2016 Data Breach Investigations Report

Understand what you’re up against.

Beltug X-change
March 29, 2017

Fabrice Wynants
Manager Security Solutions BeNeLux & France
fabrice.wynants@be.verizon.com
The DBIR
2016 Data Breach Investigations Report

Ninth edition.

100K incidents.

82 countries.

2,260 analyzed breaches.

Data from 67 contributors.

Use the lessons learned from analyzing more than 2,000 confirmed data breaches.

- Data Breach Investigation Reports
- Data Breach Digest Reports
- Industry Oriented Reports

http://www.verizonenterprise.com/verizon-insights-lab/dbir/
Some Breach Trends.
89% of breaches had a financial or espionage motive.

The actors in the breaches were predominantly external.
Threat Actions – Hacking, Malware & Social on the rise
Threat Actions – Don’t Forget the Human Errors

Top 10 threat action varieties within miscellaneous error private industry incidents, n=153, Public Sector Misdelivery=10094

- Capacity shortage: 61
- Misdelivery: 40
- Publishing error: 18
- Misconfiguration: 15
- Disposal error: 10
- Gaffe: 3
- Other: 2
- Programming error: 2
- Data entry error: 1
- Omission: 1

Human Error is involved in 37% of the Breaches
The Detection Deficit

Percent of breaches where time to compromise (green) and time to discovery (blue) as days or less

Detection GAP

+ Less than 10% of breaches are discovered by internal means
Birth of a Data Breach
Birth and rebirth of a data breach

Many incidents share the same threat actions in the early stages of the attack.

Three-pronged attacks highly familiar, repeatable, used frequently

Source: Verizon 2016 Data Breach Investigations Report
**View from our Sr. Data Analyst**

**Understanding the Opening Moves is Key.**

**Focus & block on the Intersections: Phishing, Malware & Credentials.**

What happens next is determined by the attacker’s end game.
Phishing

41% of breaches involved phishing

30% recipients opened phishing messages

13% clicked on attachments

3:45 median time to first click
Malware and Crimeware

68% of breaches involved malware

Mainly introduced through Email as executables
Credentials

63% of confirmed data breaches involved leveraging a weak, default or stolen password (credential theft or use).

Top threat action varieties within incidents

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Incident Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking - Use of stolen creds</td>
<td>1,095</td>
</tr>
<tr>
<td>Malware - Export data</td>
<td>1,031</td>
</tr>
<tr>
<td>Malware - C2</td>
<td>980</td>
</tr>
<tr>
<td>Social - Phishing</td>
<td>847</td>
</tr>
<tr>
<td>Malware - Spyware/keylogger</td>
<td>841</td>
</tr>
</tbody>
</table>
What can you do?
86% of security incidents fit into just nine incident classification patterns.

- Miscellaneous errors: 18%
- Privilege misuse: 16%
- Physical theft and loss: 15%
- Denial of service: 15%
- Crimeware: 12%
- Web app attacks: 8%
- POS intrusions: 1%
- Cyber-espionage: <1%
- Payment card skimmers: <1%
Over 90% of breaches fit into just nine incident classification patterns.

- Miscellaneous errors: 9%
- Privilege misuse: 8%
- Physical theft and loss: 2%
- Denial of service: <1%
- Crimeware: 2%
- Web app attacks: 40%
- POS intrusions: 23%
- Cyber-espionage: 7%
- Payment card skimmers: 4%
## Patterns by Industry

<table>
<thead>
<tr>
<th>Incident patterns by industry (only confirmed data breaches)</th>
<th>Accommodation (72)</th>
<th>Educational (61)</th>
<th>Entertainment (71)</th>
<th>Finance (52)</th>
<th>Healthcare (62)</th>
<th>Information (51)</th>
<th>Manufacturing (31-33)</th>
<th>Professional (54)</th>
<th>Public (92)</th>
<th>Retail (44-45)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crimeware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber-espionage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everything Else</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stolen Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc. Errors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Point of Sale</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privilege Misuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2016 Data Breach Investigations Report
Some Recommendations

✓ Tailor your mitigations.
✓ Make people your first line of defense.
✓ Only keep data on a “need to know” basis.
✓ Focus around Phishing, Malware and Credentials.
✓ Patch promptly.
✓ Use two-factor authentication where possible.
✓ Ensure proper Detection & Response

http://www.verizonenterprise.com/verizon-insights-lab/dbir/