RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

APAC Data Compromise Trends

Marc Bown

Managing Consultant, SpiderLabs APAC

Trustwave

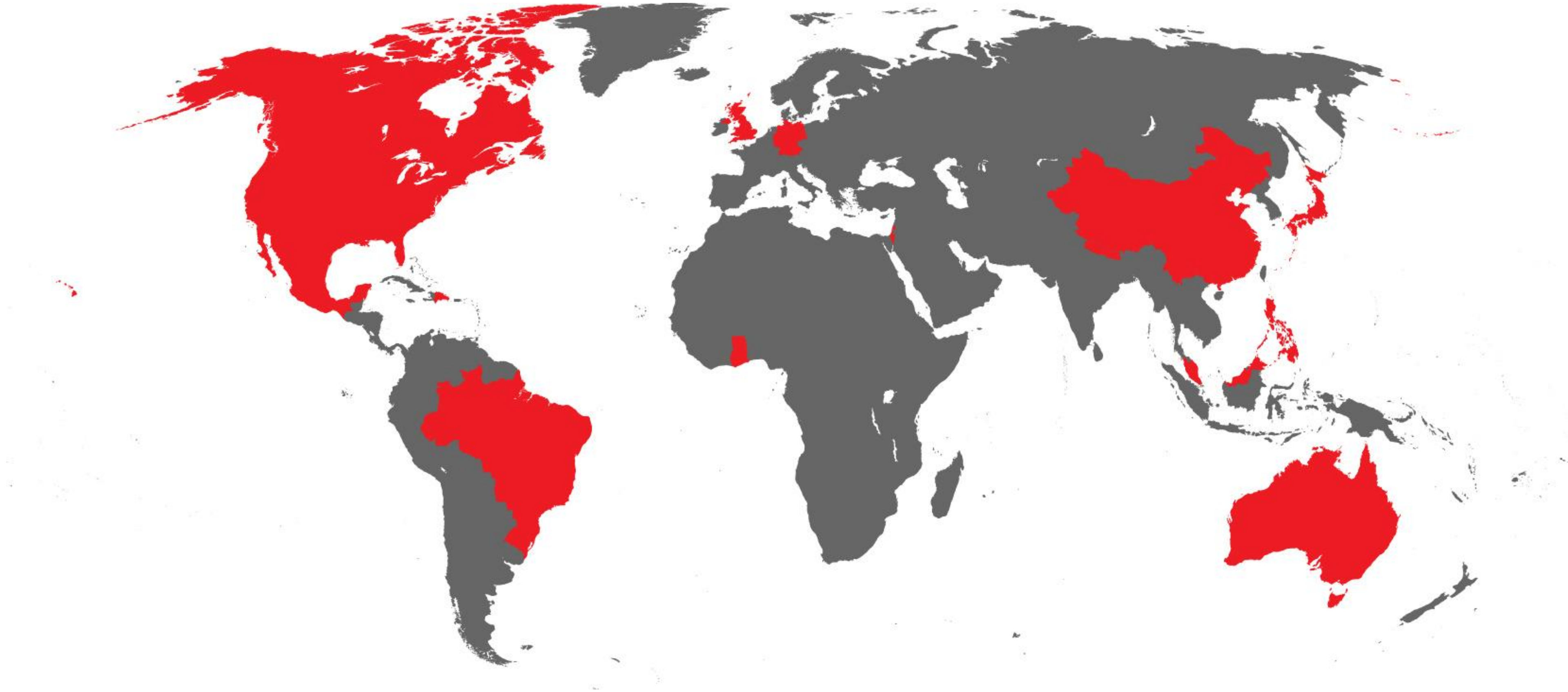
Agenda

- Introduction
- Compromise Trends
- ATM Specifics
- Point of Sale Specifics
- Malware Statistics
- Questions?

Introduction

- Information today derived from Trustwave's Global Security Report (GSR20110) which is issued annually
- Based on findings and evidence from work conducted by Trustwave's SpiderLabs in 2010
- More than 200 investigations and 2,000 penetration test results contributed to the analysis and conclusions
  - Data gathered from Top 20 GDP countries
- Download GSR: https://www.trustwave.com/GSR
- Download ATM Malware Report: https://www.trustwave.com/downloads/spiderlabs/Trustwave-Security-Alert-ATM-Malware-Analysis-Briefing.pdf

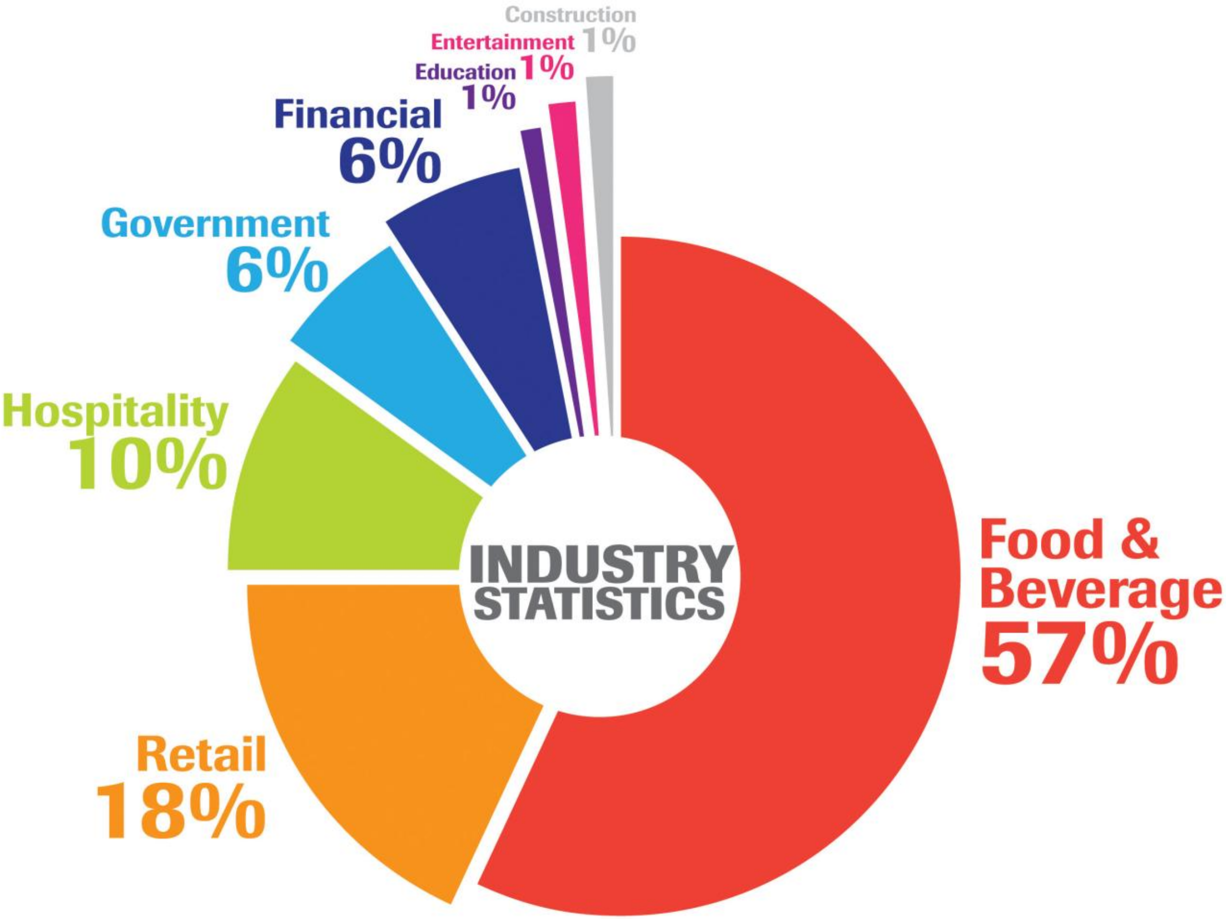
Countries Represented



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

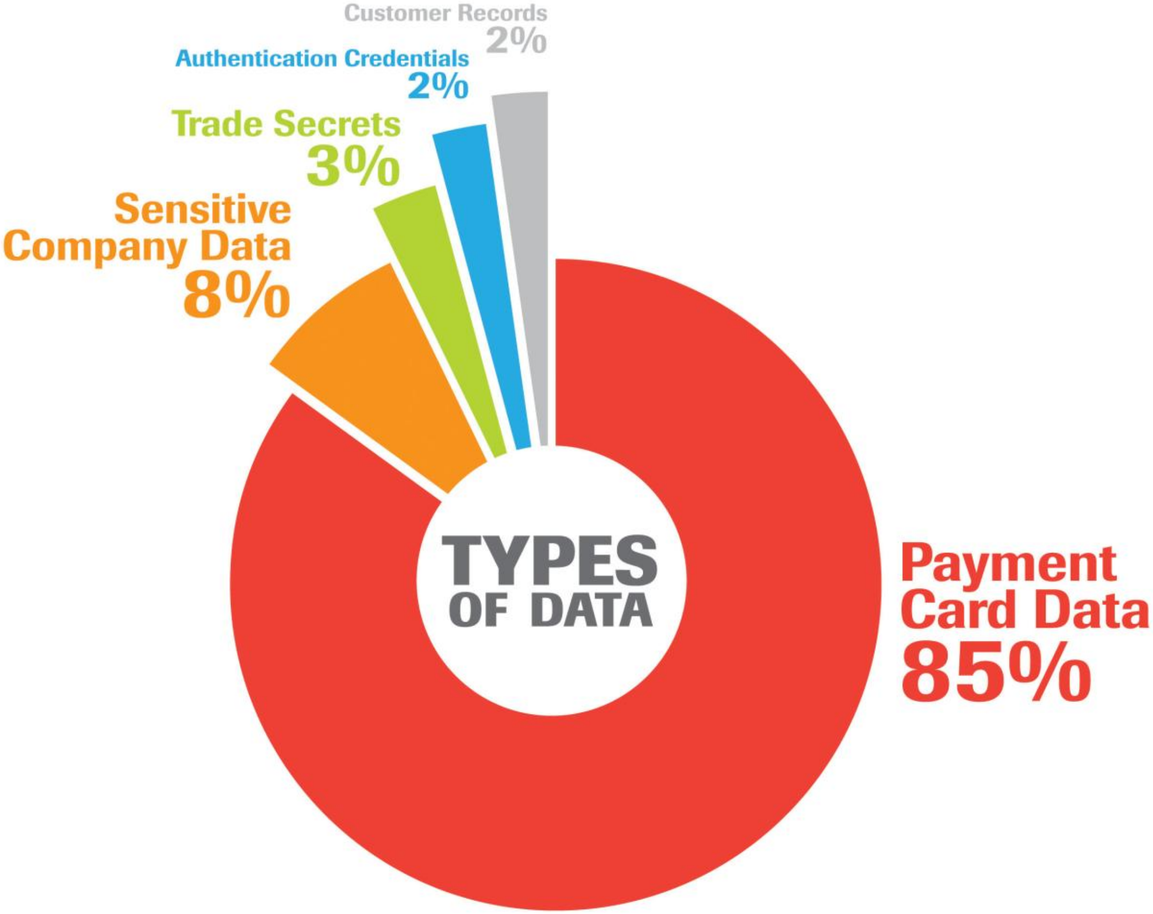
Industries Represented

- Globally, 75% of cases - Food & Beverage and Retail
- Less focus on hospitality than previous year
- Within APAC, e-commerce made up majority of attacks



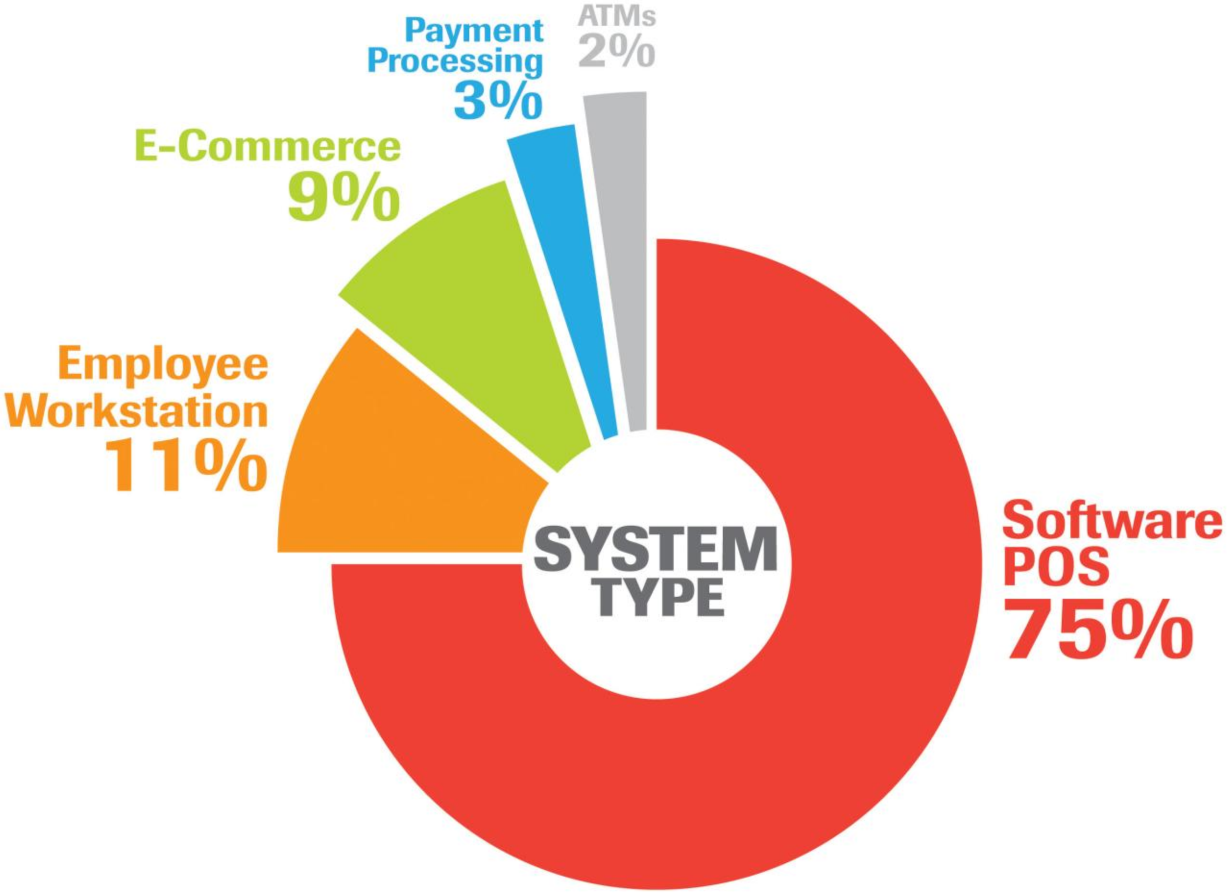
Data at Risk

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



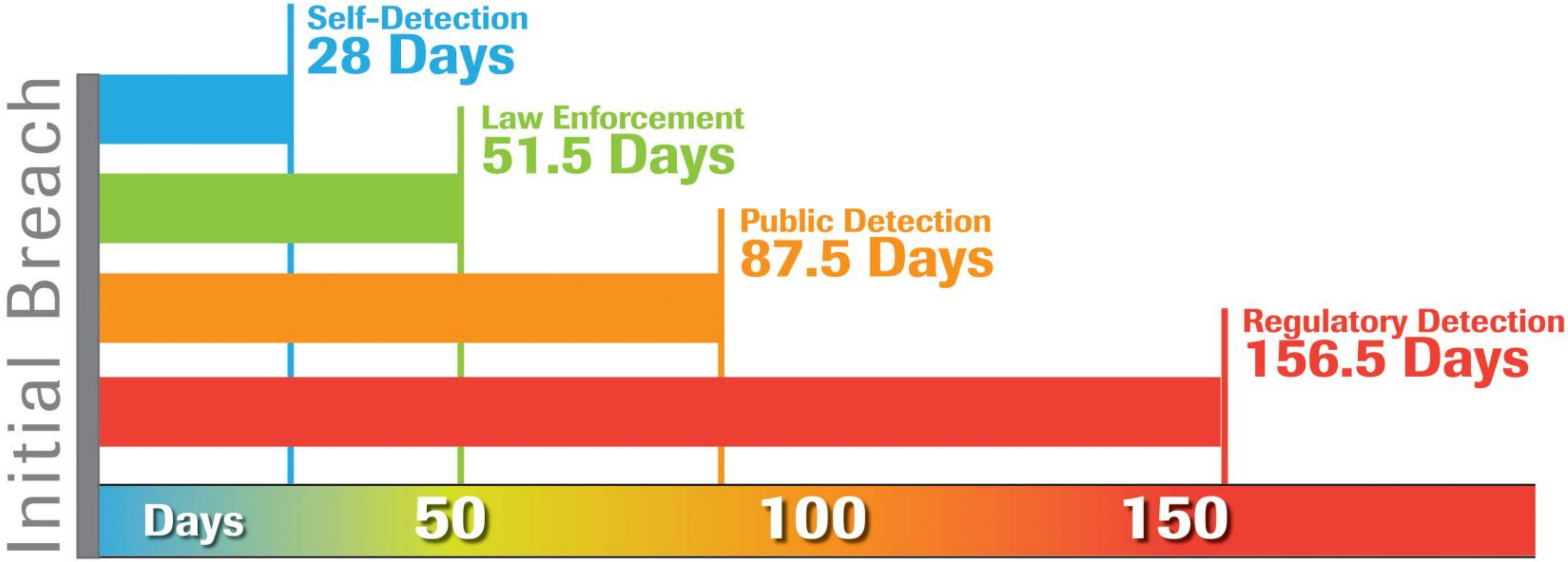
Target Assets

- E-Commerce still a significant target in APAC
- EMV countries, like those in APAC, still a target
  - Focus on card present environments
  - As mag-reader POS still in use



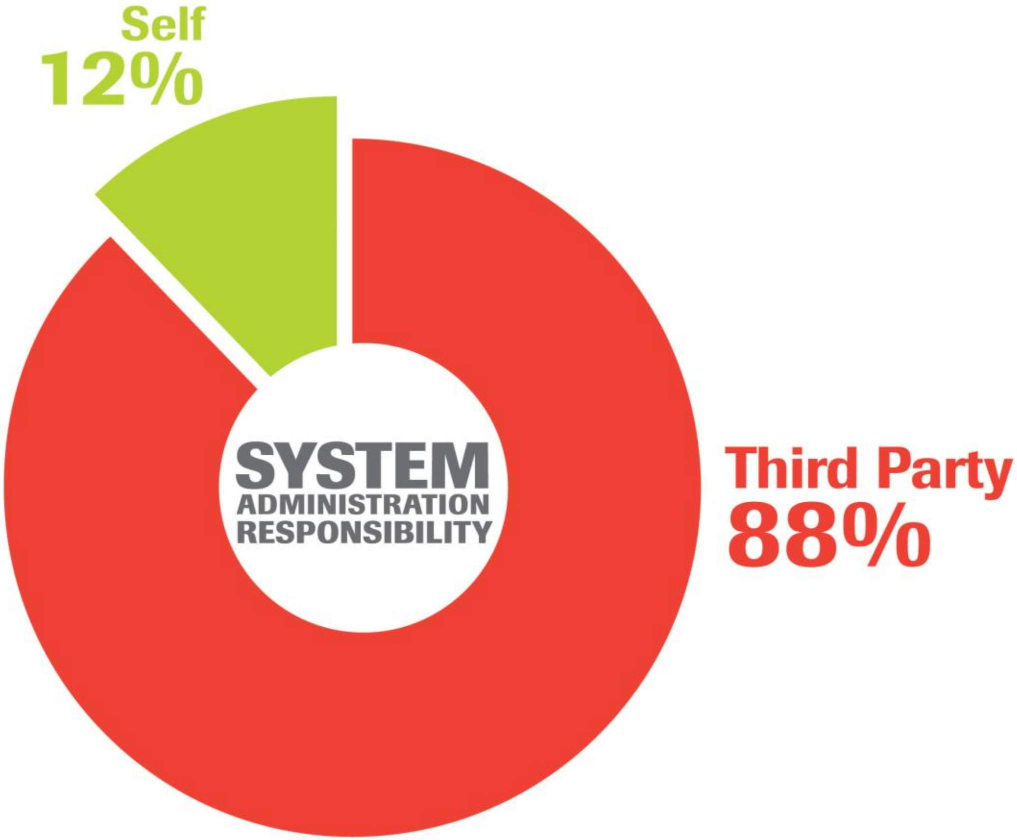
Detection Methods vs. Time

- 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



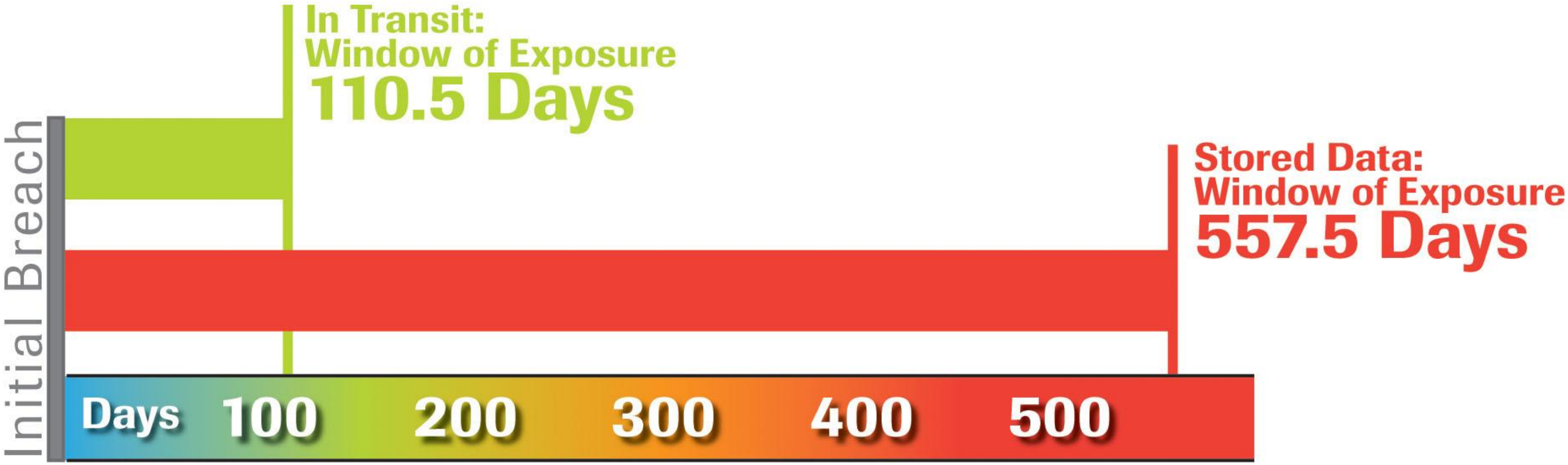
Administrator Responsibility

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

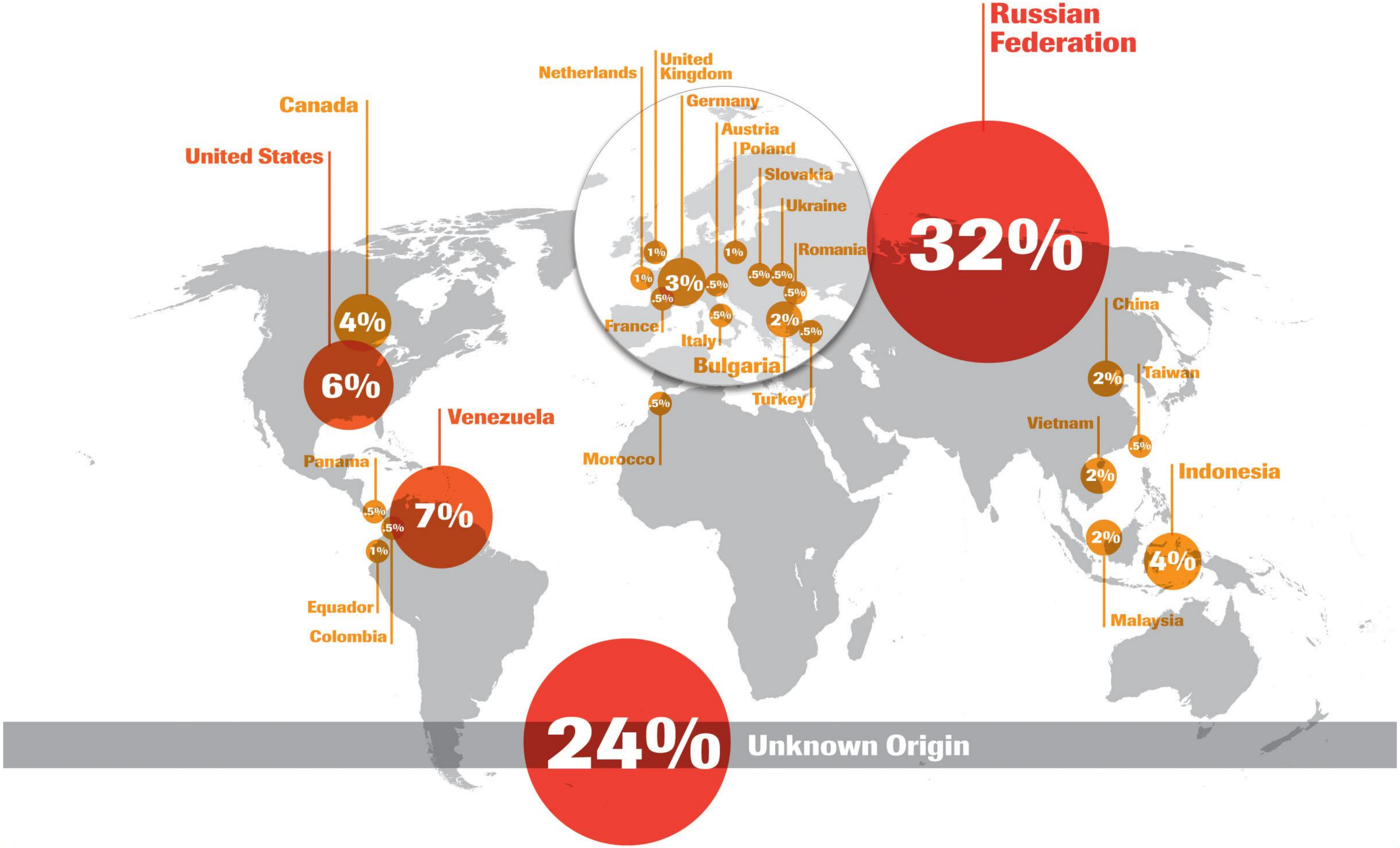


Window of Data Exposure

- Reality reflects intuition
- Storing data increases impact of breach
- Average "compromised" transactions
- In-transit data – 3 months
- Stored data – 18 months



Origin of Attack



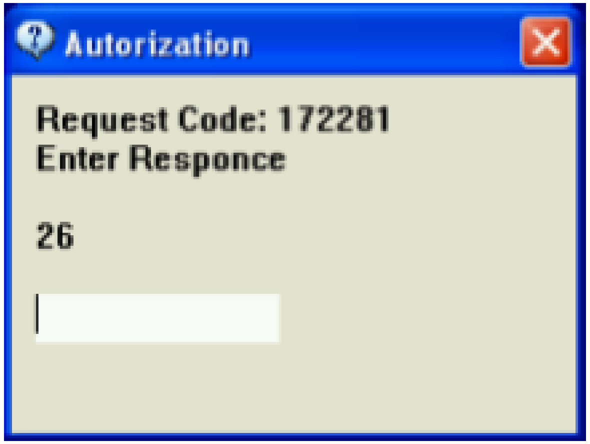
ATM Attacks

- Have seen an increase in ATM-focused attacks
- The occur across the world (including cases in the USA, Latin America, Asia Pacific and Europe)
- Attacks to date take two forms:
  - Malware-based attacks - apparently using the USB interface of the ATM
  - Network-based attacks – often leveraging poorly secured remote access interfaces, like VNC

Image from
http://www.diebold.com/solutions/atms/opteva/html/model_520c.htm

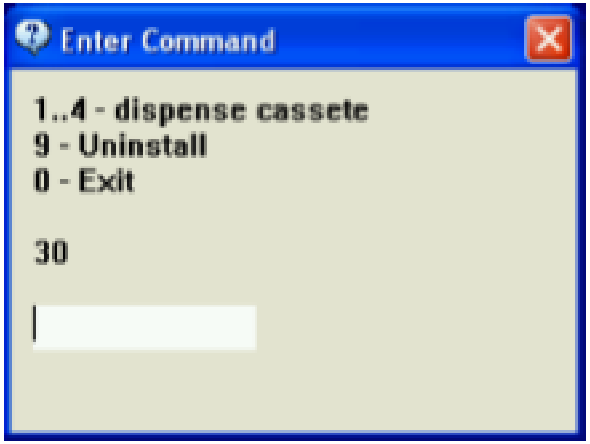
ATM Malware Example

- Ranges from rudimentary memory sniffing to sophisticated role-based plugins
- Attacker has specific key cards to trigger functionality.
- Includes two-factor authentication.
- Includes the ability to print “dumps” (with PIN) to the receipt printer.
- Key cards exist for mules to dispense funds. Different cards dispense different amounts so leaders know who is cheating them.
- Can also dispense from different cassettes
- Malware is specific to brand of ATM – though evidence of different flavours of malware exist



Request Code: 172281
Enter Responce

26



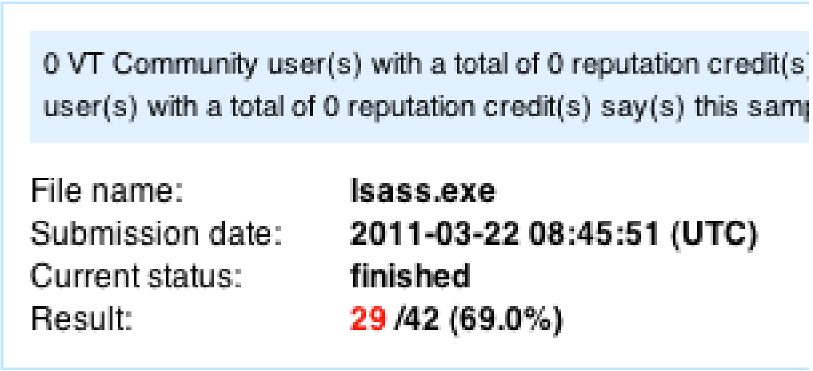
1..4 - dispense cassete
9 - Uninstall
0 - Exit

30

ATM Malware Intelligence

- Intelligence about the spread of malware possible using several online tools.
- E.G. We first analysed the malware on the previous slide in Q1 2009.
- Someone still had reason to analyse this sample in 2011.

VIRUS TOTAL



0 VT Community user(s) with a total of 0 reputation credit(s
user(s) with a total of 0 reputation credit(s) say(s) this samp

```
File name:          lsass.exe
Submission date:    2011-03-22 08:45:51 (UTC)
Current status:     finished
Result:             29 /42 (69.0%)
```

Network-Based ATM Attacks

- Most recent cases have resulted from network-based attacks
- Lack of segmentation between ATM and other networks
- Poorly secured network interfaces on ATMs (especially kiosk-based ATMs)
- ATMs often shipped with poor default security settings
  - Default local administrator password
  - Use of remote access technologies such as VNC with poor passwords
  - Missing patches
- Trend for ATMs to be internet connected, especially in developing economies
- Blind-trust in ATM vendors – “its an ATM – it must be secure”

Malware Isn’t Always Required…

- Many ATMs, especially legacy devices, store a large amount of sensitive data in log files
- For fraud on the card brands cards (e.g. Visa, MasterCard) a track 2 dump is often sufficient
- Example of exploitation:
  - SQL injection on public-facing website, leads to
  - Access to database server, leads to
  - Mapping of internal network, leads to
  - Access to WAN and branch-office networks, leads to
  - Discovery of VNC with blank password on ATM, leads to
  - Discovery of default administrator password on ATM, leads to
  - Discovery of log files containing track 2 data

ATM Developments

- Much more research ongoing since Barnaby Jack presentation at BlackHat 2010.
  - Discovered both network and physical security flaws
  - Developed custom firmware for ATMs to harvest data and dispense cassettes
  - http://www.youtube.com/watch?v=qwMuMSPW3bU
- Our assessment: ATMs are likely to become more heavily targeted
  - Motive is there – real money
  - Barriers to entry do not appear to be high
  - A lot of existing infrastructure in place that will be difficult to update
  - Most ATMs not making use of EMV so track 2 + PIN is usually sufficient for fraud

Point of Sale Attacks

- For the first time in 2011, we have seen wide-spread point of sale (POS) attacks in APAC.
- Several issues have led to this:
  - PIN Entry Devices (PED) sending data in clear-text
  - PED devices sending cardholder data to POS
  - POS software storing cardholder data
  - Poor security controls in POS environments (particularly relating to remote access)
- Attacks have revealed a false sense of security
  - Previously the belief was that the PED was a hardware device that was inherently secure

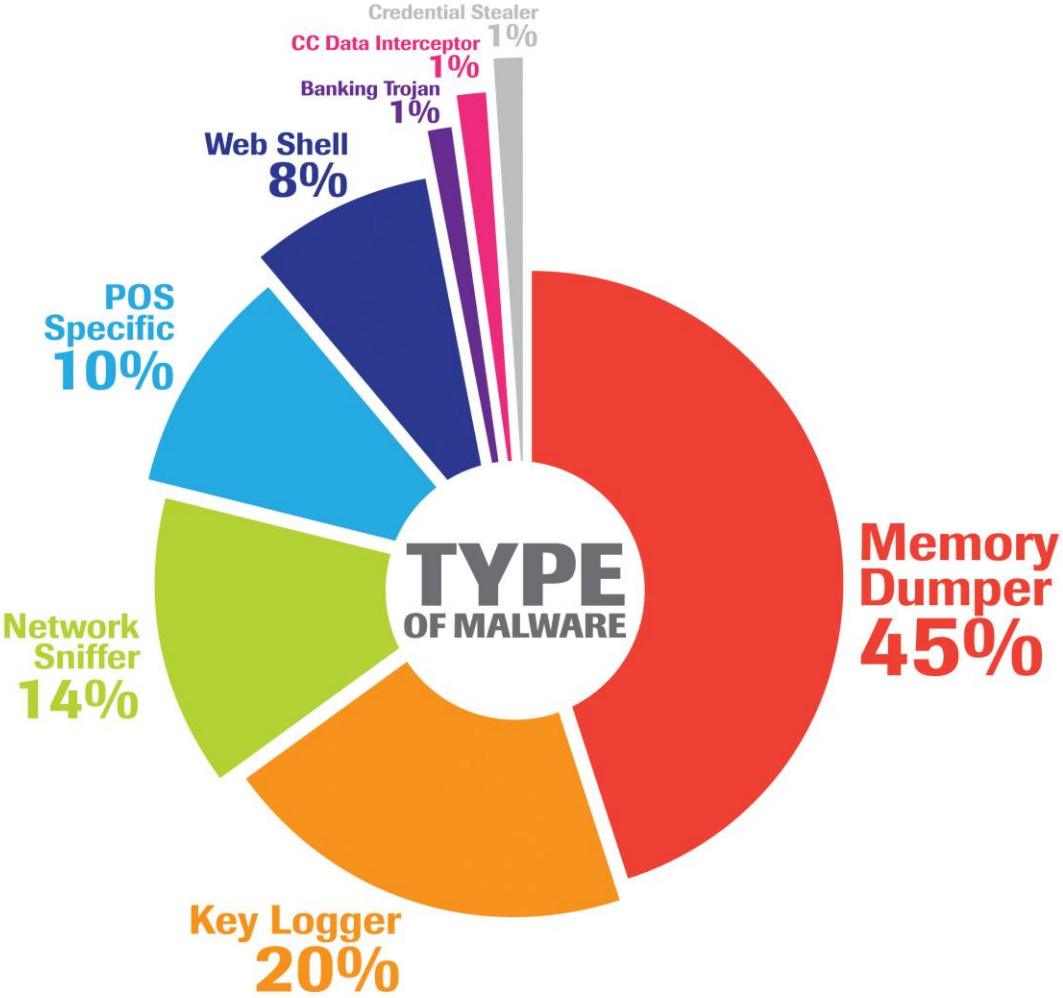
Image from http://www.ingenico.com/en/products/payment_terminals/countertop/i5100_fm4nst7z.html

POS Attacks

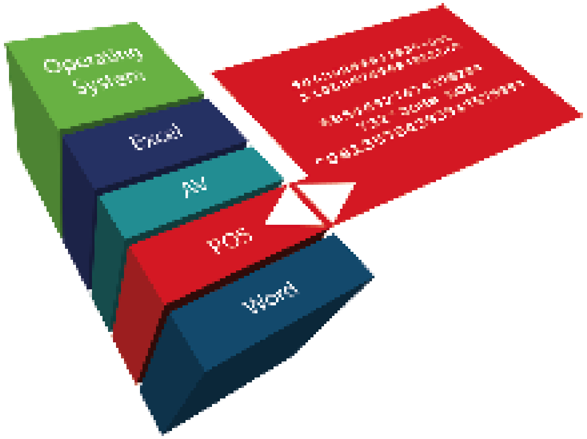
- Stored Data
  - Attackers locate remote access and login using default credentials
  - Locate log files containing historic cardholder data
  - Copy these files via FTP or some other network technology
- Volatile Data
  - Memory dumping malware

Classification

- New Malware Developments
  - POS-specific malware
  - Requires POS-specific knowledge
- POS Malware Highlight Case
  - Encryption algo/key identified
  - Decrypted and extracted the data



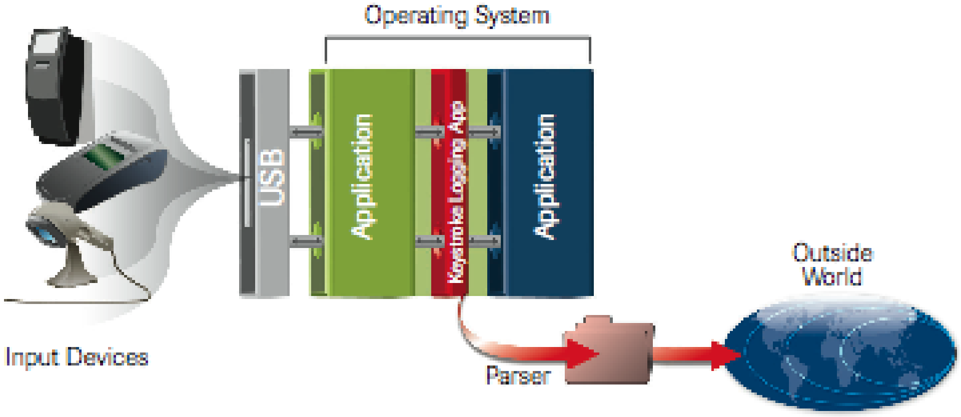
Memory Parsers



- Software application that monitors the RAM being used by a process
- Uses regular expressions or some other filtering technique to look for information
- Either stores this information on disk for an attacker to access later, or exfiltrates this data directly

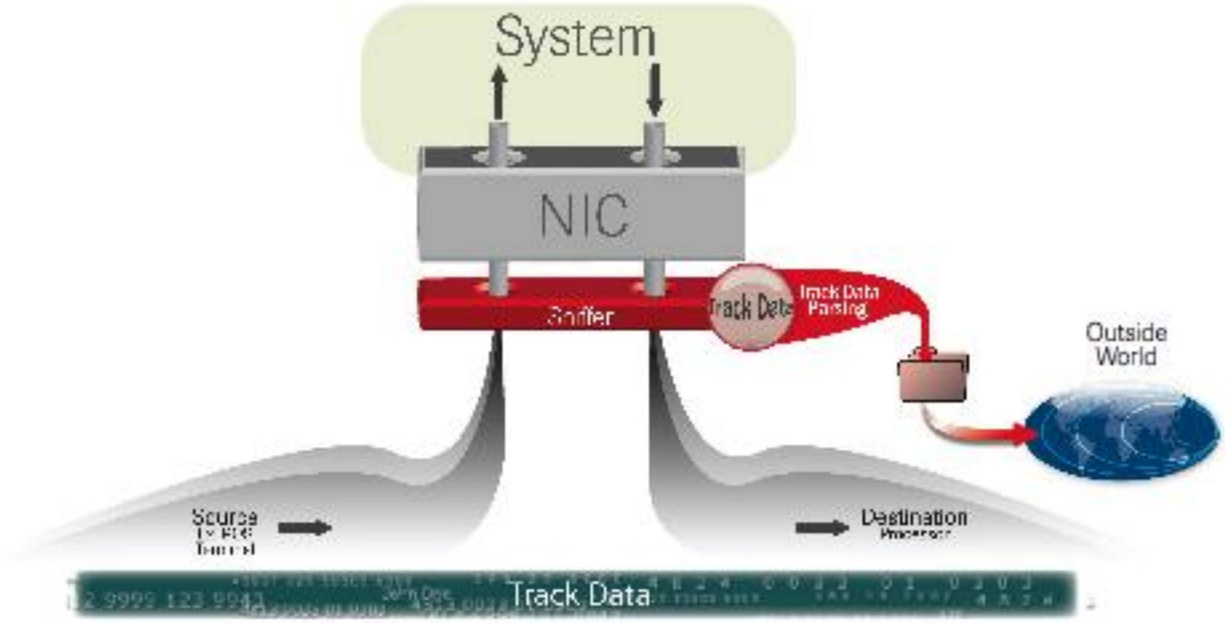
Keystroke Loggers

- Intercepts data as it is being entered into the computer
- For example - a keyboard, barcode scanner, USB card reader or touch screen
- Either stores this information on disk for an attacker to access later, or exfiltrates this data directly

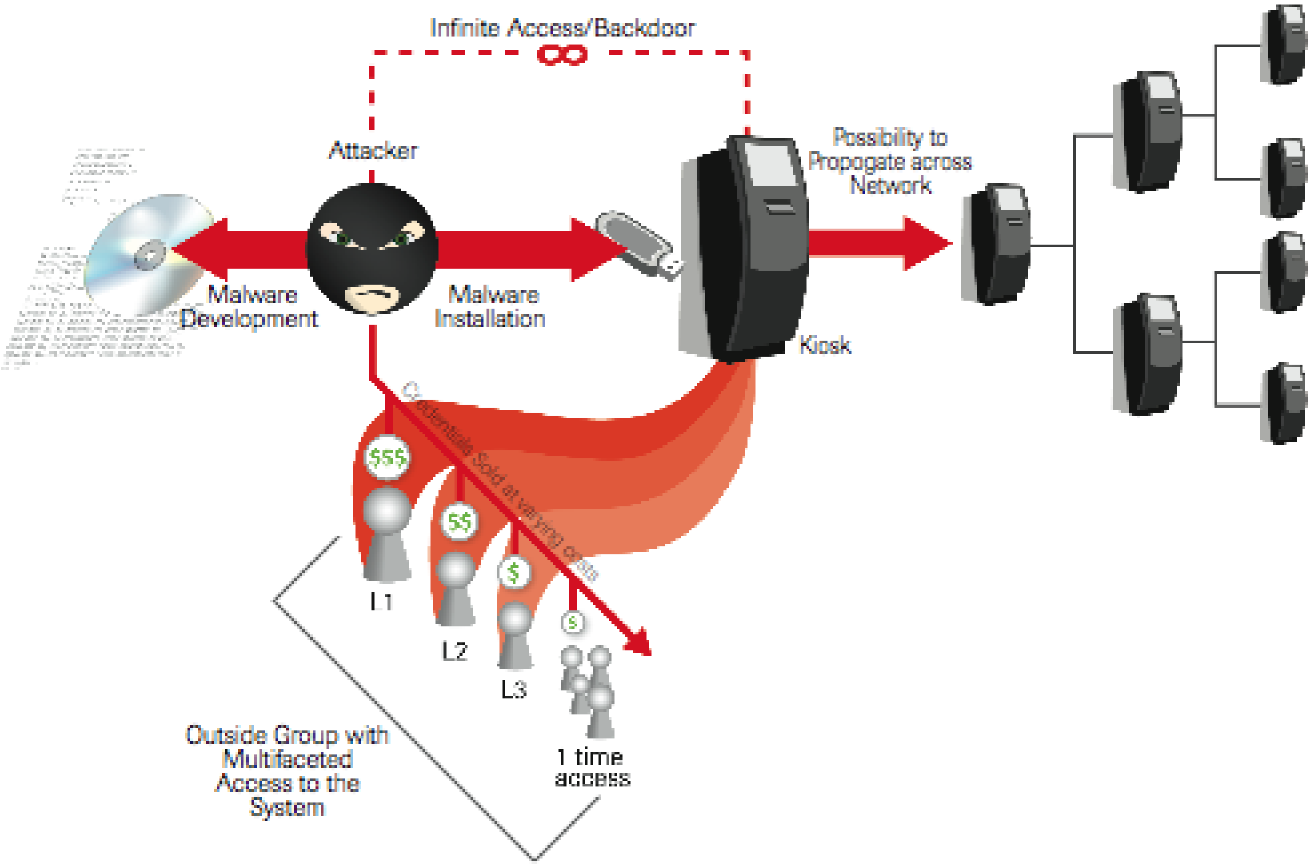


Network Sniffers

- Listens to traffic on the network and filters for interesting data
- Needs to have access to interesting network traffic:
  - E.g. be on a central system or a non switched network

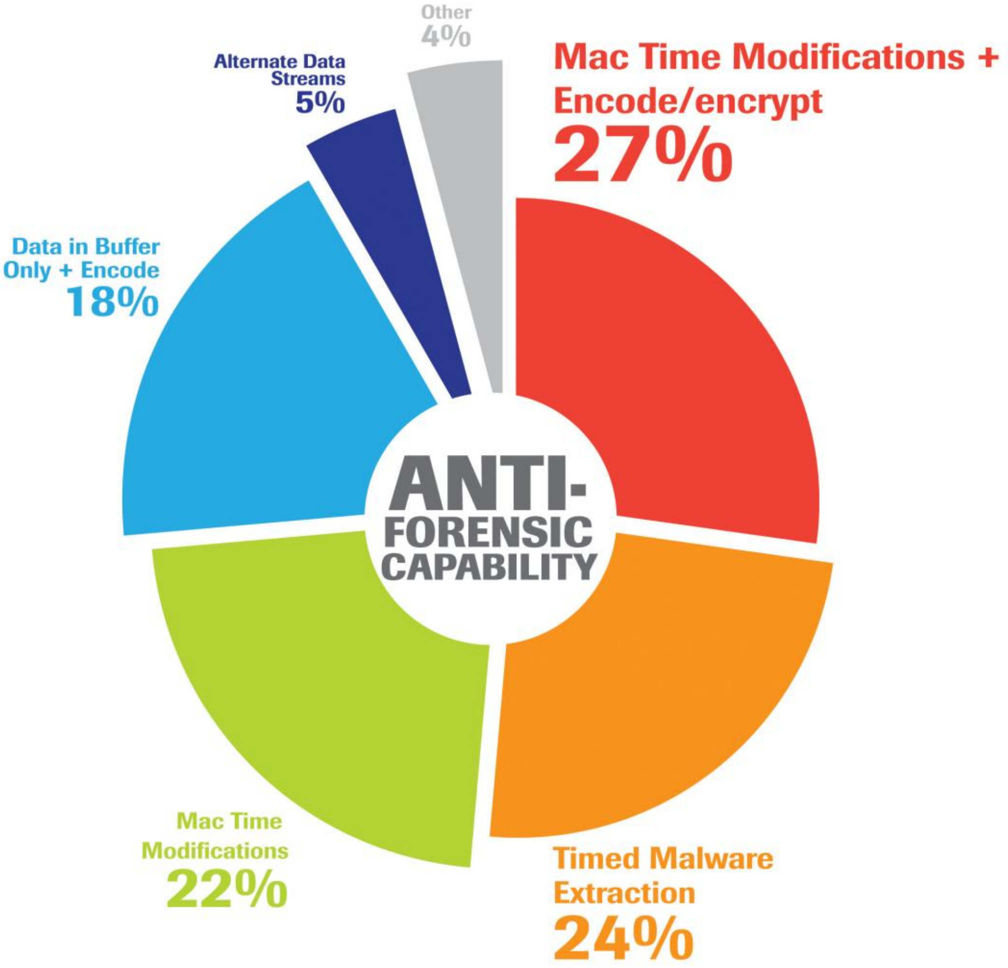


Credentialed Malware

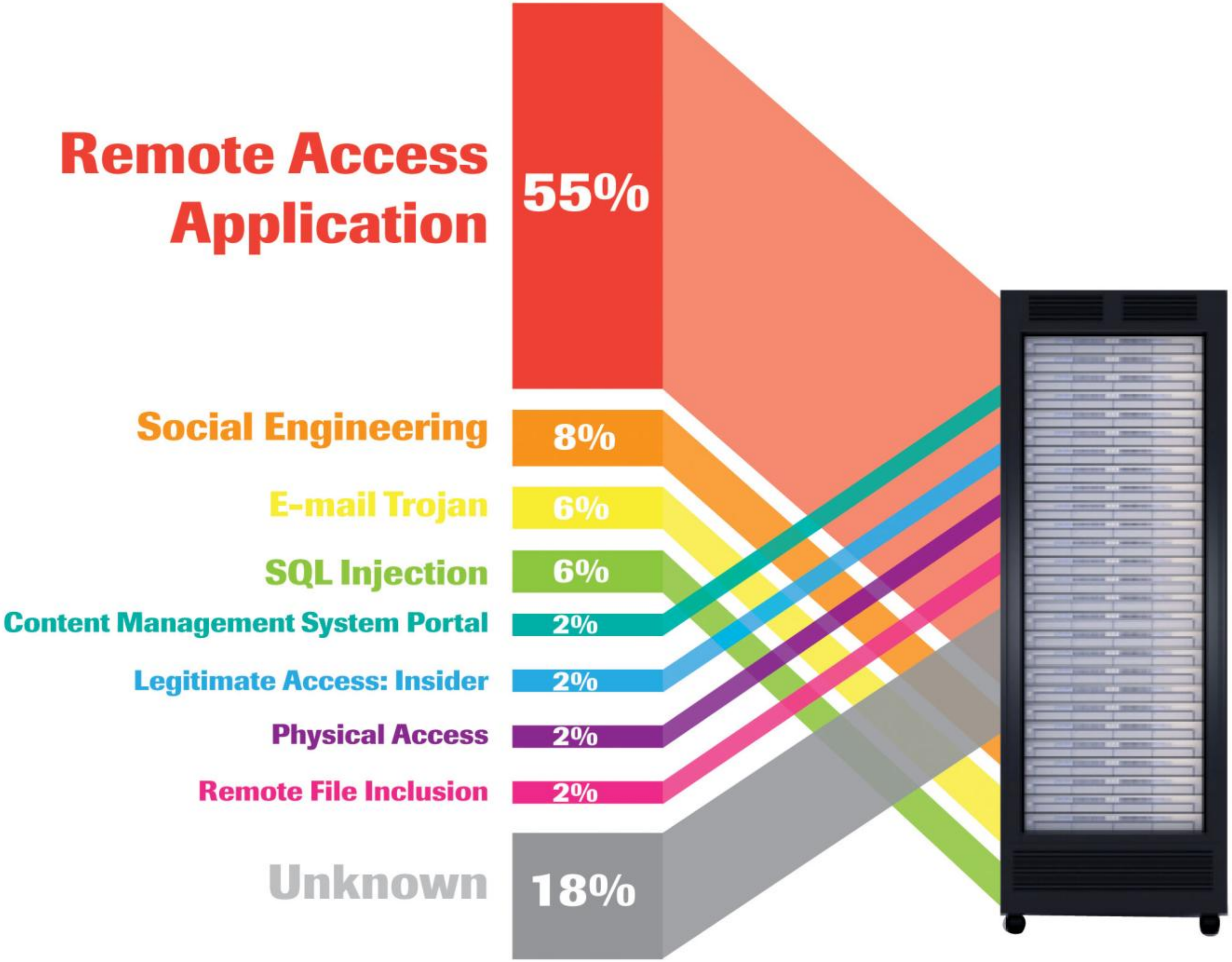

Infinite Access/Backdoor
∞
Attacker
Malware Development
Malware Installation
Kiosk
Possibility to Propogate across Network
Credentials Sold at varying costs
$$$
$$
$
$
L1
L2
L3
1 time access
Outside Group with Multifaceted Access to the System

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

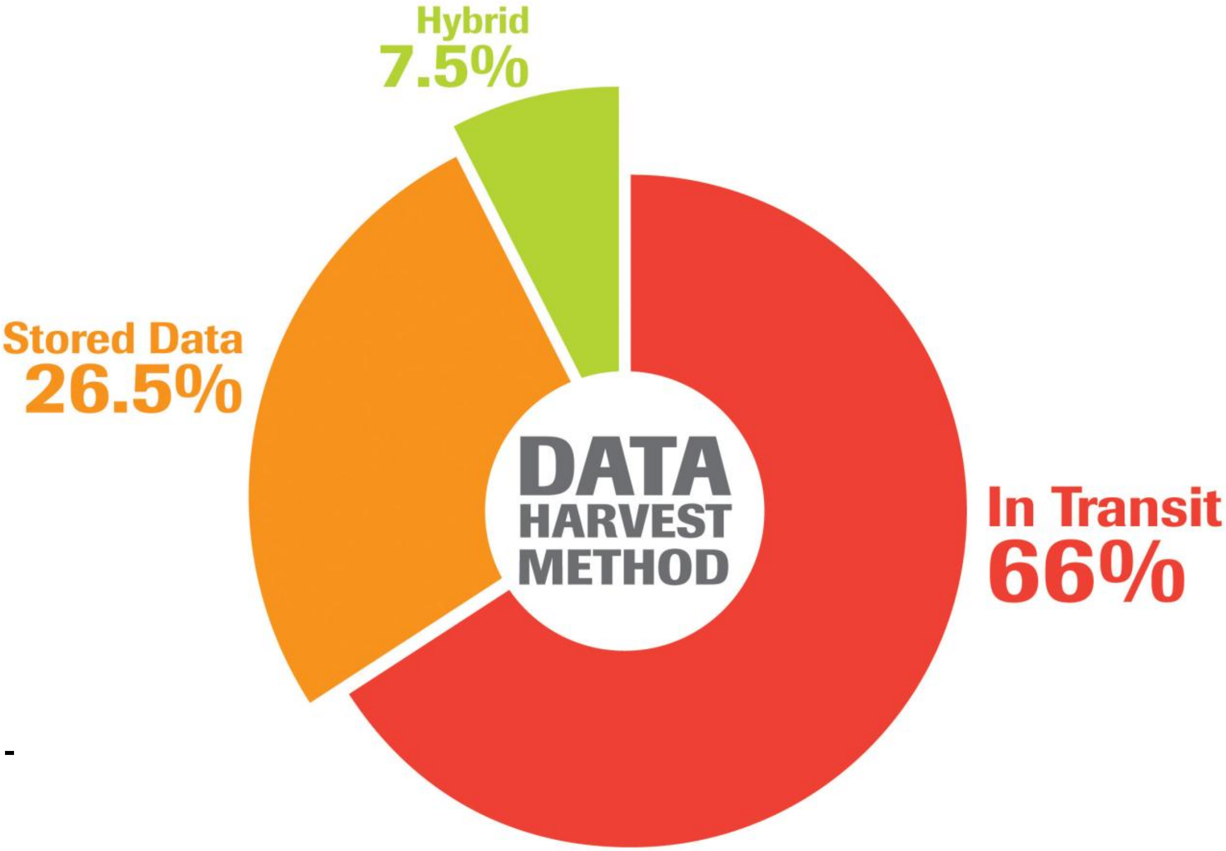


Breach Triad: Infiltration

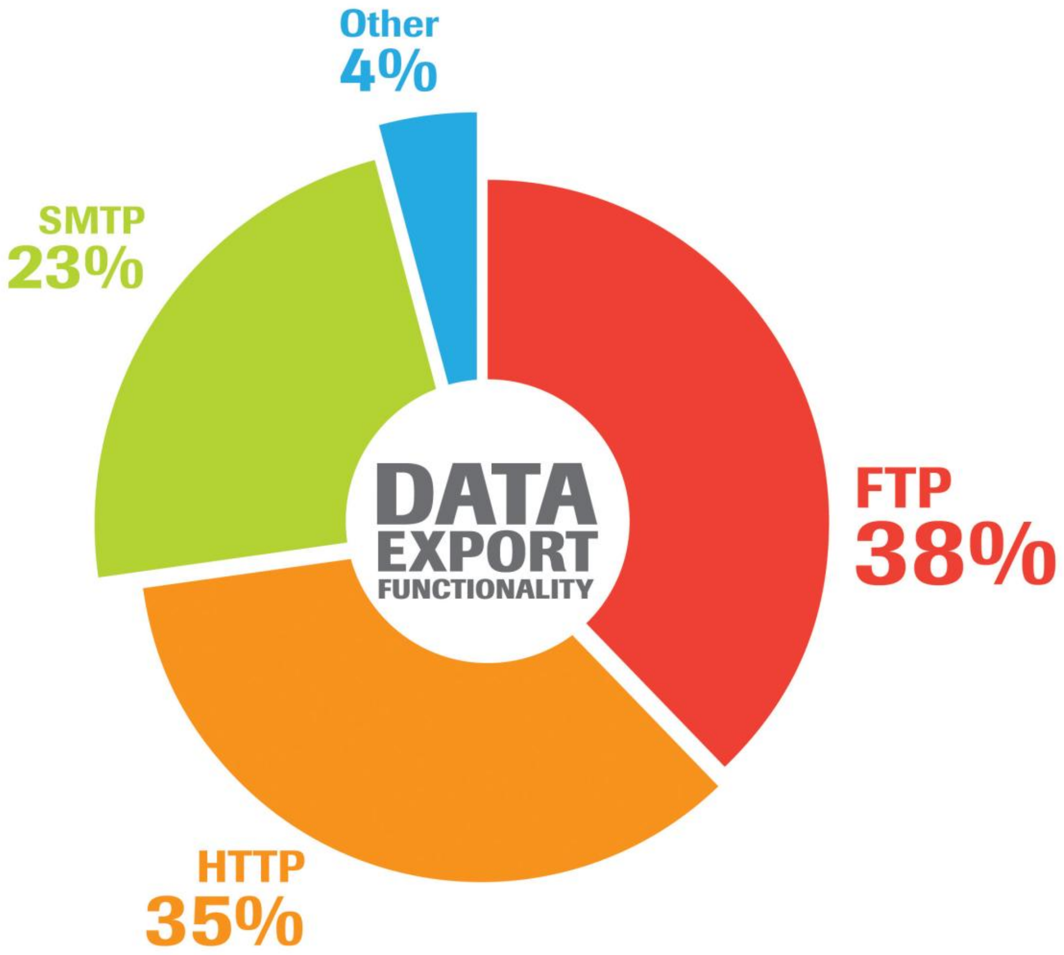


Breach Triad: Aggregation

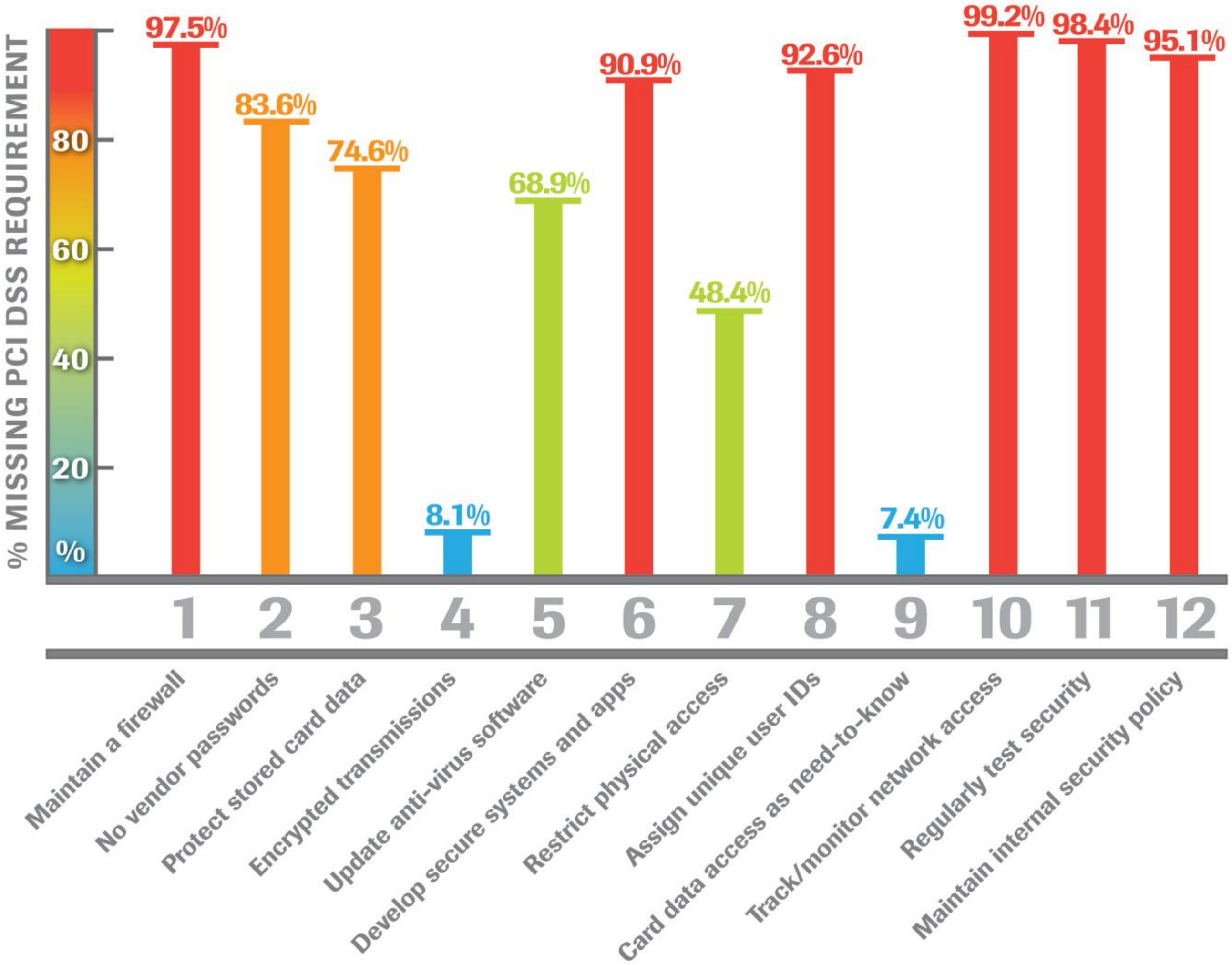
- Shift away from “smash & grab” of stored data
- **Why?**
  1. Less unsafe data being stored
     - PCI DSS, PA-DSS, OWASP
  2. Card data expires
     - More complex to harvest
     - The data is fresh
     - Worthwhile trade-off for criminals
- In-transit attacks and use of custom malware correlate



Breach Triad: Exfiltration



Payment Card Industry Compliance

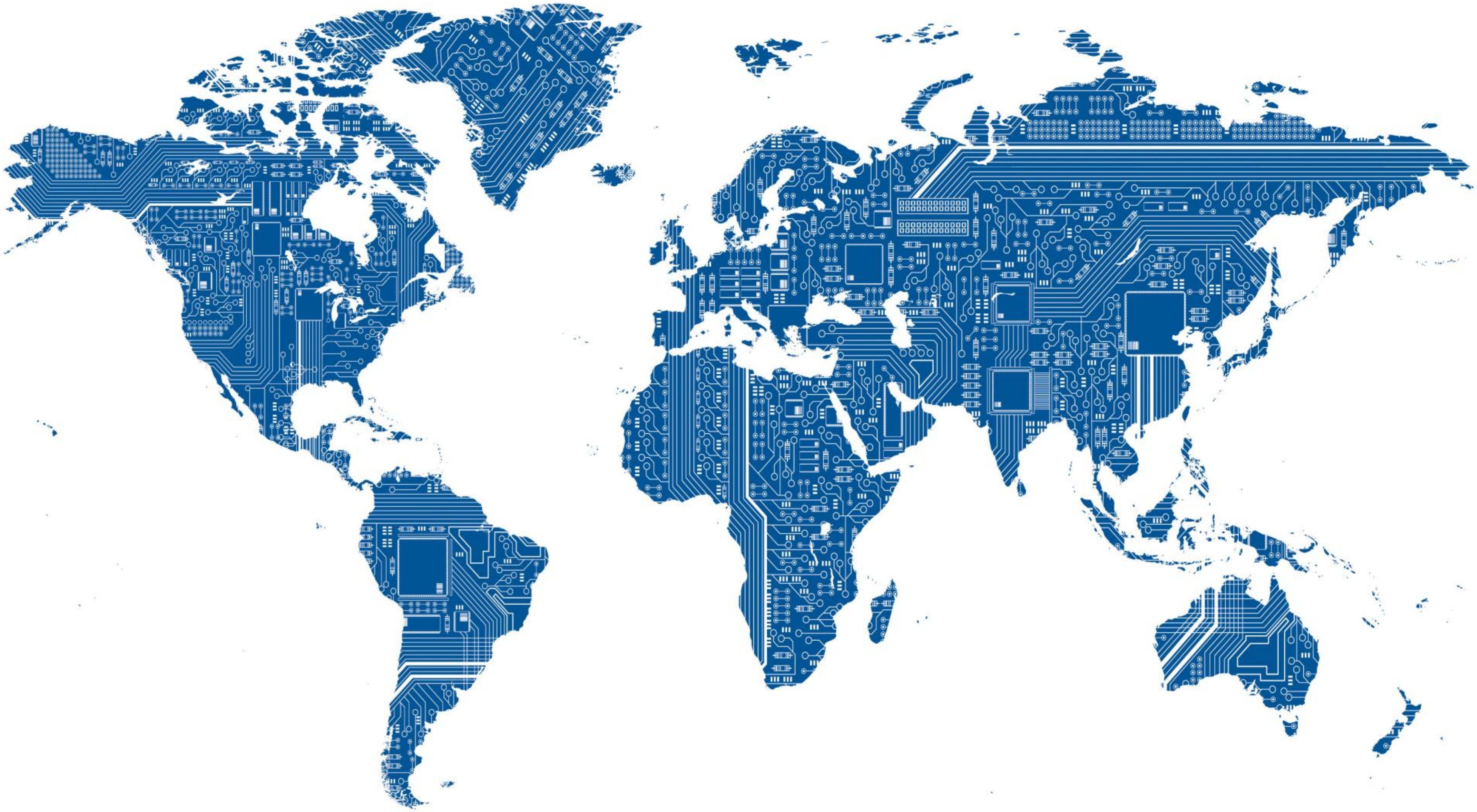


- 97% insufficient firewall policy
- 83% default/ guessable password
- 48% not using PA-DSS application

Key Countermeasures

1. Ensure that your key business partners know their security obligations
2. Focus on the basic security controls first, before focusing on the latest hype
3. Evaluate your need to store sensitive data and remove superfluous data
4. Test your security controls, and your incident response capacity regularly

Questions?



Contact Us

+86 21 6103 7235

GSR2011@trustwave.com

https://www.trustwave.com/spiderlabs

Twitter: @SpiderLabs / @Trustwave