SECURITY RISK
ADVISORS

FINANCIAL
SECURITY
OFFICERS
OF EASTERN PENNSYLVANIA

FSOEP

Web Banking & Fraud: Corporate Treasury Attacks

Your Presenters

↳ Who Are We?

Tim Wainwright
Managing Director

- ✓ Led 200+ penetration tests
- ✓ Mobile security specialist
- ✓ Speaker at RSA eFraud Forum and ISC(2)
- ✓ DLP / data protection strategy

Chris Salerno
Senior Consultant

- ✓ 150+ penetration tests including Financial Web Applications
- ✓ Mobile application specialist
- ✓ Researcher and director of content and knowledge management

Banking & Corporate Treasury Fraud
↳ Today's Discussion

- General Fraud Statistics
- Corporate Treasury Attack Lifecycle
- Exploitation Techniques
- Common Vulnerabilities
- Covering Tracks
- Defending & Monitoring
- Q&A

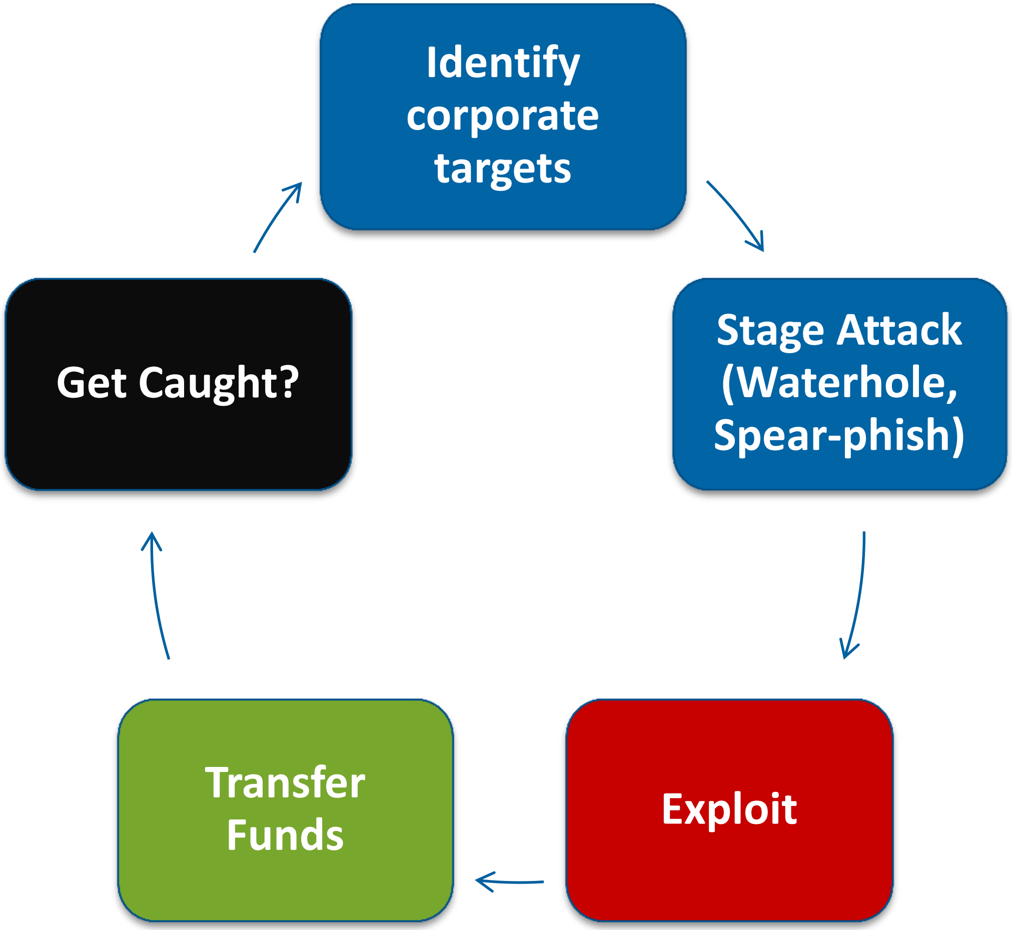
Statistics

2012 Business Banking Trust Study

- **75%** of participating businesses experienced online ATO and/or fraud
- **54%** increase in businesses accessing online banking from mobile devices.
- **43%** of banks did not change security practices at all following a fraud.
- **40%** of businesses said they have moved their banking activities elsewhere after a fraud incident
- **72%** of businesses still feel that their institution should be ultimately responsible for securing online accounts
- **70%** of businesses that suffered fraud losses were not fully reimbursed by their financial institution.

Source: Ponemon Institute

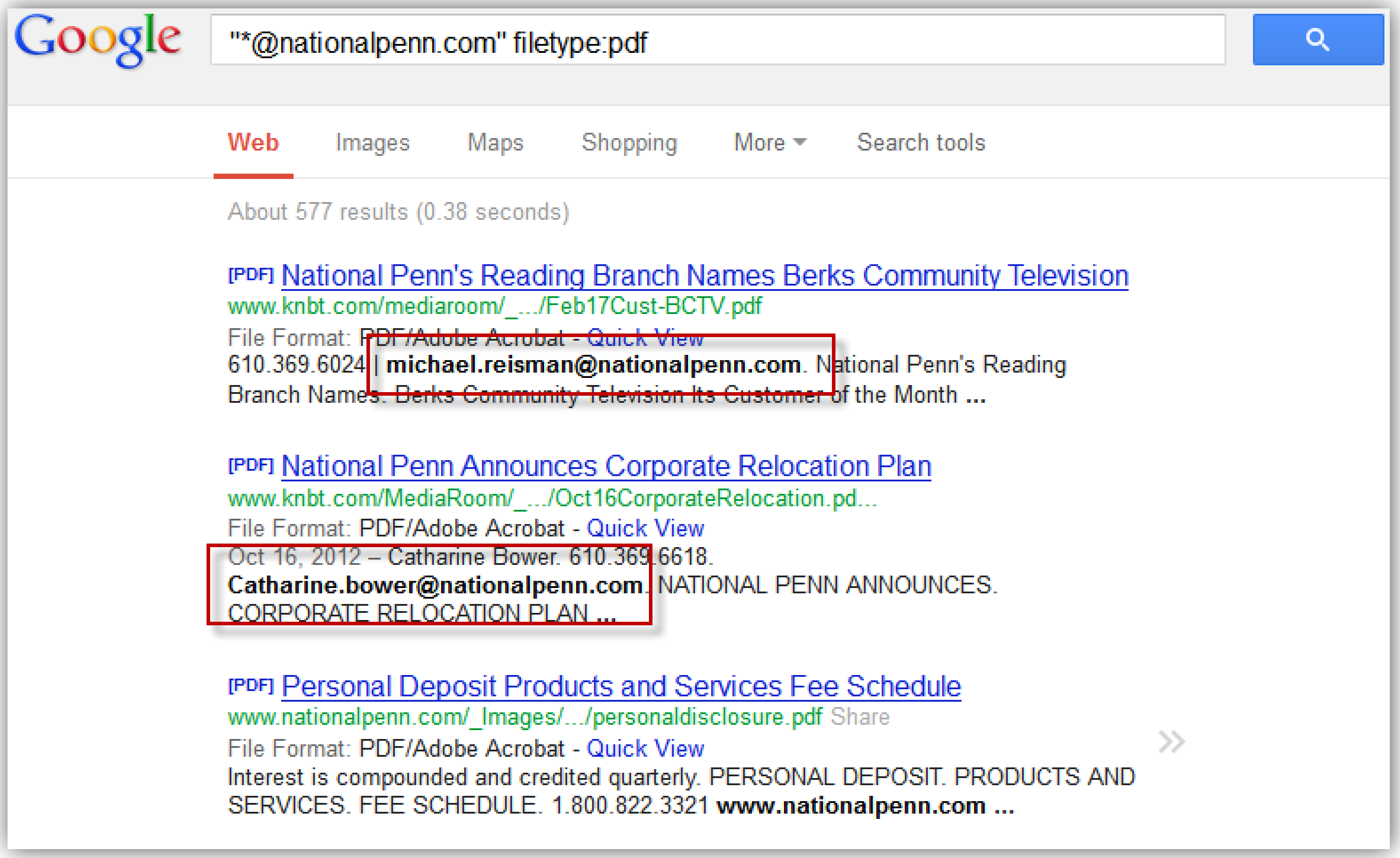
Banking Fraud
↳ Attacker Lifecycle



Identify corporate targets
Stage Attack (Waterhole, Spear-phish)
Exploit
Transfer Funds
Get Caught?

Reconnaissance
↳ Building a Target List

- Google search to obtain the email address "format"



"*@nationalpenn.com" filetype:pdf

About 577 results (0.38 seconds)

[PDF] National Penn's Reading Branch Names Berks Community Television
www.knbt.com/mediaroom/_.../Feb17Cust-BCTV.pdf
File Format: PDF/Adobe Acrobat - Quick View
610.369.6024 | **michael.reisman@nationalpenn.com**. National Penn's Reading Branch Names. Berks Community Television Its Customer of the Month ...

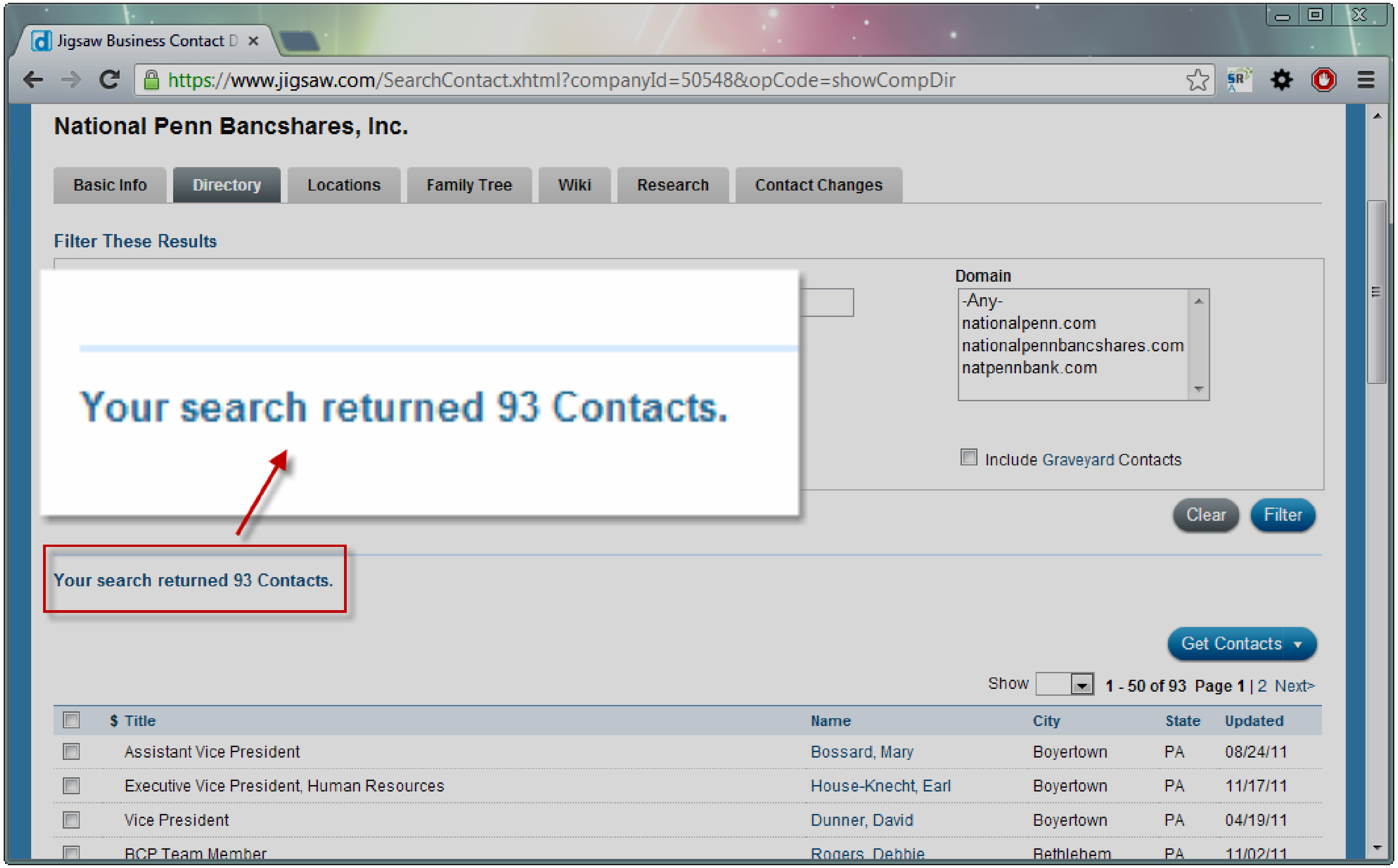
[PDF] National Penn Announces Corporate Relocation Plan
www.knbt.com/MediaRoom/_.../Oct16CorporateRelocation.pd...
File Format: PDF/Adobe Acrobat - Quick View
Oct 16, 2012 – Catharine Bower. 610.369.6618. **Catharine.bower@nationalpenn.com**. NATIONAL PENN ANNOUNCES. CORPORATE RELOCATION PLAN ...

[PDF] Personal Deposit Products and Services Fee Schedule
www.nationalpenn.com/_Images/.../personaldisclosure.pdf Share
File Format: PDF/Adobe Acrobat - Quick View
Interest is compounded and credited quarterly. PERSONAL DEPOSIT. PRODUCTS AND SERVICES. FEE SCHEDULE. 1.800.822.3321 **www.nationalpenn.com** ...

Identification

Building a Target List

- Use free services to create a list (Jigsaw, Google, LinkedIn, etc)


Jigsaw Business Contact D
https://www.jigsaw.com/SearchContact.xhtml?companyId=50548&opCode=showCompDir
Basic Info
Directory
Locations
Family Tree
Wiki
Research
Contact Changes
Clear
Filter
Get Contacts

National Penn Bancshares, Inc.

Filter These Results

Domain
-Any-
nationalpenn.com
nationalpennbancshares.com
natpennbank.com

□ Include Graveyard Contacts

Your search returned 93 Contacts.

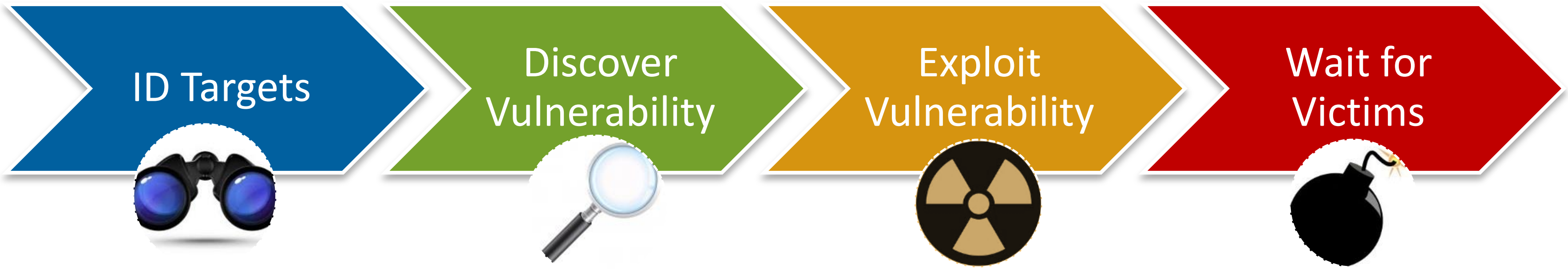
Your search returned 93 Contacts.

Show 1 - 50 of 93 Page 1 | 2 Next>

□	$ Title	Name	City	State	Updated
□	Assistant Vice President	Bossard, Mary	Boyertown	PA	08/24/11
□	Executive Vice President, Human Resources	House-Knecht, Earl	Boyertown	PA	11/17/11
□	Vice President	Dunner, David	Boyertown	PA	04/19/11
□	BCP Team Member	Rogers, Debbie	Bethlehem	PA	11/02/11

Exploitation

↳ Techniques: Watering Hole



ID Targets

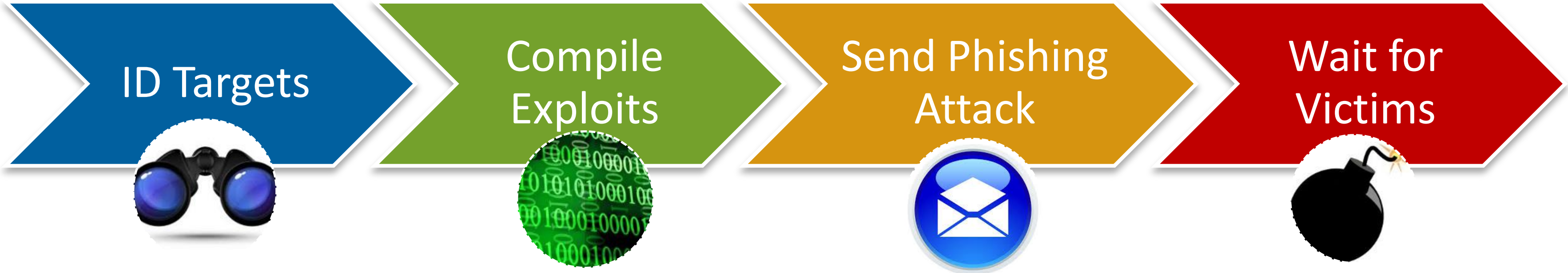
Discover Vulnerability

Exploit Vulnerability

Wait for Victims

1. The attacker identifies and profiles who they want to target
2. Attacker tests and identifies sites for vulnerabilities
3. Attacker injects JavaScript redirection code into the site
4. Attacker waits for victims to visit the website. Once someone visits, they are prompted to run malicious Java code, download malware or are redirected to a malicious site.
5. The attacker can redirect the user to a replica banking site that captures customer banking credentials

Exploitation
↳ Techniques: Spear Phishing



1. The attacker identifies and profiles who they want to target
2. Attacker identifies a flaw in common 3rd party or Operating System software such as Java or Windows
3. Attacker sends a convincing phishing attack to the victim's that may include a custom domain name and malicious replica site.
4. Attacker waits for victims to click the link inside the email and gain full control over the victim machine.
5. Once full control is obtained, the attacker can run a keystroke logger that captures banking credentials

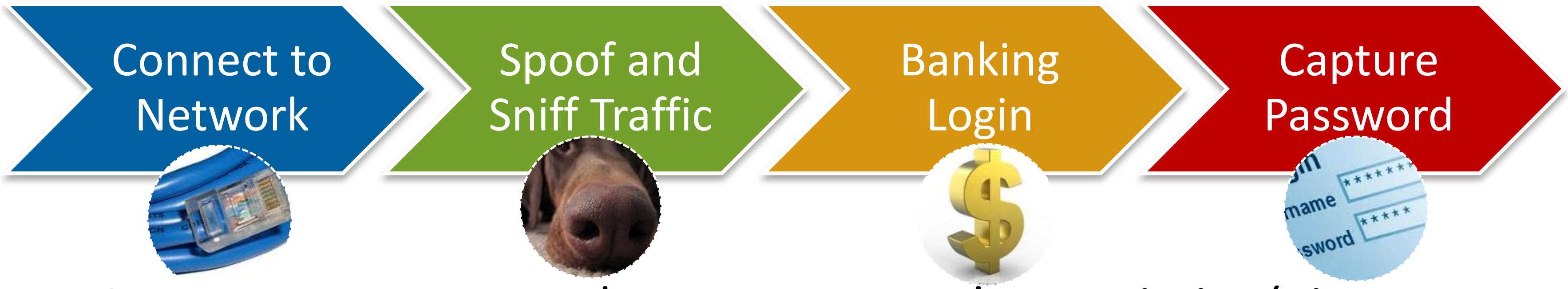
Case Studies
Good Examples!

- **EMI v. Comerica Bank**
  - $1.9mm in fraudulent transactions, 560k reimbursed by bank
  - Bank should have detected volume and anomalies
  - Comerica's client were experience phishing attacks

- **Village View Escrow v. Professional Business Bank**
  - Settlement > 400k (more than actual losses!)
  - 26 unauthorized wire transfers
  - Simple user name and password login for bank website
  - Hackers disabled email alerts
  - No procedures to recover funds (incident response)

Exploitation

Techniques: Man in the Middle



Connect to Network

Spoof and Sniff Traffic

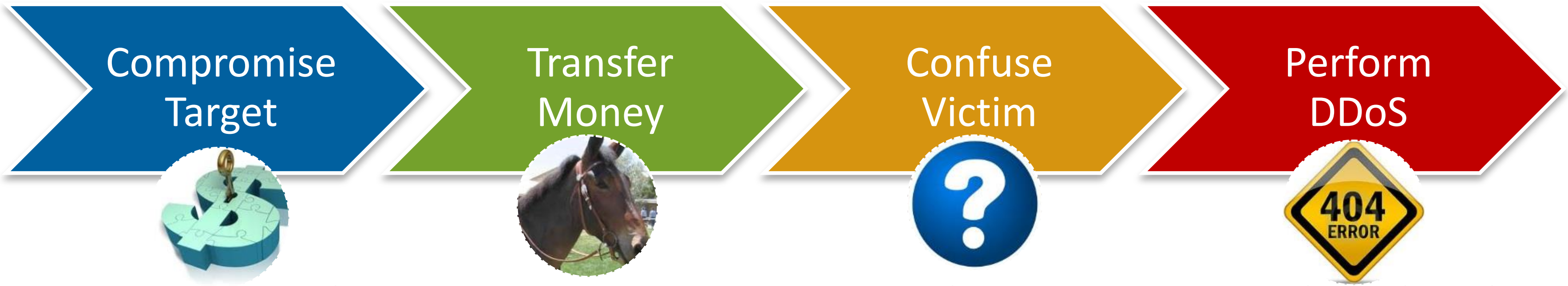
Banking Login

Capture Password

1. Attacker connects to the same network as a victim (airport, coffee shop, home, local office network)
2. Attacker spoofs and sniffs traffic between the victim and the Internet
3. Victim visits treasury sites and systems not protected against MiTM attacks.
4. Attacker captures banking login credentials

Hiding Tracks

Techniques: Denial of Service



Compromise Target

Transfer Money

Confuse Victim

Perform DDoS

1. Attacker obtains access to victim workstation and online banking site through an exploitation technique
2. Use Mule’s to initiate transfers for money from the victim to an offshore account.
3. Use access to victim’s machine to prevent them from accessing their bank account
4. Perform a Distributed Denial of Service (DDoS) attack on the victim’s banking site to mask the money transfers and prevent others from authenticating

Case Studies

Legal Lessons

- **PATCO v. Ocean Bank**
  - Originally ruled for bank, but appealed and settled for undisclosed amount
  - ATO was not prevented due to “one size fits all” controls
  - Dispute over simple user name and password login for bank website. Originally, court found it adequate.
  - Article 4A: banks typically liable for losses in unauthorized transfers

Exploitation
Common Attacks

- **Using Your Resources Against You**
  - Cross-site Scripting (XSS)
  - URL Redirection
- **Social Engineering**
  - Your employees (Helpdesk, Support)
  - Insider Jobs
  - Your 3rd parties (hosting and service providers, partners)
- **Banking Specific Trojans**
  - Zeus / Spyeye
  - Citadel
  - Guass
  - Gozi

Exploitation

Exploits Used in 2011 / 2012

Exploit Pack	Java Exploit	Adobe Exploit	Microsoft Exploit
Blackhole	X	X	X
Kein	X	X	
Sakura	X		
Nuclear	X		
Redkit	X		
Neosploit	X		
Gong DA	X	X	X
Sweet Orange	X		
Crimeboss	X		
Cool Pack	X		X
Phoenix	X	X	

Source: Deepend Research (2012)

Defending and Monitoring
↳ Spear-phishing controls

Desktop Controls

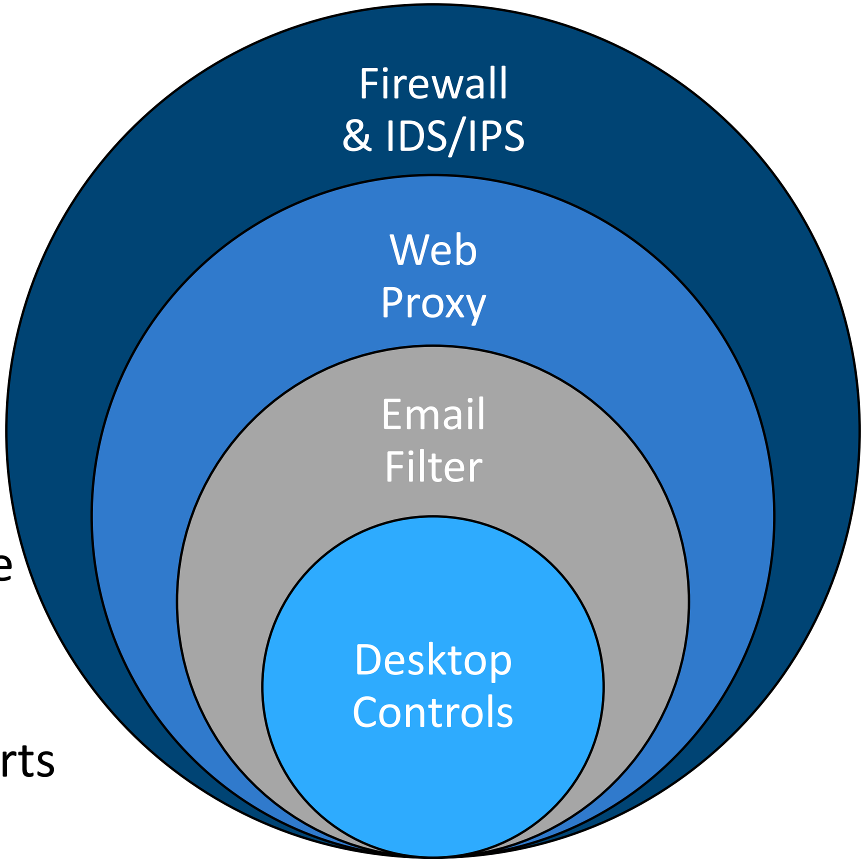
- Patch the operating system and browsers
- Update 3rd party apps (Java, Flash, etc)

Email Filter

- Don't allow risky attachments
- Executables, scripts, PDF's with java code, office documents with macros

Web Proxy

- Restrict known unsafe sites, be proactive



Firewall & IDS/IPS

- Restrict outbound traffic on unknown ports
- Baseline and alert on anomalies
- Advanced malware detection

Defending and Monitoring
↳ Hardening Cash Mgmt Systems

Treasury & Cash Management Systems

- Segment / isolate banking workstations
- Increase workstation logging and monitoring
- Additional security software
- Secure password management software for users
- Limited outbound access

Banking Partners

- Strong authentication to treasury systems and bank websites
- Trusteer or custom from the bank
- Whitelisted payees / confirmations from bank

Procedures

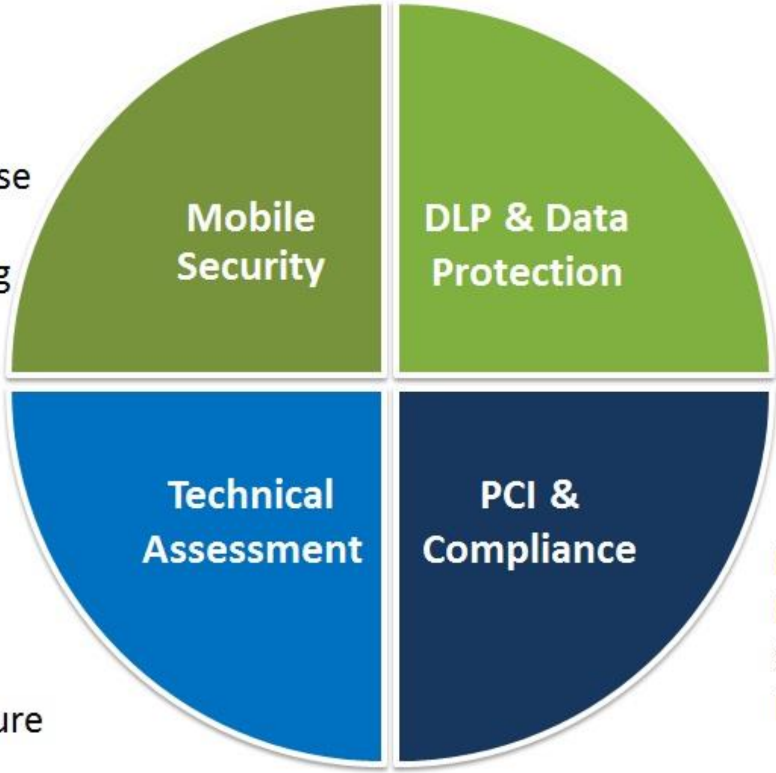
- Do reconciliation frequently
- Expect attacks to be staged on Friday and carried out over the weekend

Q&A

You Ask, We Answer

SECURITYRISK ADVISORS

- ✓ Mobile security strategy
- ✓ Policy and controls expertise
- ✓ Development standards
- ✓ Mobile app security testing


Mobile Security

DLP & Data Protection

Technical Assessment

PCI & Compliance

- Data Loss Prevention (DLP) requirements and selection ✓
- DLP implementation ✓
- DLP process improvement ✓

- ✓ Penetration testing
- ✓ Web application security
- ✓ Cloud applications
- ✓ SAP risk assessment
- ✓ Product security architecture

- PCI gap analysis ✓
- Remediation assistance ✓
- Scope reduction advice ✓
- ISO, FFIEC, HIPAA/HITECH ✓