Digital Gold

Trace Hollifield

CISSP, C|CISO, CISM, GSLC, GCIH, ITILv3
Large Breach Examples

• Big Breach Examples via Information is Beautiful
  • *The trend is growing?!?!*

• World View via Verizon DBIR
  • *How are they getting in?*

• Passwords, Vulnerabilities & Malware (Oh My)

• But we are PCI Compliant...
  • *Are companies really staying in compliance?*

• Risk Assessments
  • *Do you know all the right questions?*

• State, Federal & International Views
Large Breach Examples

**July 2015**

- Ebay – 145 M
- Anthem – 80 M
- Target – 70 M
- Home Depot – 56 M
- Living Social – 50 M
- Ashley Madison – 37 M
- US Office of Personnel Management – 21.5 & 4 M

**July 2017**

- River City Media – 1.3 B
- Friend Finder – 412 M
- My Space – 167 M
- Daily Motion – 85 M
- Turkish Citizen Database – 46 M
- Yahoo – 32 M
- Mail.RU – 25 M

The 2017 DBIR reveals what’s really happening in cyber security. This year’s report is based on analysis of over 40,000 incidents, including 1,935 confirmed data breaches.

62% of breaches featured hacking

81% of hacking involved weak and or stolen passwords

66% of malware was installed via malicious email attachments

### Easy to Guess Credentials

#### The 50 Most Used Passwords

<table>
<thead>
<tr>
<th></th>
<th>Password</th>
<th></th>
<th>Password</th>
<th></th>
<th>Password</th>
<th></th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td></td>
<td>11.</td>
<td>123123</td>
<td></td>
<td>21.</td>
<td>mustang</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td></td>
<td>12.</td>
<td>baseball</td>
<td></td>
<td>22.</td>
<td>666666</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td></td>
<td>13.</td>
<td>abc123</td>
<td></td>
<td>23.</td>
<td>qwertyuiop</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
<td></td>
<td>14.</td>
<td>football</td>
<td></td>
<td>24.</td>
<td>123321</td>
</tr>
<tr>
<td>5</td>
<td>123456789</td>
<td></td>
<td>15.</td>
<td>monkey</td>
<td></td>
<td>25.</td>
<td>1234...890</td>
</tr>
<tr>
<td>6</td>
<td>12345</td>
<td></td>
<td>16.</td>
<td>letmein</td>
<td></td>
<td>26.</td>
<td>p<em>s</em>y</td>
</tr>
<tr>
<td>7</td>
<td>1234</td>
<td></td>
<td>17.</td>
<td>shadow</td>
<td></td>
<td>27.</td>
<td>superman</td>
</tr>
<tr>
<td>8</td>
<td>111111</td>
<td></td>
<td>18.</td>
<td>master</td>
<td></td>
<td>28.</td>
<td>270</td>
</tr>
<tr>
<td>9</td>
<td>1234567</td>
<td></td>
<td>19.</td>
<td>696969</td>
<td></td>
<td>29.</td>
<td>654321</td>
</tr>
<tr>
<td>10</td>
<td>dragon</td>
<td></td>
<td>20.</td>
<td>michael</td>
<td></td>
<td>30.</td>
<td>1qaz2wsx</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>77777777</td>
<td></td>
<td>32.</td>
<td>f<em>cky</em>u</td>
<td></td>
<td>33.</td>
<td>qazwsx</td>
</tr>
<tr>
<td>34</td>
<td>jordan</td>
<td></td>
<td>35.</td>
<td>jennifer</td>
<td></td>
<td>36.</td>
<td>123qwe</td>
</tr>
<tr>
<td>37</td>
<td>121212</td>
<td></td>
<td>38.</td>
<td>killer</td>
<td></td>
<td>39.</td>
<td>trustno1</td>
</tr>
<tr>
<td>40</td>
<td>hunter</td>
<td></td>
<td>41.</td>
<td>harley</td>
<td></td>
<td>42.</td>
<td>zxcvbnm</td>
</tr>
<tr>
<td>43</td>
<td>asdfgh</td>
<td></td>
<td>44.</td>
<td>buster</td>
<td></td>
<td>45.</td>
<td>andrew</td>
</tr>
<tr>
<td>46</td>
<td>batman</td>
<td></td>
<td>47.</td>
<td>soccer</td>
<td></td>
<td>48.</td>
<td>tigger</td>
</tr>
<tr>
<td>49</td>
<td>charlie</td>
<td></td>
<td>50.</td>
<td>robert</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Over 10 Million dumped accounts have been analyzed for password patterns.

~60,000 accounts used “123456” as the password.

http://wpengine.com/unmasked/
Vulnerabilities are a weakness of a system which can compromise the system and data confidentiality, integrity or availability.

In the last 12 months, 1361 CVE 9 and 10s have been discovered and indexed. Over 4,000 vulnerabilities which will fail compliance requirements such as PCI.
Malware continues to grow and morph as new vulnerabilities are discovered and old vulnerabilities are not remediated.

Malware – Attack Vectors and Cost

Crimeware (Malware) Infection Vectors

Malware Cost

Trojans:
- Keylogger Detective 2.3.2 (w/ hidden installation). Price: US$3
- Web Browser Based (Opera, Mozilla Firefox, Chrome, Safari, etc). Price: US$8
- Spider Keylogger Pro v. 1.2.4. Price: US$50

Ransomware:
- Winlocker Activation Key. Price: US$10-20

Source – Trendmicro "Russian Underground 101"

Malware Highlights

- **Low Cost** ... The cost of various malware is extremely low for the possible greater rewards
- **Accuracy by Volume** ... The attacker only needs to be right once while defense has to be right all the time
- **Go Where the People Are** ... Web attacks are the most popular vector to infect hosts due to people’s habits, advertising conduits, and rapid changes in the environment which create challenges for data security defenders.
Sustaining PCI Compliance

- PCI Requirement 5 = Malware Protection
- PCI Requirement 6 = Vulnerability Management
- See a problem ???

Standardized Information Gathering (SIG)

The Standardized Information Gathering (SIG) questionnaire is a holistic tool for risk management assessments of cybersecurity, IT, privacy, data security and business resiliency in an information technology environment. The robust set of questions within the SIG are reviewed annually with updates and revisions, and are based on referenced industry regulations, guidelines and standards, including NIST, FFIEC, ISO, HIPAA and PCI. New risk areas are added on a regular basis, with End User Device Security, Threat Management and Server Security, as examples of some of the more recent additions. The SIG is in Excel format, which should be familiar to most users.

Over 1075 questions in the following categories:

A. Risk Management
B. Security Policy
C. Organizational Security
D. Asset Management
E. Human Resources Security
F. Physical and Environmental
G. Communications and Operations Management
H. Access Control
I. Information Systems Application Development and Maintenance
J. Incident Event and Communications Management
K. Business Continuity and Disaster Recovery
L. Compliance
M. Mobile
P. Privacy
Q. Software Security
V. Cloud Security

https://sharedassessments.org/products/2017-sig-bundle/
The SIG questions are

- Clear and concise
- Allow for drop down Response (Yes / No / NA)
- Fields for comments
- References to other frameworks such as ISO
- Answers are summarized

A tool good for internal assessment as well as vendor and cloud services
State Level – Security Breach Notification Laws

• Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

• Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

• Florida Information Privacy Act (FIPA) 2014 - ENFORCEMENT.
  o (a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent.
  o (b) In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:
    ▪ In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
    ▪ If the violation continues for more than 180 days, in an amount not to exceed $500,000.
    ▪ The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.
  o (c) All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund.

http://laws.flrules.org/2014/189
The Communications Security, Reliability and Interoperability Council's (CSRIC) mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. CSRIC’s members focus on a range of public safety and homeland security-related communications matters, including: (1) the reliability and security of communications systems and infrastructure, particularly mobile systems; (2) 911, Enhanced 911 (E911), and Next Generation 911 (NG911); and (3) emergency alerting.

The CSRIC’s recommendations will address the prevention and remediation of detrimental cyber events, the development of best practices to improve overall communications reliability, the availability and performance of communications services and emergency alerting during natural disasters, terrorist attacks, cyber security attacks or other events that result in exceptional strain on the communications infrastructure, the rapid restoration of communications services in the event of widespread or major disruptions and the steps communications providers can take to help secure end-users and servers.

On March 18, 2015, following an effort by over 100 cybersecurity experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and the financial, banking, and energy sectors, CSRIC IV unanimously adopted a detailed report that includes segment-specific analysis of the application of the Cybersecurity Framework as well as recommendations in response to the Commission’s charge.

On July 12, 2017, CSRIC Working Group VI began the next step of evolving the security framework and finalizing the requirements for testing.

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. It will enter in force 20 days after its publication in the EU Official Journal and will be directly application in all members states two years after this date. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

http://eugdpr.org

The shift is about giving the consumer called “Data Subjects” rights to their own data.

• Section 3: Rectification and Erasure
  • Article 16 – Right to Rectification
  • Article 17 – Right to Erasure
  • Article 18 – Right to Restriction of Processing
  • Article 19 – Notification
  • Article 20 – Right to Data Portability

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Questions? Comments?