Trends in Cyber Crime

- Ike Barnes, Secret Service
Actors Perpetrating Cyber Crimes
Actors Perpetrating Cyber Crimes
Actors Perpetrating Cyber Crimes
Actors Perpetrating Cyber Crimes
Actors Perpetrating Cyber Crimes
Actors Perpetrating Cyber Crimes

Figure 6.
Percent of breaches per threat actor motive over time

Criminals
Spies
Activists

Source: verizonenterprise.com/DBIR/2014
Types of Attacks

- **2013 breaches, n=1,367**
  - POS Intrusions: 14%
  - Web App Attacks: 35%
  - Insider Misuse: 8%
  - Physical Theft/Loss: <1%
  - Miscellaneous Errors: 2%
  - Crimeware: 4%
  - Card Skimmers: 9%
  - DoS Attacks: <1%
  - Cyber-espionage: 22%
  - Everything else: 6%

- **2013 incidents, n=63,437**
  - POS Intrusions: <1%
  - Web App Attacks: 6%
  - Insider Misuse: 18%
  - Physical Theft/Loss: 14%
  - Miscellaneous Errors: 25%
  - Crimeware: 20%
  - Card Skimmers: <1%
  - DoS Attacks: 18%
  - Cyber-espionage: 1%
  - Everything else: 12%

- **2011-2013 breaches, n=2,861**
  - POS Intrusions: 31%
  - Web App Attacks: 21%
  - Insider Misuse: 8%
  - Physical Theft/Loss: 1%
  - Miscellaneous Errors: 1%
  - Crimeware: 1%
  - Card Skimmers: 14%
  - DoS Attacks: <1%
  - Cyber-espionage: 15%
  - Everything else: 5%
## Tactics, Techniques, and Procedures

**Figure 19.** Frequency of incident classification patterns per victim industry

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>POS INTRUSION</th>
<th>WEB APP ATTACK</th>
<th>INSIDER MISUSE</th>
<th>THEFT/LOSS</th>
<th>MISC. ERROR</th>
<th>CRIMWARE</th>
<th>PAYMENT CARD SKIMMER</th>
<th>DENIAL OF SERVICE</th>
<th>CYBER ESPIONAGE</th>
<th>EVERYTHING ELSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>75%</td>
<td>1%</td>
<td>8%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>10%</td>
<td>4%</td>
<td>7%</td>
</tr>
<tr>
<td>Administrative</td>
<td>8%</td>
<td>27%</td>
<td>12%</td>
<td>&gt;43%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>7%</td>
</tr>
<tr>
<td>Construction</td>
<td>7%</td>
<td>13%</td>
<td>13%</td>
<td>7%</td>
<td>33%</td>
<td></td>
<td>&lt;1%</td>
<td>6%</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>Education</td>
<td>&lt;1%</td>
<td>19%</td>
<td>8%</td>
<td>15%</td>
<td>20%</td>
<td>6%</td>
<td>&lt;1%</td>
<td>6%</td>
<td>2%</td>
<td>22%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>7%</td>
<td>22%</td>
<td>10%</td>
<td>7%</td>
<td>12%</td>
<td>2%</td>
<td>2%</td>
<td>32%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>Finance</td>
<td>&lt;1%</td>
<td>27%</td>
<td>7%</td>
<td>3%</td>
<td>5%</td>
<td>4%</td>
<td>22%</td>
<td>26%</td>
<td>&lt;1%</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
<td>3%</td>
<td>15%</td>
<td>46%</td>
<td>3%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Information</td>
<td>&lt;1%</td>
<td>41%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>31%</td>
<td>&lt;1%</td>
<td>9%</td>
<td>1%</td>
<td>16%</td>
</tr>
<tr>
<td>Management</td>
<td>11%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td></td>
<td></td>
<td>11%</td>
<td>44%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>14%</td>
<td>8%</td>
<td>4%</td>
<td>2%</td>
<td>9%</td>
<td></td>
<td>24%</td>
<td>30%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Mining</td>
<td>25%</td>
<td>10%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>40%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td>&lt;1%</td>
<td>9%</td>
<td>6%</td>
<td>4%</td>
<td>3%</td>
<td>3%</td>
<td>37%</td>
<td>29%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>&lt;1%</td>
<td>24%</td>
<td>19%</td>
<td>&gt;34%</td>
<td>21%</td>
<td></td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td>10%</td>
<td>37%</td>
<td>13%</td>
<td>20%</td>
<td>7%</td>
<td></td>
<td></td>
<td>3%</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>31%</td>
<td>10%</td>
<td>4%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>10%</td>
<td>33%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Trade</td>
<td>6%</td>
<td>30%</td>
<td>6%</td>
<td>6%</td>
<td>9%</td>
<td>9%</td>
<td>3%</td>
<td>3%</td>
<td>27%</td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td>15%</td>
<td>16%</td>
<td>7%</td>
<td>6%</td>
<td>15%</td>
<td>5%</td>
<td>3%</td>
<td>24%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Utilities</td>
<td>38%</td>
<td>3%</td>
<td>1%</td>
<td>&gt;2%</td>
<td>31%</td>
<td></td>
<td>14%</td>
<td>7%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>29%</td>
<td>13%</td>
<td>13%</td>
<td>10%</td>
<td>3%</td>
<td>9%</td>
<td>6%</td>
<td>17%</td>
<td></td>
</tr>
</tbody>
</table>

For more information on the NAICS codes [shown above] visit: [https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012](https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012)
Figure 21. Top 10 threat action varieties within POS Intrusions (n=196)
- Ram scraper [mal] 85%
- Export data [mal] 79%
- Brute force [hac] 50%
- Use of stolen creds [hac] 37%
- Offline cracking [hac] 8%
- Use of backdoor or C2 [hac] 2%
- Spyware/Keylogger [mal] 2%
- Backdoor [mal] 1%
- Misconfiguration [err] <1%
- Phishing [soc] <1%

Figure 22. Hacking variety within POS Intrusions (n=187)
- Brute force 53%
- Use of stolen creds 38%
- Offline cracking 9%
- Unknown 9%
- Use of backdoor or C2 2%
- SQLi <1%

Figure 23. Hacking vector within POS Intrusions (n=187)
- 3rd party desktop 55%
- Desktop sharing 35%
- Physical access 9%
- Backdoor or C2 1%
- Command hell 1%
- VNP <1%
- Web application <1%
TTP

Installation of Malware Through Known Vulnerabilities

• Infiltration (malware/keyloggers/sniffers)
• Aggregation
• Exfiltration (email/servers)

Data Flow
TTP

Victim country within Cyber-espionage (n=470)

- United States: 54%
- South Korea: 6%
- Japan: 4%
- Russian Federation: 3%
- Colombia: 2%
- Ukraine: 2%
- Vietnam: 1%
- Belarus: 1%
- Kazakhstan: 1%
- Philippines: 1%
Top threat action varieties within Cyber-espionage (n=426)

- Use of backdoor or C2 [hac]: 70%
- C2 [mal]: 68%
- Phishing [soc]: 67%
- Backdoor [mal]: 65%
- Downloader [mal]: 60%
- Capture stored data [mal]: 57%
- Export data [mal]: 43%
- Spyware/Keylogger [mal]: 38%
- Exploit vuln [mal]: 37%
- Scan network [mal]: 37%
- Use of stolen creds [hac]: 30%
- Disable controls [mal]: 28%
- Rootkit [mal]: 24%
- Brute force [mal]: 24%
- Brute force [hac]: 24%
- Password dumper [mal]: 19%
- Packet sniffer [mal]: 16%
- Ram scraper [mal]: 14%
- Other [mal]: 14%
- Client-side attack [mal]: 13%
Phishing

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Phishing

Figure 28: The inevitability of the click

Probability of at least one click

E-mails per campaign

2 4 6 8 10 12 14 16 18 20

0% 20% 40% 60% 80% 100%
What Can I Do to Prevent Breaches?

http://www.sans.org/critical-security-controls

<table>
<thead>
<tr>
<th>No.</th>
<th>Critical Security Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory of Authorized and Unauthorized Devices</td>
</tr>
<tr>
<td>2</td>
<td>Inventory of Authorized and Unauthorized Software</td>
</tr>
<tr>
<td>3</td>
<td>Secure Configurations for Hardware &amp; Software on Laptops, Workstations, and Servers</td>
</tr>
<tr>
<td>4</td>
<td>Continuous Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>5</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>6</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>7</td>
<td>Wireless Device Control</td>
</tr>
<tr>
<td>8</td>
<td>Data Recovery Capability</td>
</tr>
<tr>
<td>9</td>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
</tr>
<tr>
<td>10</td>
<td>Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
</tr>
<tr>
<td>11</td>
<td>Limitation and Control of Network Ports, Protocols, and Services</td>
</tr>
<tr>
<td>12</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>13</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>14</td>
<td>Maintenance, Monitoring, and Analysis of Security Audit Logs</td>
</tr>
<tr>
<td>15</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>16</td>
<td>Account Monitoring and Control</td>
</tr>
<tr>
<td>17</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>18</td>
<td>Incident Response Management</td>
</tr>
<tr>
<td>19</td>
<td>Secure Network Engineering</td>
</tr>
<tr>
<td>20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Software Inventory</td>
<td>24</td>
</tr>
<tr>
<td>Standard Configs</td>
<td>31</td>
</tr>
<tr>
<td>Malware Defenses</td>
<td>32</td>
</tr>
<tr>
<td>Secure Development</td>
<td>38</td>
</tr>
<tr>
<td>Backups</td>
<td>41</td>
</tr>
<tr>
<td>Skilled Staff</td>
<td>42</td>
</tr>
<tr>
<td>Restricted Access</td>
<td>44</td>
</tr>
<tr>
<td>Limited Admin</td>
<td>45</td>
</tr>
<tr>
<td>Boundary defense</td>
<td>46</td>
</tr>
<tr>
<td>Audit Logging</td>
<td>47</td>
</tr>
<tr>
<td>Identity Management</td>
<td>48</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>49</td>
</tr>
<tr>
<td>Incident Response</td>
<td>50</td>
</tr>
<tr>
<td>Network Segmentation</td>
<td>51</td>
</tr>
</tbody>
</table>
Dark Web

The Internet (more or less)

You can turn a computer on. Yay.

You must be really bored.

Either use a proxy, or say hi to the FBI.

Has anyone really been far enough as decided to use even, go want to do look more like?