Trustwave®

SpiderLabs℠

Global Security Statistics and Trends
Analysis of 2009 Investigations and Penetration Tests

Nicholas J. Percoco

Senior Vice President, Trustwave SpiderLabs

Agenda

- **About the Report**
- **Analysis of 2009 Incident Response Investigations**
  - About the Sample Set
  - Investigative Conclusions
  - Anatomy of a Data Breach
- **Analysis of 2009 Penetration Tests**
  - About the Sample Set
  - Top 10 Lists
- **Conclusions**
- **Where to get it?**
- **Contacts**

About The Report

- Planning started in early 2009
- 10x the number of PenTests vs. Investigations
- A tool for organizations in prioritizing 2010 initiatives
- This is NOT a survey; only real-life data
- A tool for individuals at multiple levels

Analysis of Incident Response Investigations

Why? Organizations are Reacting!

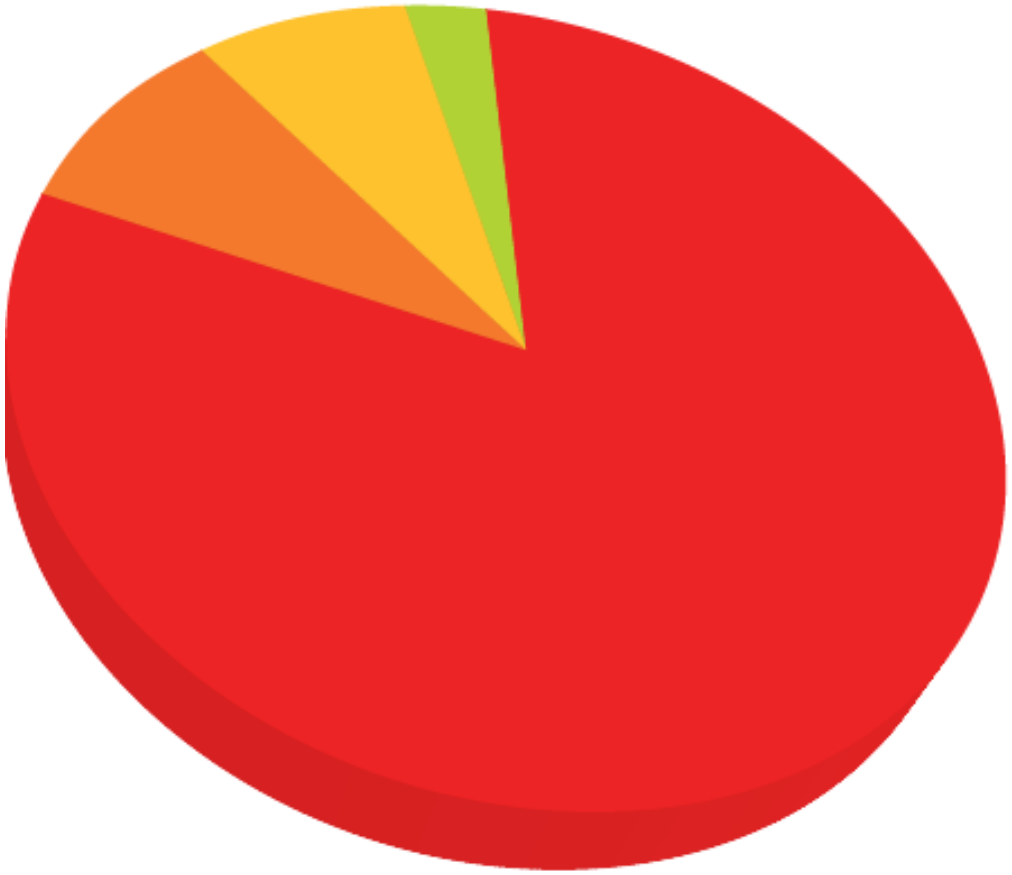
- Perform Actions to Stop an Attack
  - Understand the attack
  - Understand the losses
- Provide Reporting to Interested Parties
- Assist Law Enforcement
  - Apprehend criminals

Incident Response – About the Sample Set

218 Investigations

- 24 countries
- 18% Found Inconclusive
  - No evidence of critical data leaving
  - Many factors impact an inconclusive case
- Average of 156 Days Lapse Between Initial Breach and Detection (!?!?!)

Incident Response – About the Sample Set



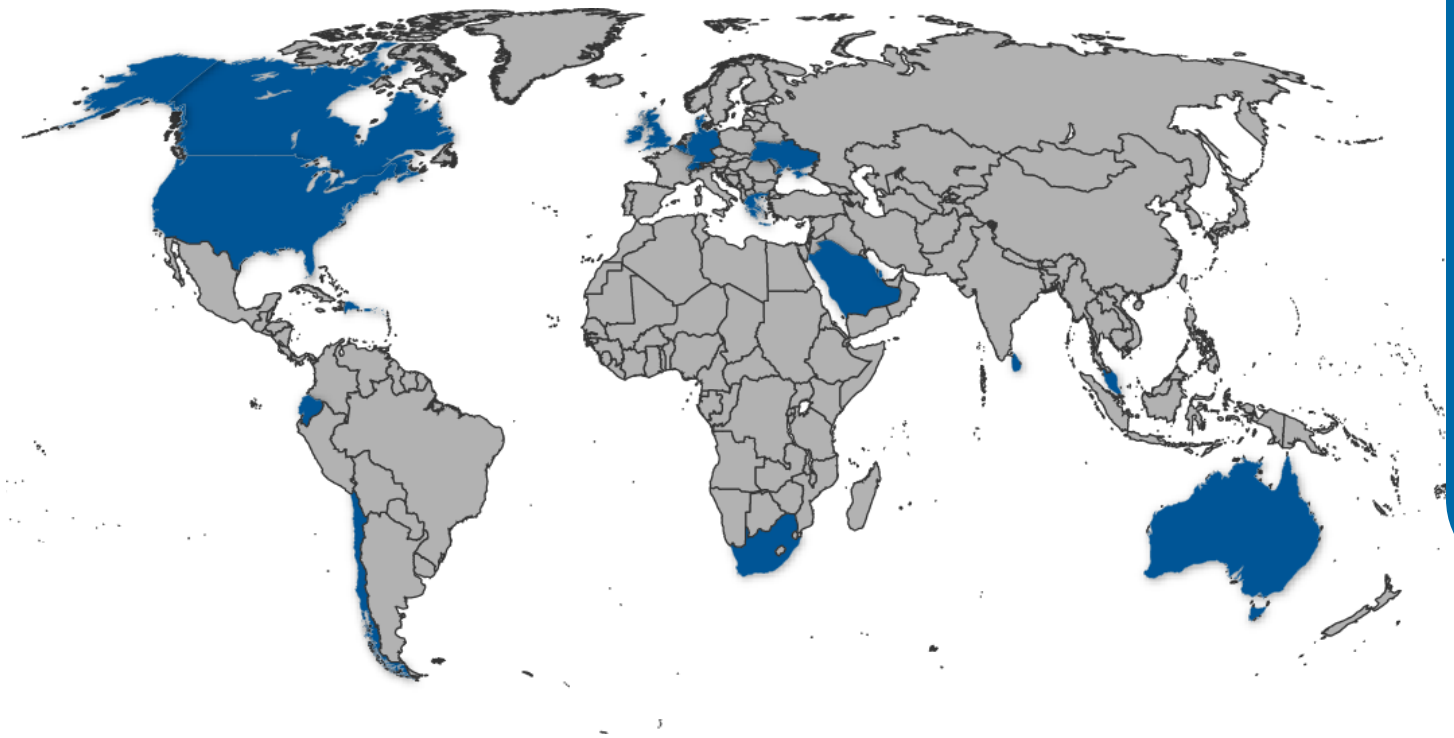
Types of Detection

- Regulator Detection 80%
- Self-Detection 9%
- Public Detection 8%
- Law Enforcement 3%

Regulator detection is the most successful because card brands are able to correlate fraud use with common legitimate sources.

Incident Response – About the Sample Set

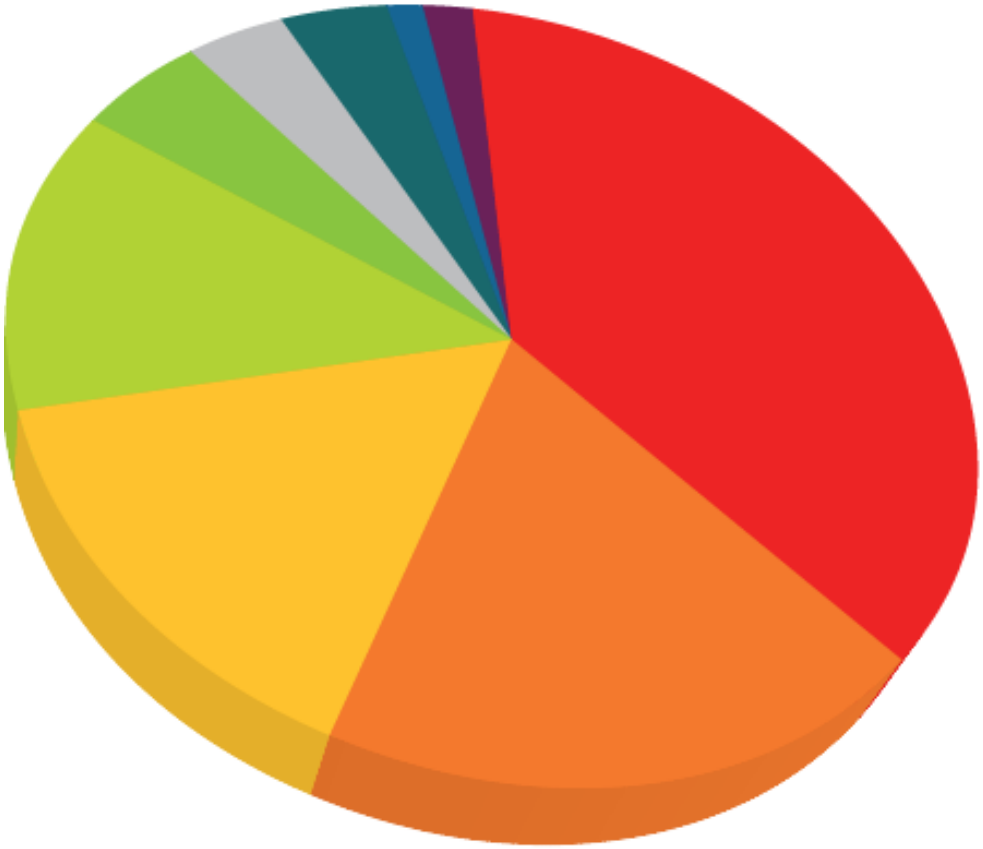
Countries Represented in 2009



Australia
Belgium
Canada
Chile
China
Cyprus
Denmark
Dominican Republic
Ecuador
Germany
Greece
Ireland
Luxembourg
Malaysia
Puerto Rico
Saudi Arabia
South Africa
Sri Lanka
Switzerland
Ukraine
United Arab Emirates
United Kingdom
United States
Virgin Islands

SpiderLabs visited 24 different countries in 2009 to perform compromise investigations.

Incident Response – About the Sample Set

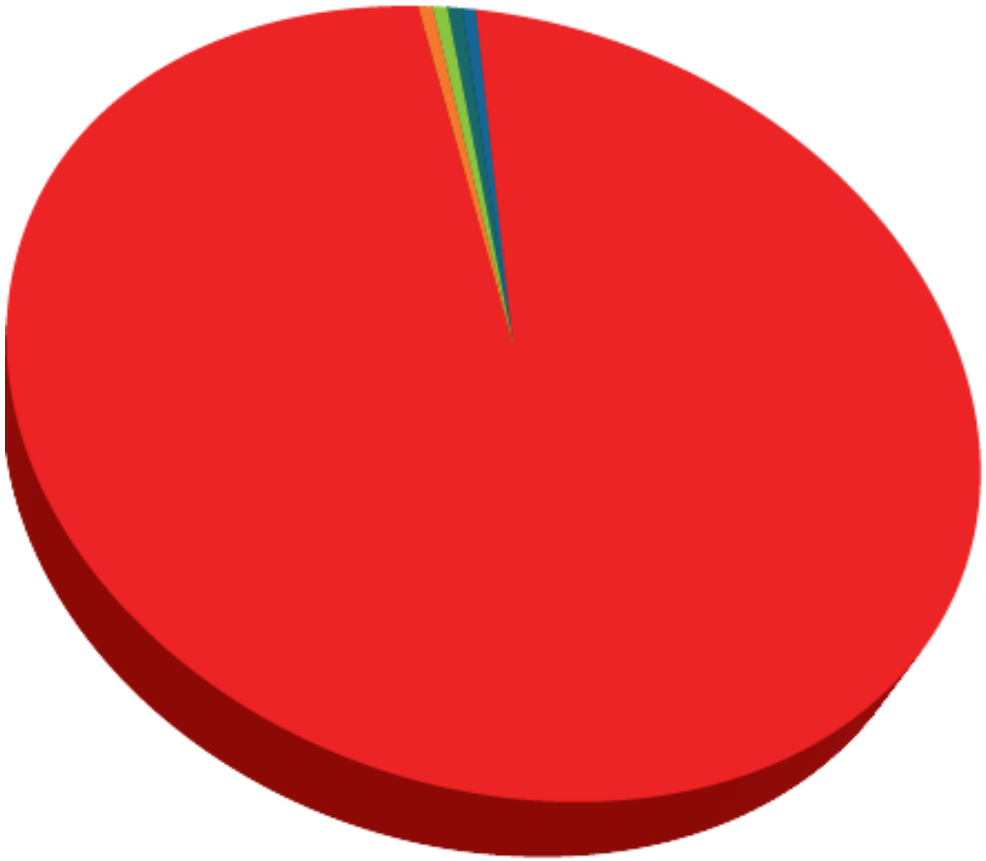


Industries

- Hospitality 38%
- Financial Services 19%
- Retail 14.2%
- Food & Beverage 13%
- Business Services 5%
- Other 4%
- Technology 4%
- Education 1.4%
- Manufacturing 1.4%

Non-traditional targets made up more than 50% of the 2009 cases.

Incident Response – Investigative Conclusions

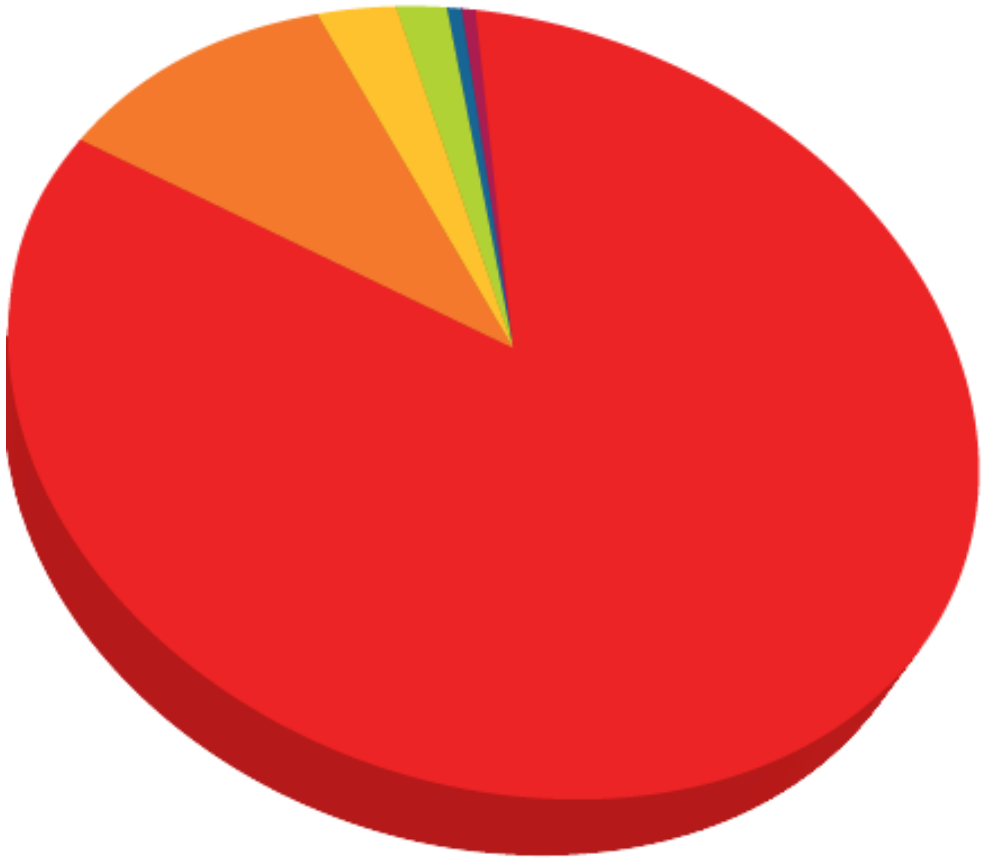


Types of Data at Risk

- Payment Card Data 98%
- Authentication Credentials <1%
- Financial Information <1%
- Other Sensitive Data <1%
- Health Care <1%

Payment Card Data is a target for criminals looking to turn data into cash quickly.

Incident Response – Investigative Conclusions



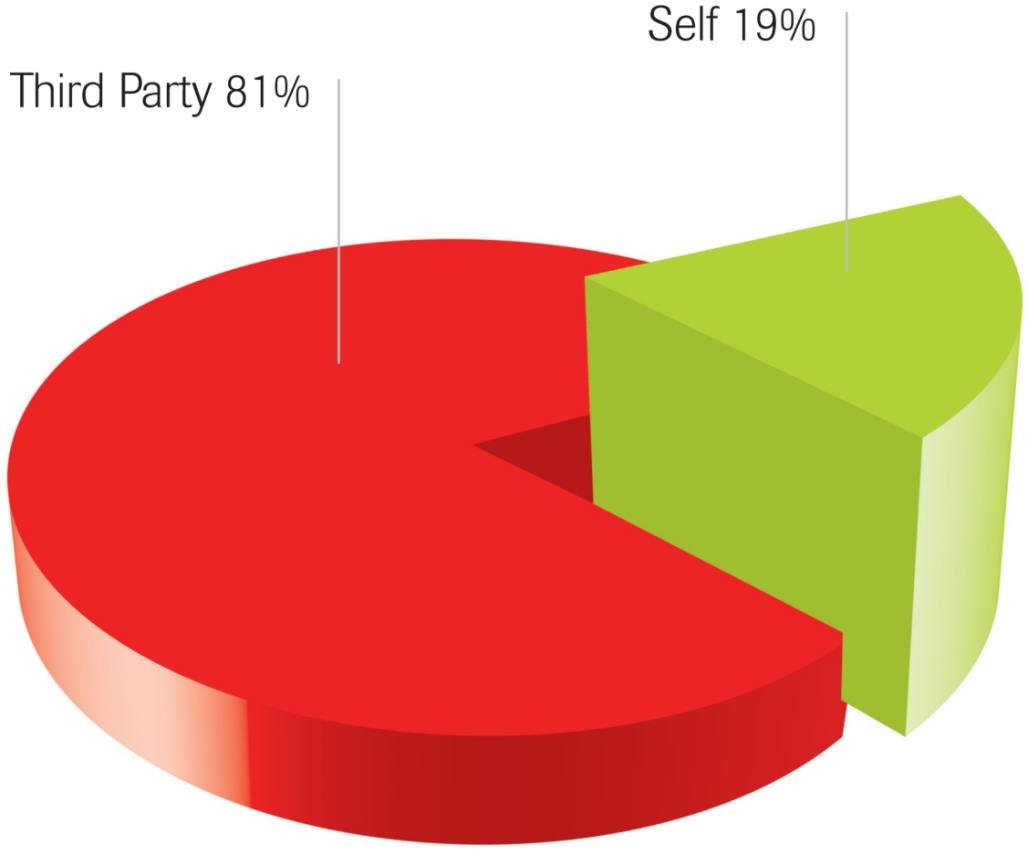
Types of Target Assets

- Software-based POS 83%
- E-commerce 11%
- Payment Processing 3%
- ATM 2%
- Web-based Portal <1%
- Workstation <1%

While many POS vendors have patched their systems to support security controls, many companies are still running very old software.

Incident Response – Investigative Conclusions

System Administration Responsibility



Third Party vendors are often negligent in their administration of security controls and best practices.

Incident Response – Investigative Conclusions

Attacker Source Address Geography

Anatomy of a Data Breach

Three Components:

1. Initial Entry
2. Data Harvesting
3. Exfiltration

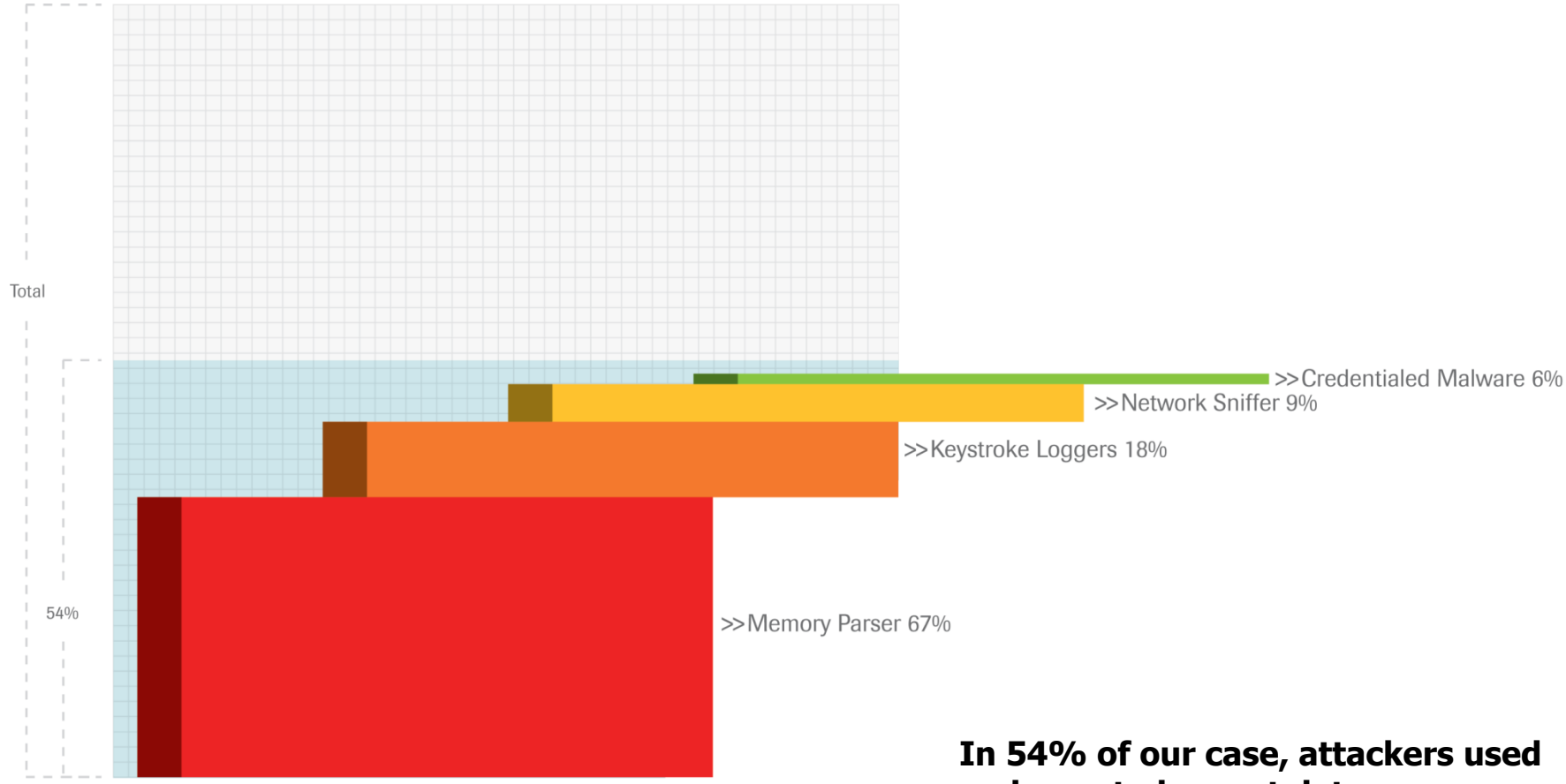
Anatomy of a Data Breach – Initial Entry

Top Methods of Entry Included:

- **Remote Access Applications [45%]**
  - Default vendor supplied or weak passwords [90%]
- **3rd Party Connections [42%]**
  - MPLS, ATM, frame relay
- **SQL Injection [6%]**
  - Web application compromises [90%]
- **Exposed Services [4%]**
- **Remote File Inclusion [2%]**
- **E-mail Trojan [<1%]**
  - 2 recent Adobe vulnerability cases
- **Physical Access [<1%]**

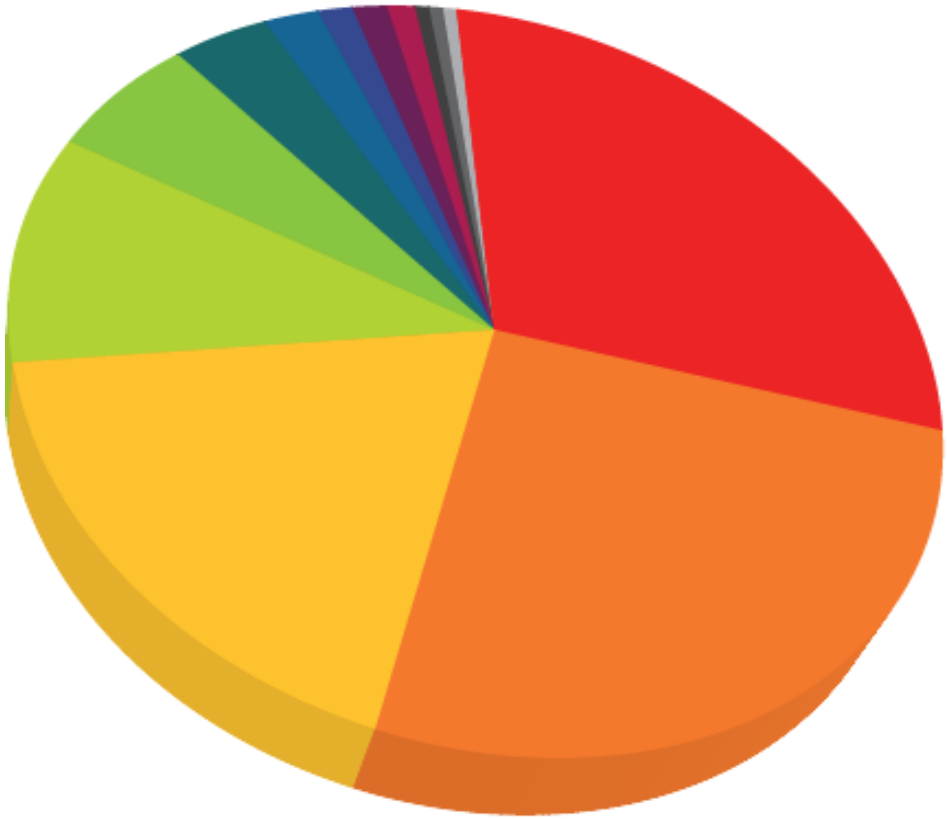
Anatomy of a Data Breach – Data Harvesting

Top Methods of Harvesting (Using Malware):



In 54% of our case, attackers used malware to harvest data.

Anatomy of a Data Breach - Exfiltration



Top Methods of Data Exfiltration

- Microsoft Windows Network Shares 28%
- Native Remote Access Application 27%
- Malware Capability: FTP 17%
- Native FTP Client 10%
- SQL Injection 6%
- Malware Capability: SMTP 4%
- Malware Capability: IRC 2%
- HTTP File Upload Site 1.5%
- Exposed Private Web Application Interface 1.5%
- Backdoor: Nalicious PHP-based Web Shell 1%
- Physical Access <1%
- Anonymous FTP <1%
- Encrypted Backdoor <1%

Network shares were used to transfer data between organization that had "trusted" links with each other.

Analysis of Penetration Tests

Why? Organizations are Proactive!

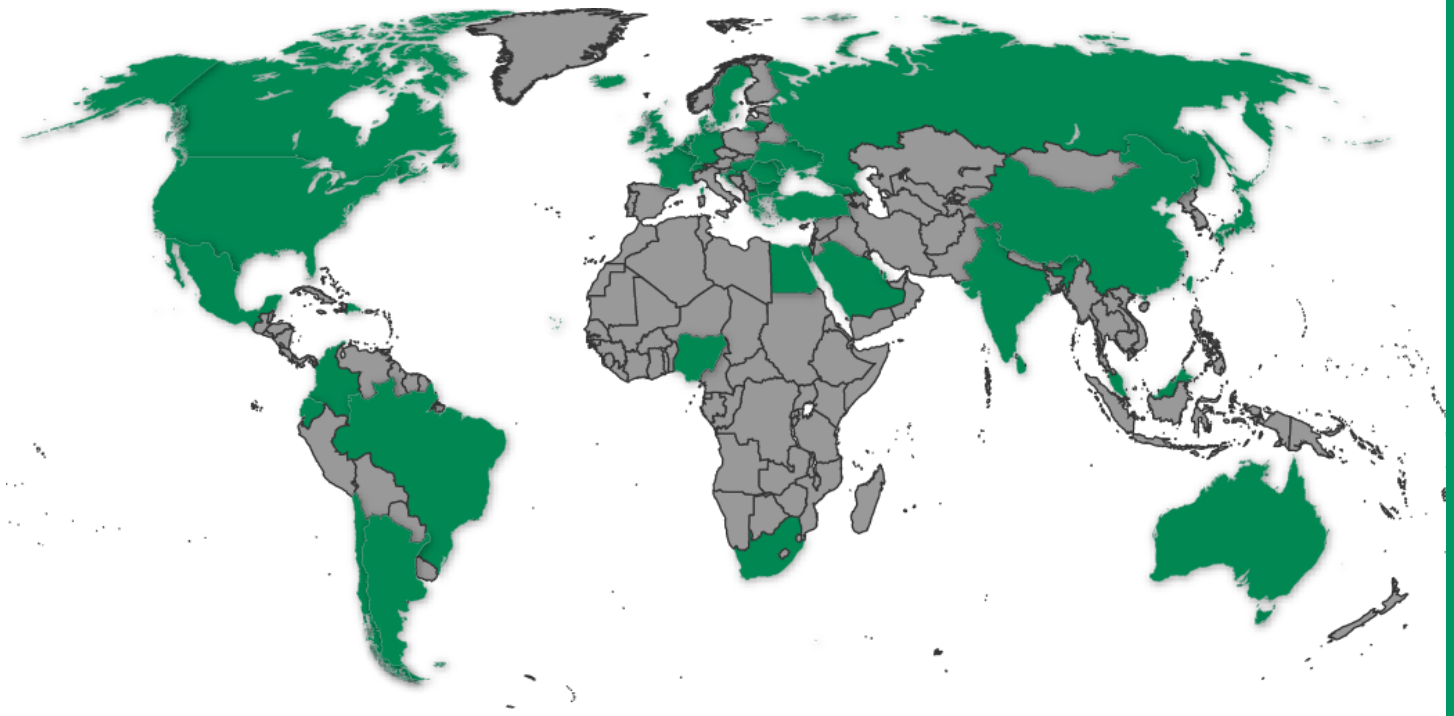
- Understand Security Posture
  - Multiple vectors
    - External network
    - Internal network
    - Wireless
    - Physical/social
    - Application
  - "What is our risk to compromise?"
- Provide Reporting to Executives and Technical Staff
- Assist in Prioritization of Risks

Penetration Tests – About the Sample Set

- 1,894 Penetration Tests
  - 48 countries
- Many Included a Mixture of Vectors
  - Network, application, wireless, physical
- Tests Averaged 80 hours in Length
  - Over 100,000 hours of testing was performed
- Classified as Manual Testing
  - Some tools are used but mostly for low level tasks

Penetration Tests – About the Sample Set

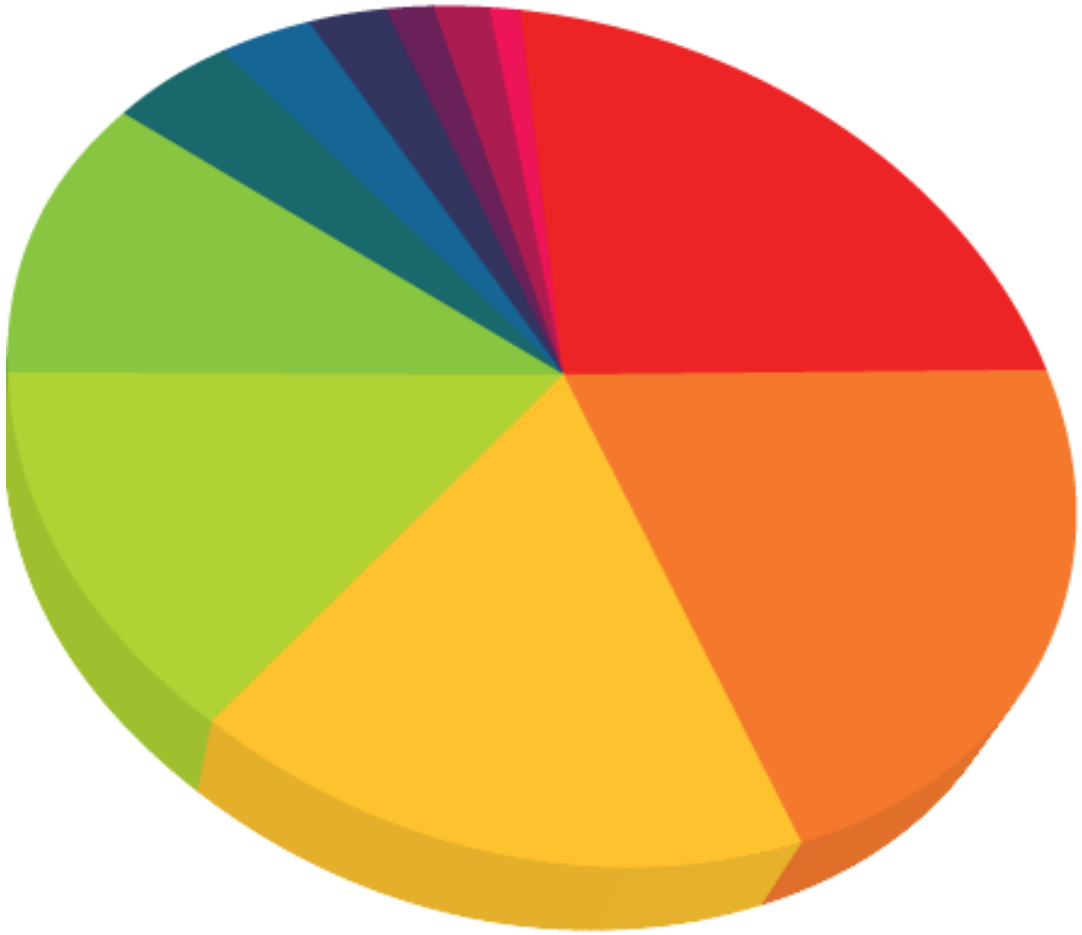
Countries Represented in 2009



Australia
Argentina
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Croatia
Denmark
Dominican Republic
Ecuador
Egypt
France
Georgia
Germany
Greece
Hungary
India
Japan
Iceland
Ireland
Lithuania
Luxembourg
Macedonia
Malaysia
Malta
Mexico
Moldova
Netherlands
Nigeria
Rep. of Cape Verde
Romania
Russian Federation
Saudi Arabia
Singapore
South Africa
Sri Lanka
Sweden
Switzerland
Taiwan
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States

Most tests were performed remotely by the SpiderLabs team.

Penetration Tests – About the Sample Set



Industries

- Technology 23.5%
- Retail 21.6%
- Financial Services 16.1%
- Business Services 12.6%
- Other 11.1%
- Food & Beverage 4.5%
- Hospitality 3.1%
- Transportation 2.9%
- Telecommunication 1.8%
- Education 1.7%
- Manufacturing (1.1%)

Penetration Tests – About the Top 10s

- Intersection of Frequency & Criticality
- Not Meant to Replace other Industry Lists
  - Validate them?
- Organized in the Following Way:
  - Vulnerability = Name
  - Definition = How do we define the vulnerability?
  - Impact = What is the technical and/or business result of attack execution?
  - Circa = When did the security/IT industry first become aware of the issue?
  - Attack Difficulty = How much skill does this take?

Penetration Tests – Top 10 – External Network

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Unprotected Application Management Interface	1994	Easy
2	Unprotected Infrastructure Management Interface	1993	Easy
3	Access to Internal Application via the Internet	1997	Medium
4	Misconfigured Firewall Permits Access to Internal	1993	Hard
5	Default or Easy to Determine Credentials	1979	Trivial
6	Sensitive Information, Source Code, etc. in Web Dir	1990	Easy
7	Static Credentials Contained in Client	1980	Easy
8	Domain Name Service (DNS) Cache Poisoning	2008	Medium
9	Aggressive Mode IKE Handshake Support	2001	Easy
10	Exposed Service Version Issues (Buffer Overflows)	1996	Hard

Penetration Tests – Top 10 – Internal Network

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Address Resolution Protocol (ARP) Cache Poisoning	1999	Medium
2	Microsoft SQL Server with Weak Creds for Admin	1979	Trivial
3	Weak Password for Admin Level System Account	1979	Trivial
4	Client Sends LM Response for NTLM Authentication	1997	Medium
5	Crypto Keys Stored Alongside Encrypted Data	1974	Easy
6	Cached Domain Credentials Enabled on Hosts	1999	Easy
7	NFS Export Share Unprotected	1989	Medium
8	Sensitive Information Transmitted Unencrypted	1991	Trivial
9	Sensitive Info Stored Outside Secured Zone	1993	Trivial
10	VNC Authentication Bypass	2006	Trivial

Penetration Tests – Top 10 – Wireless

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Wireless Client Associates While on Wired Network	2004	Medium
2	Wireless Client Probes from Stored Profiles (KARMA)	2005	Medium
3	Continued Use of WEP Encryption	2004	Easy
4	Easily Determined WPA/WPA2 Pre-Shared Key	2006	Easy
5	Legacy 802.11 FHSS with No Security Controls	1999	Hard
6	Lack of Publicly Secure Packet Forwarding Enabled	2004	Medium
7	Wireless Clients Using "Guest" Instead of "Secured"	2003	Easy
8	Lack of Segmentation Between Wireless and Wired	1993	Easy
9	Wireless Device Connected and Left Unattended	2000	Easy
10	WPA used with TPIK and 802.11e QOS	2008	Hard

Penetration Tests – Top 10 – Physical/Social

Rank	Vulnerability Name	Attack Difficulty
1	Lack of Plate Covering Gap from Door Lock to Strike Plate	Medium
2	Motion Sensors Allow Egress from Sensitive Areas	Medium
3	Sensitive Data Left in Plain View	Trivial
4	Credentials/Pretext Not Verified Effectively	Easy
5	Dumpsters are Accessible and Unlocked	Easy
6	Bypass Route to Secured Areas Available	Easy
7	Motion Sensors Mounted Incorrectly – No Coverage	Medium
8	Unlocked and Otherwise Accessible Computers	Trivial
9	Network Not Protected Against Rogue Devices	Easy
10	Sensitive Data Cabling is Accessible from Public Areas	Easy

Penetration Tests – Top 10 – Application

Rank	Vulnerability Name	Circa	Attack Difficulty	OWASP (2010)
1	SQL Injection	1998	Medium	A1
2	Logic Flaw	1985	Easy	None
3	Authorization Bypass	1997	Easy	A3
4	Authentication Bypass	1960	Easy	A4/A7
5	Session Handling	1997	Medium	A3
6	Cross-Site Scripting (XSS)	2000	Hard	A2
7	Vulnerable Third-Party Software	1960	Medium	A6
8	Cross-Site Request Forgery (CSRF)	1988	Hard	A5
9	Browser Cache-Related Flaws	1998	Medium	None
10	Verbose Errors	1980	Medium	None

Conclusions

- Attackers are using old vulnerabilities
- Attackers know they won't be detected
- Blind trust in 3rd parties is a huge liability
- Fixing new/buzz issues, but not fixing basic/old issues
- In 2010, take a step back before moving forward

Where to get it?

On the Trustwave Web site

https://www.trustwave.com/whitePapers.php

Contacts

Phone: +1 312 873-7500
E-mail: GSR2010@trustwave.com
Web: https://www.trustwave.com/spiderlabs
Twitter: @SpiderLabs / @Trustwave

Nicholas J. Percoco
Senior Vice President, SpiderLabs
Trustwave
Phone: +1 312 873-7471
E-mail: npercoco@trustwave.com
Twitter: @c7five

Trustwave®

SpiderLabs℠

Questions