Trustwave® SpiderLabs®

Caipirinha Security Recipe

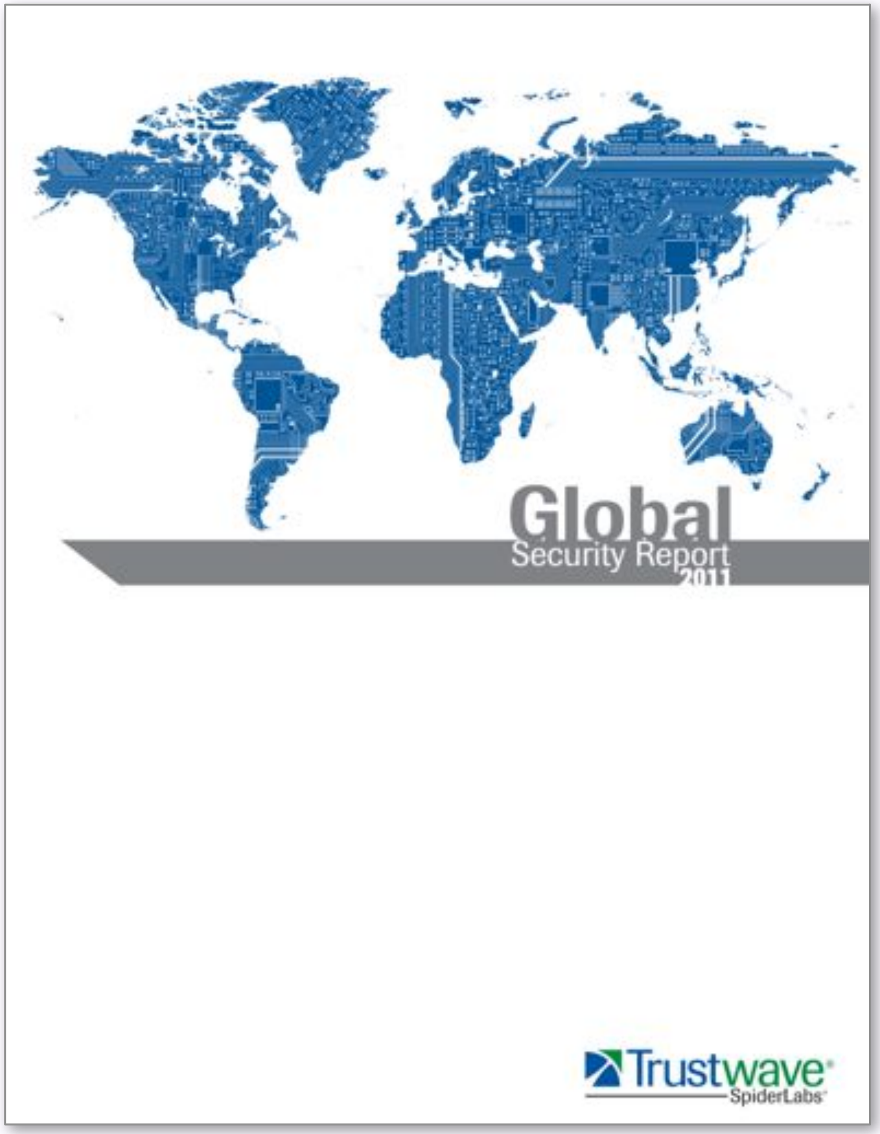
2011 Global Security Statistics and Trends

Blackhat/Defcon/BSidesLV 2011

Agenda

- Introduction
- Incident Response Investigations
- Malware Statistics
- Attack Vector Evolution
- Strategic Initiatives
- Global Conclusions
- Questions?

Introduction



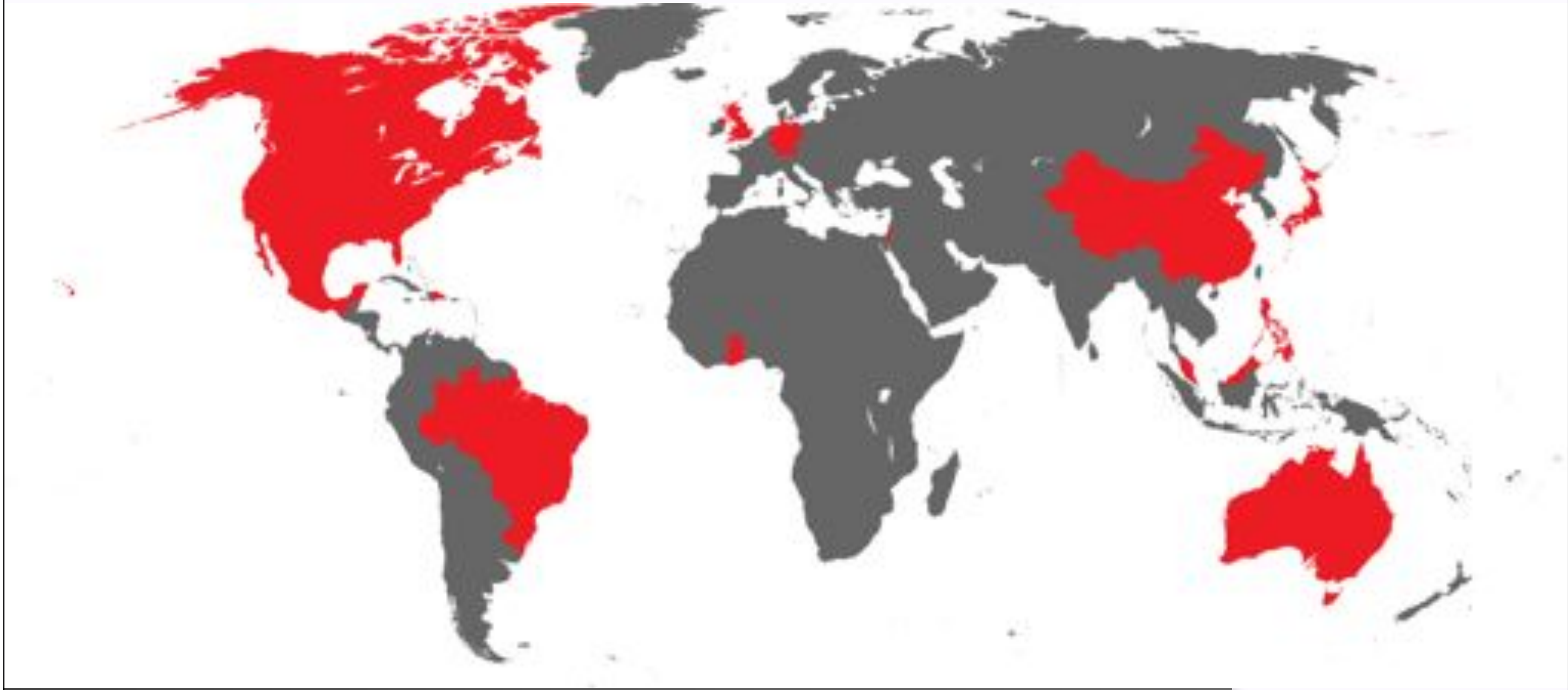
About Trustwave's Global Security Report:

- Issued annually
- Based on findings and evidence from work conducted by Trustwave's SpiderLabs in 2010
- Serves as a tool to educate and assist in planning business security strategy
- More than ***200*** investigations and ***2,000*** penetration test results contributed to the analysis and conclusions
  - Data gathered from Top 20 GDP countries
- Download report:

  https://www.trustwave.com/GSR

Incident Response Investigations

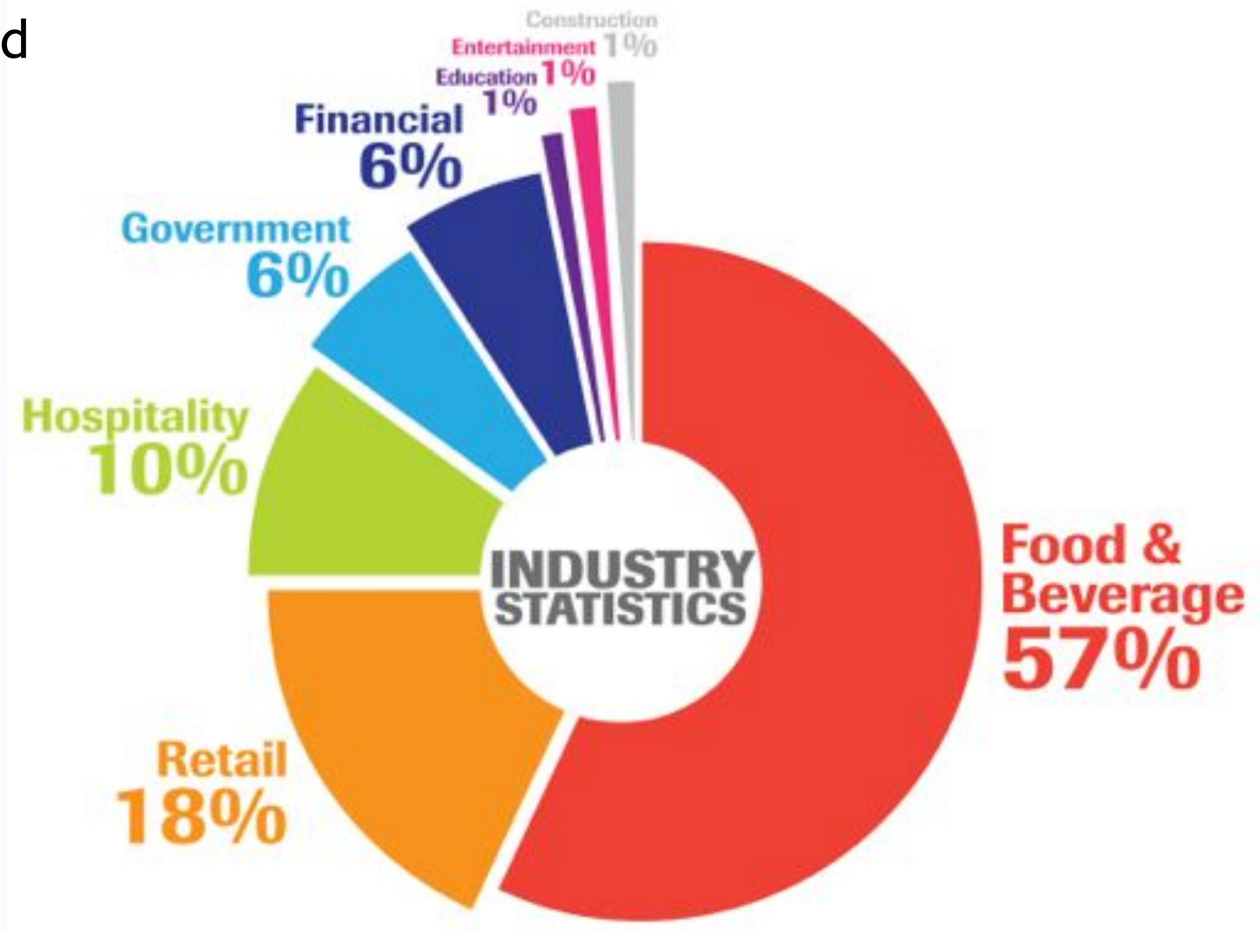
- Countries Represented



Australia, Brazil, Canada, China, Dominican Republic, Germany, Ghana, Israel, Japan, Malaysia, Mexico, Nepal, Philippines, United Kingdom, USA

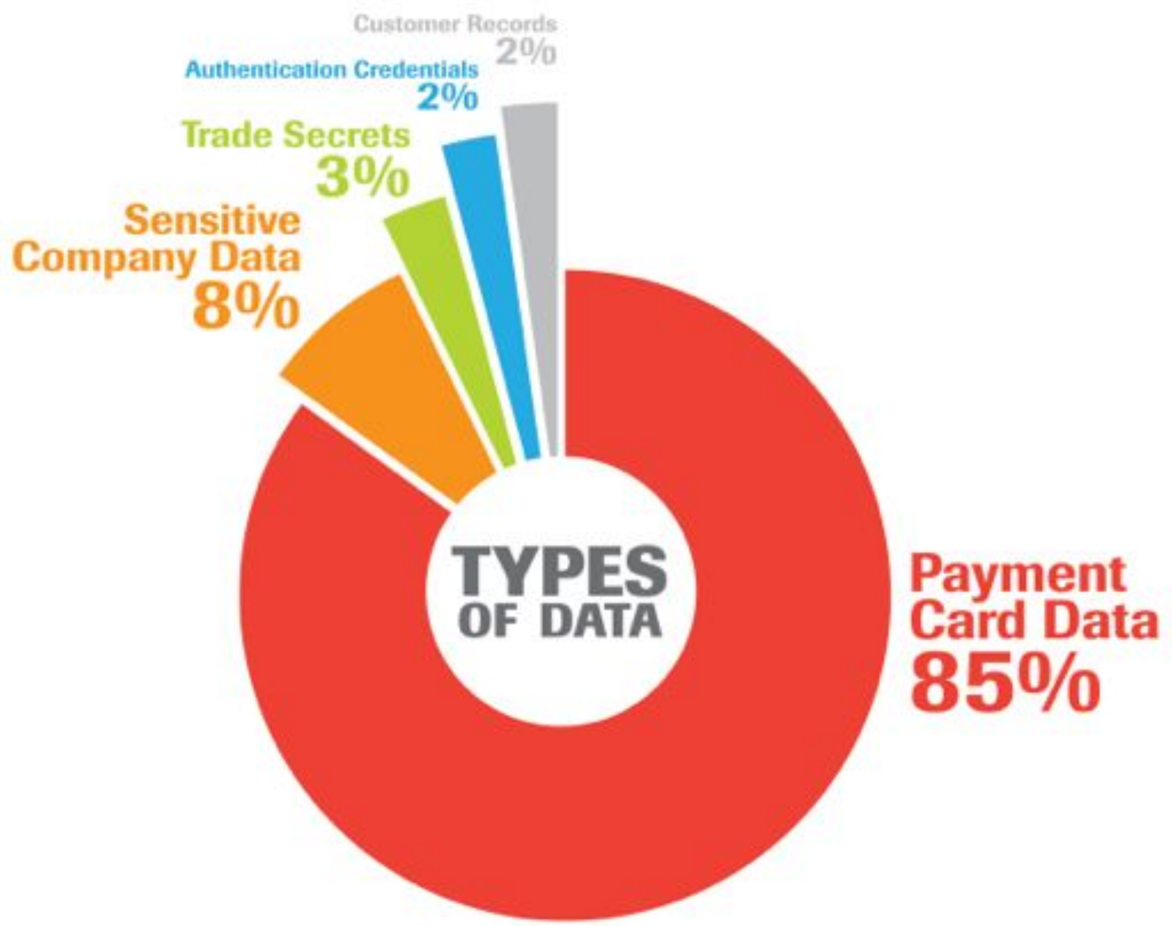
Incident Response Investigations

- Industries Represented
  - 75% of cases - Food & Beverage and Retail
  - Less focus on hospitality than previous year
  - A group responsible for the majority increased their scope



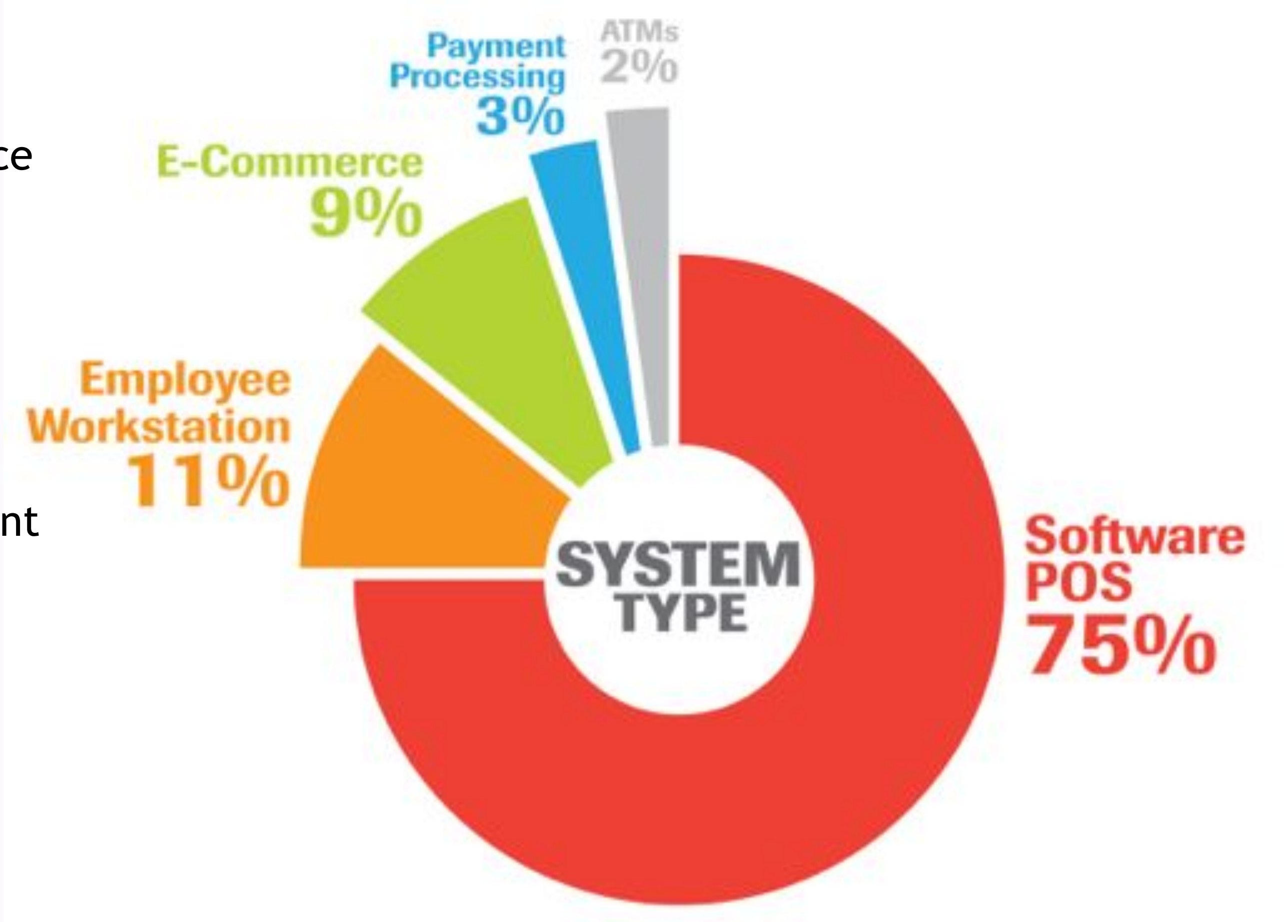
Incident Response Investigations

- Data at Risk
  - Payment card data- simplest to monetize
  - Sensitive data
    - M&A activity
    - Board minutes
    - Intelligence
    - Proprietary data
    - Trade secrets



Incident Response Investigations

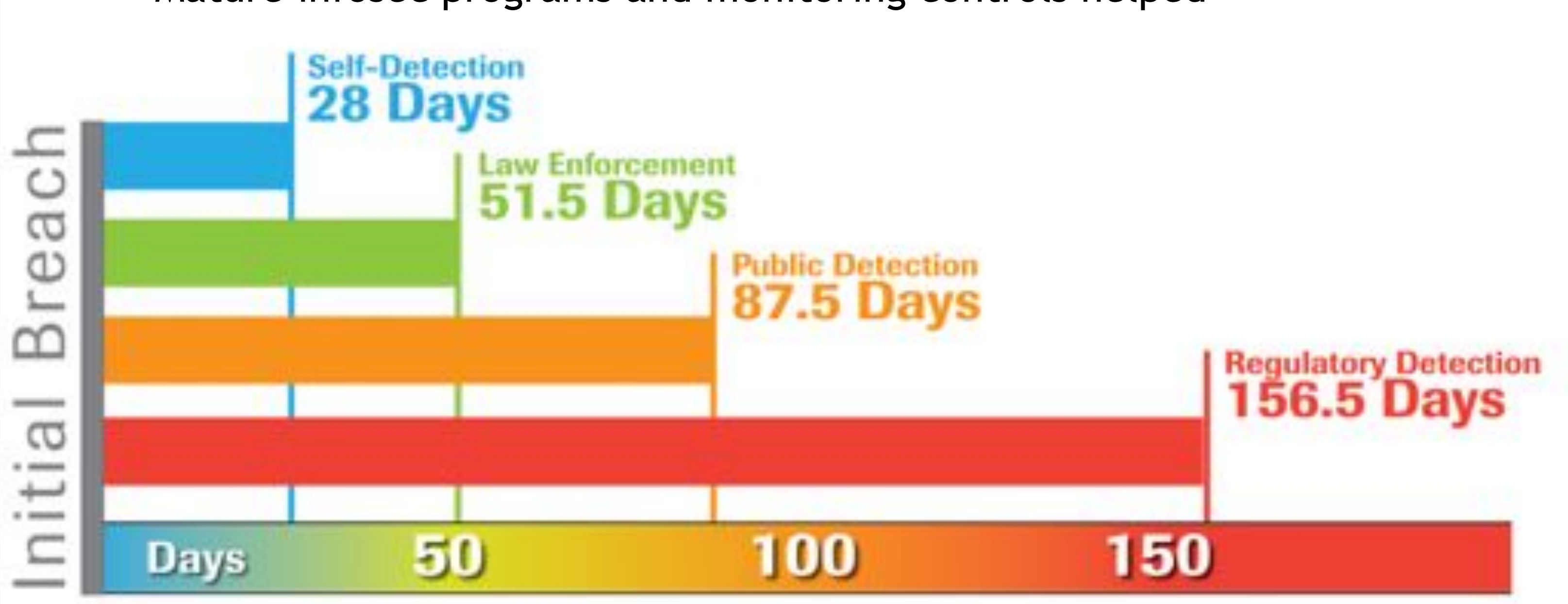
- Target Assets
  - POS systems continue to be path of least resistance
  - Most relied on 3rd party integrators
  - EMV countries still a target
    - Focus on card present environments
    - As mag-reader POS still in use



Trustwave

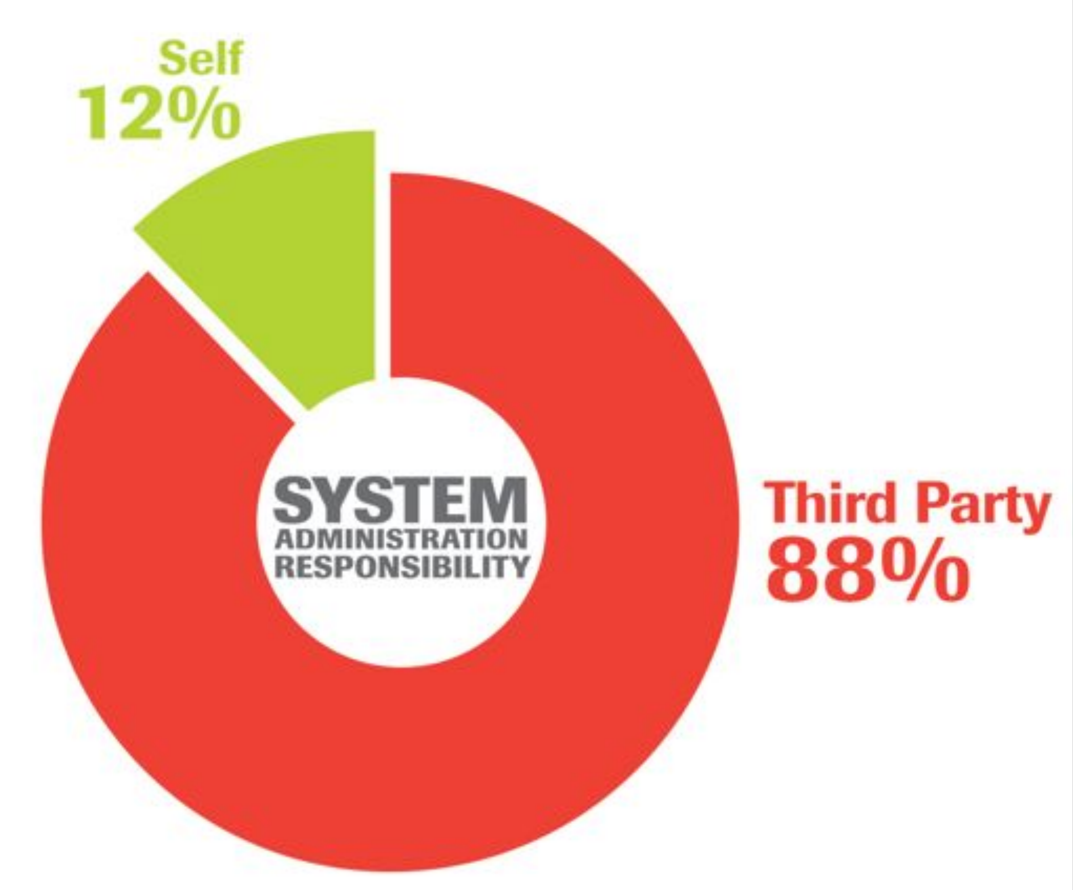
Incident Response Investigations

- Detection Methods vs. Time
- As expected, those able to self detect, detect quicker
- Unable to self-detect, 5x longer exposure time
- Investigations showed:
  - Role-based security training = improved detection capability
  - Mature infosec programs and monitoring controls helped



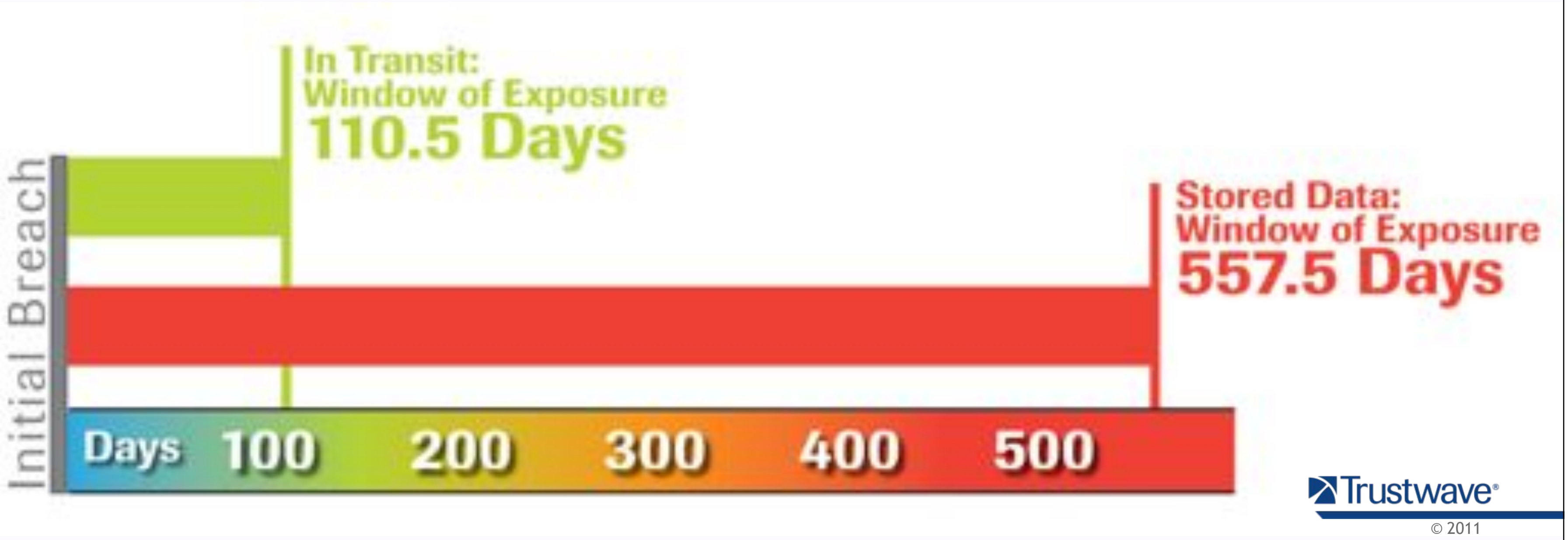
Incident Response Investigations

- Administration Responsibility
  - Third party implementation and maintenance agreement?
  - Build in non-functional security requirements



Incident Response Investigations

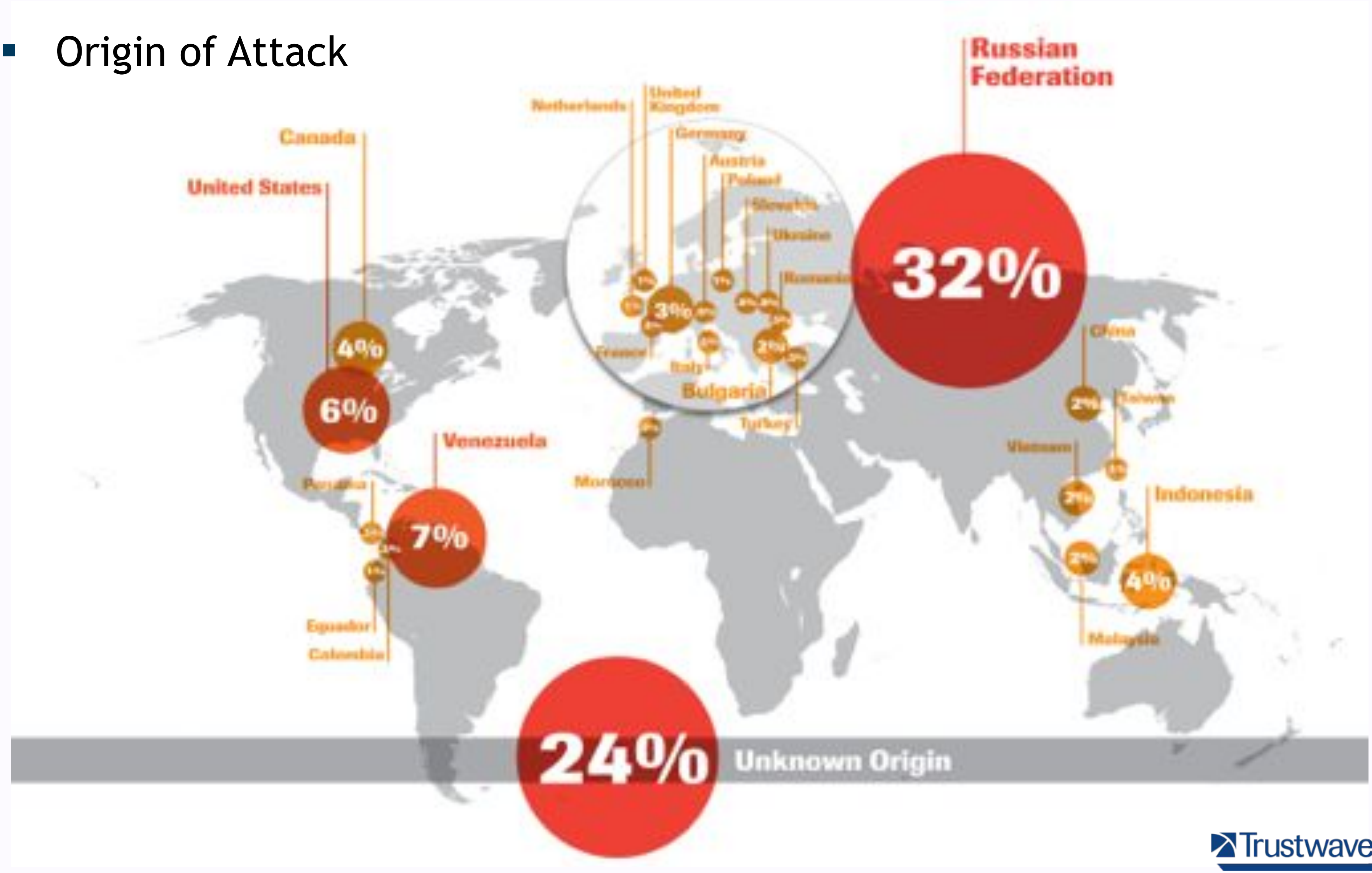
- Window of Data Exposure
  - Reality reflects intuition
  - Storing data increases impact of breach
  - Average “compromised” transactions
  - In-transit data – 3 months
  - Stored data – 18 months



Trustwave

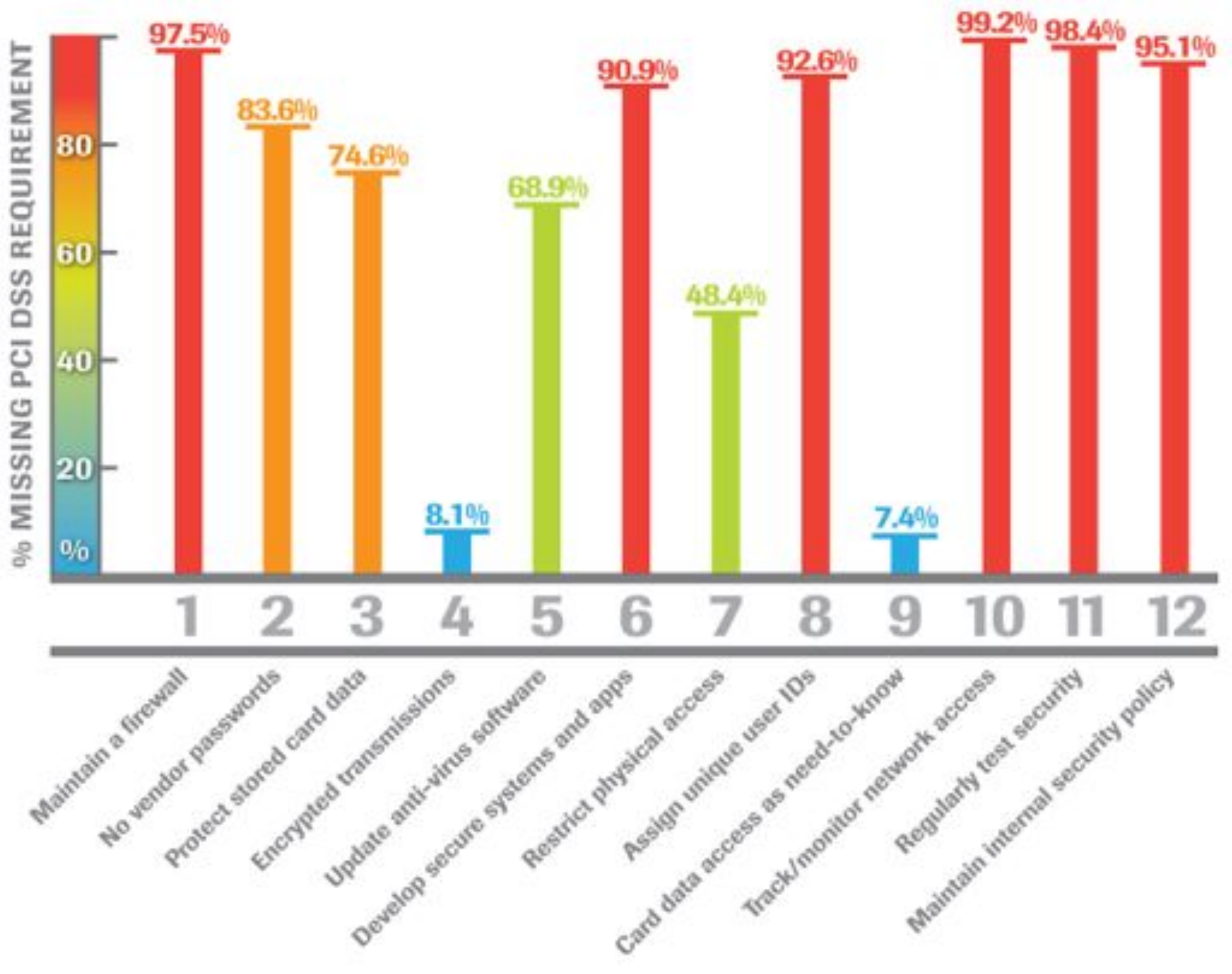
Incident Response Investigations

- Origin of Attack



Trustwave

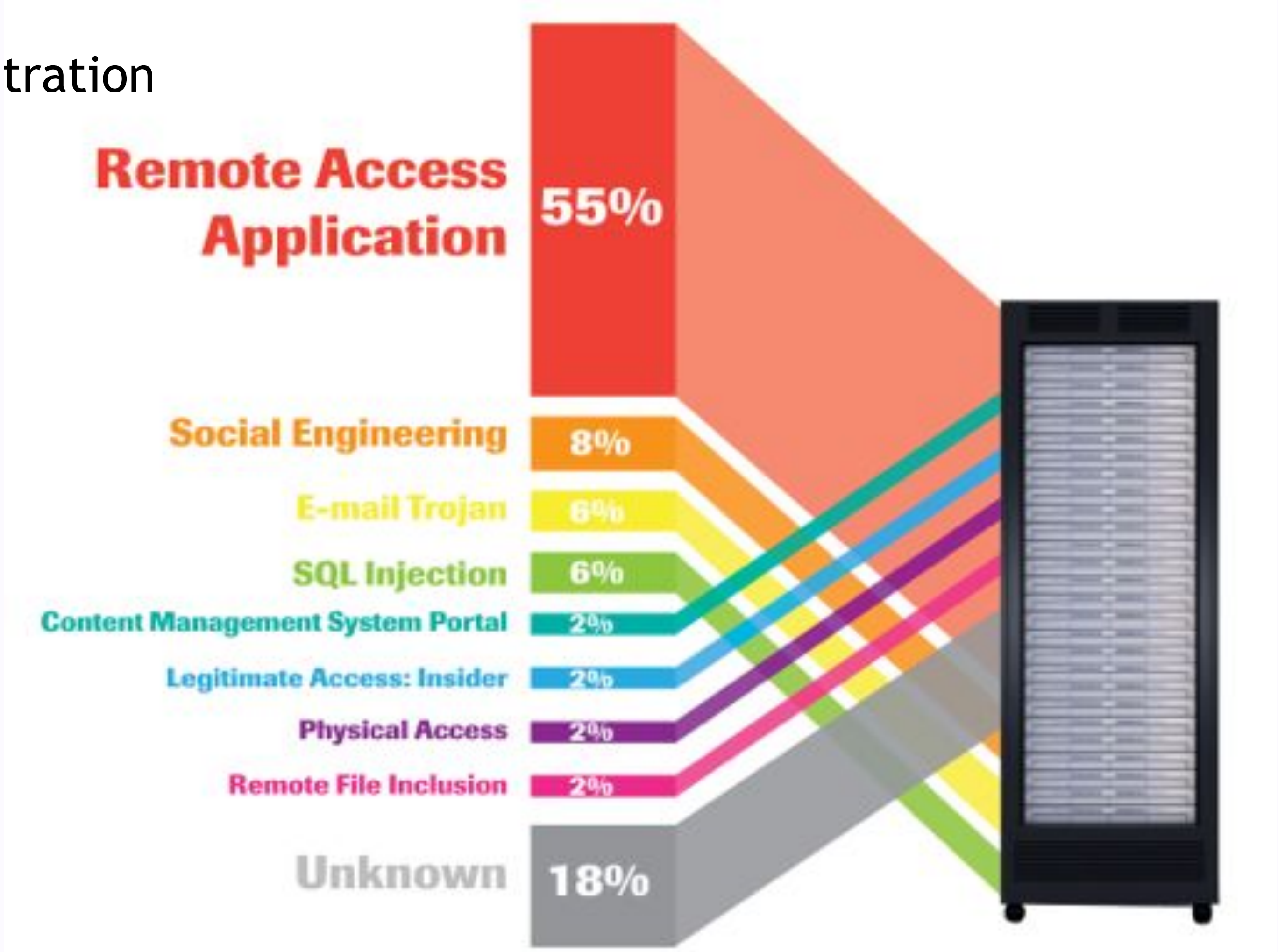
Incident Response Investigations



- 97% insufficient firewall policy
- 83% default/ guessable password
- 48% not using PA-DSS application

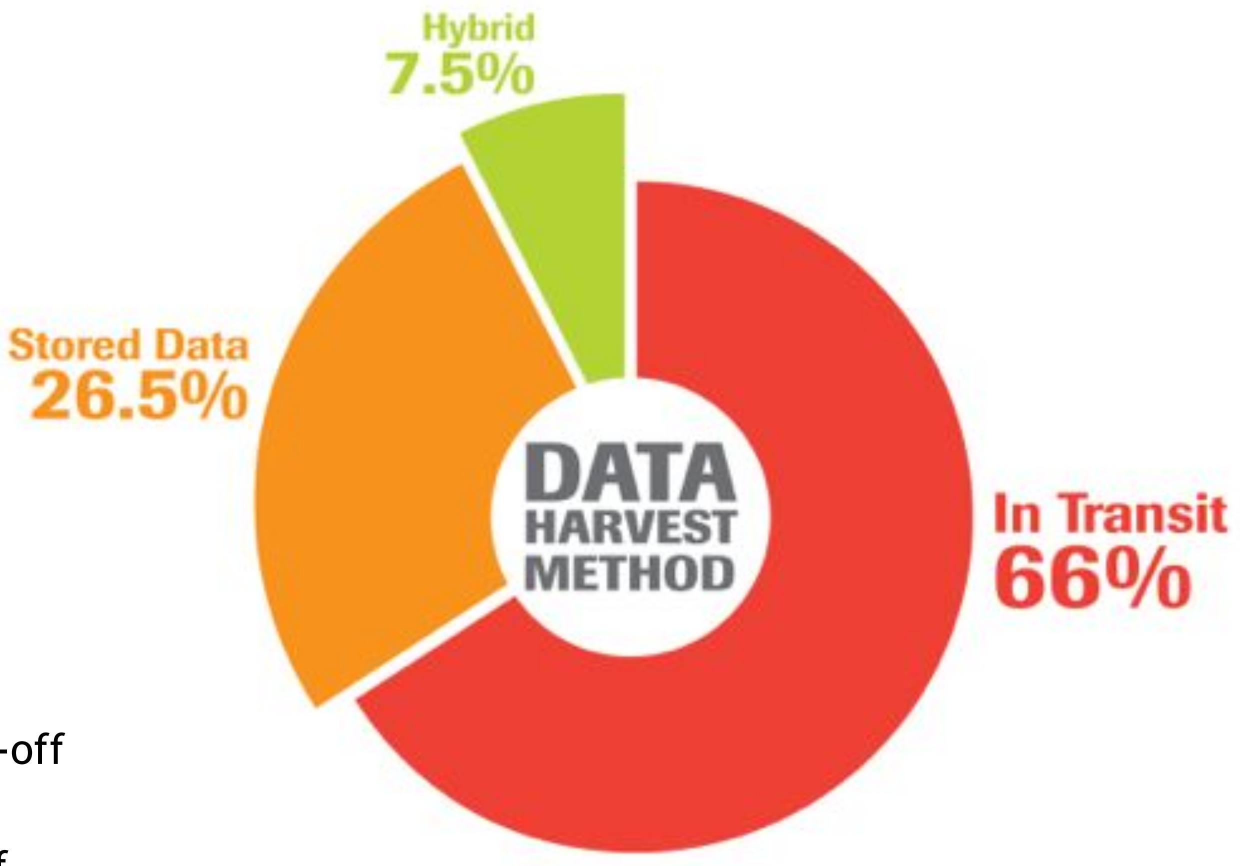
Breach Triad – Infiltration, Aggregation, Exfiltration

- Infiltration



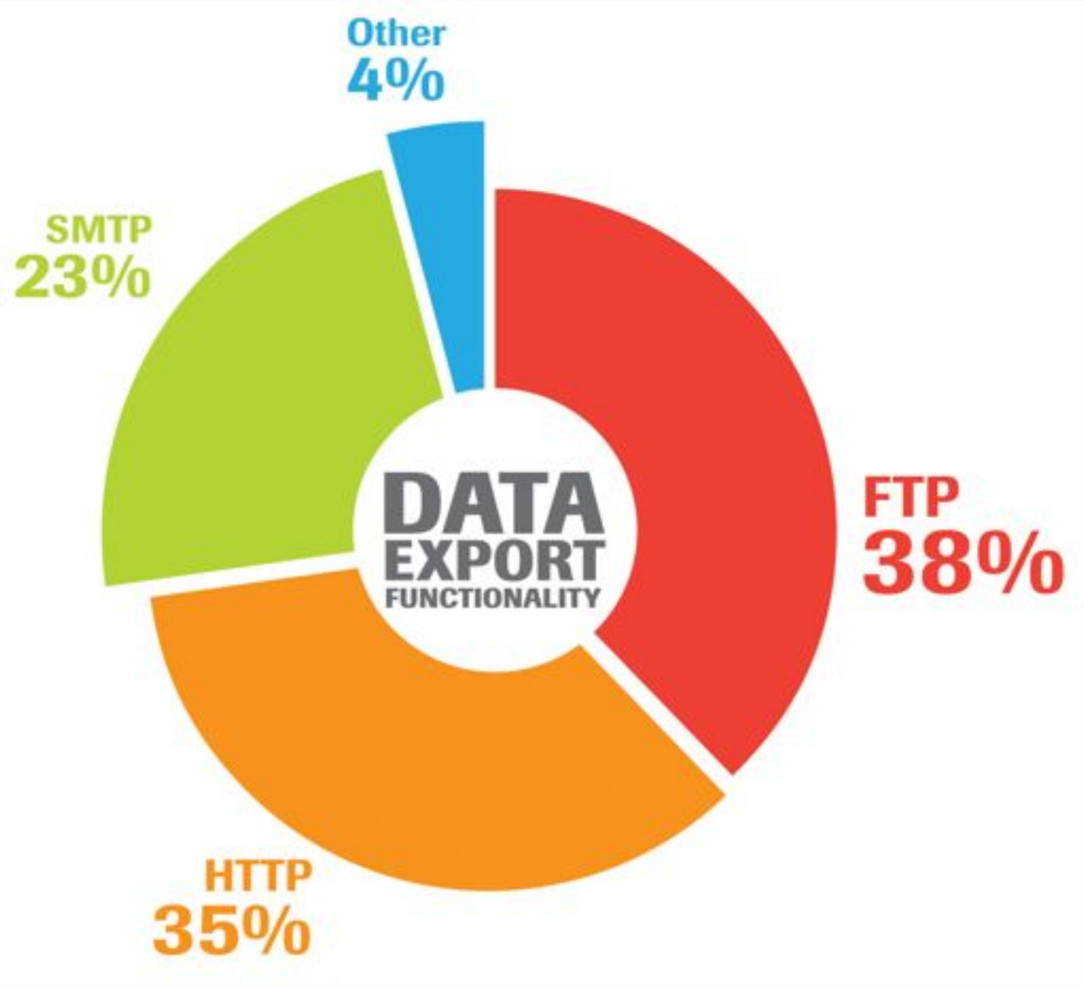
Breach Triad – Infiltration, Aggregation, Exfiltration

- Aggregation
  - Shift away from “smash & grab” of stored data
  - **Why?**
    1. Less unsafe data being stored
       - PCI DSS, PA-DSS, OWASP
    2. Card data expires
       - More complex to harvest
       - The data is fresh
       - Worthwhile trade-off for criminals
  - In-transit attacks and use of custom malware correlate



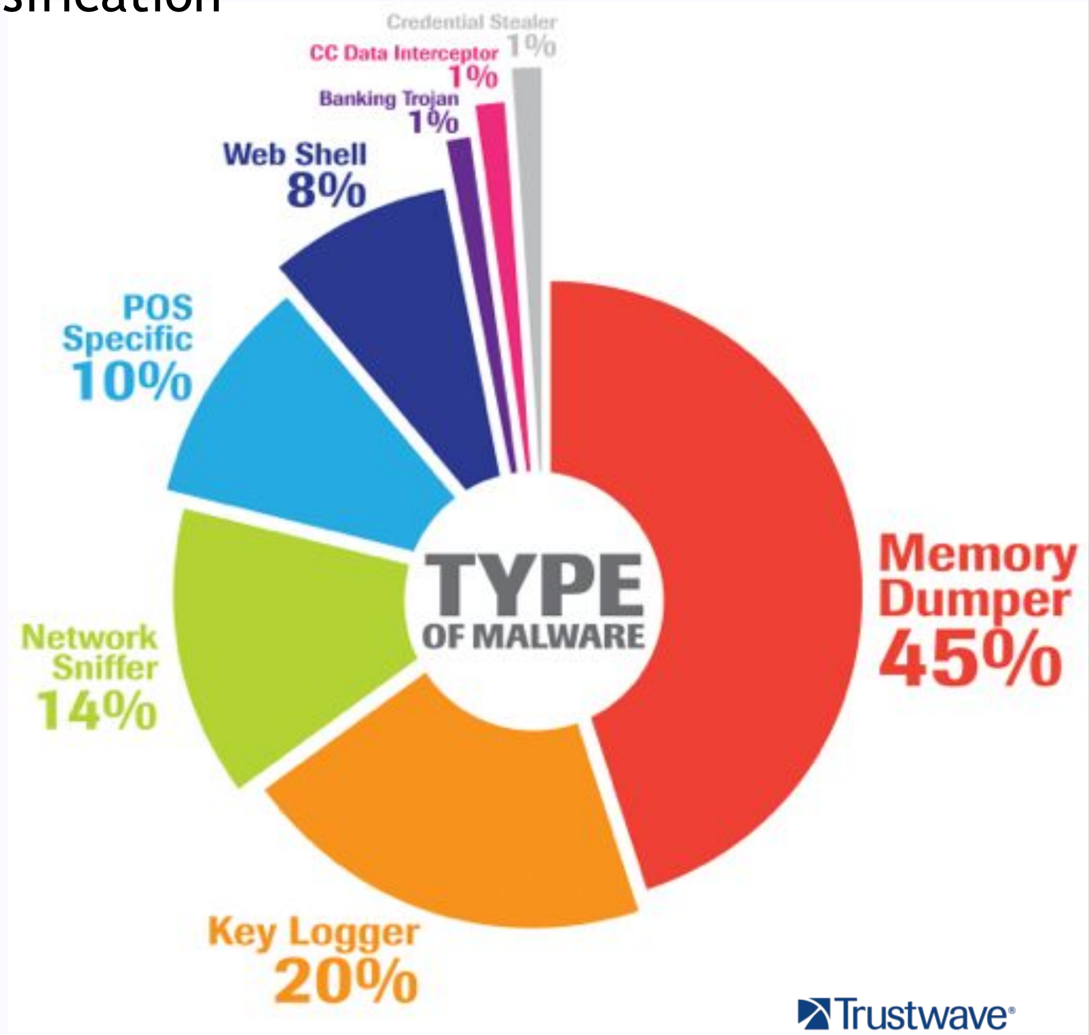
Breach Triad – Infiltration, Aggregation, Exfiltration

- Exfiltration



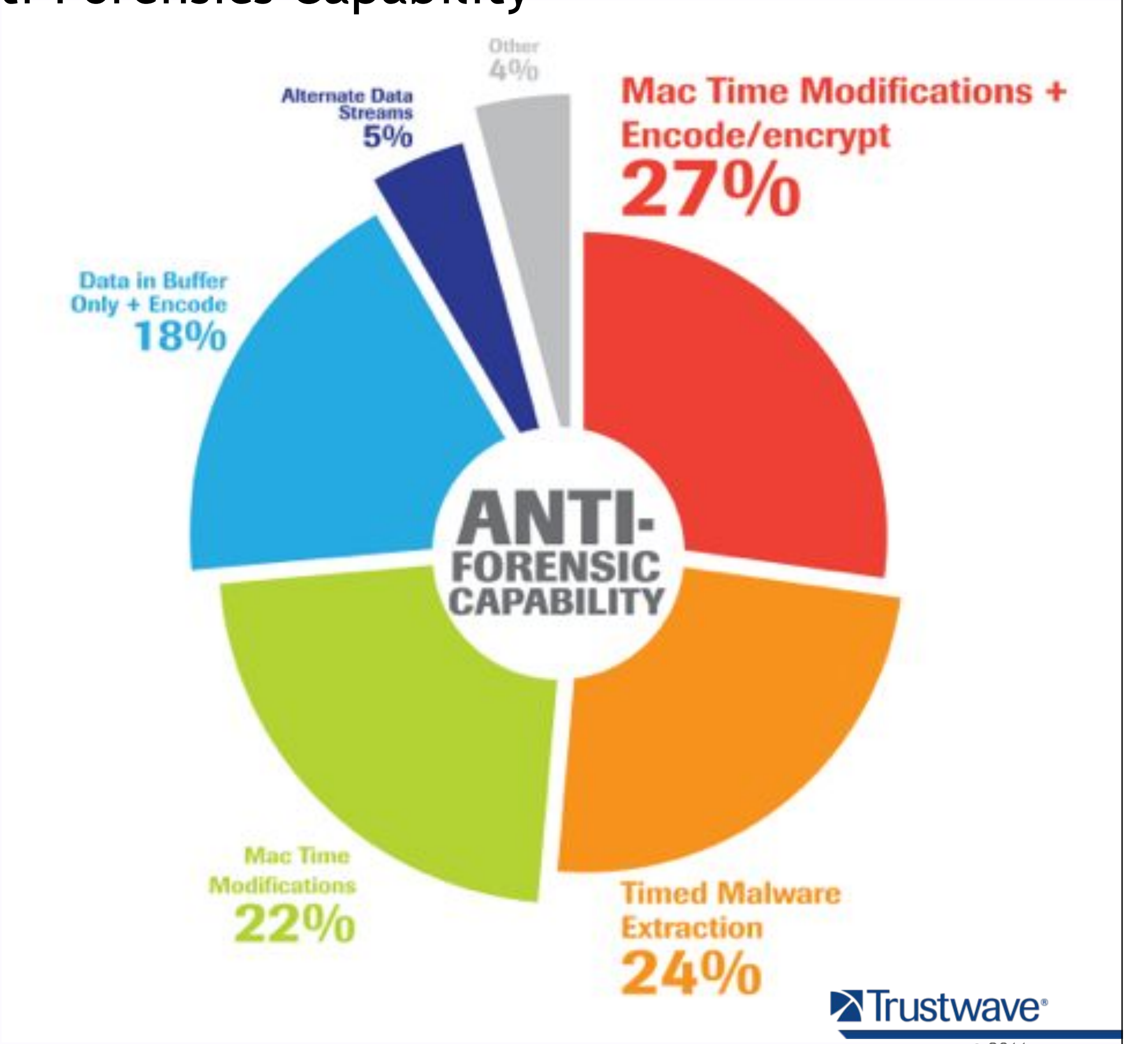
Malware Statistics

- **Data Points of Interest:** Classification
  - New Malware Developments
    - POS-specific malware
    - Requires POS-specific knowledge
  - POS Malware Highlight Case
    - Encryption algo/key identified
    - Decrypted and extracted the data

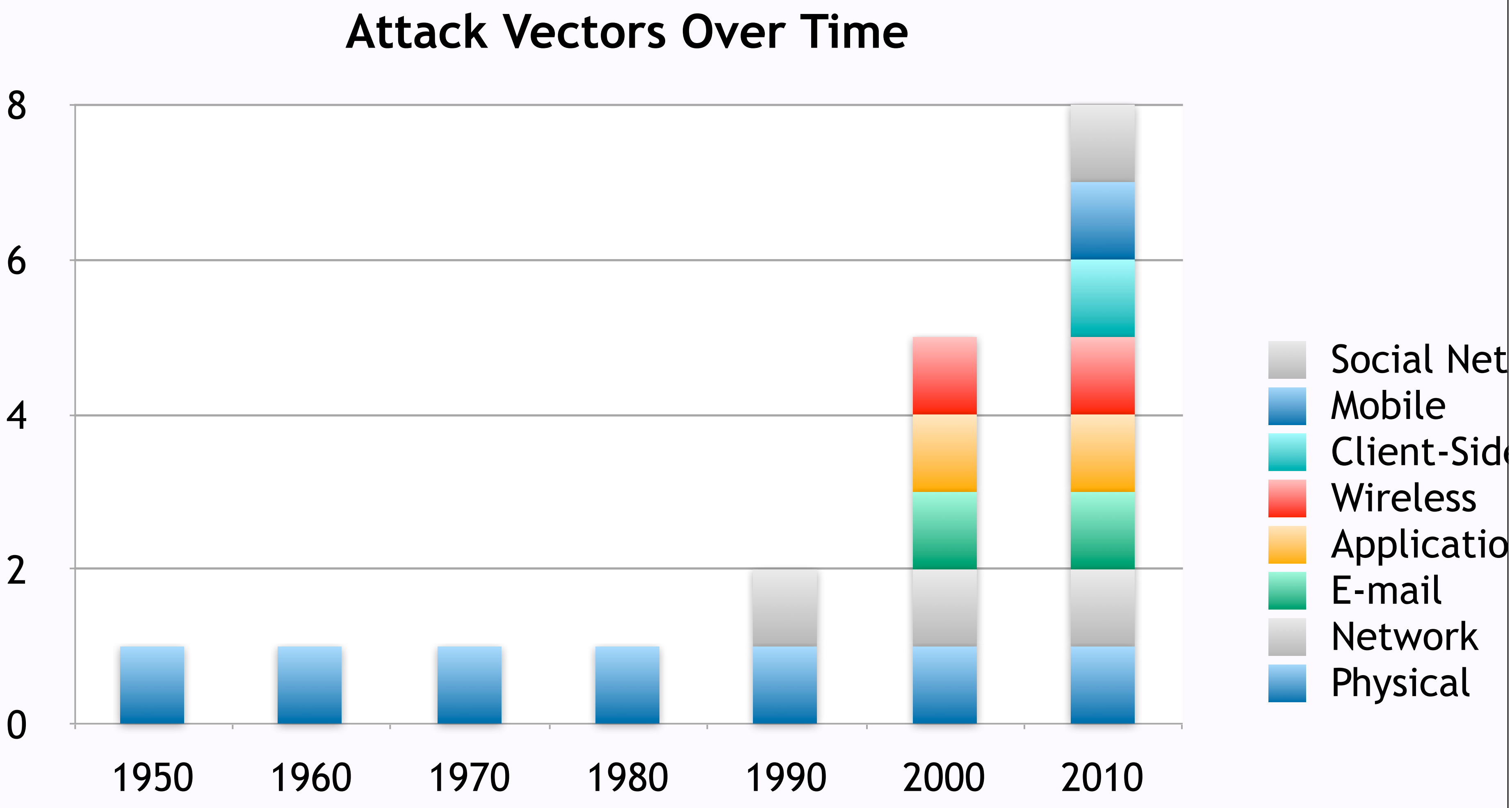


Malware Statistics

- **Data Points of Interest:** Anti-Forensics Capability
  - Main Themes
    - More anti-forensic features
    - Primarily to avoid DLP/IDS
    - Memory data storage
    - Obfuscation
  - Malware analysis skills are now a must for investigators



Attack Vector Evolution



Attack Vector Evolution

- **1980s:** Physical

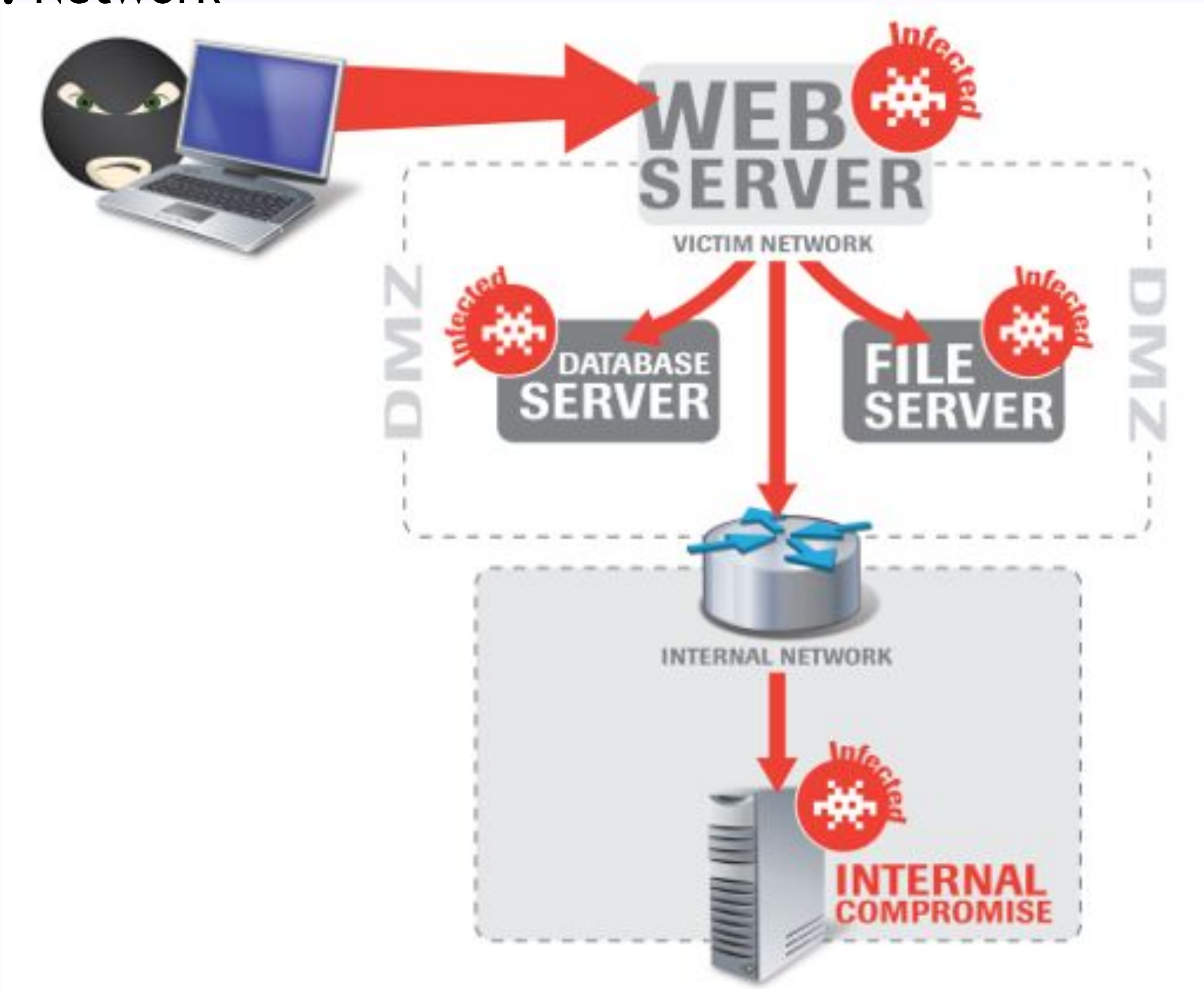
Attack Vector Evolution

- **2010:** Physical

1. Sensitive Data Left in Plain View
2. Unlocked Accessible Computer Systems
3. Data Cabling Accessible from Public Areas

Attack Vector Evolution

- **1990s:** Network



Trustwave®

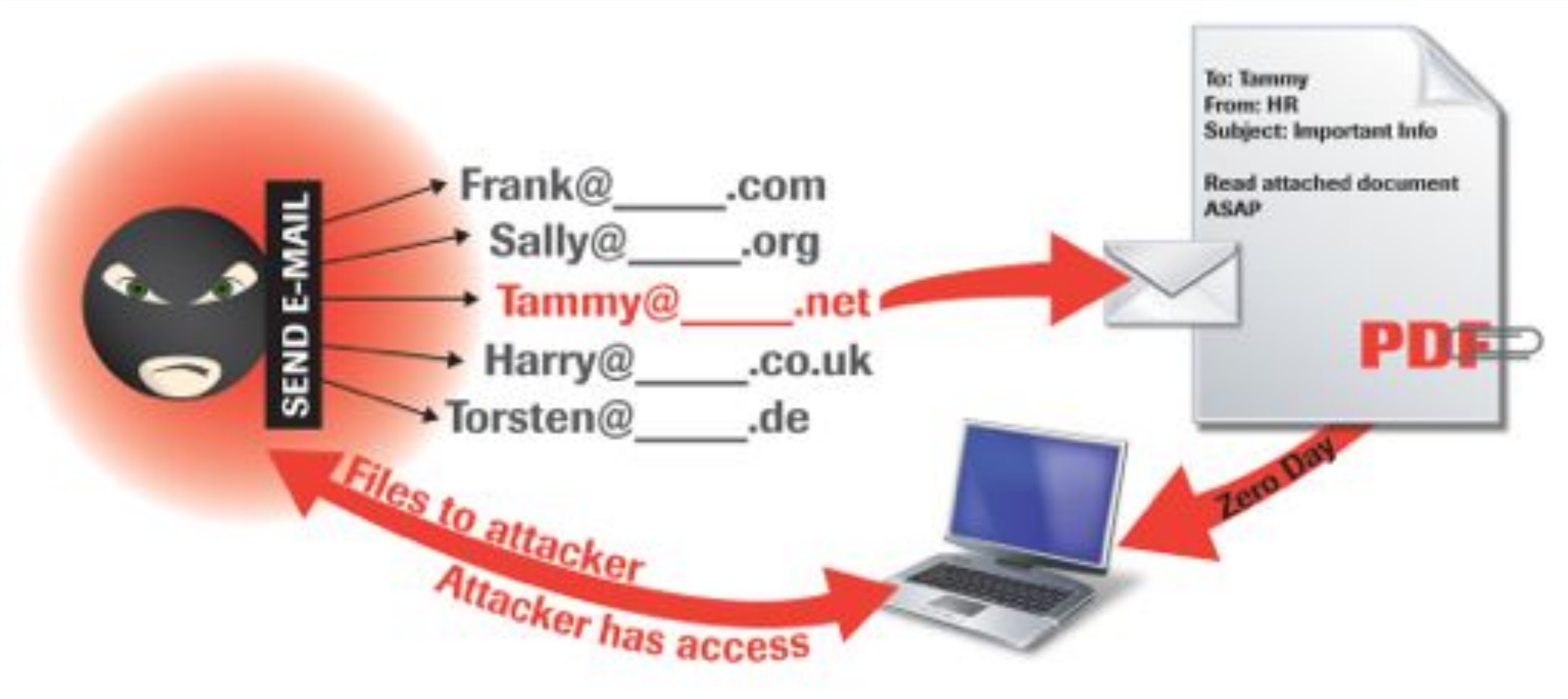
Attack Vector Evolution

- **2010:** Network

1. Weak or Blank Administrator Passwords
2. Database Servers Accessible
3. ARP Cache Poisoning

Attack Vector Evolution

- **2000s:** E-mail

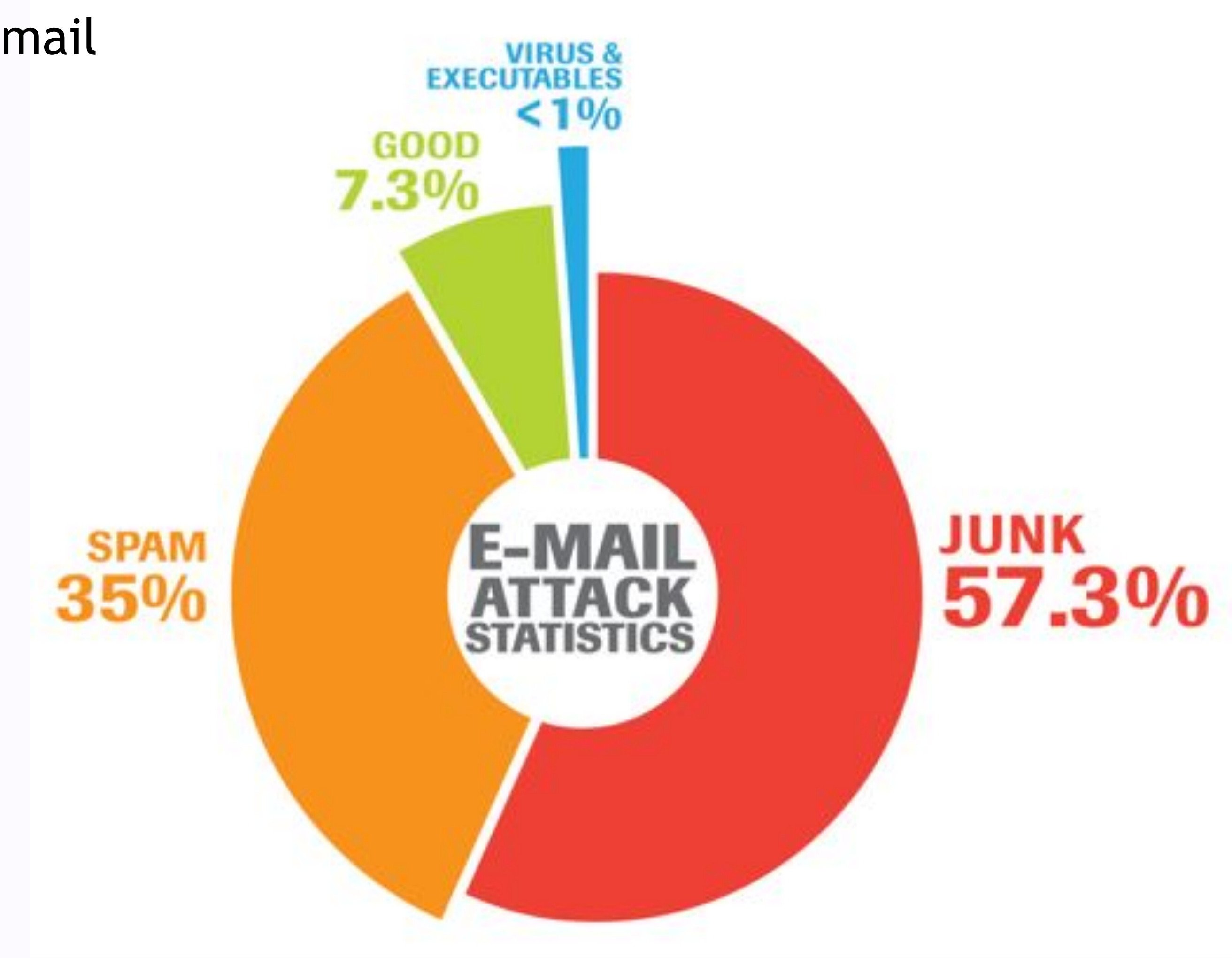


To: Tammy
From: HR
Subject: Important Info

Read attached document ASAP

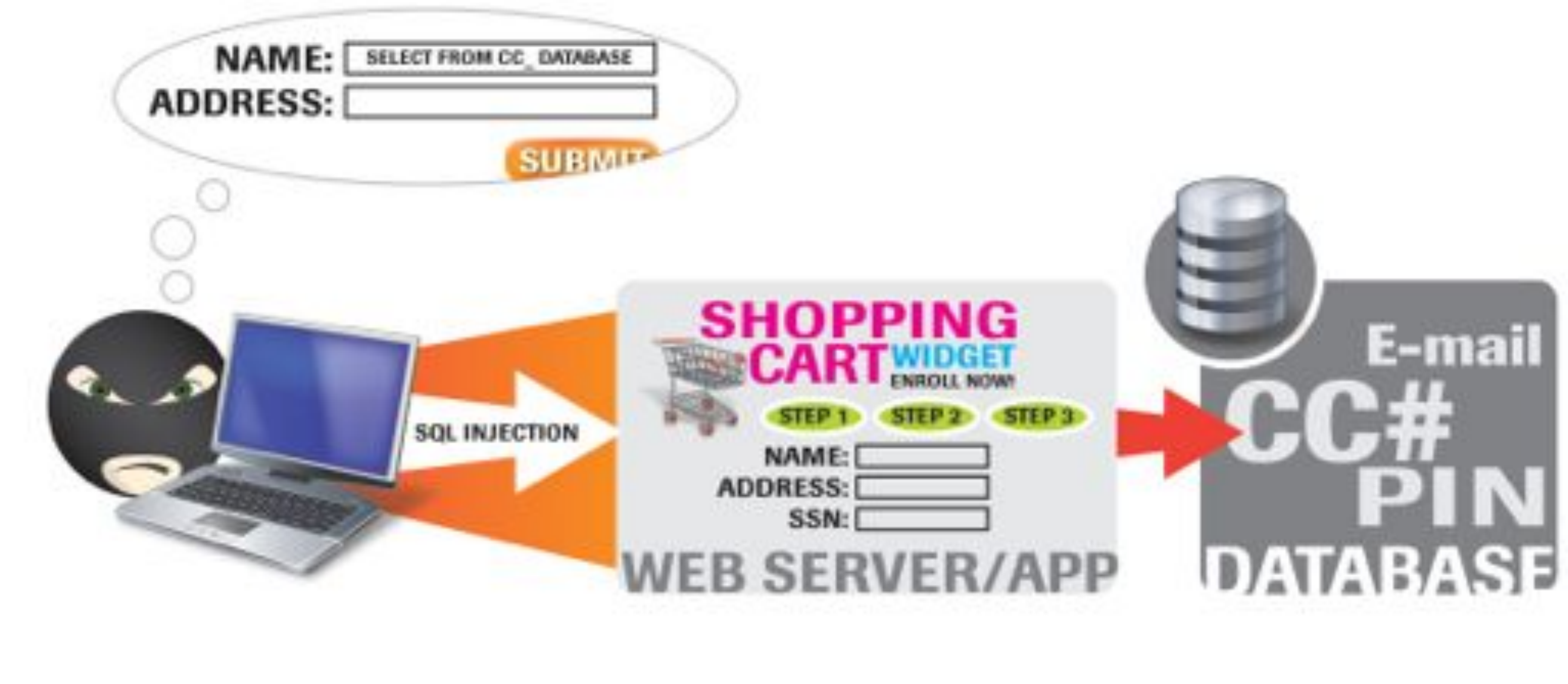
Attack Vector Evolution

- **2010:** E-mail



Attack Vector Evolution

- **2000s:** Application



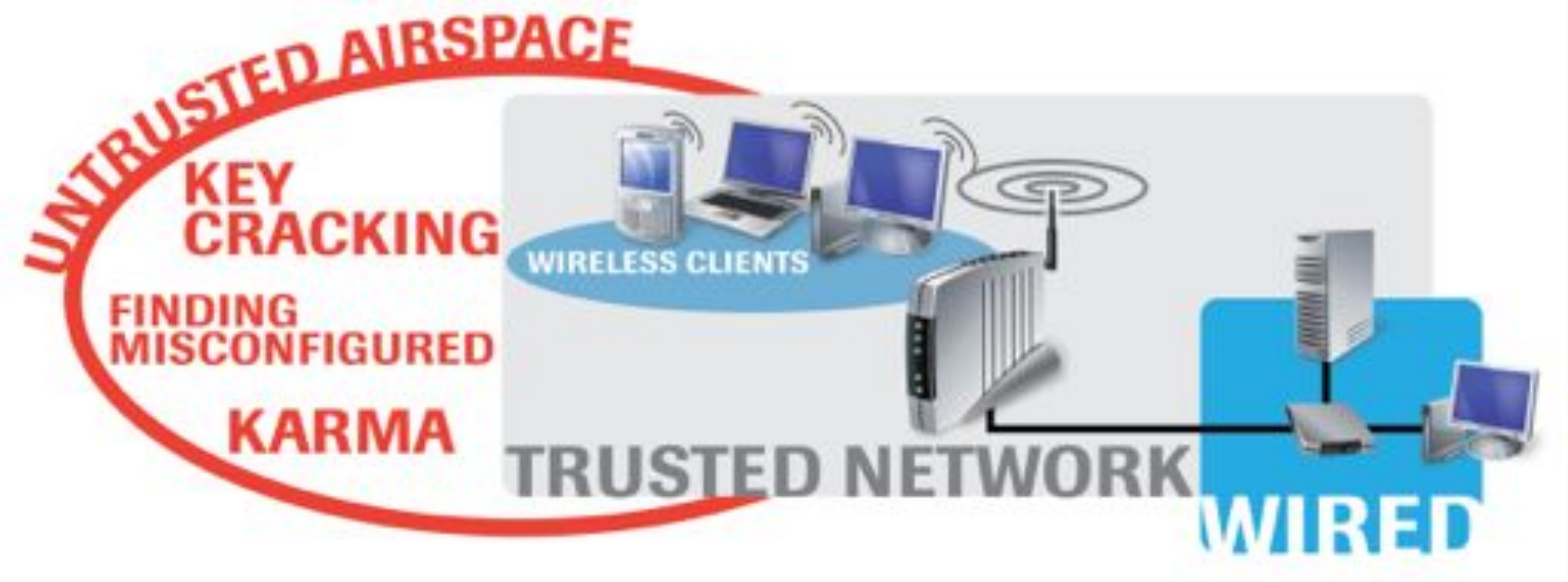
Attack Vector Evolution

- **2010:** Application

1. SQL Injection
2. Logic Flaws
3. Authorization Bypass

Attack Vector Evolution

- **2000s:** Wireless



Attack Vector Evolution

- **2010:** Wireless

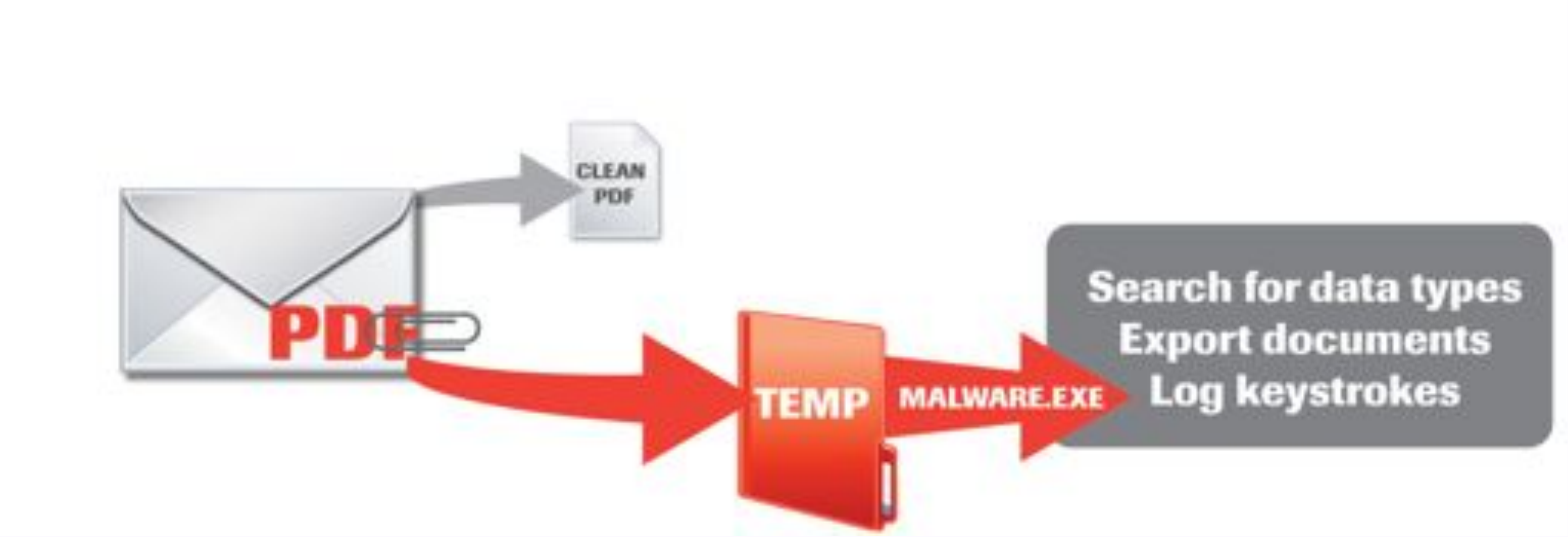
1. Wireless Enabled while on Wired Network

2. Wireless Clients Associate w/ “Known” Networks

3. Easily Guessed WPA/WPA2 Pre-Shared Key

Attack Vector Evolution

- **2010s:** Client-Side



Search for data types
Export documents
Log keystrokes

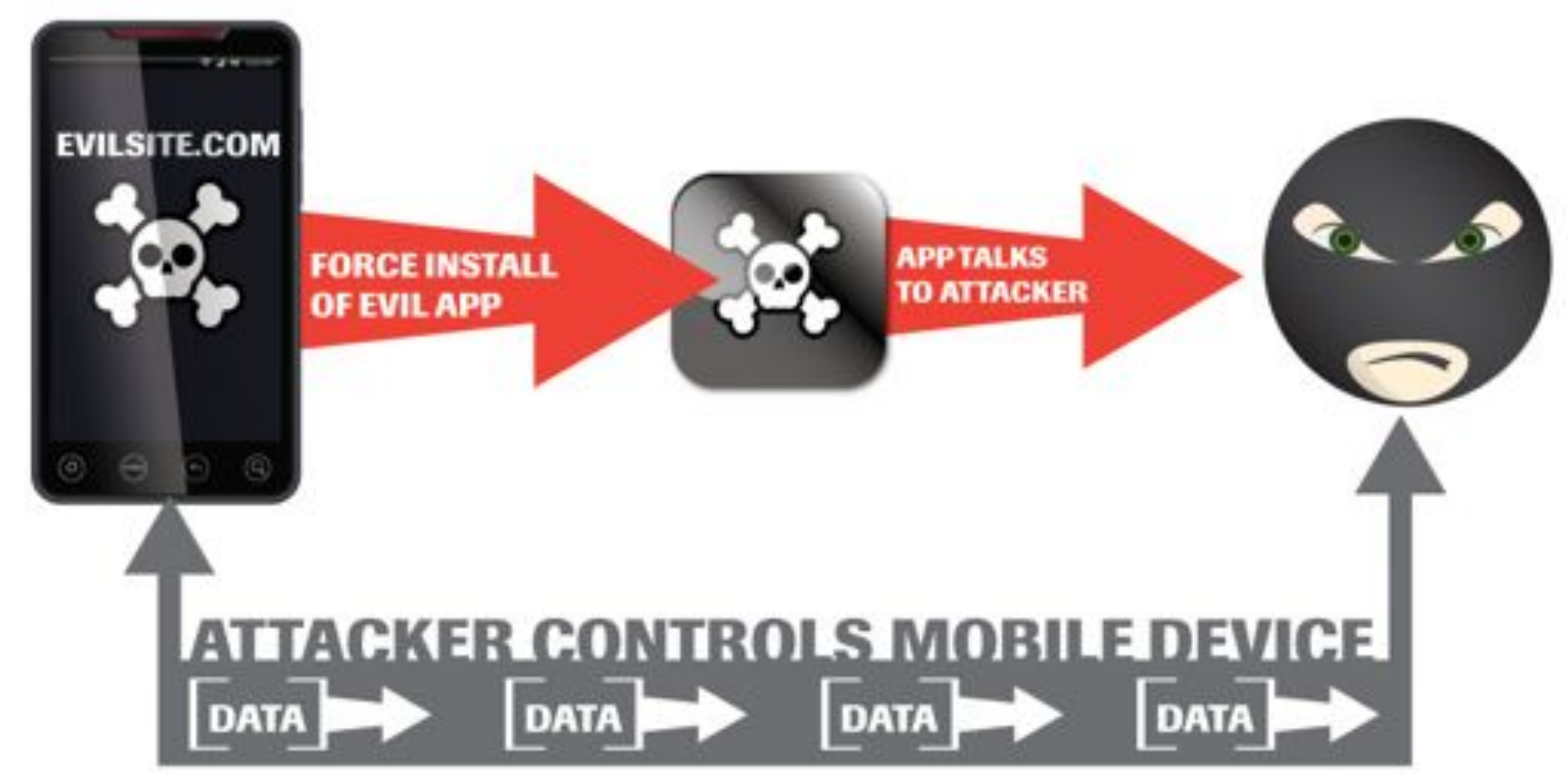
Attack Vector Evolution

- **2010:** Client Side (Malware)

1. Targeted Attack
2. Drive-by Infection
3. Manual Installation

Attack Vector Evolution

- **2010s:** Mobile



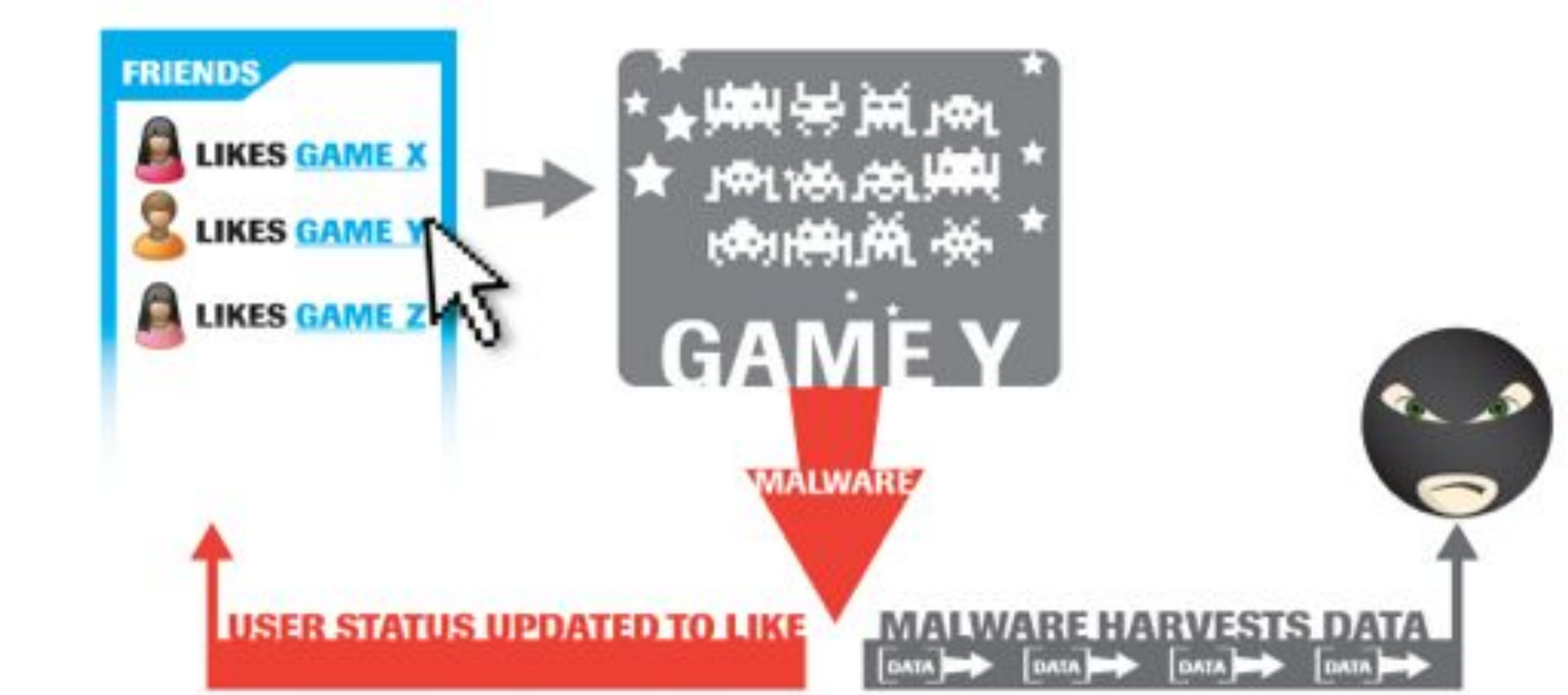
Attack Vector Evolution

- **2010:** Mobile

1. Mobile Phishing Attacks
2. Mobile Ransomware
3. Fake Firmware and Jailbreaks

Attack Vector Evolution

- **2010s:** Social Networking



Attack Vector Evolution

- **2010:** Social Networking

1. Malware Propagation

2. Personal Information Exposure

3. Data Mining

Strategic Initiatives

1. Assess, Reduce and Monitor Client-side Attack Surface
2. Embrace Social Networking, but Educate Staff
3. Develop a Mobile Security Program
4. Use Multifactor Authentication
5. Eradicate Clear-text Traffic
6. Virtually Patch Web Applications Until Fixed
7. Empower Incident Response Teams
8. Enforce Security Upon Third Party Relationships
9. Implement Network Access Control
10. Analyze All Events
11. Implement an Organization-wide Security Awareness Program

Global Conclusions

In 2010, the security landscape changed:

- Targets shifted towards endpoints and users
- Individuals became easily identifiable to attackers
- Malicious tools became more sophisticated
- New attack vectors introduced as we innovate; old vectors never die

In 2011, organizations that are firmly committed to security will be:

- Resilient to attack
- Reduce risk of data compromise
- Protect sensitive data and reputation

Semper Fidelis, Sine Metu

Tom Brennan CISSP, CISM, CEH, NSA-IAM

Director, Strategic Initiatives

Trustwave, SpiderLabs

Download FULL REPORT at:

http://www.trustwave.com/GSR

Caipirinha