Trustwave®

2012 Global Threats and Trends

Presented by:

Nicholas J. Percoco
Trustwave SVP & Head of SpiderLabs

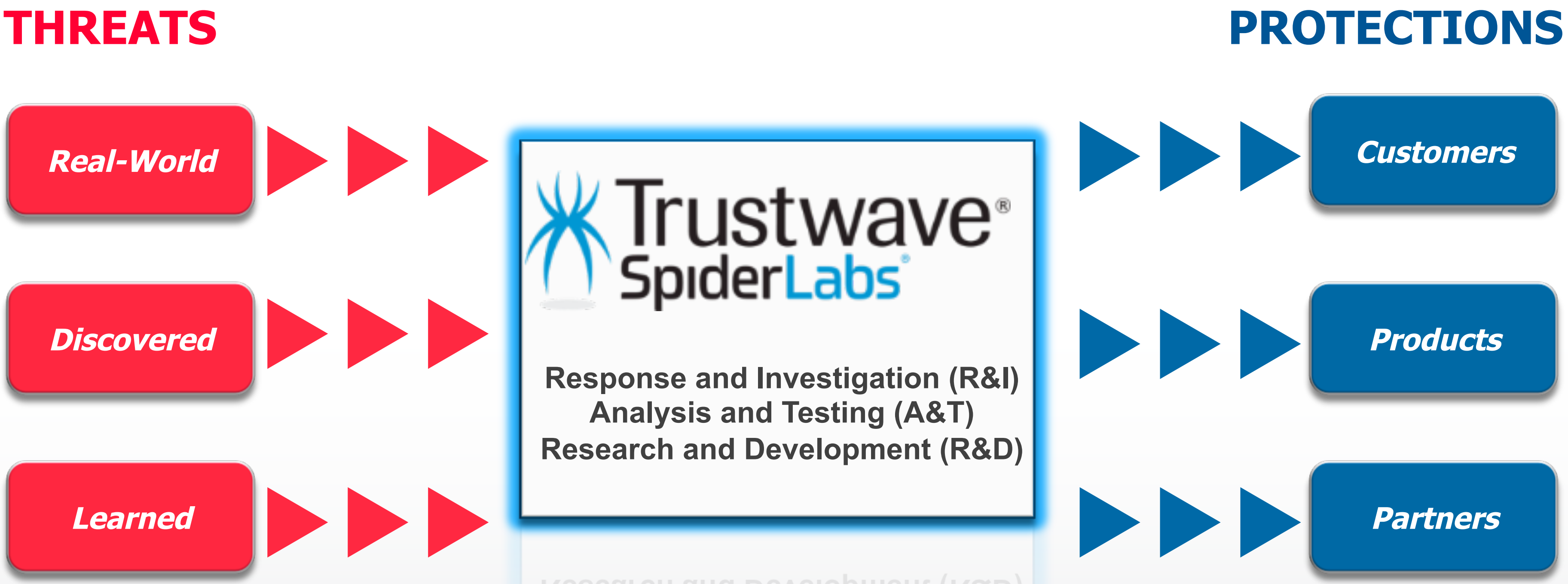
Agenda

- Introduction
- 2011 Incident Investigations
- The Breach Triad
- Malware Trends
- Security Weaknesses Under the Microscope
- Our Defenses
- Conclusion
- Questions?

Introduction

Trustwave SpiderLabs®

Trustwave SpiderLabs uses real-world and innovative security research to improve Trustwave products, and provides unmatched expertise and intelligence to customers.



THREATS

PROTECTIONS

Real-World

Discovered

Learned

Trustwave® SpiderLabs®

Response and Investigation (R&I)
Analysis and Testing (A&T)
Research and Development (R&D)

Customers

Products

Partners

Trustwave 2012 Global Security Report

- Results from more than **300 incident response and forensic investigations** performed in **18 countries**.
- Research analysis performed on data collected from **SpiderLabs engagements** combined with **Trustwave's Managed Security Service** and **SSL offerings**.
- Analysis from more than **2,000 manual penetration tests** and **2 million network and application vulnerability scans**.
- Review of more than **25 different anti-virus vendors**.
- Trends from **16 billion emails** collected from 2008-2011.
- Review of **300 publically disclosed Web-based breaches** from 2011.
- Usage and weakness trends of more **then 2 million real-world passwords** from corporate information systems.

Focus

In this presentation, we will:

- Highlight the threats targeting your organization's assets
- Explain state-of-the-art attack methods as seen through our data breach investigations
- Place the most common weaknesses under the microscope based upon our real-world security research

2011 Incident Investigations

Data and trends from more than 300 investigations

Trustwave SpiderLabs

Trustwave

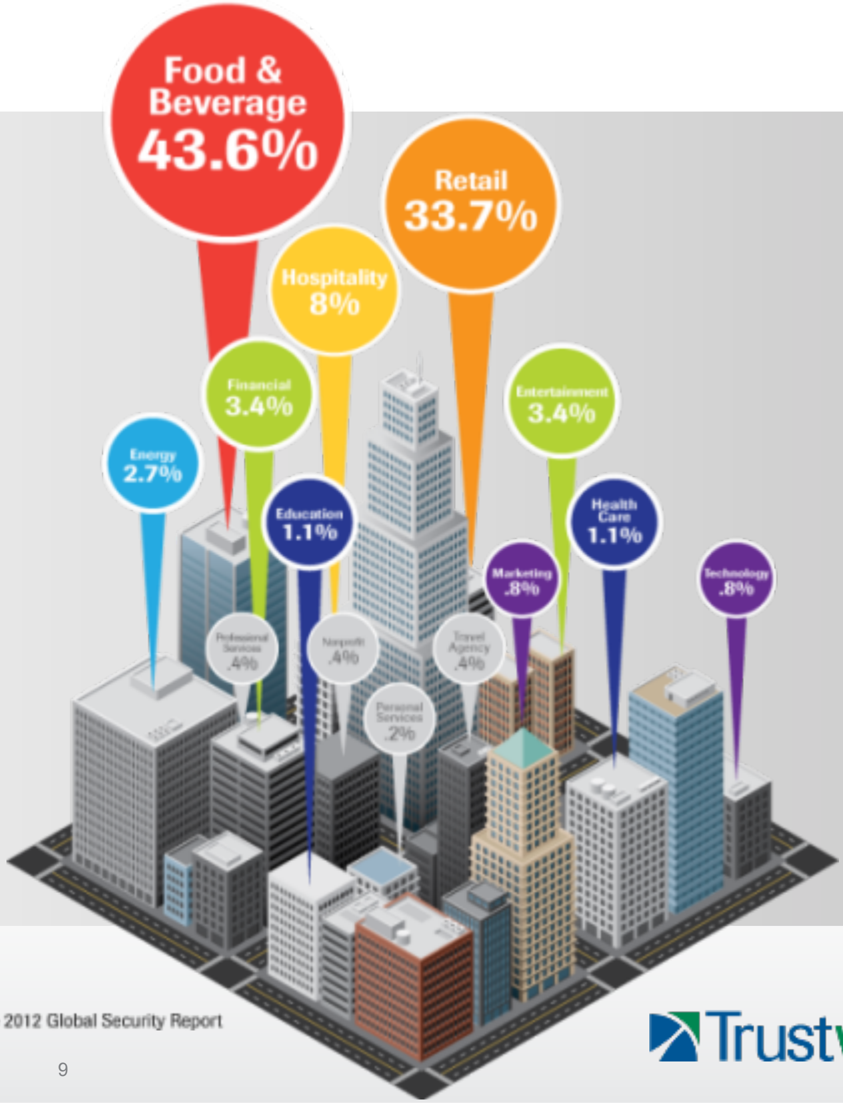
Active Year for Incident Response

- More than 300 investigations in 2011
- Represented data breaches in 18 different countries
- 42% more investigations than 2010
  - Attacks are increasing
  - Organizations more aware of breach disclosure requirements

Industries & Data Targeted

Food & Beverage and Retail industries continue to be major focus of criminal groups:

- 77% (2010: 75%)

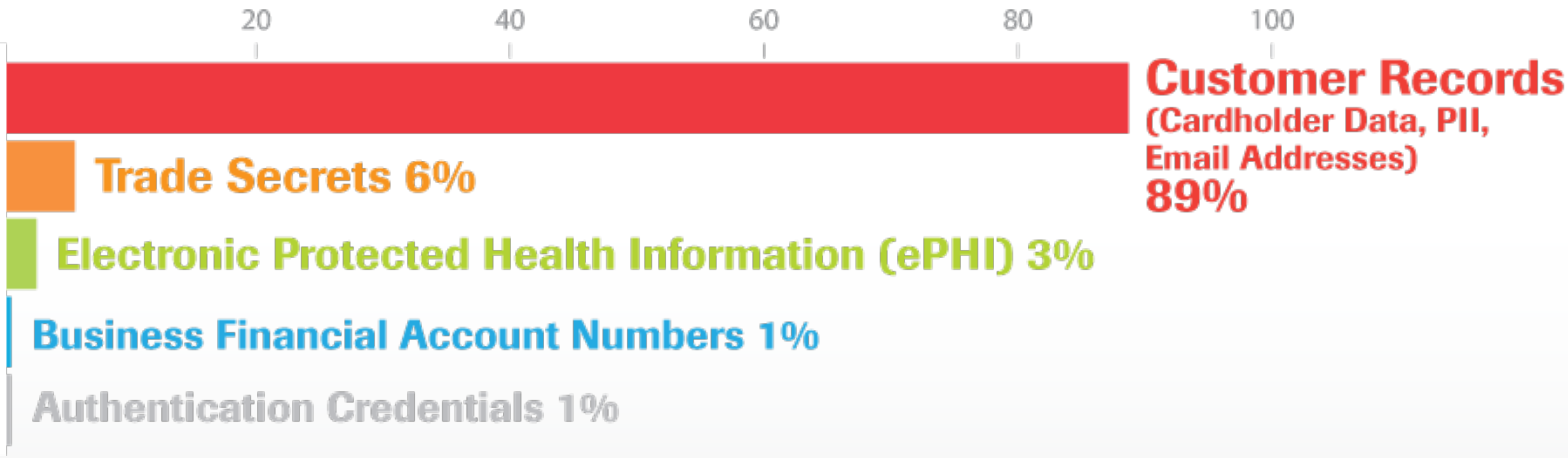


Source: Trustwave 2012 Global Security Report

Industries & Data Targeted

Customer Records are the data attackers target most, specifically payment card data:

- 89% (2010: 89%)



Source: Trustwave 2012 Global Security Report

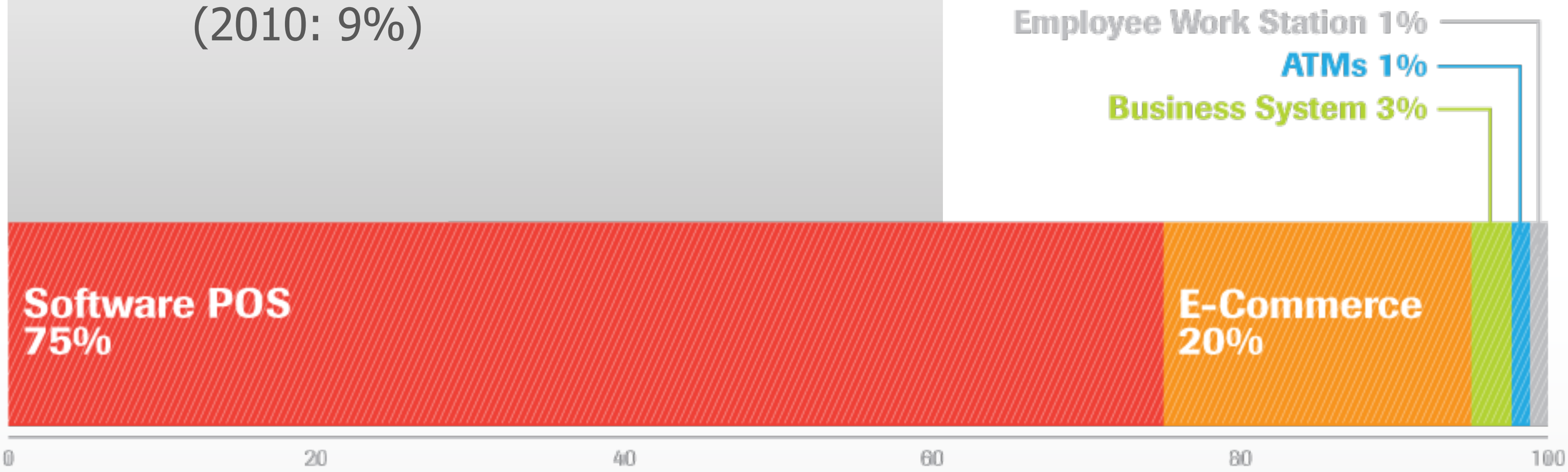
Demo #1

Targeted Attack

Assets Targeted

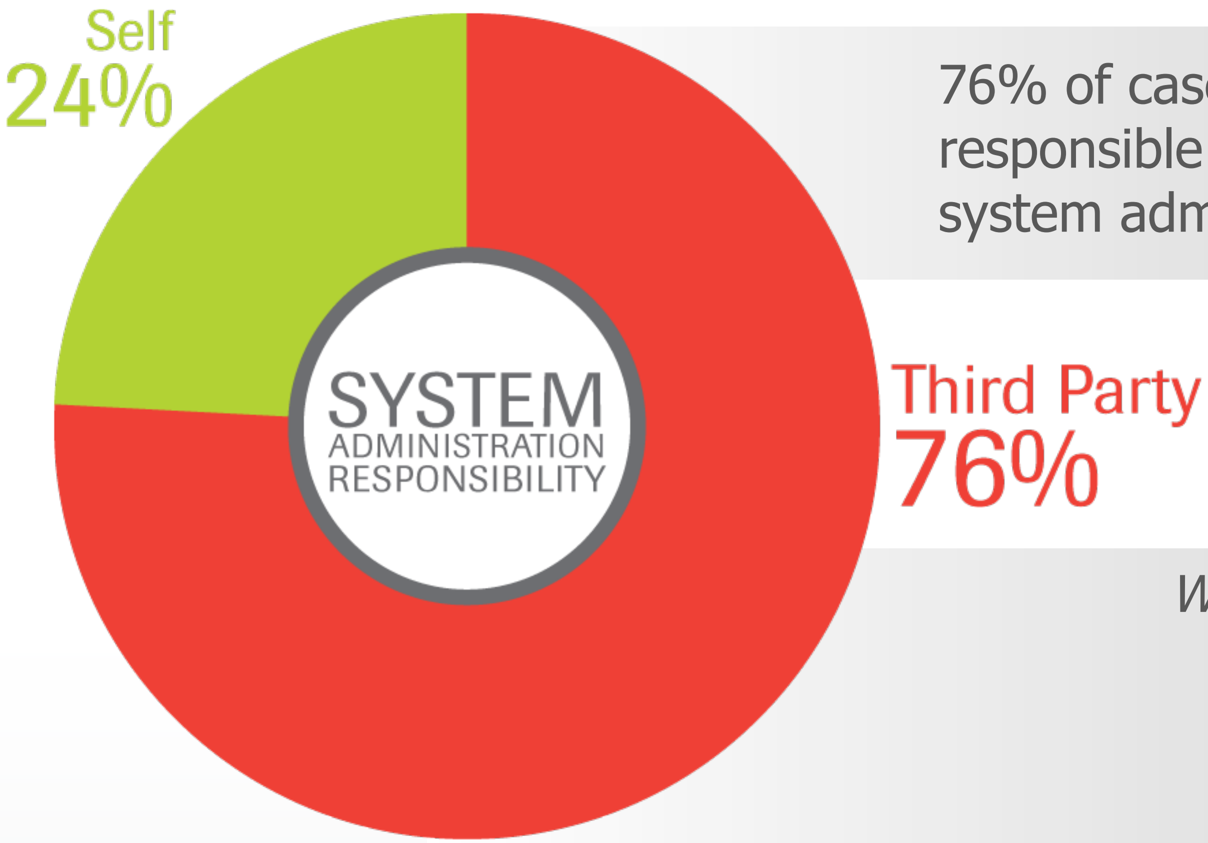
Assets attackers went after:

- 75% Software POS terminals (2010: 75%)
- 20% E-commerce (2010: 9%)



Source: Trustwave 2012 Global Security Report

System Admin Responsibility



Source: Trustwave 2012 Global Security Report

76% of cases: a third party was responsible for a major component of system admin (2010: 88%)

What you can do?

- Contractually build in security requirements
- Impose your policies and procedures on third parties (e.g., password policies)

Detection Method

Self-Detection is vital to stop attackers early in their efforts

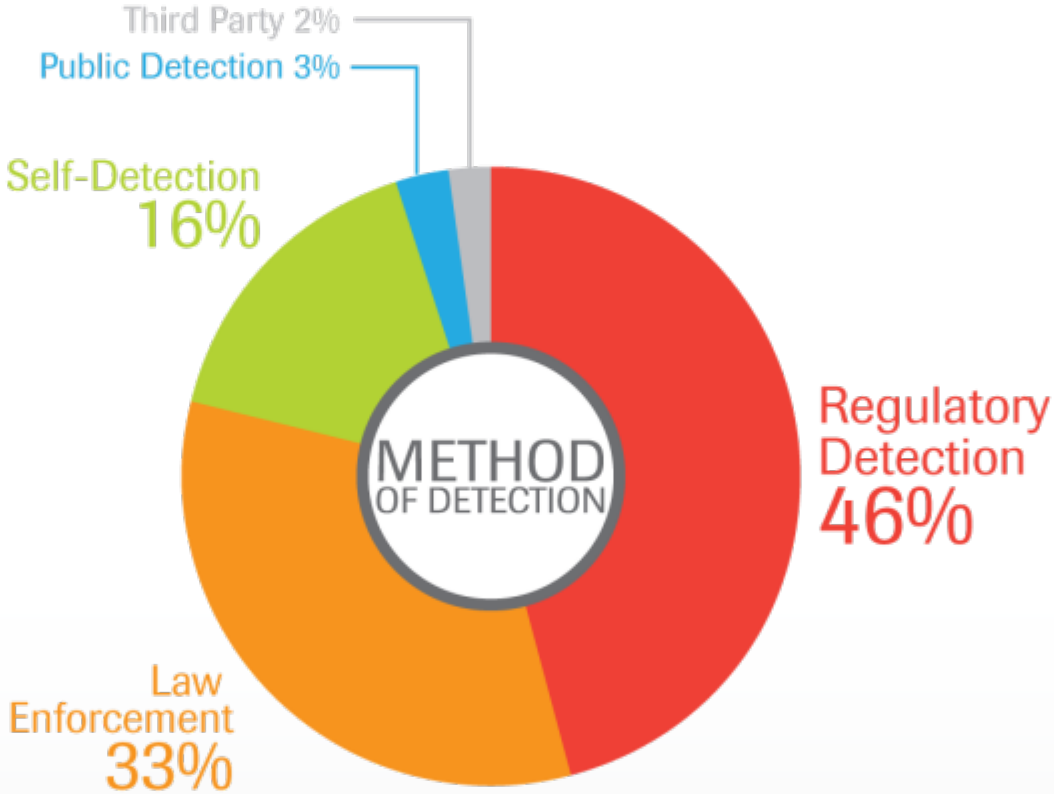
- 16% (2010: 20%)

Law Enforcement increased their efforts

- 33% (2010: 7%)

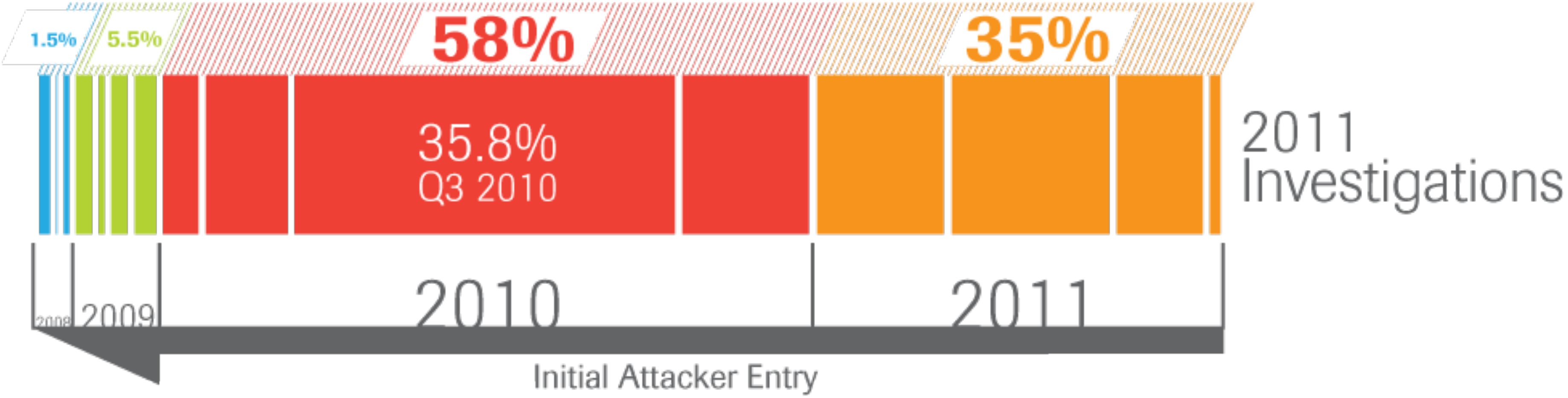
Reliance on external detection increases the attack window

- 173.5 days vs. 43 days



Source: Trustwave 2012 Global Security Report

Attack Timeline



- 2011 cases spanned approximately 44 months
- 35.8% had an initial attack entry within Q3 2010

Origin of Attack

32.5% Unknown (2010: 24%)

29.6% Russia (2010: 32%)

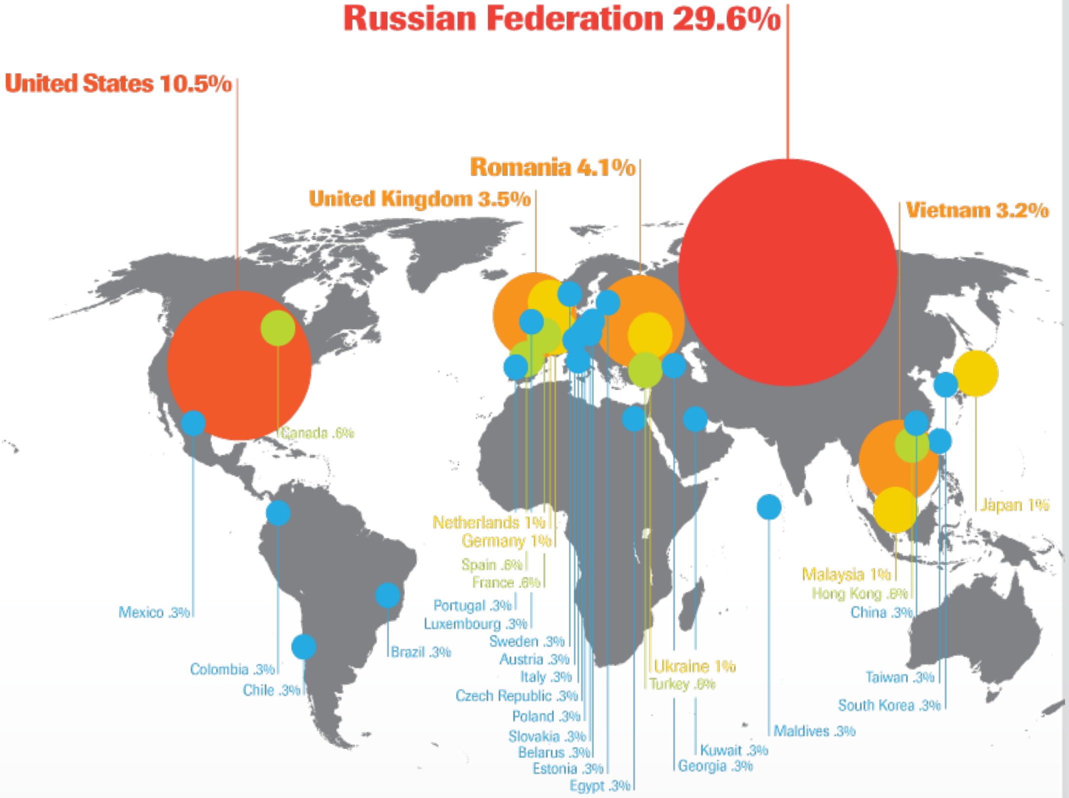
10.5% USA (2010: 6%)

Caveats

- Easy to 'fake' origin
  - Anon proxies (like Tor)
  - Route via hacked systems

Challenges

- Cross border LE
- Do attackers need to hide?



✱ 32.5% Unknown Origin

Source: Trustwave 2012 Global Security Report

The Breach Triad

How attackers infiltrate, harvest data and exfiltrate

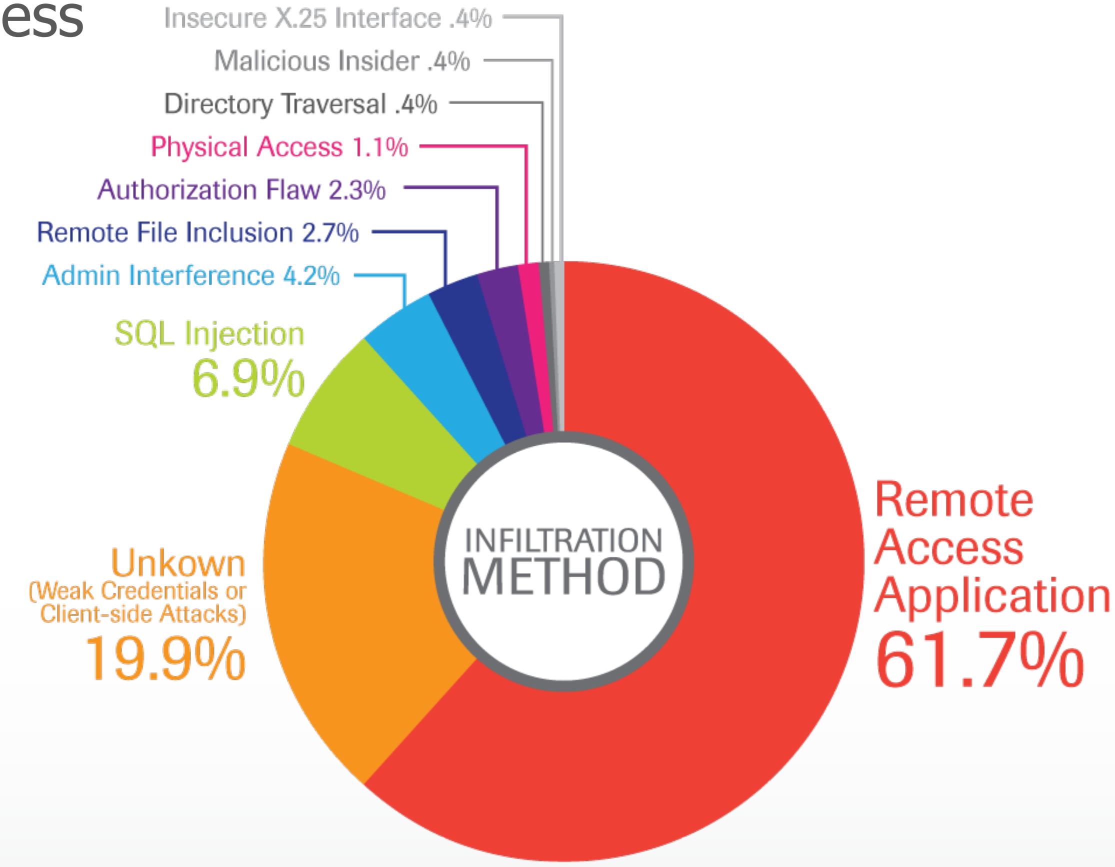
Infiltration

Gaining unauthorized access

- 62% RAS/RAA (2010:55%)
- 7% SQLi (2010: 6%)
- 20% Unknown 2010: 18%)

Why are some methods unknown?

- Weak credentials
- Client side attacks
- Insufficient logging/ monitoring



Source: Trustwave 2012 Global Security Report

Aggregation or Data Harvesting

Capturing sensitive data

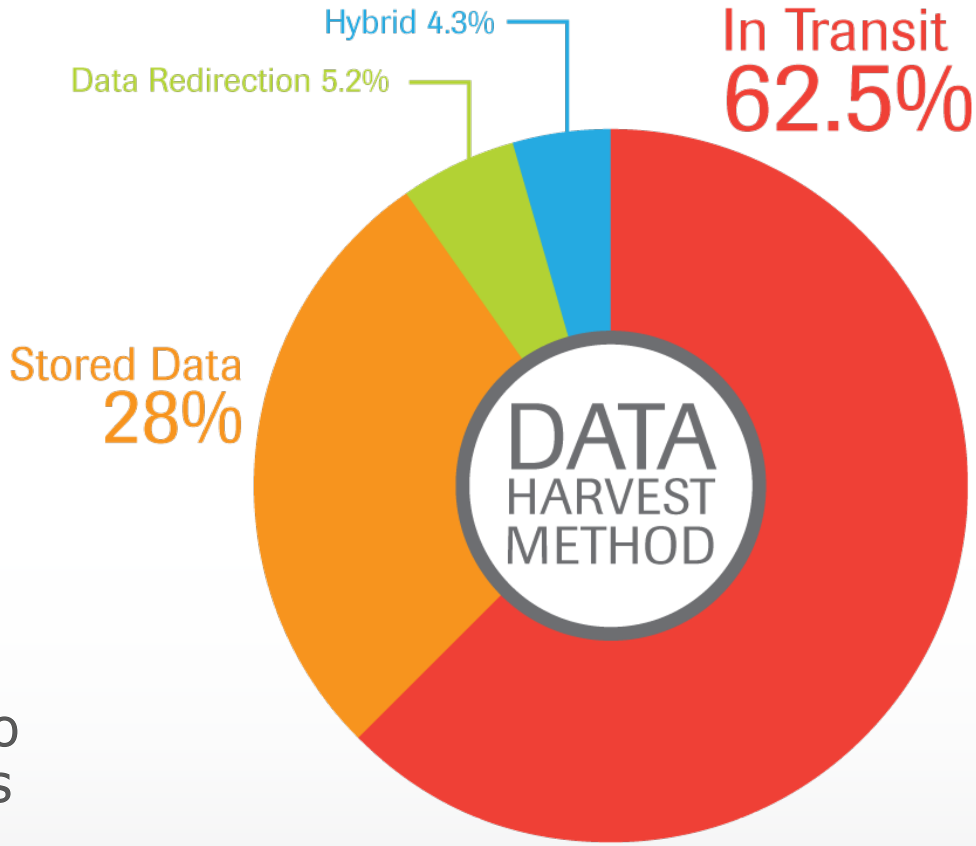
- Approximately flat on last year
- Hiding malware in plain sight

In-transit attacks

- Memory, network and sniffers
- Key-loggers

Data re-redirection

- Process modification to reroute data to attacks systems or tool

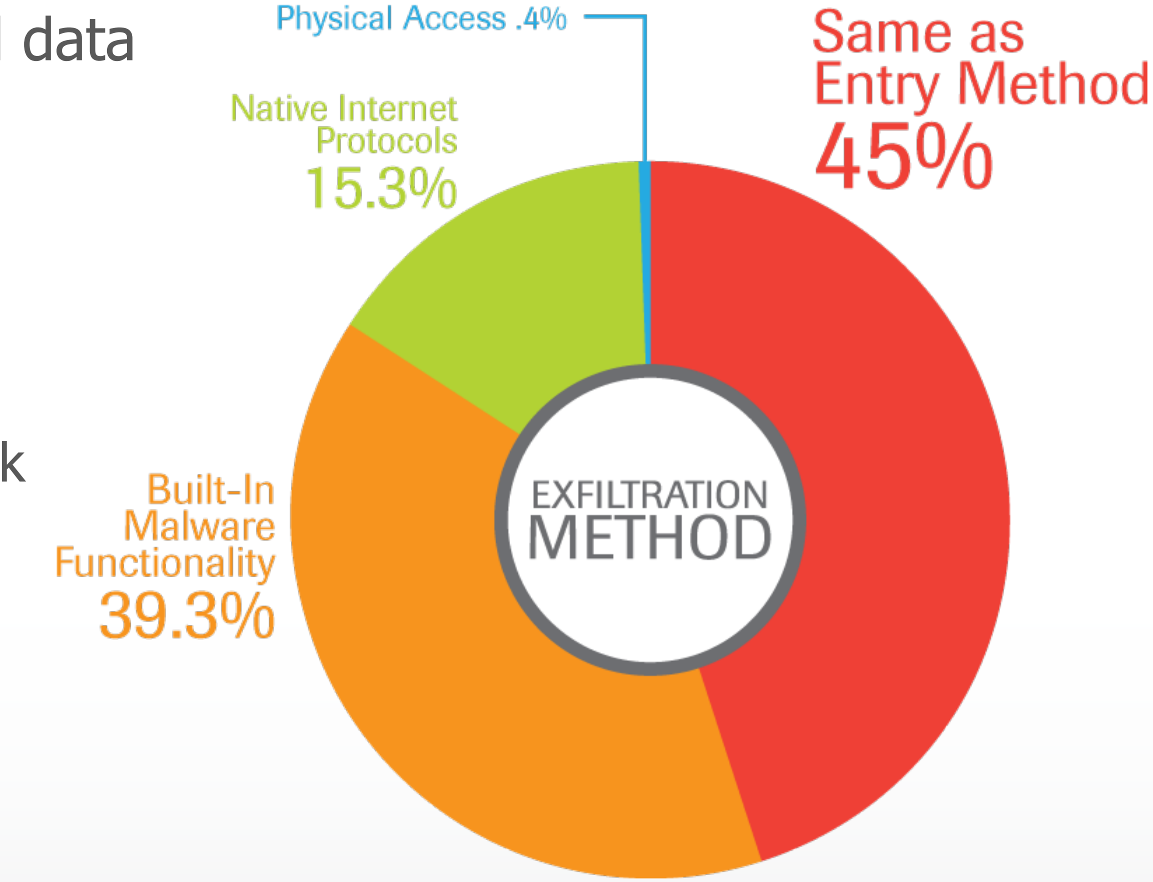


Source: Trustwave 2012 Global Security Report

Exfiltration

Removing compromised data

- Reuse of Infiltration mechanisms
- Malware with auto-export functionality
- Emulate end-user traffic on the network to avoid detection



Source: Trustwave 2012 Global Security Report

Malware Trends

Common and targeted

Many Differences

Common

- **Self-propagation** through vulnerabilities or user actions
- **Widely distributed**
- Easily **detectable** by AV vendors

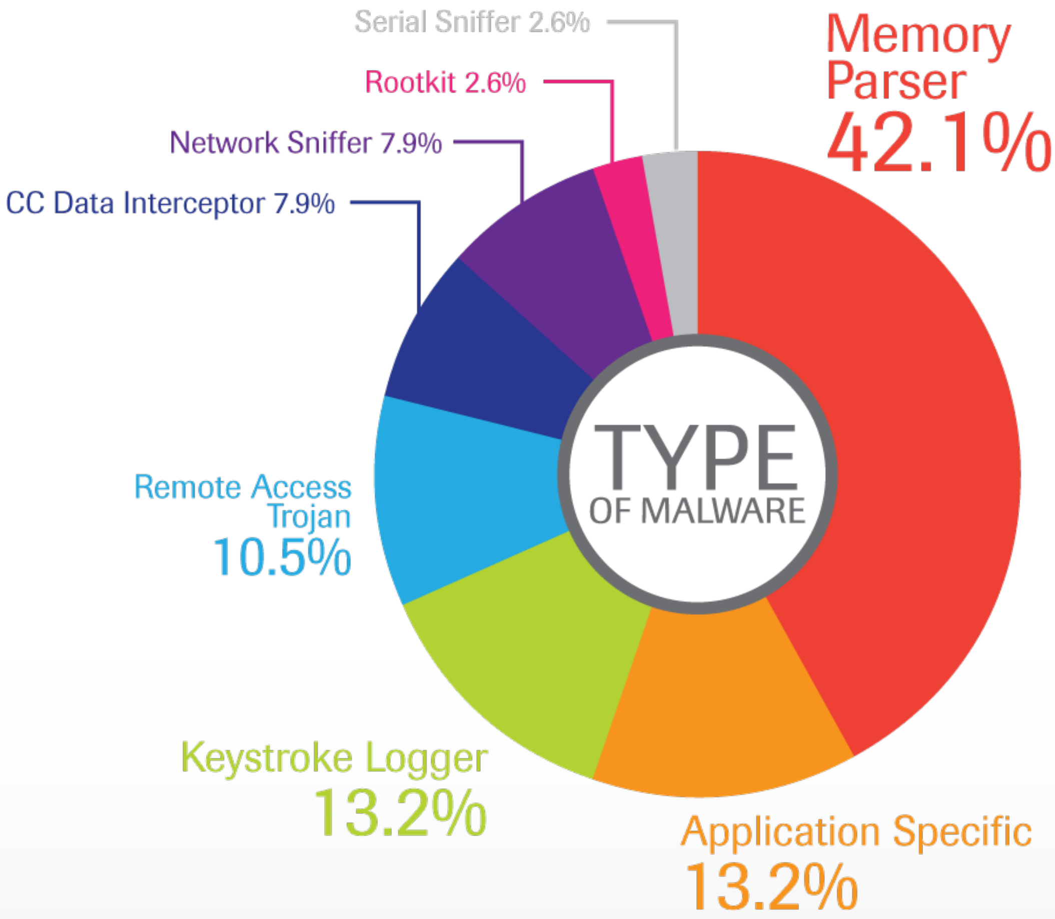
Targeted

- **No propagation** and may not exploits vulnerabilities
- Application/system specific
- Only **found in target environments**
- Most found in Trustwave 2011 investigations were **undetectable** by AV; *only 12% by top AV vendors*

Targeted Malware Types

Popular Types

- **Memory Parser** obtains data in use out of system memory
- **Keystroke Loggers** target user and device input
- **Application Specific** hook the applications with access to target data



Source: Trustwave 2012 Global Security Report

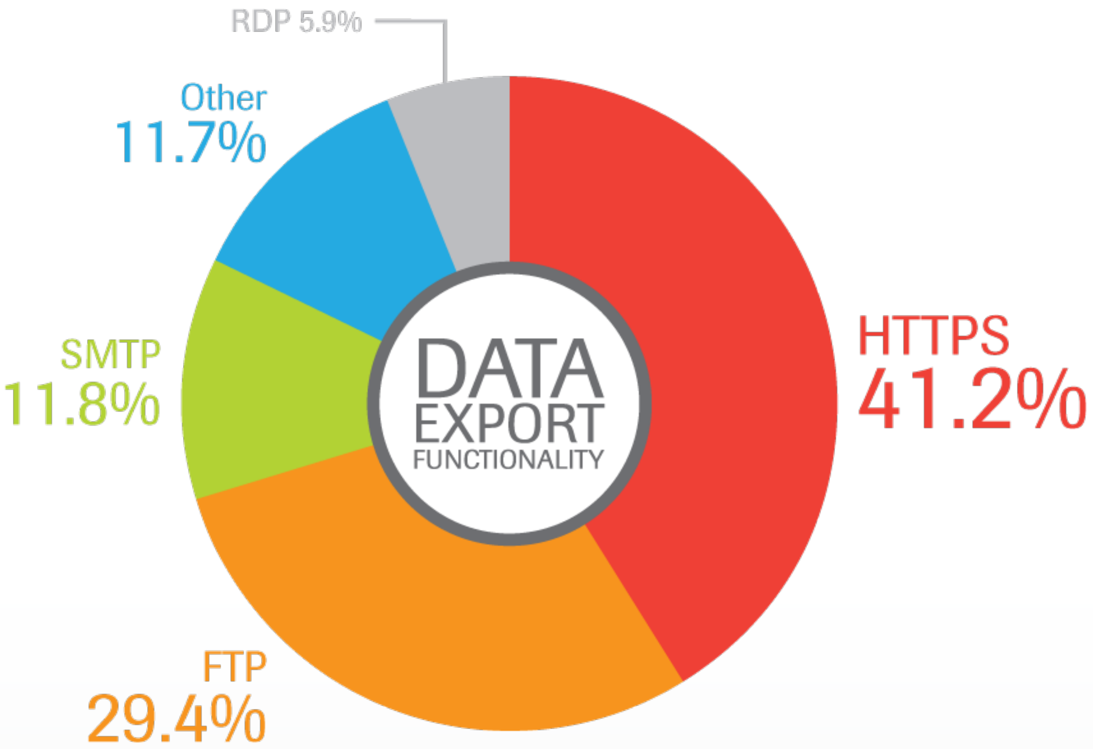
Trustwave SpiderLabs

Trustwave

Demo #2

Memory Dumper

Data Export Functionality



Source: Trustwave 2012 Global Security Report

Malware Delivers

- **HTTPS** is the most popular way to get compromised data out
- Blends into user traffic

Some Stay Quiet

- Some malware does not have ANY export capabilities
- Found in the highly targeted cases we investigated in 2011

Security Weaknesses under the Microscope

Four vulnerable resources in the workplace

The Network

Trustwave offers a **vulnerability scanning service** with more than **2 million customers**.

Trustwave SpiderLabs performs more than **2,000 manual penetration** tests annually.

The data from these combined efforts revealed the top network issues facing organizations today.

The Network – Default Credentials

Many devices come shipped with default accounts.

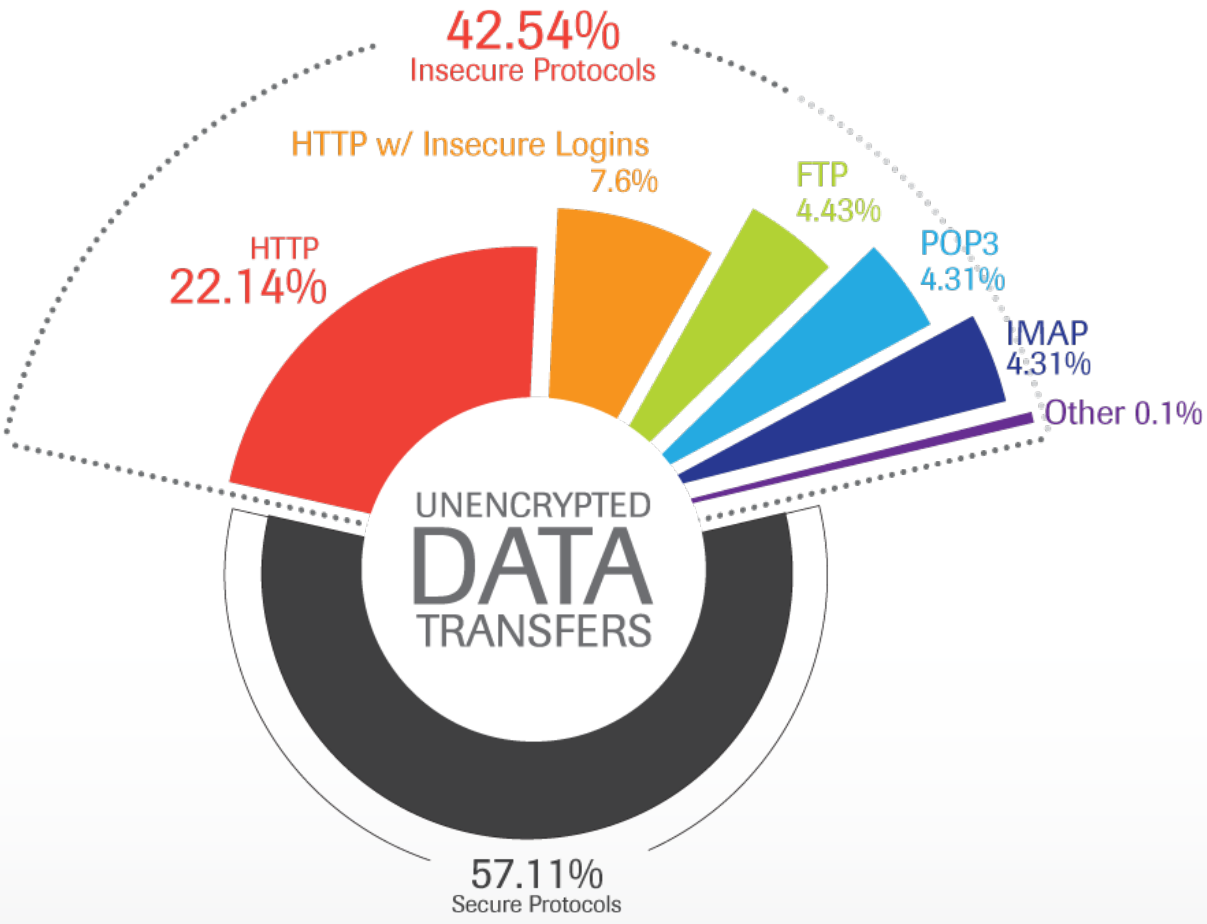
These accounts/password can be easily changed upon installation.

Many administrators fail to do so.

We found them everywhere:

- **28% of Apache Tomcat**
- **10% of Jboss Installs**
- **9% of phpMyAdmin sites**
- **2% of ALL Cisco devices**

The Network – Clear Text Traffic



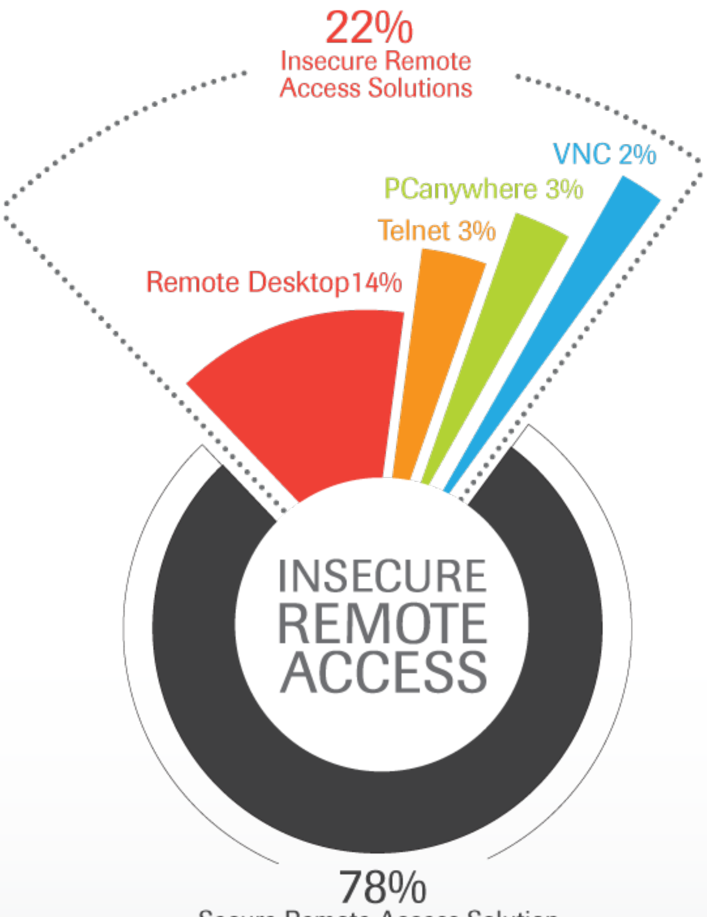
Source: Trustwave 2012 Global Security Report

Encrypted methods for nearly every Internet protocol have existed for more than a decade.

Legitimate reasons exist for unencrypted web traffic but not for:

- Web Application Logins
- File Transfers
- Email

The Network – Remote Access



Source: Trustwave 2012 Global Security Report

Remote Access was the **number one infiltration method** for data breaches in 2011 (62%).

Sending clear text credentials over the Internet can result in accounts being compromised.

One in five organizations **use insecure remote access solutions**.

The Network – Top 10 Issues

1. Weak or Blank Admin Passwords
2. Sensitive Data Transmitted Unencrypted
3. Weak Database Credentials
4. ARP Cache Poisoning
5. Wireless Clients Probe for Stored Profiles
6. Use of WEP in Wireless Networks
7. LAN Manager Response for NTLM
8. Firewalls Allows Access to Internal Systems.
9. Sensitive Information Stored Outside of Secured Networks
10. Sensitive Information Transmitted Over Bluetooth

Trustwave® SpiderLabs®

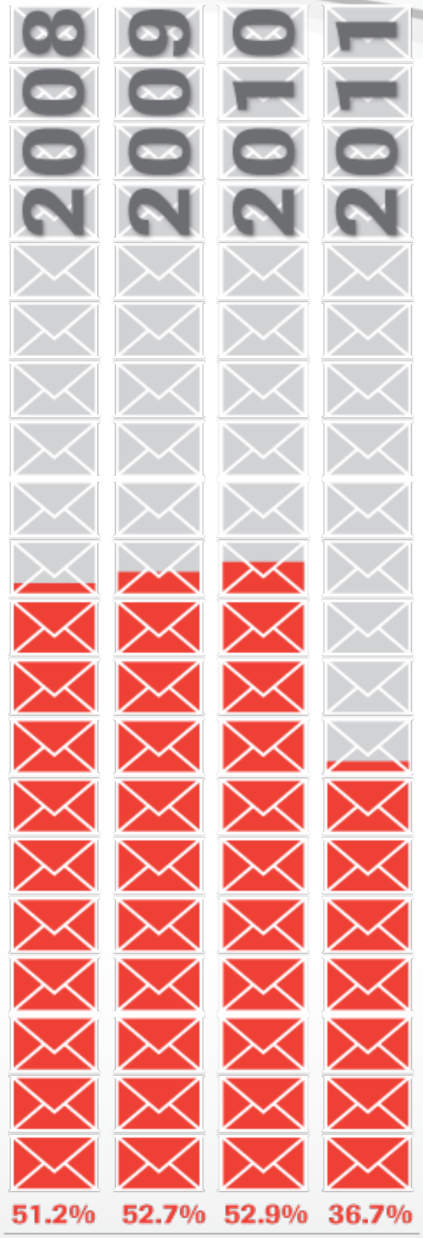
Trustwave®

Email

Trustwave offers mailMAX, a **cloud-based secure email service** that scans more than **4 billion emails per year.**

We reviewed all emails processed from **2008 to 2011** to produce email security trends.

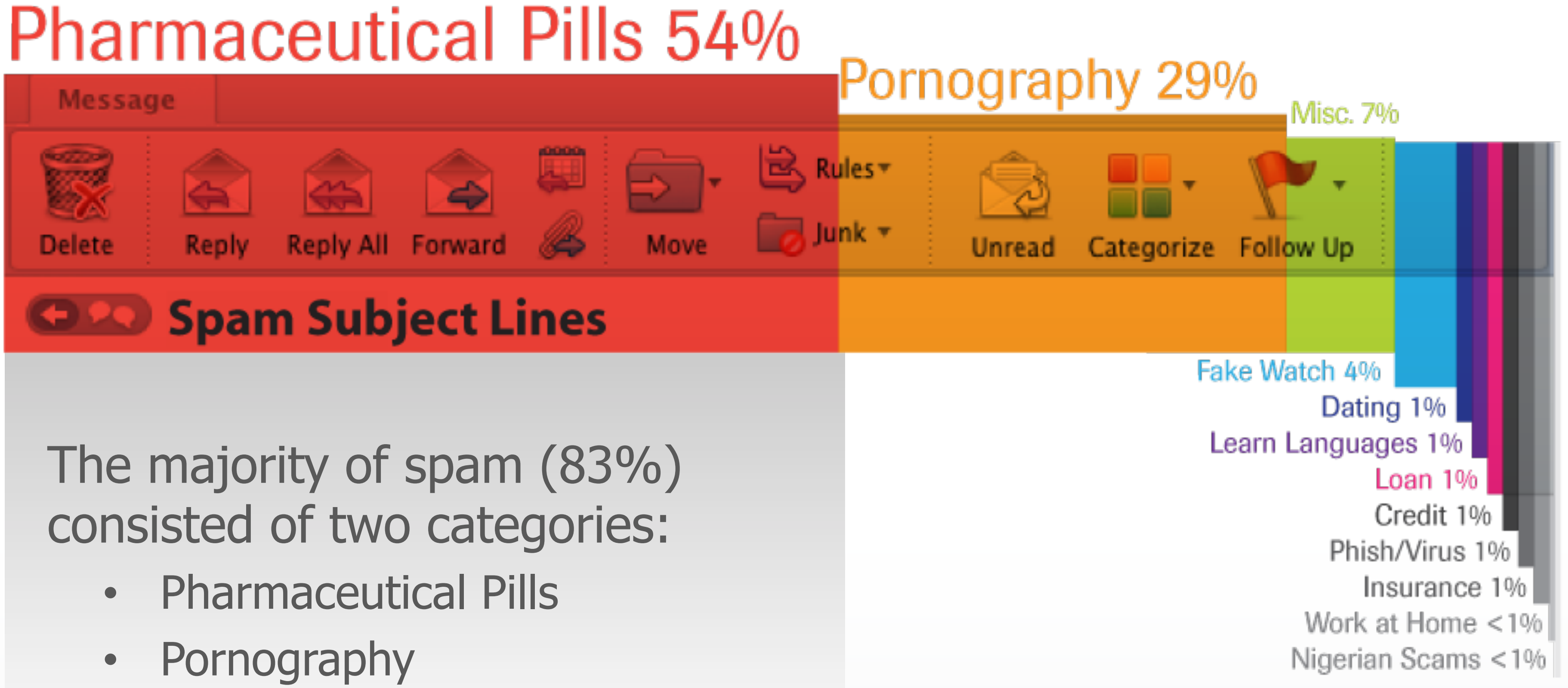
Spam sharply decreased in 2011 (36% of all email processed) after peaking at 53% in 2010.



ANNUAL SPAM TOTALS

Source: Trustwave 2012 Global Security Report

Email – Spam Subject Lines



The majority of spam (83%) consisted of two categories:

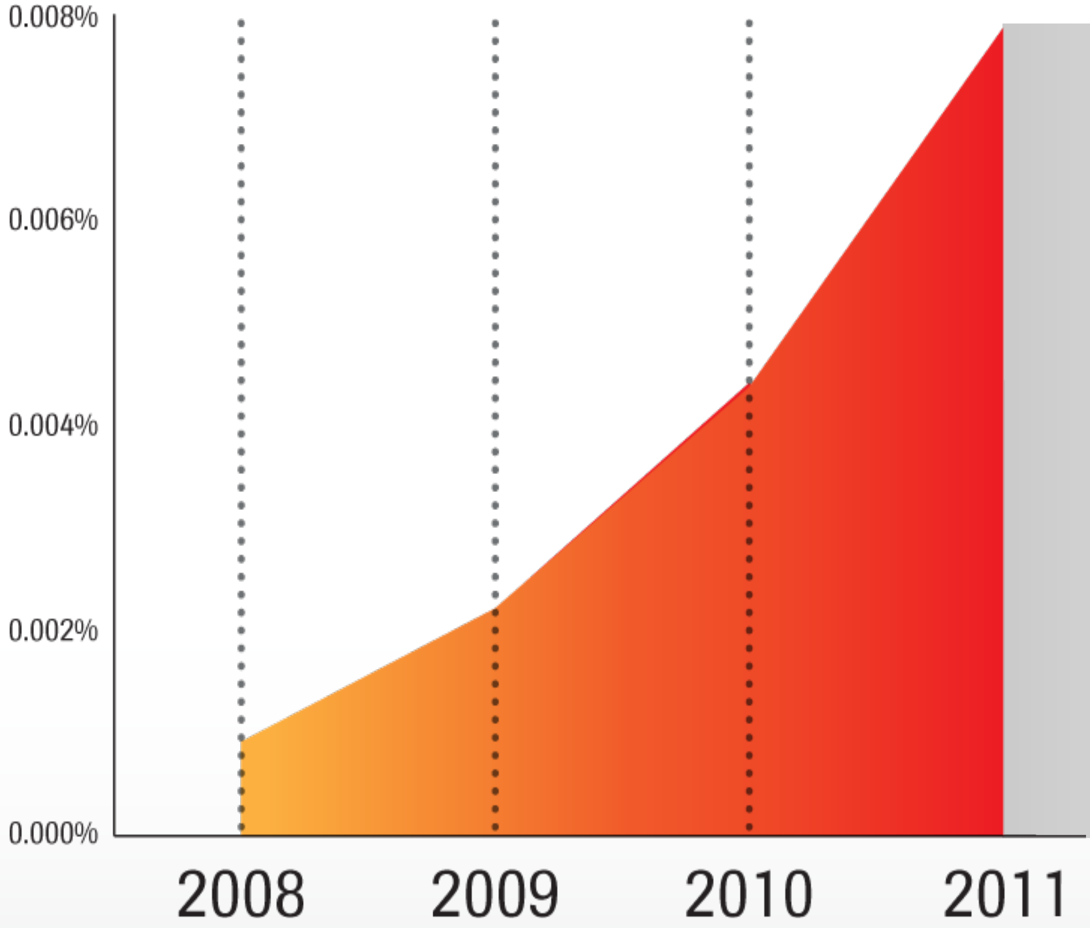
- Pharmaceutical Pills
- Pornography

Source: Trustwave 2012 Global Security Report

Trustwave SpiderLabs

Trustwave

Email – Dangerous Files



Source: Trustwave 2012 Global Security Report

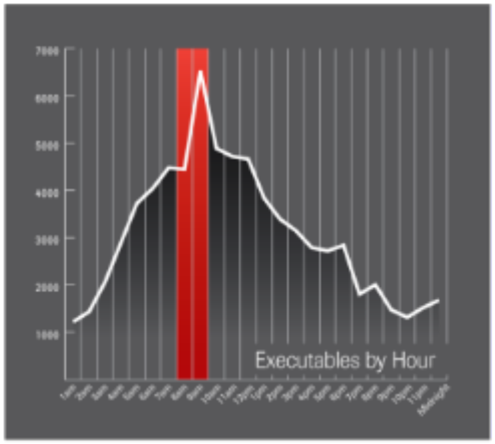
Our **interception of executable** files via email has **almost doubled** each year since 2008.

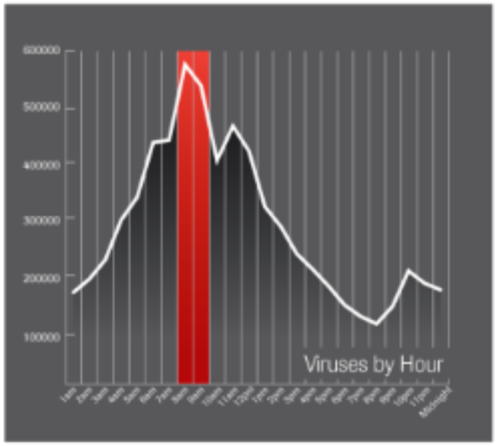
Executables are often use to send **malware** to victims or part of **worm** propagation.

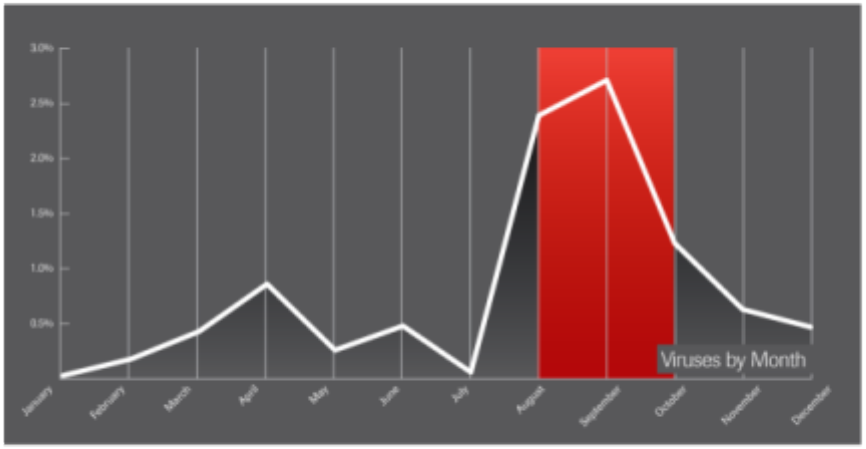
Trustwave SpiderLabs

Trustwave

Email – Temporal Analysis







Executable Alert!
Start: 8:00 AM
End: 9:00 AM

Virus Alert!
Start: 8:00 AM
End: 9:00 AM

Virus Alert!
Start: August
End: September

Trustwave SpiderLabs

Trustwave

The Web

Trustwave is a sponsor and active contributor to the **Web Hacking Incident Database** (WHID) containing more than 300 incidents from 2011.

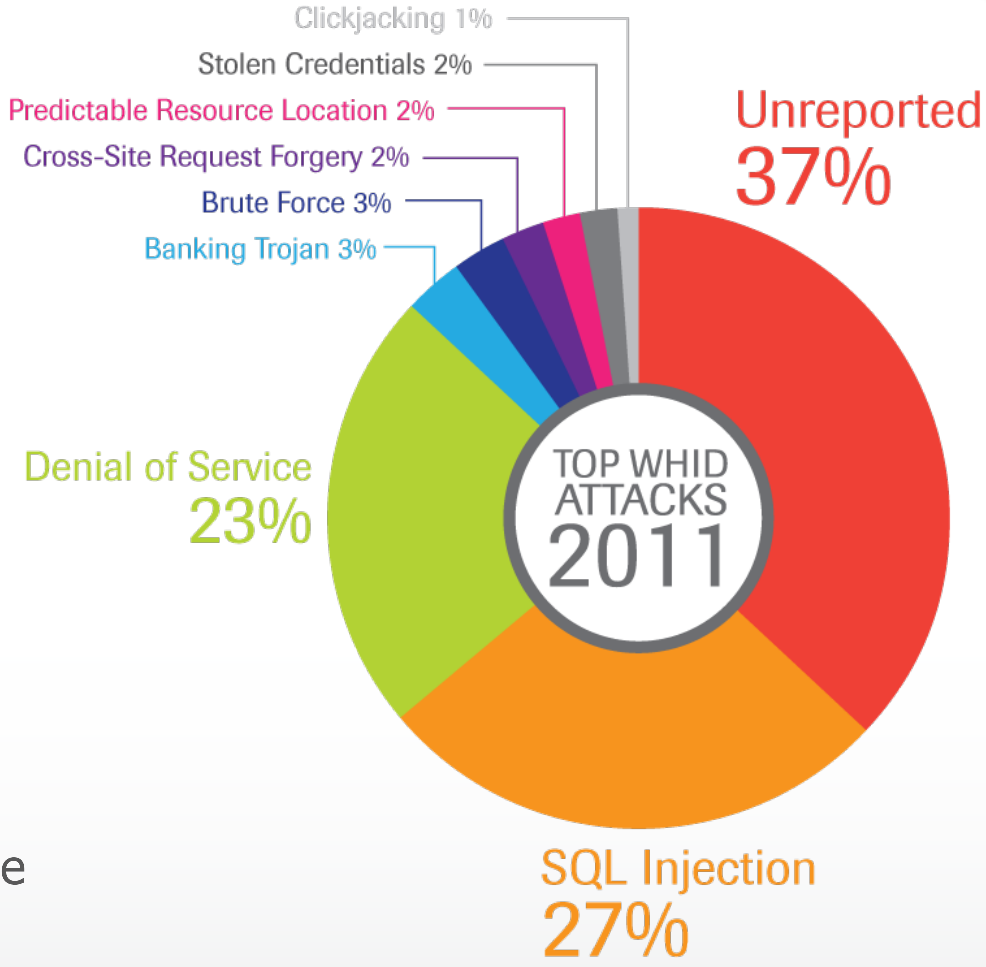
Trustwave SpiderLabs performs **hundreds of manual application security** tests on an annual basis.

The data from these combined efforts revealed the top Web application issues facing organizations today.

The Web – Top Attacks

The top attack category is **Unreported** which means either:

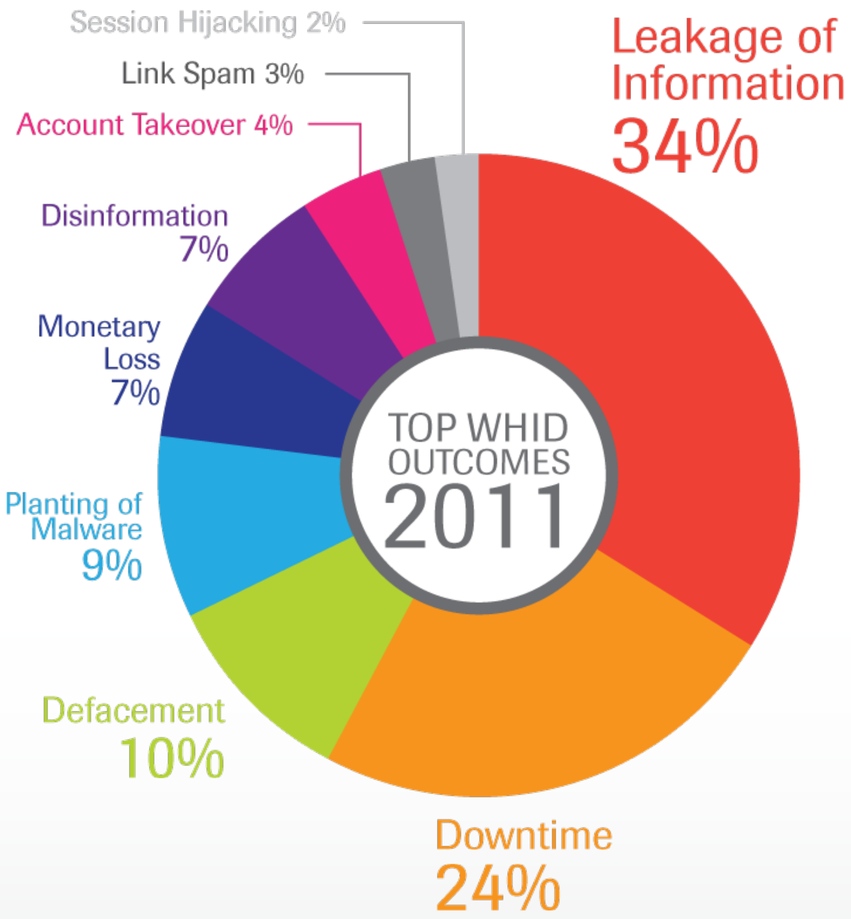
- **Insufficient Logging**
  - Not Configured Correctly
  - No Visibility Into Web Traffic
- **Public Disclosure Resistance**
  - Fear of Public Perception
  - Impact to Custom Confidence



The Web – Top Outcomes

There two main motivations for these attacks:

- **Hacking for Profit**
  - Extraction of Customer Data
  - Bank Fraud
- **Ideological Hacking**
  - Embarrassment
  - Occupy *XYZ*



Trustwave SpiderLabs

Trustwave

The Web – Vertical Market Attacks

Government	Denial of Service 41%
Entertainment	SQL Injection 43%
Web 2.0	Cross-Site Request Forgery 14%
Finance	Banking Trojan 36%
Retail	SQL Injection 27%
Technology	SQL Injection 37%
Hosting Providers	Cross-Site Request Forgery 14%
Media	SQL Injection 17%
Education	SQL Injection 40%
Politics	Denial of Service 78%

SQL injection and **denial of service** are vertical agnostic.

Cross-Site Request Forgery (CSRF) are most common in **social networks** and shared **hosting providers**.

Source: Trustwave 2012 Global Security Report

The Web – Top 10 Issues

1. SQL Injection
2. Logic Flaw
3. Cross-Site Scripting (XSS)
4. Authorization Bypass
5. Session Handling Flaws
6. Authentication Bypass
7. Cross-Site Request Forgery (CSRF)
8. Source Code Disclosure
9. Detailed Error Messages
10. Vulnerable Third-Party Software

Mobile

Trustwave SpiderLabs **actively performs research** in the area of mobile security.

Most organizations treat mobile devices as **miniature PCs** in their **security programs**.

Attack trends started to appear in 2011 as **mobile security** just **begins to evolve**.

Mobile – Banking Trojans

Historically, banking Trojans targets PCs but in 2011:

- **Zeus** and **SpyEye** made an appearance on Android and iOS.
- **Targeting** Mobile Transaction Authentication Numbers (**mTANs**)
- **Self-propagation** ability first appeared in **2012** via **SMS**

Mobile – Location Aware Malware

Mobile devices are **designed** to perform **GPS tracking**.

Malware can **easily access** this information.

Creates **physical security issues** for **employees** and **executives** in transit!

Mobile – The Android Situation

Android has **> 50%** of the Mobile Device Market

Google only began screening Apps for **security issues**.

Third-party markets are also **littered with malware**.

Demo #3

Android Malware

Our Defenses

Basic controls

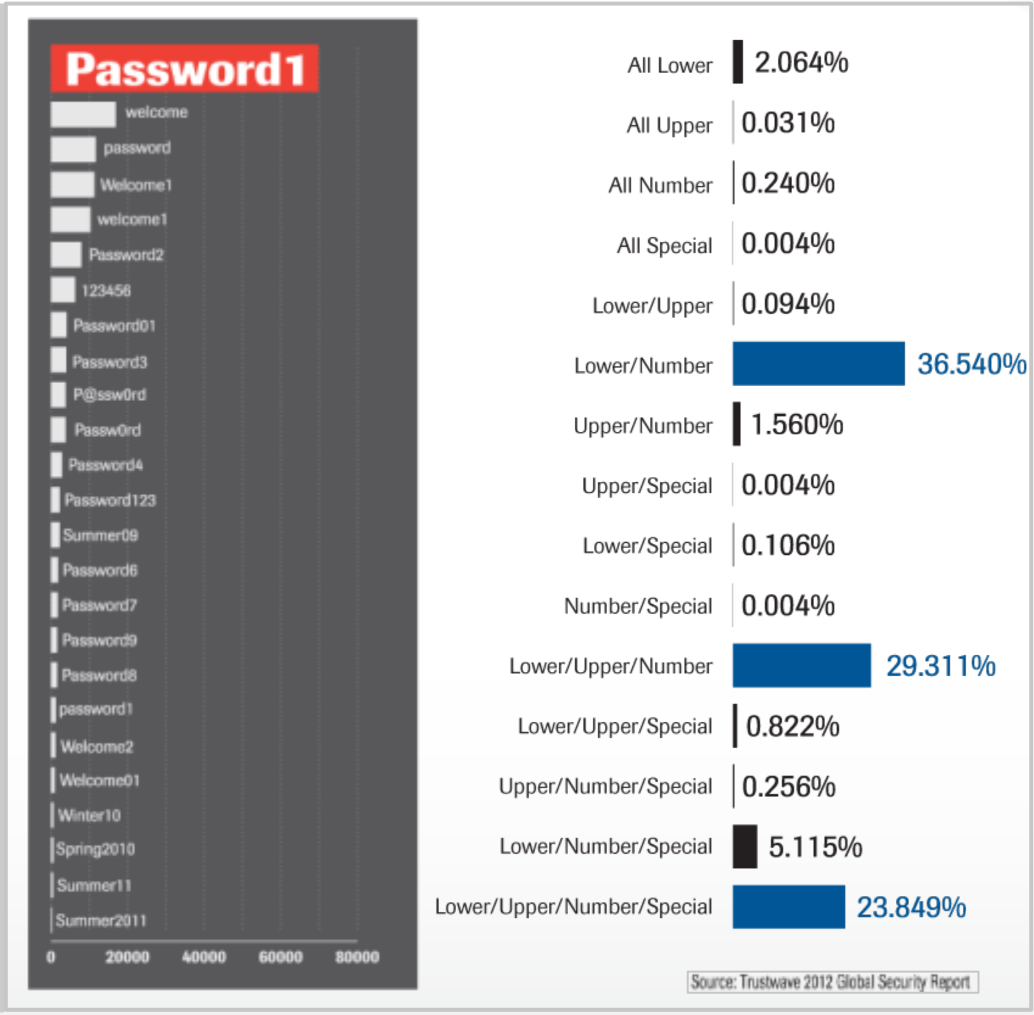
Passwords

2.5+ Million Passwords Analyzed

- All in use within the enterprise

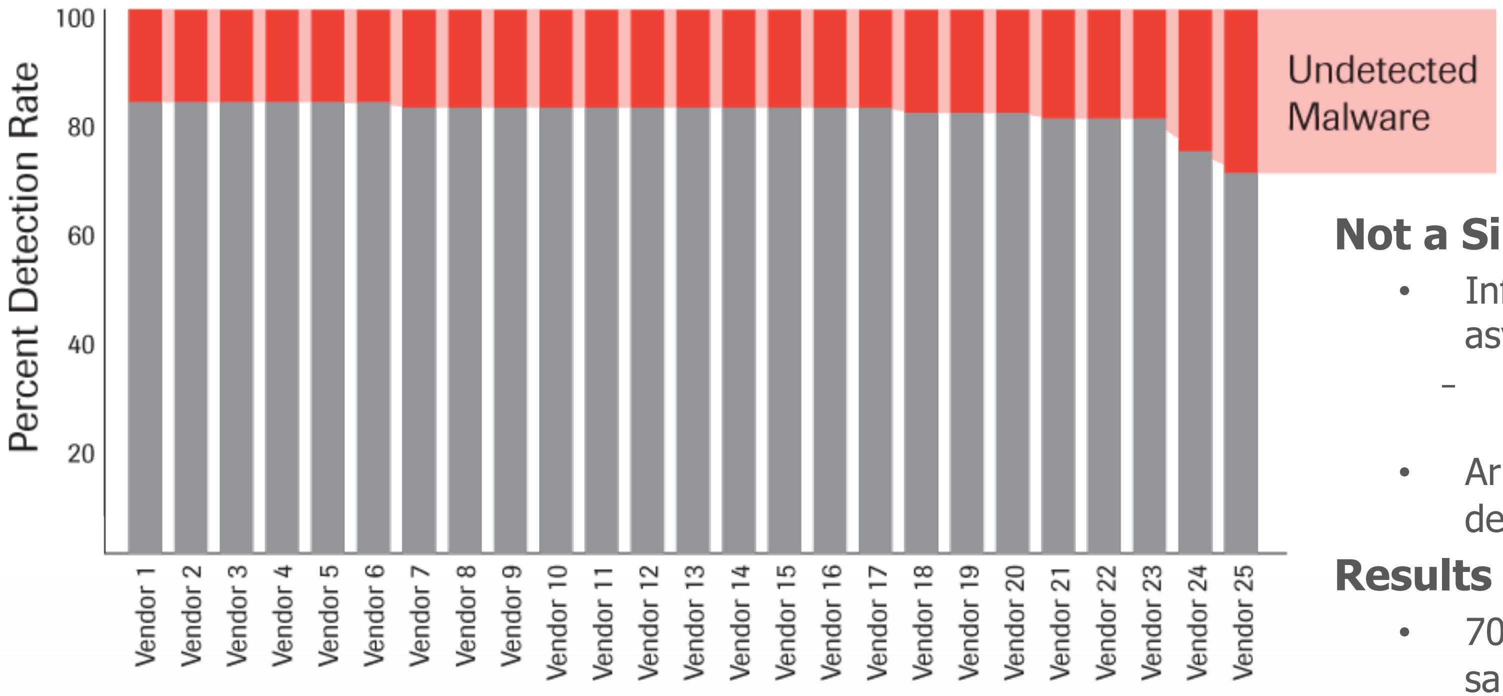
Common Weaknesses

- Shared 'admin' p/w
- New employee default p/w
- Poor complexity requirement
- 5% based on "password"
- 1% based on "welcome"



Source: Trustwave 2012 Global Security Report

Anti-Virus



Source: Trustwave 2012 Global Security Report

Not a Silver Bullet

- Information asymmetry
  - malware authors/ signature writers
- Arms-race, signature dependence

Results

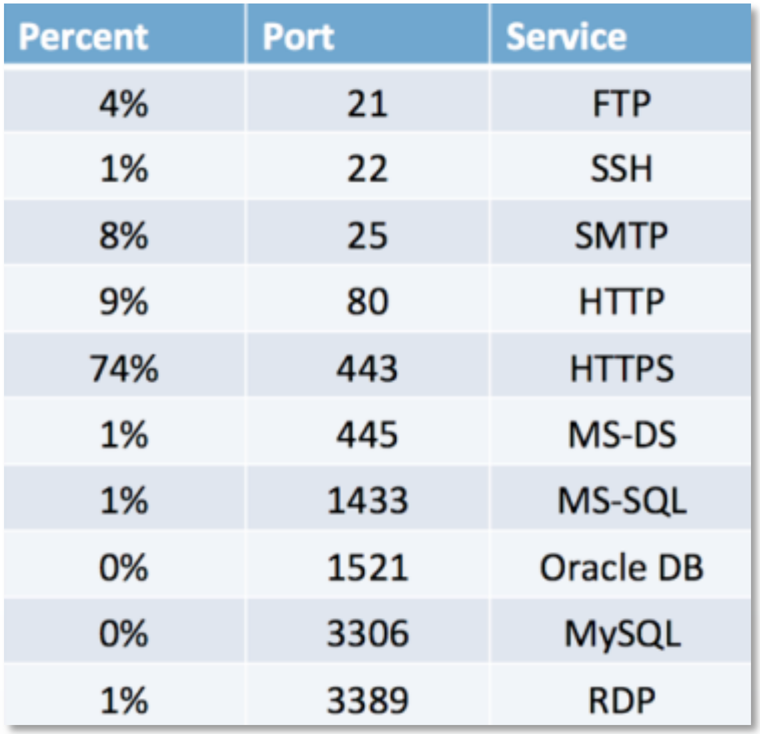
- 70,000 malicious samples
- A/V identified 81% of all samples
- Lowest vendor scored just 70%

Firewalls

Firewalls commonly use **Network Address Translation** (NAT) to **preserve public address space**.

Trustwave SpiderLabs found that about **1 of ever 800 hosts** were protected by a firewalls with **misconfigured NAT**.

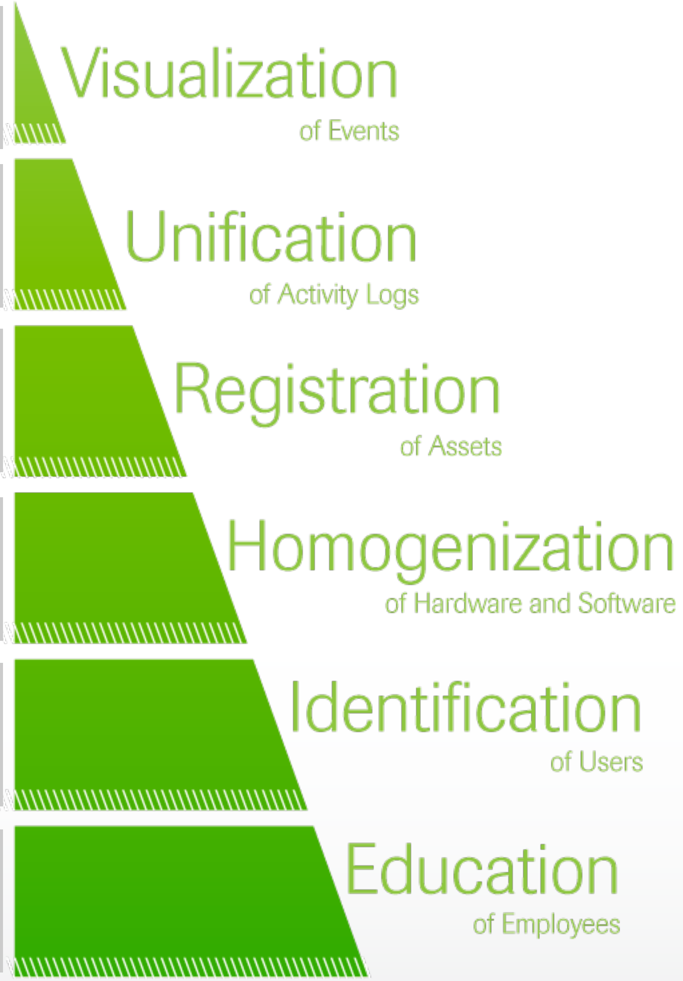
This would allow an **attacker to gain access to services** thought to be **firewall protected**.



Percent	Port	Service
4%	21	FTP
1%	22	SSH
8%	25	SMTP
9%	80	HTTP
74%	443	HTTPS
1%	445	MS-DS
1%	1433	MS-SQL
0%	1521	Oracle DB
0%	3306	MySQL
1%	3389	RDP

Conclusion

2012 Information Security Pyramid



Visualization of Events: Data mining of large volume of events are best performed with the aid of visualizations, making life easier to detect anomalies and suspicious activity

Unification of Activity Logs: Correlating logs and events from physical and digital activities users performs allows for a clearer view of potential security incidents

Registration of Assets: A complete inventory/asset register provides insight needed to help identify and contain malware outbreaks and intrusions

Homogenization of Hardware and Software: Reducing complexity through common hardware and software stacks simplifies management, maintenance and security

Identification of Users: Every user initiated action within an environment should be linked to a specific user

Education of Employees: Employees are the foundation of both preventative and detective & monitoring controls

Trustwave SpiderLabs

Trustwave

Conclusions

Storage of customer records makes any organization a target

- Don’t think in terms of network or application security: be data-security centric.

Outsourcing is still a major risk factor associated with data compromise

- Impose your own policies and procedures on third parties when your data is at stake.

Employees and administrators choose poor passwords

- Enforce better password complexity, use 2-factor and educate users.

Out of the box anti-virus is not sufficient

- Unknown-unknowns are best identified with regular security testing and review.

Legacy firewall technologies can be broken

- Maintain updated technology. Review security configurations frequently and aggressively.

Questions?

Resources

Download the report: www.trustwave.com/GSR

Follow us online:

- Twitter: @Trustwave / @SpiderLabs
- Facebook: http://www.facebook.com/Trustwave
- LinkedIn: http://www.linkedin.com/company/trustwave
- Google+: https://plus.google.com/103260594120163717290