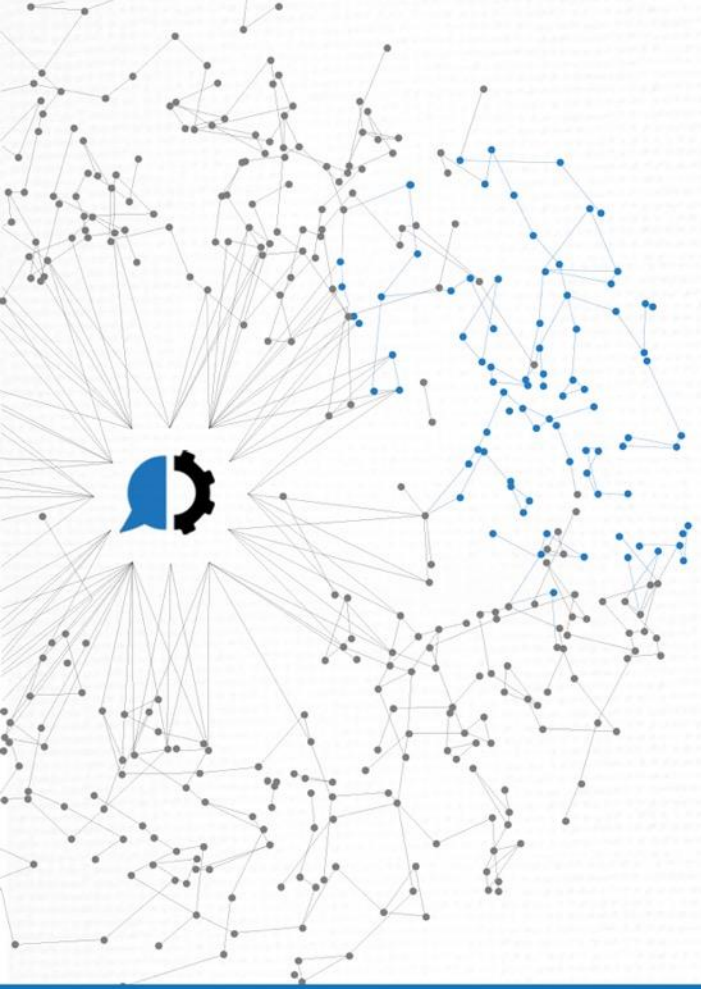


How to Think Like a Hacker and Secure Your Data

Common Techniques Used During Data Breaches

Introductions

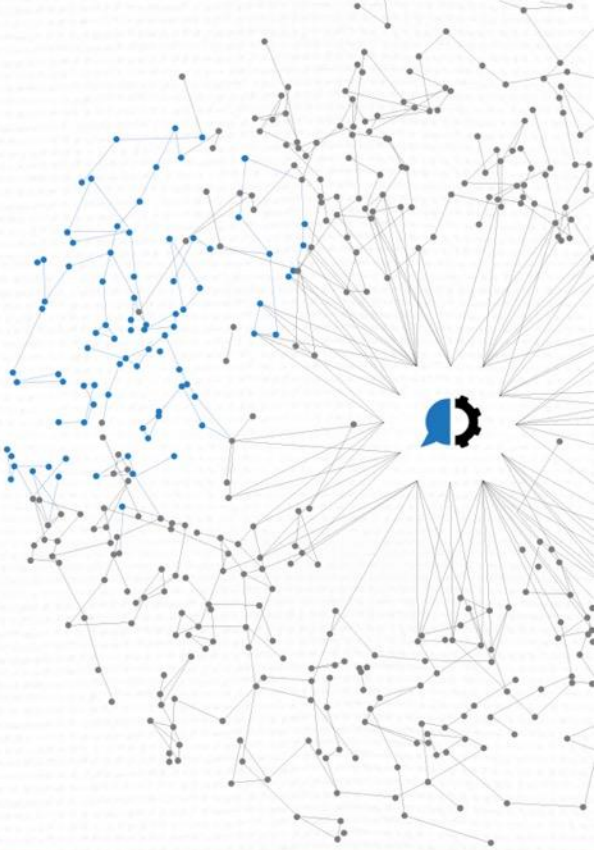
Dan Freeman

Senior Solutions Consultant

CISSP

Agenda

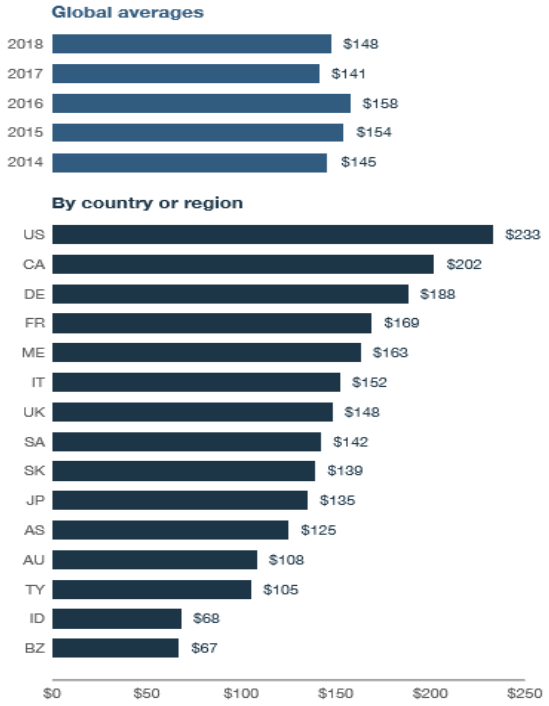
1. Cybersecurity statistics
2. Basic terminology
3. Common techniques for hacking
4. Dissecting data breaches
5. Advanced Persistent Threat
6. What can you do?
7. Q&A



UP NEXT

Cybersecurity Statistics – Cost

- The consolidated average per capita cost for all samples was $148 compared to an average of $141 last year.
- The United States, Canada, and Germany continue to have the highest per capita costs at $233, $202, and $188, respectively.
- Turkey, India, and Brazil have much lower per capita costs at $105, $68, and $67, respectively.

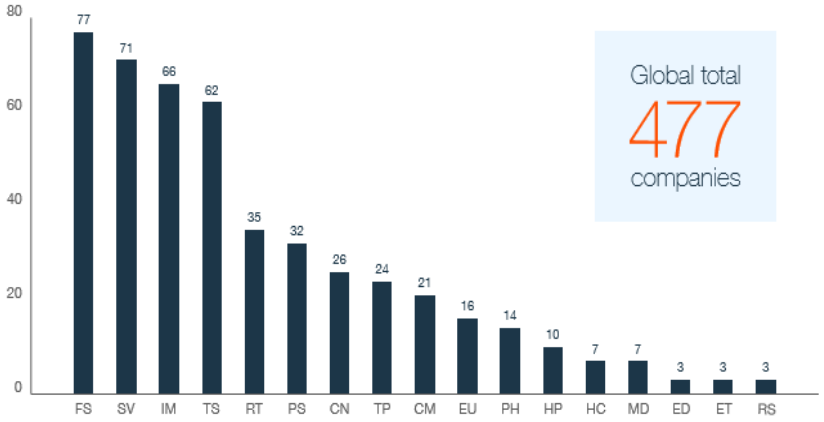


Cybersecurity Statistics – Cost

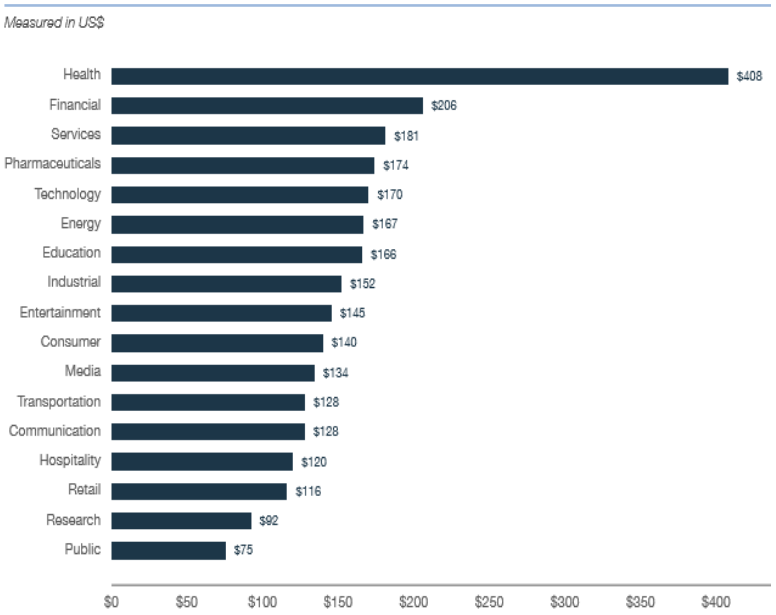
Frequency of Data Breaches by Industry

> FS — Financial Services
> SV — Services
> IM — Industrial Manufacturing
> TS — Technology
> RT — Retail
> PS — Public Sector
> CN — Consumer
> TP — Transportation
> CM — Communications
> EU — Energy
> PH — Pharmaceuticals
> HP — Hospitality
> HC — Healthcare
> MD — Media
> ED — Education
> ET — Entertainment
> RS — Research

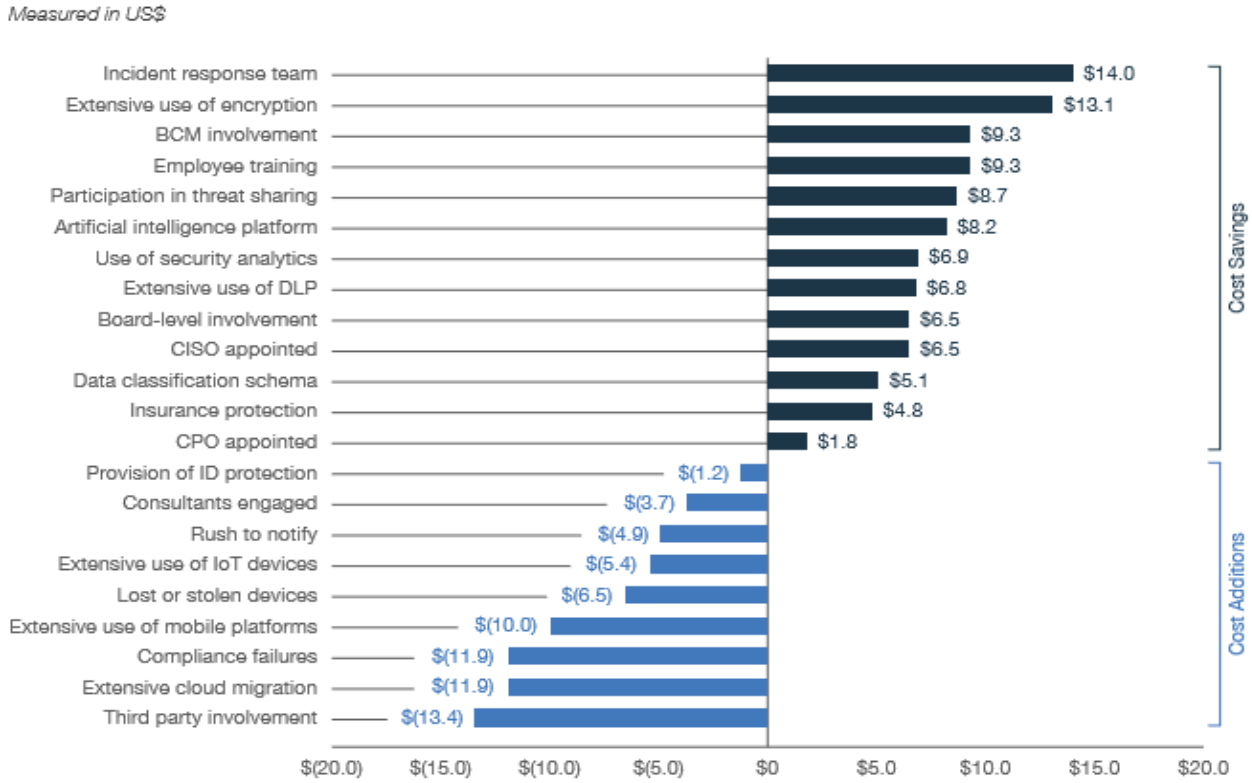
Figure 3. Frequency of benchmark samples by industry



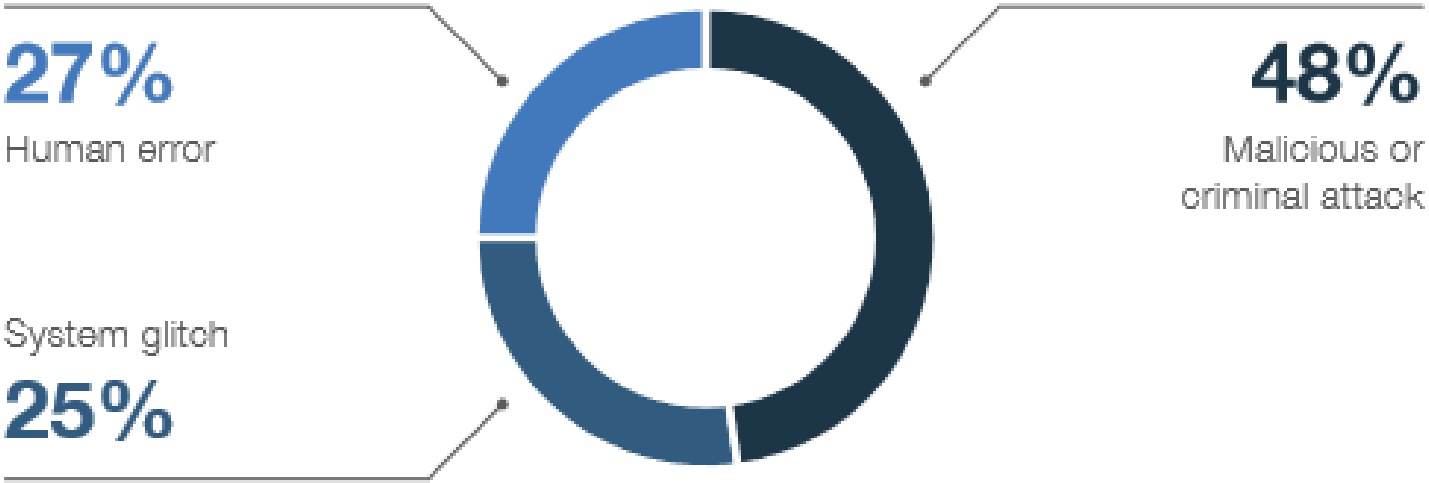
Per Capita Cost by Industry



Cybersecurity Statistics – Cost



Cybersecurity Statistics – Root Causes



Cybersecurity Statistics – Key Findings

- Global cost of data breach increased in 2018
  - 6.4% total cost, 4.8% per capita, 2.2% size (number of records)
- U.S. and ME had the most costly data breaches
- Hackers and insider threats comprised 48% of total breaches
- Faster breach can be identified, lower the costs
  - Mean Time To Identify (MTTI) – 197 days
  - Mean Time To Contain (MTTC) – 69 days
  - Both MTTI/MTTC were highest for malicious/criminal attacks vs. human error
- Third-party involvement cost increase
  - Cost increased by $13 per compromised record
  - Those undergoing cloud migration saw increase by $12 per record
- Loss of customer trust = loss of customers = loss of “bottom line”

Basic Terminology

- Attack Surface: threat vector or sum of all possible attack points
- Attack Pivot: usually targeting a lower security host to then escalate the attack on the real target
- Attack Escalation: evolving the attack from low to high (or critical) value
- Critical Value Data (CVD): prized organizational data (crown jewels)
  - Secret ingredients
  - Proprietary formulas
  - Manufacturing processes
- Reconnaissance
  - Passive: information gathering (googling), social engineering, dumpster diving
  - Active: probing network for hosts, IP addresses, services, etc. – risky
- RAT – Remote Access Trojan
- Command and Control

Hacking Techniques

- Fake WAP
- Cookie theft
- Bait and Switch
- Clickjacking
- Browser locker
- IoT attacks
- Credential reuse
- Phishing

Hacking Techniques – Fake WAP

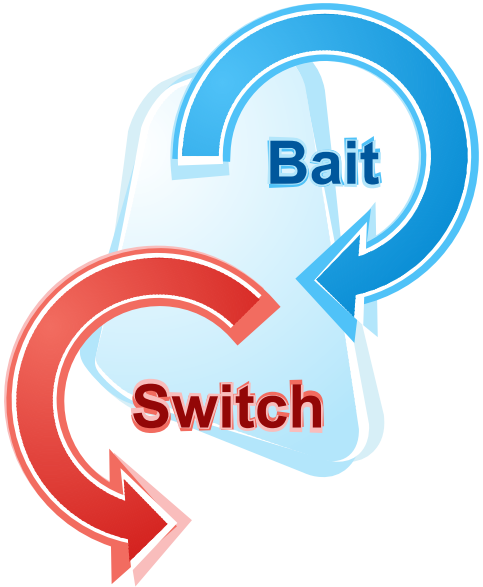
- Leverage Wireless Access Point in public spot
  - Key to have legitimate naming convention
  - Open, non-secure network with no password
  - Extremely easy to set up
  - Extremely easy to fall for
  - Once connected, all traffic will traverse rogue Access Point for inspection
- What to do?
  - Don’t connect to free, open Wireless Networks
  - Make sure you get network name and password from provider
  - Host VPN solution to encrypt your traffic

Hacking Techniques – Cookie Theft

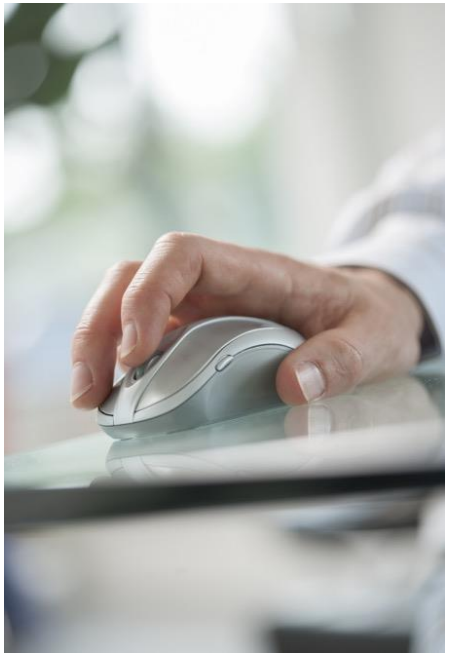
- Also known as Sidejacking/Session Hacking
- Cookie sent by website to user for session persistence
- Unsecure connection can allow theft
- Attacker can pretend they are you
  - Can’t necessarily gain access to login creds
  - Can change settings to hijack the account
- What to do?
  - Make sure that you are always visiting a secure site – https
  - Use a host VPN to encrypt your traffic

Hacking Techniques – Bait and Switch

- Leverage internet clickable ads to divert to malicious sites
- Largely depends on host site (advertiser)
- Larger the advertiser (Facebook or Google) more safeguards
- Install malware or adware on your computer
- Gain access to your computer
- What to do?
  - Don’t click on ads while browsing
  - Use secure browser – plug-ins and pop-up blocker
  - Host solution with known malicious sites



Hacking Techniques – Clickjacking



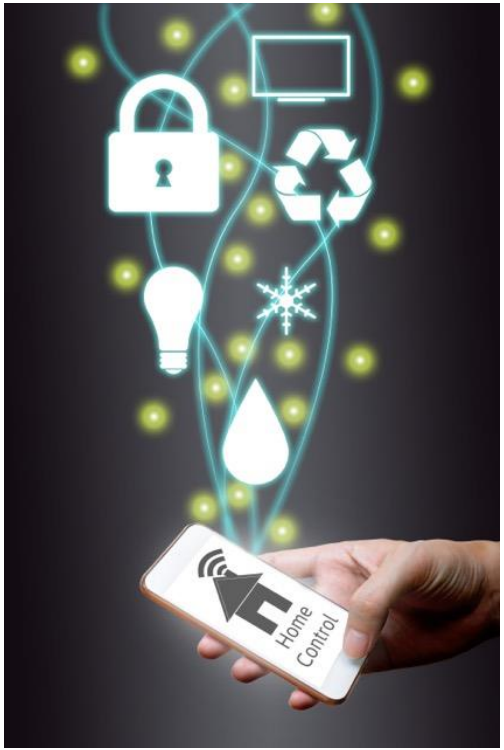
- Otherwise known as UI Redress
- Lay invisible frame over the site that you see
- Invisible buttons
- Buttons that follow your mouse – any click
- Click on ads to generate revenue, unlock camera, or microphone
- What to do?
  - Use up-to-date secure browser with built-in defenses
  - Adblocker and script-blocking browser
  - Host solution that has list of known clickjacking sites

Hacking Techniques – Browser Locker

- Pop-up window with fake virus or infected message
- Encouraged to click on options that lead to rogue/malicious sites or phone numbers
- Fake technician gets you to pay for “fixing” your computer
- What to do?
  - Host solution to block malicious online links and ads
  - Do not call any numbers provided or click on any links within message

Hacking Techniques – IoT Attacks

- Exciting new products/features
- General public disconnect with security risk they pose
- Passwords are often left as default
- Compromise home appliances
  - AC, refrigerator, TV – watch you via cameras in your house
  - Use compromised devices as bots
- What to do?
  - Change out the locks on front door (router)
    - Place on different VLAN if possible
    - Default admin username and password
    - Router name
  - Use strong encryption
  - Use strong (at least 15 characters) password
  - Keep software up to date
  - Leverage two-factor authentication on devices



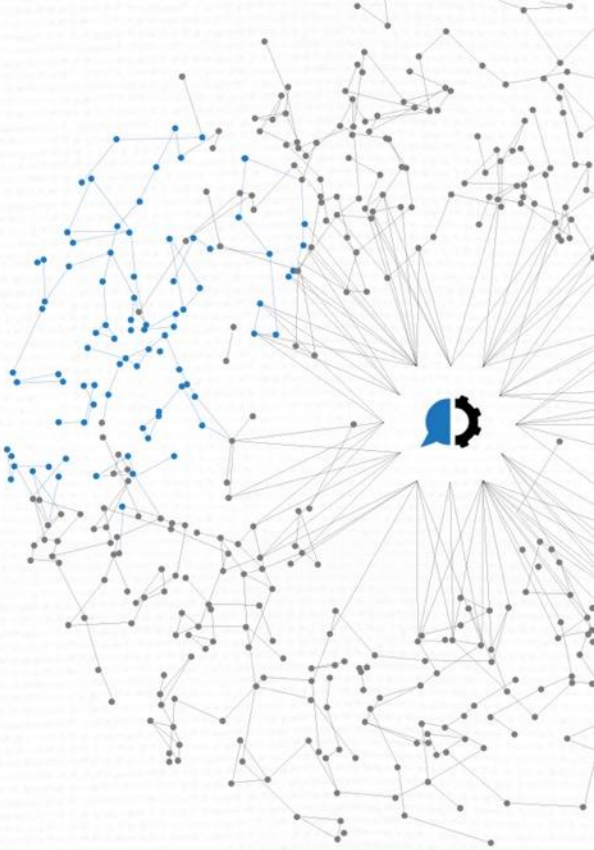
Hacking Techniques – Credential Reuse

- Attack following a data breach containing login information
- Many users apply same password to multiple sites
- Yahoo gets breached
  - Most may not be too concerned about email account
  - Hacker uses these creds to attack other more sensitive sites
- What to do?
  - Don’t use the same passwords across sites/applications
  - Keep informed of what sites or companies have been breached
  - Use password vault application
  - Leverage password compromise website
    - https://haveibeenpwned.com

Hacking Techniques – Phishing

- Type of Social Engineering
- Attack the user instead of the device
- Why hack when you can ask for the keys?
  - AOL users called by “technicians”
  - Microsoft “technicians” calling users
  - Spoofed email from CEO to CFO asking for money transfer transaction
  - Job applicant with pdf “resume” attached
- What to do?
  - User training

Data Breaches



UP NEXT

Facebook – 2018

- 90 million user accounts
- Vulnerability in code featuring “View As” tool
- Zuckerberg’s account was affected
- Stock price tumbling ever since
- GDPR implications
  - Maximum fine of up to 4% of global annual revenue
  - 1.63 billion

Equifax – 2017

- 143 million U.S. consumers
- Names, SSNs, birth dates, and addresses of almost half population
- Stock price fell 13% immediately
- 3 executives sold shares BEFORE disclosure
- Website vulnerability – Apache Struts CVE-2017-5638
  - CVE (Common Vulnerabilities and Exposers)
  - CVEs are developed or published by a group of CVE Numbering Authorities
  - NVD – National Vulnerability Database – hosted by NIST

Yahoo – 2013, 2016, 2017

- Initial disclosure in 2016
  - 500 million users
  - Increased to 1 billion by end of 2016
  - 2017 disclosure “based on an analysis of the information” determined that all 3 billion accounts were affected
- Required all users to change passwords
- Invalidated all unencrypted security questions and answers
- Forged cookies
- State-sponsored actor

Anthem – 2015: Featured Breach

- 79 million users
- Very detailed records
  - Full name, address, gender, DOB, SSN, Medical ID, Employer, Title, Years Employed, Previous Employers, UserID, Passwords, Secret Phrases, Account ID, Employer Data
  - Value: approximately $150 - $250/record
- $115 million dollar settlement just this year
- Huge Forensic and Cleansing Operation
- Huge increase in Hardening network = large budget increases
- Careers at risk
- Let’s dive into Anthem breach a bit….

Anthem

- Started somewhere around March 2014
- Discovered January 27, 2015
- Announced publicly in February 2015

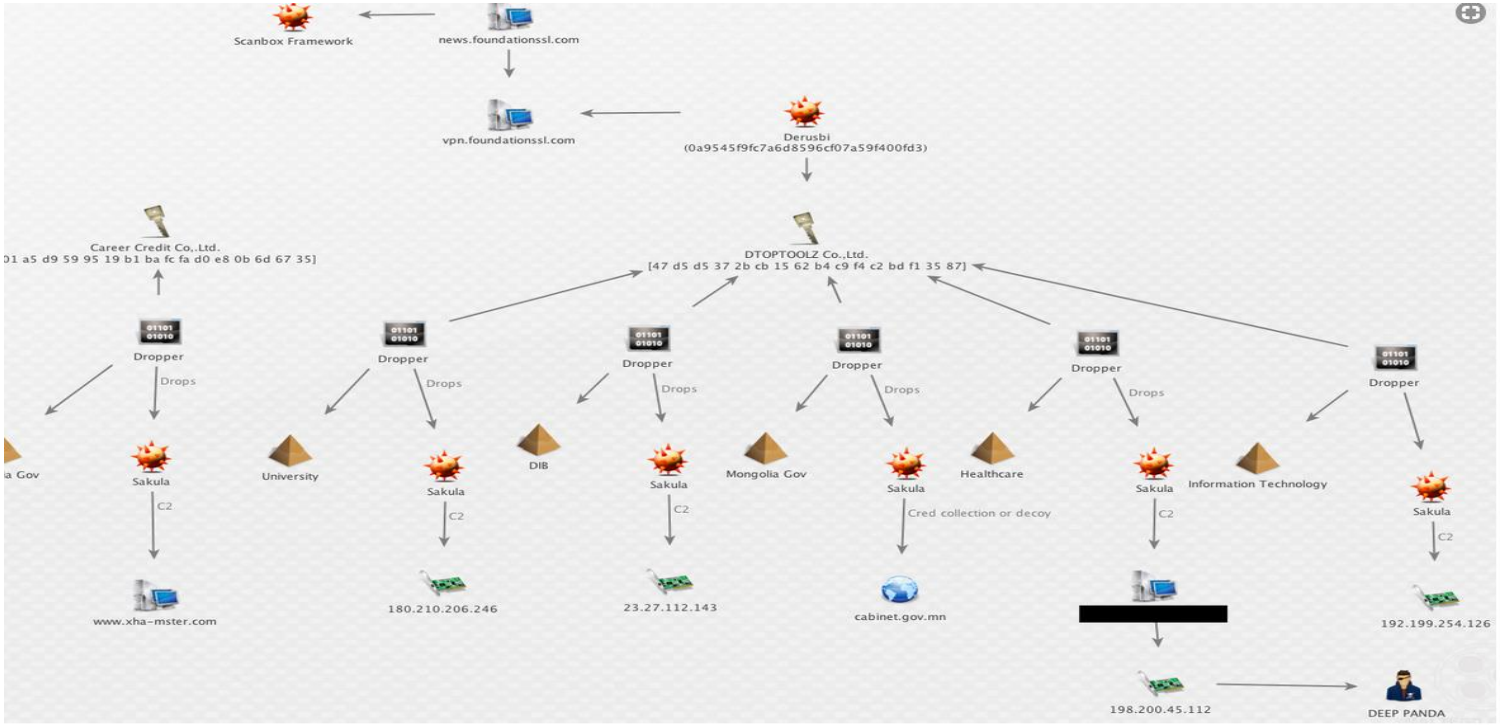
Anthem – Reconnaissance

- Many months if not a year or more
- Not your script kiddies, but most likely nation state or specialized organization
- LinkedIn – looking for job postings to see what kind of systems they have – use that information to find out vulnerabilities
- Reading press releases – knowing name changes
- April 2014 – we11point.com was registered
  - Myhr.we11point.com
  - Hrsolutions.we11point.com
  - Extcitrix.we11point.com
- Extcitrix.we11point.com
  - Remote access via VPN to employees
  - Registered April 22, 2014
  - Certificate signed by DTOPToolZ – compromised machine created

Anthem – The Breach

	2014-04-21	2014-04-22
1	Domain Name: WELLPOINT.COM	Domain Name: WELLPOINT.COM
2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	Registrar URL: http://www.godaddy.com
5	Update Date: 2014-04-21 03:13:19	Update Date: 2014-04-21 03:21:23
6	Creation Date: 2014-04-21 03:13:19	Creation Date: 2014-04-21 03:13:19
7	Registrar Registration Expiration Date: 2015-04-21 03:13:19	Registrar Registration Expiration Date: 2015-04-21 03:13:19
8	Registrar: GoDaddy.com, LLC	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.480-624-2505	Registrar Abuse Contact Phone: +1.480-624-2505
12	Domain Status: clientTransferProhibited	Domain Status: clientTransferProhibited
13	Domain Status: clientUpdateProhibited	Domain Status: clientUpdateProhibited
14	Domain Status: clientRenewProhibited	Domain Status: clientRenewProhibited
15	Domain Status: clientDeleteProhibited	Domain Status: clientDeleteProhibited
16	Registry Registrant ID:	Registry Registrant ID:
17	Registrant Name: wen ben zhou	Registrant Name: ad fire
18	Registrant Organization:	Registrant Organization:
19	Registrant Street: wen ren zheng fei ren chun 120hao	Registrant Street: fdsbcacfdt43
20	Registrant City: xiamen	Registrant City: new
21	Registrant State/Province: fu jian	Registrant State/Province:
22	Registrant Postal Code: 366115	Registrant Postal Code: 366512
23	Registrant Country: China	Registrant Country: Cayman Islands
24	Registrant Phone: +86.5925035801	Registrant Phone: +65.561235001
25	Registrant Phone Ext:	Registrant Phone Ext:
26	Registrant Fax:	Registrant Fax:
27	Registrant Fax Ext:	Registrant Fax Ext:
28	Registrant Email: e59e@qq.com	Registrant Email: admin@wellpoint.com
29	Registry Admin ID:	Registry Admin ID:
30	Admin Name: wen ben zhou	Admin Name: ad fire
31	Admin Organization:	Admin Organization:

Anthem – The Breach



Anthem – The Breach

- Thought to have started around March/April 2014
- Attack Vectors
  - Phishing
    - Emails asking for user information
    - Escalated privileges through Attack Pivots
    - Attack Pivots led to Attack Escalation
  - Vulnerability Exploitation
    - Known vulnerabilities
    - Most likely after successful Phishing campaign
  - Custom Tools
- Slow extraction of information
- Potentially allowed for secondary attackers (Espionage as a Service; EAS)

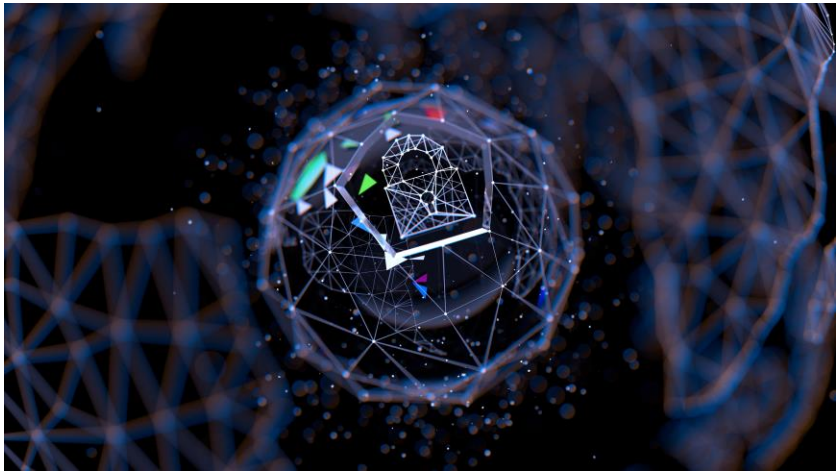
Anthem – Discovery of Breach

- Inadvertently and probably a bit lucky
- IT team member noticed his account already had login session
- Actually took notice and did some digging

- NOTE: wasn’t technical solution per se, but human diligence or awareness and actually taking action

Advanced Persistent Threat

- Cyberattack performed by nation-states and very skilled hackers
- Utilize multiple methods
- Specific target
- Steal data for political espionage or financial gain
- Usually long timeline



Advanced Persistent Threat

- Six “Steps” of APT attack
  - Reconnaissance
  - Gain access to network
  - Network probing
  - Establish multiple entry points
  - Gather target data
  - Data exfiltration

Advanced Persistent Threat

- 5 signs you may have been hit by APT
  - Elevated Late Night logins
  - Widespread backdoor Trojans
  - Unexpected Information Flows
  - Unexpected data bundles
  - Focused spear phishing campaigns

What can you do?

- Get your C-level folks on board and understand
- Download CIS top 20 Controls and take unbiased look
- Encrypt your data at rest and in transfer
- Identify your CVD – Risk-Based Management approach
- Identify any contractors, BAs, vendors; vet your supply chain
- Incident Response Plan
- Educate your staff
  - Human error consists of 27% of breaches
  - Phishing (attacking the human) has been estimated to be responsible for 90% of all major breaches in the last 5 years

Lasting Thought

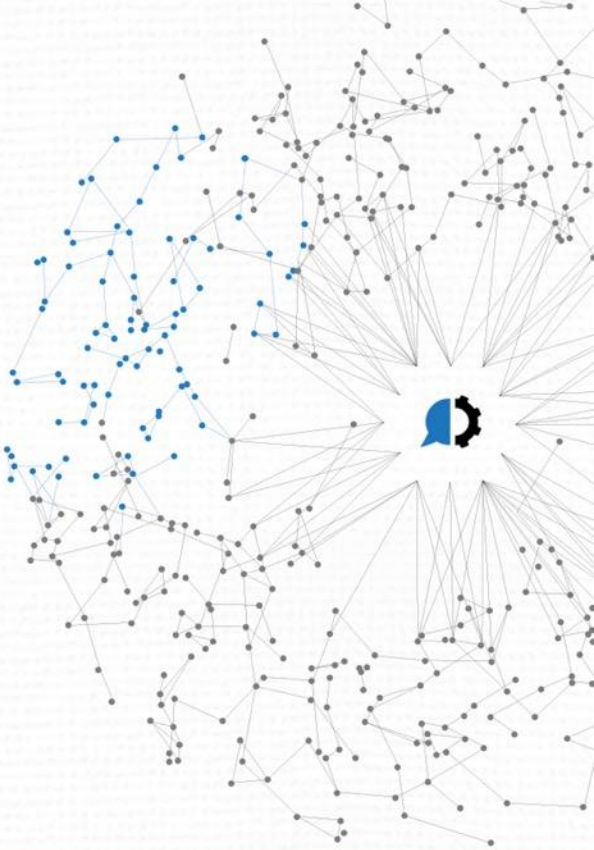
- Anything with computer chip can technically be hacked
- Cars, hospital equipment (life support systems), infrastructure
- Headlines could change from “Record Data Breach at 5 Billion Accounts” to “Record Number of Lives Lost in Latest Hospital Attack!”

Thank you for attending!

What's next?

- **Tell us what cybersecurity challenges you're facing.** Take the quick survey that pops up after the webinar. You can also share feedback on today's presentation.
- **Join our next webinar** April 17 on "How to Avoid Data Breaches with GoAnywhere." Register at http://bit.ly/data-breaches-webinar
- **Let us know how we can help you!**
  - dan.freeman@helpsystems.com
  - Toll-free: 1-800-949-4696
  - Direct: 402-944-4242

Q&A



UP NEXT