Malware

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 11

ravi.utsa@gmail.com
www.profsandhu.com
<table>
<thead>
<tr>
<th>Industry Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Internet Security Threat Report</td>
</tr>
<tr>
<td>AT&amp;T Cybersecurity Insights Report</td>
</tr>
<tr>
<td>Cisco Annual Security Report</td>
</tr>
<tr>
<td>Dell Security Annual Threat Report</td>
</tr>
<tr>
<td>Google Android Security Annual Report</td>
</tr>
<tr>
<td>IBM X-Force Cyber Security Intelligence Index Report</td>
</tr>
<tr>
<td>McAfee Labs Threat Predictions Report</td>
</tr>
<tr>
<td>Verizon Data Breach Investigation Report</td>
</tr>
<tr>
<td>......</td>
</tr>
</tbody>
</table>
A new zero-day vulnerability was discovered on average each week (total 54)
  - Doubled from 2014

Over half a billion personal records were stolen or lost
  - Companies choosing not to report the number of records lost increased by 85 percent

Major security vulnerabilities in 75% of popular websites
  - 15% of legitimate websites have critical vulnerabilities

Spear-phishing targeting employees increased 55%
  - 43% of all attacks targeted at small businesses

Ransomware increased 35%
  - moved beyond PCs to smart phones, Mac, and Linux systems

Symantec blocked 100 million fake tech support scams
  - first reported in 2010
Big numbers

- Pages 8 and 9 of report
Malware

Classic Malware
- Trojan Horse (1971)
- Logic Bomb
- Virus (1985)
- Worm

Modern Crimeware
- Adware
- Spyware
- Ransomware
- Rootkit
- Exploit
- Zero-Day
- Keylogger
- Drive by
- Phishing
- Spam
- DDOS
- Botnet
Malware

Delivery
- Self-Propagating
  - Virus
  - Worm
- Planted By Attacker
- Inadvertent By User
- Local Condition

Trigger
- External Command
  - Host
    - Damage
    - Exfiltrate
- External

Target