Data Breaches – Trends & Real Stories from the Trenches

Ashish Thapar
CISSP, CISA, CISM, GCFA, PCI QSA
Managing Principal - Investigative Response, APJ
Verizon RISK Team
Current Landscape

Laws / Regulations
- PDPA, EU-GDPR
- MAS TRM
- AU DSD ISM
- IT Act 2011
- Lack of Mandatory Disclosure Laws

Industry Compliances
- PCI DSS
- ISO/IEC
- SSAE-16
- J-SOX
- HIPAA / HITECH
- IT/BPO Contracts

Geo-Political Environment
- Fast-Growing Economies
- Conflicts / Terrorism
- Diversity
- Black Money Eradication

Technology Enablement
- Dark-Web
- Bitcoins
- IoT
- SMAC
- Plastic Money/Wallets
Some of the Incidents that made recent news in the APJ region

<table>
<thead>
<tr>
<th>Month, Year</th>
<th>Attacked Entity</th>
<th>Type of Data Breached/ Impact as Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul, 2016</td>
<td>First Commercial Bank, Taiwan</td>
<td>2.17 Mn USD Cash out using an ATM Malware</td>
</tr>
<tr>
<td>Jun, 2016</td>
<td>JTB (Travel Bureau), Japan</td>
<td>8Mn PII Records of Travelers</td>
</tr>
<tr>
<td>May, 2016</td>
<td>7-Eleven, Japan</td>
<td>13Mn USD cashed out of ATMs</td>
</tr>
<tr>
<td>Apr, 2016</td>
<td>Gumtree, Australia</td>
<td>Unconfirmed number of PII records</td>
</tr>
<tr>
<td>Mar, 2016</td>
<td>Commission on Elections, Philippines</td>
<td>Biometric and PII Data (55 Mn Voters)</td>
</tr>
<tr>
<td>Feb, 2016</td>
<td>Bangladesh Bank, Bangladesh</td>
<td>81 Mn USD Siphoned off</td>
</tr>
<tr>
<td>Feb, 2016</td>
<td>Parliament, Western Australia</td>
<td>Outage of critical IT systems</td>
</tr>
<tr>
<td>Dec, 2015</td>
<td>Vtech Toy Company, Hong Kong</td>
<td>6.4 Mn PII Records of Children</td>
</tr>
<tr>
<td>Dec, 2015</td>
<td>Weather Bureau, Australia</td>
<td>Unconfirmed intrusion/recon incident</td>
</tr>
<tr>
<td>Sep, 2015</td>
<td>Govt. websites, Thailand</td>
<td>DDoS Attack, Websites unavailable for 1 day</td>
</tr>
</tbody>
</table>

Source: Data gathered from public sources on Internet
Cyber-Risk Mitigation Options

- **Prevention Controls**
  - Firewall
  - Security Hardening
  - Web App Firewall
  - Anti-Malware
  - Auth/Access Controls

- **Detection Controls**
  - IDS
  - SIEM
  - Endpoint Detection/Analytics
  - Full Packet Capture / Network Analytics

- **Response Controls**
  - Incident Response
  - Cyber Forensics
  - Information Sharing / Intel Sharing
  - Crisis Management

- **Other options**
  - First Party/ Third Party Cyber Insurance
  - Comprehensive Cyber Insurance
  - Outsourcing / Penalties in contracts
Data Breaches: Trends and learnings

Be Prepared: Forewarned is Forearmed
DBIR 2016 – Ninth Edition

“It’s like déjà vu, all over again.”
- Yogi Berra

- Ninth edition of DBIR
- 11+ years of cumulative research
- View into adversary’s playbook
- Attacker’s Vs Defender’s economics
- Three-pronged attacks highly familiar, repeatable, used frequently
Key Statistics

- 100K incidents
- 2,260 analysed breaches
- 82 countries
- 67 contributors

Source: Verizon 2016 Data Breach Investigations Report
Contributors

- Law Enforcement Organisations
- Cyber-Insurance Companies
- Research Groups
- Security Services/Solutions/Product Vendors & Training Providers
VERIS Framework – The Science behind DBIR

Vocabulary for Event Recording and Incident Sharing

http://veriscommunity.net
Incident DNA leads to Patterns

Analysis of 300+ data points/ enumerations in VERIS

Leads to clusters/patterns that have similarities
Nine Incident Classification Patterns

- Crimeware
- Cyber-espionage
- Denial of service
- Insider and privilege misuse
- Miscellaneous errors
- Payment card skimmers
- Physical theft and loss
- Point-of-sale Intrusions
- Web app attacks

The universe of threats may seem limitless but...

95% of 100,000+ security incidents fit into just nine incident classification patterns.

Source: Verizon 2016 Data Breach Investigations Report
Who are they?

Percent of breaches per threat actor category over time (n=8,158)

Source: Verizon 2016 Data Breach Investigations Report
What are they really after?

Percent of breaches per threat actor motive over time (n=6,762)

Source: Verizon 2016 Data Breach Investigations Report
What do they do?

Percent of breaches per threat actions category over time (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report
What are they targeting?

Percent of breaches per threat asset category over time (n=7,736)

Source: Verizon 2016 Data Breach Investigations Report
The Detection Deficit

% of breach timeframes measured in days or less

Source: Verizon 2016 Data Breach Investigations Report
Who found it first?

Breach discovery methods over time (n=6,133)

Source: Verizon 2016 Data Breach Investigations Report

---

18
How do they get in?

30% of phishing messages were opened.

13% of targets went on to click the attachment or link.

225 seconds
On average it takes less than 4 minutes for a phishing campaign to get its first click.

Source: Verizon 2016 Data Breach Investigations Report
They’ve got the right credentials

63% of confirmed data breaches involved leveraging a weak, default or stolen password.

Source: Verizon 2016 Data Breach Investigations Report
The same old vulnerabilities exist
It mostly starts with 3-pronged attacks

Phishing
Emails sent to user interaction via a “click” is the first goal. Once the interaction occurs, malware is dropped on the user device.

Malware
The initial malware provides the foothold on the device in the form of Command and Control or backdoor.

Credentials
In order to move laterally or deeper into a network credentials are captured via keyloggers and reused to access additional systems.

Many incidents share the same threat actions in the early stages of the attack; and what happens next is determined by the attacker’s end game!
### Security Incidents by Industry & Pattern

<table>
<thead>
<tr>
<th>Industry</th>
<th>Incident patterns by industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accomodation</td>
<td>n=362</td>
</tr>
<tr>
<td>Administrative</td>
<td>n=44</td>
</tr>
<tr>
<td>Educational</td>
<td>n=254</td>
</tr>
<tr>
<td>Entertainment</td>
<td>n=2,707</td>
</tr>
<tr>
<td>Finance</td>
<td>n=1,368</td>
</tr>
<tr>
<td>Healthcare</td>
<td>n=166</td>
</tr>
<tr>
<td>Information</td>
<td>n=1,028</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>n=171</td>
</tr>
<tr>
<td>Professional</td>
<td>n=916</td>
</tr>
<tr>
<td>Public</td>
<td>n=47,237</td>
</tr>
<tr>
<td>Retail</td>
<td>n=370</td>
</tr>
<tr>
<td>Transportation</td>
<td>n=31</td>
</tr>
<tr>
<td>Utilities</td>
<td>n=24</td>
</tr>
</tbody>
</table>

- DoS is prevalent across all industries
- Industries with reporting requirements have higher % of Lost/Stolen assets, Misuse, and Error incidents
- Filters have been applied to incident numbers in line with complexity and completeness checks

<table>
<thead>
<tr>
<th>Threats</th>
<th>Cyber- Espionage</th>
<th>Denial of Service</th>
<th>Everything Else</th>
<th>Lost and Stolen Assets</th>
<th>Miscellaneous Errors</th>
<th>Payment Card Skimmers</th>
<th>Point of Sale</th>
<th>Privilege Misuse</th>
<th>Web Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>20%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>74%</td>
<td>2%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>2%</td>
<td>2%</td>
<td>81%</td>
<td>2%</td>
<td>3%</td>
<td>4%</td>
<td>1%</td>
<td>1%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>2%</td>
<td>&lt;1%</td>
<td>34%</td>
<td>5%</td>
<td>&lt;1%</td>
<td>1%</td>
<td>6%</td>
<td>&lt;1%</td>
<td>3%</td>
<td>48%</td>
</tr>
<tr>
<td>4%</td>
<td>2%</td>
<td>11%</td>
<td>32%</td>
<td>18%</td>
<td>5%</td>
<td>23%</td>
<td>4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4%</td>
<td>3%</td>
<td>46%</td>
<td>21%</td>
<td>&lt;1%</td>
<td>11%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>12%</td>
<td></td>
</tr>
<tr>
<td>5%</td>
<td>16%</td>
<td>33%</td>
<td>33%</td>
<td>1%</td>
<td>1%</td>
<td>6%</td>
<td>6%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1%</td>
<td>2%</td>
<td>90%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16%</td>
<td>&lt;1%</td>
<td>1%</td>
<td>17%</td>
<td>20%</td>
<td>24%</td>
<td>&lt;1%</td>
<td>22%</td>
<td>&lt;1%</td>
<td></td>
</tr>
<tr>
<td>1%</td>
<td>&lt;1%</td>
<td>45%</td>
<td>2%</td>
<td>1%</td>
<td>3%</td>
<td>32%</td>
<td>1%</td>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td>16%</td>
<td>26%</td>
<td>8%</td>
<td>4%</td>
<td>6%</td>
<td>6%</td>
<td>35%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19%</td>
<td>38%</td>
<td>12%</td>
<td>8%</td>
<td>4%</td>
<td>12%</td>
<td>8%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Confirmed Breaches by Industry & Pattern

<table>
<thead>
<tr>
<th>Industry</th>
<th>Point of Sale</th>
<th>Web Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Educational</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Retail</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Professional</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Public</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Financial</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Cyber-Espionage</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Insider Misuse</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Cyber-Espionage</td>
<td>1%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Point of Sale is a major problem for Accommodation and Retail
Insider Misuse is strongly associated with Healthcare
Cyber-Espionage is common in Manufacturing, Professional Services, and the Public sector
Web Applications went up this year notably against Financial victims
89% of breaches had a financial or espionage motive

63% of confirmed data breaches involved weak, default, or stolen passwords

Over 900 confirmed data breaches involved phishing attacks

30% of phishing messages were opened in 2015, and 13% of targets clicked on the malicious attachment or link.

DDoS attacks were found to be either large in magnitude or long in duration, but typically not both (and sometimes neither)

There are evident interrelations between patterns

- Crimeware on an organization’s B2B or B2C customers, can lead to use of stolen credentials against that organization’s assets

- Many breaches are beginning with phishing, leading to malware, leading to attacks against credentials
Data Breaches:  
Real Stories from the Trenches

*Think what you don’t know can’t hurt you?  
Think again.*
You may not always be dealing with sophisticated attacks that have never been seen before.

At any given time, most incidents fit into one of just 15 to 20 data breach scenarios.

These patterns can be even further reduced by looking at specific industries.

Understanding how these common attacks can affect your organization is key to defending against them.
## Scenarios Overview

### The Human Element
- S1. Social Engineering – The Hyper Click
- S2. Financial Pretexting – The Slick Willie
- S3. Digital Extortion – The Boss Hogg
- S4. Insider Threat – The Rotten Apple
- S5. Partner Misuse – The Busted Chain

### Conduit Devices
- S6. USB Infection – The Porta Bella
- S7. Peripheral Tampering – The Bad Tuna
- S8. Hacktivist Attack – The Dark Shadow
- S9. Rogue Connection – The Imperfect Stranger
- S10. Logic Switch – The Soup Sammich

### Configuration Exploitation
- S11. SQL Injection – The Snake Bite
- S12. CMS Compromise – The Roman Holiday
- S14. DNS Tunneling – The Rabbit Hole

### Malicious Software
- S15. Data Ransomware – The Catch 22
- S16. Sophisticated Malware – The Flea Flicker
- S17. RAM Scraping – The Leaky Boot
- S18. Credential Theft – The Poached Egg

---

- **Four Groupings**
  - **Eighteen (18) Scenarios**
    - **Most Prevalent (12)**
    - **Most Lethal (6)**
  - **Attack-Defend Card for every scenario**
  - **Whimsical title given to each scenario**

Source: Verizon 2016 Data Breach Digest
## Understand the threats to your industry

### Incident patterns → POS Intrusions: Web app attacks: Cyber-espionage: Crimeware: Privilege misuse: Payment card skimmers

<table>
<thead>
<tr>
<th>Industry (NAICS #)</th>
<th>POS Intrusions</th>
<th>Web app attacks</th>
<th>Cyber-espionage</th>
<th>Crimeware</th>
<th>Privilege misuse</th>
<th>Payment card skimmers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72)</td>
<td>53%</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative (56)</td>
<td>4%</td>
<td>1%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educational (61)</td>
<td>9%</td>
<td>12%</td>
<td>22%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment (71)</td>
<td>58%</td>
<td>11%</td>
<td>11%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial services (52)</td>
<td>17%</td>
<td>1%</td>
<td>21%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare (62)</td>
<td>7%</td>
<td>8%</td>
<td>3%</td>
<td>3%</td>
<td></td>
<td>20%</td>
</tr>
<tr>
<td>Information (51)</td>
<td>26%</td>
<td>9%</td>
<td>46%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing (31-33)</td>
<td>3%</td>
<td>36%</td>
<td>19%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mining (21)</td>
<td></td>
<td></td>
<td>11%</td>
<td></td>
<td>67%</td>
<td>6%</td>
</tr>
<tr>
<td>Other services (81)</td>
<td>1%</td>
<td>28%</td>
<td>3%</td>
<td>36%</td>
<td></td>
<td>6%</td>
</tr>
<tr>
<td>Professional (54)</td>
<td>2%</td>
<td>2%</td>
<td>26%</td>
<td>10%</td>
<td></td>
<td>1%</td>
</tr>
<tr>
<td>Public (92)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18%</td>
<td>26%</td>
</tr>
<tr>
<td>Retail (44-45)</td>
<td>20%</td>
<td>2%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation (48-49)</td>
<td></td>
<td></td>
<td>41%</td>
<td>9%</td>
<td></td>
<td>18%</td>
</tr>
<tr>
<td>Utilities (22)</td>
<td>17%</td>
<td></td>
<td></td>
<td></td>
<td>50%</td>
<td>17%</td>
</tr>
</tbody>
</table>

### Most-relevant scenarios — read these ones first!

7, 10, 11, 12, 13, 14, 16, 17, 18
8, 10, 11, 12, 14, 15, 16, 18
1, 6, 13, 14, 16, 18
2, 9, 13, 14, 15, 16, 18
3, 4, 5, 6, 13, 14, 16, 18
5, 7

Source: Verizon 2016 Data Breach Digest
Scenario #13: The Alley Cat

- Suspicious connections between R&D department and internet. 2 GB data sent out
- Phishing email to engineering team
- RAT backdoor installed
- Credentials misused to get access to file shares
- Competitor brought finished product to market faster

Source: Verizon 2016 Data Breach Digest
Scenario #14: The Rabbit Hole

- Multiple drive-by infections, non targeted phishing attempts. No clear tell tale signs
- DNS server had strange – random name resolution entries
- Backup servers were sending such public DNS queries via direct outbound access
- Each request contained a domain rendered in Hex characters of equal length (actually archived ZIP data sent into parts)
- All requests ended up being routed to a single remote name server

Source: Verizon 2016 Data Breach Digest
**Scenario #17: The Leaky Boot**

- Multiple fraudulent transactions are found with cards previously used at a common location
- The original breach occurs two weeks prior through a targeted phishing email
- Custom-built RAM scraping malware is discovered
Call to action

- Be vigilant and informed
- Make people your first line of defense
- Only keep data on a “need to know” basis
- Patch promptly
- Encrypt sensitive data
- Use multi-factor authentication
- Don’t forget physical security

Questions/Comments:
ashish.thapar@intl.verizon.com

Stay Connected (Linkedin):
http://sg.linkedin.com/ashishthapar