing controls which governs the operations of the Business**
- ❑ Continuous Educational and Awareness Programs**
- ❑ Partner with Experts – Above Security**



Thank You