2021
Data Breach Investigations Report
2021 Data Breach Investigations Report

- 14 years
- 88 countries
- 83 contributors
- 79,635 total incidents
- 29,207 quality incidents
- 5,258 data breaches

https://www.verizon.com/business/resources/reports/dbir/
COVID-19 impact

Phishing increased 11% and Ransomware increased 6%.

Use of stolen creds and Publishing error stayed consistent.

Error actions (Misconfiguration, Misdelivery) decreased (due to the rapid growth of Social breaches).

Figure 22. Change in covid-related Action varieties
VERIS A4 Threat Model

VERIS employs the A4 Threat Model.

Here, an incident is viewed as a series of events that adversely affect the information assets of an organization.

VERIS resources:
- veriscommunity.net
- github.com/vz-risk/veris

<table>
<thead>
<tr>
<th>Actors (3)</th>
<th>Actions (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whose actions affected the asset?</td>
<td>What actions affected the asset?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assets (5)</th>
<th>Attributes (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which assets were affected?</td>
<td>How were assets affected?</td>
</tr>
</tbody>
</table>
Autors and motives

Breaches continued to be mostly due to external, financially motivated actors.
Action varieties

Phishing and Pretexting were top Social action varieties.

Use of stolen creds and Brute force were top Hacking actions varieties.

Ransomware was top Malware action variety.

Misconfiguration and Misdelivery were top Error action varieties (17%).
**Assets in breaches**

Server topped the list for Assets in breaches (and incidents).

Web application was the top Hacking vector, with 89% of Hacking varieties involving some sort of credential abuse (Use of stolen creds or Brute force).
Attribute varieties

Confidentiality violations involve compromising data. Credentials and Personal remained highly sought after.

Integrity violations usually resulted from Social or Malware action:

- Alter behavior (Social) involved Phishing or Pretexting
- Software installation (Malware) usually occurred after Hacking (Use of stolen creds or Brute force)

Availability violations were topped by Obscuration (such as ransomware encryption).
2021 DBIR key takeaways

- 29,207 security incidents
- 5,258 confirmed breaches
- >80% of Hacking vectors involved web apps in breaches
- 85% of breaches involved the human element
- 17% of breaches involved Errors
- 10% of breaches involved ransomware
- 61% of breaches involved credential data
### CIS Controls® (four core controls)

<table>
<thead>
<tr>
<th>No.</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory and Control of Hardware Assets</td>
</tr>
<tr>
<td>2</td>
<td>Inventory and Control of Software Assets</td>
</tr>
<tr>
<td>3</td>
<td>Data Protection</td>
</tr>
<tr>
<td>4</td>
<td>Secure Configuration of Enterprise Assets and Software</td>
</tr>
<tr>
<td>5</td>
<td>Account Management</td>
</tr>
<tr>
<td>6</td>
<td>Access Control Management</td>
</tr>
<tr>
<td>7</td>
<td>Continuous Vulnerability Management</td>
</tr>
<tr>
<td>8</td>
<td>Audit Log Management</td>
</tr>
<tr>
<td>9</td>
<td>Email and Web Browser Protections</td>
</tr>
<tr>
<td>10</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>11</td>
<td>Data Recovery</td>
</tr>
<tr>
<td>12</td>
<td>Network Infrastructure Management</td>
</tr>
<tr>
<td>13</td>
<td>Network Monitoring and Defense</td>
</tr>
<tr>
<td>14</td>
<td>Security Awareness and Skills Training</td>
</tr>
<tr>
<td>15</td>
<td>Service Provider Management</td>
</tr>
<tr>
<td>16</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>17</td>
<td>Incident Response Management</td>
</tr>
<tr>
<td>18</td>
<td>Penetration Testing</td>
</tr>
</tbody>
</table>

Source: [https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)

**Figure 140. CIS to pattern mapping**
Mappings

MITRE ATT&CK Techniques

VERIS A4 Threat Model

CIS Controls

Source: 2020 DBIR

Source: http://veriscommunity.net

Source: 2021 DBIR

Attacker Activities

Incident Aspects

Defender Countermeasures
Coverage

12 x Industry segments (NAICS #)
- Accommodation and Food Services (72)
- Arts, Entertainment and Recreation (71)
- Educational Services (61)
- Financial and Insurance (52)
- Healthcare (62)
- Information (51)
- Manufacturing (31-33)
- Mining, Quarrying, Oil & Gas Extraction + Utilities (21+22)
- Professional, Scientific, and Technical Services (54)
- Public Administration (92)
- Retail Trade (44-45)

SMB segment
- Comparing Small | Medium to Large Business Breaches

World regions
- Northern America (NA)
- Europe, Middle East and Africa (EMEA)
- Asia Pacific (APAC)

Other highlights
- New Incident Classification Patterns
- Measuring Incident Impact
- Center for Internet Security (CIS) Controls v8
2021 DBIR resources

Learn to protect your organization from cyberthreats.

https://www.verizon.com/business/resources/reports/dbir/