TRENDS AND LESSONS LEARNED FROM CARDHOLDER DATA COMPROMISES
MAC is an organization of Bankcard professionals involved in the risk management side of Card Processing. We have members from Banks, ISOs, Card Associations and others related to the risk management side of the industry. MAC’s mission is to strengthen the payment ecosystem through ongoing education, communication and cooperation among acquirers, card brands and enforcement agencies.

To learn more about MAC or to become a member of MAC please visit the website below.

https://www.macmember.org/
SUMMARY

1. Types of cardholder data compromises
2. Impact of EMV and P2PE in Australia
3. Current trends in North America
4. Investigation challenges and roadblocks
5. Predications for 2017 and beyond
TRUSTWAVE SPIDERLABS

Threat Intelligence through applied research and ethical hacking

EXPERT TESTING
Offensive security testing delivered on time, on budget and on demand

INCIDENT READINESS & RESPONSE
Services designed to prevent compromise and protect integrity of business and data

FORENSICS INVESTIGATIONS
Post-incident analysis of actual security breaches and data loss

SpiderLabs Team
- Industry veterans and thought leaders in ethical hacking and security research
- Over 100 experts across 17 countries, with average 12 years of experience
- Backgrounds in law enforcement, government and military services
- Sought out industry speakers and published authors

SpiderLabs Research - Annual GSR Report
- 500+ Investigations in 15 countries
- Billions of events each day – 5 Global SOCs
- 4 million vulnerability scans
- Tens of millions of web transactions
- Millions of malicious websites blocked
- Thousands of penetration tests

150+ specialized security experts
500+ incident response investigations each year
9 million web application attacks researched
2,500+ penetration tests each year

©2017 Trustwave Holdings, Inc.
TYPES OF COMPROMISE
TARGETED ATTACK

SKB Enterprises serves a lot of customers, handles a lot of payment card transactions and probably has a lot of customer data stored somewhere. I'm going to figure out how to break in.

- Target identified first
- ONLY THEN is the attack considered
- More effort spent planning and executing
- Usually targeting larger organizations

OPPORTUNISTIC ATTACK

I know how to compromise a web server via an Adobe Cold Fusion vulnerability. I'm going to scan the Internet to find unpatched servers and see whether I can access some valuable data inject malicious code to infect visitors with malware

- Exploit and vulnerability identified first
- Target doesn't matter, just needs to be vulnerable to exploit
- Low-hanging fruit
- Smaller organizations usually fall victim
EXAMPLE ATTACK – POINT OF SALE

Card details processed via terminals, passed to back office system and then onto acquiring bank.

Third-party support providers use remote access to help.
EXAMPLE ATTACK – POINT OF SALE

Bad guys use the same remote access technology to access merchant systems

Place malware into environment that capture Transactions at the time that they are made
EXAMPLE ATTACK – ECOMMERCE, STORED DATA

1. Legitimate user enters card data
2. Card data sent to Acquiring bank
3. Card data also saved into database
EXAMPLE ATTACK – ECOMMERCE STORED DATA

Bad guy finds flaw in E-commerce application

Finds and extracts card data From the database
EXAMPLE ATTACK – ECOMMERCE, IN TRANSIT

1. Legitimate user enters card data
2. Card data sent to Acquiring bank
EXAMPLE ATTACK – ECOMMERCE, IN TRANSIT

Bad guy finds flaw in E-commerce application

1

Then modifies application to e-mail a copy of all transaction details to himself

2
ENVIROMENTS COMPROMISED BY REGION 2016

Source: 2017 Trustwave Global Security Report
EMV & P2PE AU CASE STUDY
CASE HISTORY – ASIA PACIFIC

Types of compromise per year – 2011 through 2016

- POS
- E-Commerce (In Transit)
- E-Commerce (Stored Data)
- Service Provider
CASE HISTORY – NORTH AMERICA

Types of compromise per year – 2013 through 2016

POS     E-Commerce
WHAT’S HAPPENING IN NORTH AMERICA?
MAJOR INCIDENTS USA/CANADA 2017 - INDUSTRY

- Service Provider: 20%
- Retail: 20%
- Hotel: 17%
- Finance: 14%
- Professional Services: 3%
- Legal: 10%
- Restaurant: 13%
- Entertainment: 3%
METHODS OF COMPROMISE (GLOBAL PERSPECTIVE)

Factors Contributing to Compromise

- Remote Access: 30%
- Phishing/Social Engineering: 19%
- Code Injection: 16%
- SQL Injection: 6%
- File Upload: 6%
- Misconfiguration: 6%
- Weak password: 5%
- Malware: 3%
- Malicious Insider: 3%
- Other: 6%

©2017 Trustwave Holdings, Inc.
INTRUSION TO CONTAINMENT (GLOBAL PERSPECTIVE)

Median Time between Compromise Milestones

- Intrusion to Detection
  - 2016: 50 days
  - 2015: 80 days

- Detection to Containment
  - 2016: 1 day
  - 2015: 1 day

- Intrusion to Containment
  - 2016: 60 days
  - 2015: 60 days

Days: 0 10 20 30 40 50 60 70 80 90
EXTERNAL DETECTION VS INTERNAL DETECTION (GLOBAL PERSPECTIVE)

![Bar Chart: Median Time Between Intrusion and Detection]

- **Externally Detected**
  - 2016: Orange bar
  - 2015: Blue bar

- **Internally Detected**
  - 2016: Orange bar
  - 2015: Blue bar

Days range from 0 to 180.
INVESTIGATION
CHALLENGES
INVESTIGATION PROCESS

- Identification
- Analysis
- Preservation
- Reporting
- Remediation
EVIDENCE MODIFIED PRIOR TO INVESTIGATION

Routine
- Logs overwritten
- Updates

Containment
- Deleting malware
- Updating code
- Changing payment method

Concealment
- Internal investigation
- Deleting logs
- Removing malware/modified code

Yes 68%
No 32%
WHAT'S NEXT?
PREDICTIONS

Caveat – Crystal balls can be blurry!

Increase
• eCommerce in transit
• Service Provider

Decrease
• POS
QUESTIONS

www.trustwave.com

@trustwave

mwilkinson@trustwave.com
THANK YOU
MAC 2018 Annual Conference
March 13 - 15, 2018
SLS Hotel - Las Vegas, NV

Don’t miss the premier payments industry risk conference.
Register today at www.macmember.org