BIG PROBLEMS, SCANT SOLUTIONS: ANALYZING THE VERIZON 2014 DATA BREACH REPORT

PRESENTED BY
JOHN LINKOUS

FRIDAY, SEPTEMBER 12, 2014
WHO AM I?

- Hands-On Security Consultant
  - Founder & CEO, InterPoint Group LLC
  - Consultant of the Year, 1994 – NASA/Goddard Space Flight Center
  - Global IDM solution architect – NYSE
  - Security Program Lead – Multiple BCBSs
  - Outsourced CISO – Multiple verticals

- Just Like Most of You
  - Been on the wrong end of data breaches and other realized threats
  - Called in front of BoD's to explain why Really Bad Things® happened
  - Cannot believe that users still use "password", "123456" and their childrens’ and pets’ names as passwords
WHO IS INTERPOINT GROUP?

- Trusted Information Security and Risk Advisors
  - HQ in Baltimore; offices in New York, Chicago, Boston, Charlotte
  - Verticals: Financial Services, Healthcare (Payer, Provider); Retail; Energy; Manufacturing; Technology
- What We Do
  - Enterprise Services
    - Hands-On and Strategic Security, Risk and Compliance Consulting
    - Program and Project Management
    - Research and Analysis
  - Vendor Advisory Services
    - Go-to-Market Strategy
    - Market Positioning and Messaging
    - Product Management Advisory
    - Industry Analyst Relations

Ensure vendors aren’t answering a question that nobody asked!
Information Security Efforts Have Helped a Lot of Organizations... But It’s Still Not Enough

Everyone is susceptible

- You name the industry, and there was likely a data breach somewhere in it

The problem is even worse for smaller organizations

- Exposed to the same threats as the big guys...
- ...but smaller budgets...
- ...and fewer personnel!
WHY ARE WE HERE TODAY?

From 1/2012 – 6/2014, 75% of reported data breaches have occurred at small and mid-sized organizations.

Reported Data Breaches by Industry and Size of Organization
January 2012 – June 2014

Source: Privacy Rights Clearinghouse (www.privacyrights.org)
WHY THE VERIZON DATA BREACH REPORT?

- It covers a lot of networks and systems
  - Not just Verizon networks
  - Many OEMs and ISVs provide anonymized breach and threat data

- It is supported by a lot of organizations
  - Over 50 supporting groups
    - OEMs/ISVs
    - Government Agencies
    - Research Firms

- It’s been around a long time
  - Since 2004... ten years of analysis and trends
2014 BY THE NUMBERS: THE VICTIMS

2014 Data Breaches by Pattern

- POS Intrusions: 14%
- Web App Attacks: 35%
- Insider Misuse: 8%
- Physical Theft/Loss: <1%
- Miscellaneous Errors: 2%
- Crimeware: 4%
- Card Skimmers: 9%
- DoS Attacks: 0%
- Cyber-espionage: 22%
- Everything else: 6%

2014 Data Breaches by Vertical

<table>
<thead>
<tr>
<th>Industry</th>
<th>Total</th>
<th>Small</th>
<th>Large</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>137</td>
<td>113</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>Administrative</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Construction</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Education</td>
<td>15</td>
<td>1</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>Entertainment</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Finance</td>
<td>465</td>
<td>24</td>
<td>36</td>
<td>405</td>
</tr>
<tr>
<td>Healthcare</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Information</td>
<td>31</td>
<td>7</td>
<td>6</td>
<td>18</td>
</tr>
<tr>
<td>Management</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>59</td>
<td>6</td>
<td>12</td>
<td>41</td>
</tr>
<tr>
<td>Mining</td>
<td>10</td>
<td>0</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Professional</td>
<td>75</td>
<td>13</td>
<td>5</td>
<td>57</td>
</tr>
<tr>
<td>Public</td>
<td>175</td>
<td>16</td>
<td>26</td>
<td>133</td>
</tr>
<tr>
<td>Real Estate</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Retail</td>
<td>148</td>
<td>35</td>
<td>11</td>
<td>102</td>
</tr>
<tr>
<td>Trade</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Transportation</td>
<td>10</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Utilities</td>
<td>80</td>
<td>2</td>
<td>0</td>
<td>78</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Unknown</td>
<td>126</td>
<td>2</td>
<td>3</td>
<td>121</td>
</tr>
<tr>
<td>Total</td>
<td>1,367</td>
<td>243</td>
<td>144</td>
<td>980</td>
</tr>
</tbody>
</table>

Small = organizations with less than 1,000 employees, Large = organization with 1,000+ employees
TRENDS OVER TIME: BAD ACTORS

Percent of Data Breaches per Threat Actor Category, 2004-2014

TRENDS OVER TIME: THE COMPROMISE-DISCOVERY GAP

- This is Very Unpleasant
  - The amount of time between compromise and discovery continues to grow
  - We thought 2011 was an anomaly, and we were getting better... but we were wrong

- There’s No Consistent Correlation with Organization Size or Type, or Attack Type
  - It’s all over the board
  - Everyone is affected, regardless of industry, size or breach type

## TRENDS OVER TIME: THREAT ACTIONS/ATTACK VECTORS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware/Keylogger</td>
<td>#8</td>
<td>#7</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>Use of Stolen Credentials</td>
<td>#7</td>
<td>#1</td>
<td>4.6</td>
<td></td>
</tr>
<tr>
<td>Brute Force (e.g., PW cracking)</td>
<td>#1</td>
<td>#12</td>
<td>5.0</td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>#14</td>
<td>#3</td>
<td>10.6</td>
<td></td>
</tr>
<tr>
<td>RAM Scraping</td>
<td>#5</td>
<td>#4</td>
<td>11.6</td>
<td></td>
</tr>
<tr>
<td>Adminware (e.g., BO2K)</td>
<td>#6</td>
<td>#19</td>
<td>14.0</td>
<td></td>
</tr>
</tbody>
</table>

- **Methods are Changing**
  - More breaches facilitated by hardware: skimmers, carding
  - Phishing has become the #1 enterprise malware ingress method
  - Rooting tools are less common; defined-target payloads are becoming more prevalent and more complex

#1 in 2011, 2012
SO WHAT’S THE BIGGEST PROBLEM?

- The Majority of Breaches Use Technically Complex Methods
  - Yet they exploit easily-addressed security vulnerabilities

---

| How do Data Breaches Occur? | 81% utilized hacking  
<table>
<thead>
<tr>
<th></th>
<th>69% incorporated malware</th>
</tr>
</thead>
</table>

| How Long Does it Take to Discover a Data Breach? | 85% took weeks or more to discover  
|                                                 | 92% were discovered by a third party |

Source: 2013 Verizon Data Breach Investigations Report
Yes! *(but not much...)*

- Internal detection and reporting of data breaches surpasses external detection/reporting for the first time!
  - Organizations are getting better at detecting breaches
  - Big props to security researchers and other third-party groups!
WHAT’S ALLOWING THESE PROBLEMS TO PERSIST?

- **30+ Year-Old Standards and Protocols**
  - Security was never baked-in to early standards
  - Not much you can do about that unless you’re the IETF

- **Focus on Perimeter Security**
  - “Weakest Link in the Chain” can facilitate ingress of bad actors to the soft, creamy and delicious core of your network
  - Relatively little monitoring, detection and prevention at the endpoint
    - Antivirus and signature-based solutions aren’t “effective endpoint protection”!
  - Ignores internal actors, who are increasing as threats
WHAT’S ALLOWING THESE PROBLEMS TO PERSIST?

- **Funding**
  - Especially in SMB/midmarket
  - This is not necessarily the fault of management!

- **Security Awareness**
  - People are still the weakest part of security

- **Failure to Consider Low-Tech Attack Vectors**
WHAT’S ALLOWING THESE PROBLEMS TO PERSIST?

Tools

- Can be expensive and complex
- Often have scope issues
  - “An inch deep and a mile wide”
  - “A mile deep and an inch wide”
- Interoperability is ugly
  - Too many standards, too little adoption
  - Lots of vendors trying to build the *Platform to End All Platforms®*
  - Too many vendors/tools trying to tackle the same problem in very different ways

“The great thing about standards is that there are so many to choose from.”

- Anonymous
## Verizon’s Recommendations: SANS CSC

<table>
<thead>
<tr>
<th>Critical Security Controls (SANS Institute)</th>
<th>POS Intrusions</th>
<th>Web App Attacks</th>
<th>Insider Misuse</th>
<th>Physical Theft/Loss</th>
<th>Misc Errors</th>
<th>Crimeware</th>
<th>Card Skimmers</th>
<th>Cyber-espionage</th>
<th>DoS Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Inventory</td>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard Configs</td>
<td>3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Defenses</td>
<td>5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Development</td>
<td>6.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backups</td>
<td>8.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skilled Staff</td>
<td>9.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Access</td>
<td>11.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>11.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>11.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Verizon’s Recommendations: SANS CSC

<table>
<thead>
<tr>
<th>Critical Security Controls (SANS Institute)</th>
<th>POS Intrusions</th>
<th>Web App Attacks</th>
<th>Insider Misuse</th>
<th>Physical Theft/Loss</th>
<th>Misc Errors</th>
<th>Crimeware</th>
<th>Card Skimmers</th>
<th>Cyberespionage</th>
<th>DoS Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Admin</td>
<td>12.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(12.2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(12.3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(12.4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(12.5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boundary defense</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(13.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(13.7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(13.10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(13.14)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Logging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(14.5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(16.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(16.12)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(16.13)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(17.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(17.6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(17.9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(18.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(18.2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(18.3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Segmentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(19.4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Non-Software Attack Vectors: Hardware Keyloggers

- Extremely difficult to detect through software methods
  - Don’t believe me? Ask Fabian Mihailowitsch...
- Going BT doesn’t help much, either
  - BT PIN crackers are common, and high-gain antennas can sniff traffic
WHAT’S MISSING?: HARDWARE/PHYSICAL SECURITY

- Non-Software Attack Vectors: Skimmer Technology
  - Getting really advanced!
  - Requires physical intervention; difficult to detect remotely
  - Often looks like the real thing

Photo Credits: Brian Krebs, “Krebs on Security” blog
WHAT’S MISSING?: ENDPOINT SECURITY

- Detection and (where possible) Protection
  - Configuration Hardening
    - Go agentless if possible – Promisec
  - Ingress/Egress Monitoring
    - Host level (event logs) – SIEM
    - Process level / sandboxing – Bromium
  - Anomalous Activity Detection

- Cover Everything
  - Desktops
  - Laptops
  - Tablets
  - Mobile
WHAT DOES THE DBIR TELL US WE CAN DO TO AVOID BEING THE NEXT TARGET? (PUN INTENDED...)

- Know Your Assets, and What They’re Worth
  - You don’t have to try and boil the ocean with security controls
- Do the Basics, and Do them Well
  - **Patch Management**
  - Authentication
  - Access Control
  - Perimeter Intrusion Detection
  - **DLP and Egress Monitoring**
  - Security Awareness and Training (!)
  - Develop software? Sanitize Inputs!
WHAT DOES THE DBIR TELL US WE CAN DO TO AVOID BEING THE NEXT TARGET? (PUN INTENDED…)

- **Industry-Specific Security Controls**
  - Retail
    - Protect your POS units!
  - Financial Services (Retail)
    - Protect your ATMs!

- **Countermeasures**
  - Video surveillance
  - Checksumming/testing
  - Periodic physical inspections
  - Improved customer messaging
    - "Does this ATM look weird? Then don't use it!"
  - Employee awareness of suspicious customer activity
WHAT DOES THE DBIR TELL US WE CAN DO TO AVOID BEING THE NEXT TARGET? (PUN INTENDED...)

- **Security in the Cloud**
  - Many different security solutions delivered through the cloud
    - Authentication, authorization and access control (AAA)
    - End point security and operations management
    - SIEM and log management
    - DDoS mitigation
  
  - **Small Organization? Think Cloud!**
    - Enterprise-class service
    - Low CapEx, measured OpEx
    - Easy to opt-out
WHAT DOES THE DBIR TELL US WE CAN DO TO AVOID BEING THE NEXT TARGET? (PUN INTENDED...)

- MSSPs
  - Deliver multiple security services
  - Delivered in on-premise, cloud/offsite, and hybrid models
  - Adds a SOC management layer
- Good for large or small organizations
  - Low CapEx, incremental OpEx
  - Lots of customization options
  - Fills gaps in existing capabilities
  - Easy ramp-up
The “It’s Not Security” Security Control: Cyber Insurance

- Designed to protect against the risks you don’t know about
- Usually scoped to a very specific set of business processes
- Does *not* mean organizations can abdicate risk!
- Policy riders usually require baseline compliance
  - PCI DSS, ISO 27001:2013, NIST 800-53
- Conversta many conditions
  - Malware ingress
  - Physical theft / mutilation (including installed skimmers/keyloggers)
  - Errors and omissions
Thank You!
- I really appreciate your attendance today!

Big thanks to ISSA!

Feel free to email if you have any Q’s, or would like a copy of today’s slide deck:

jlinkous@gointerpoint.com