Internet Threats and You

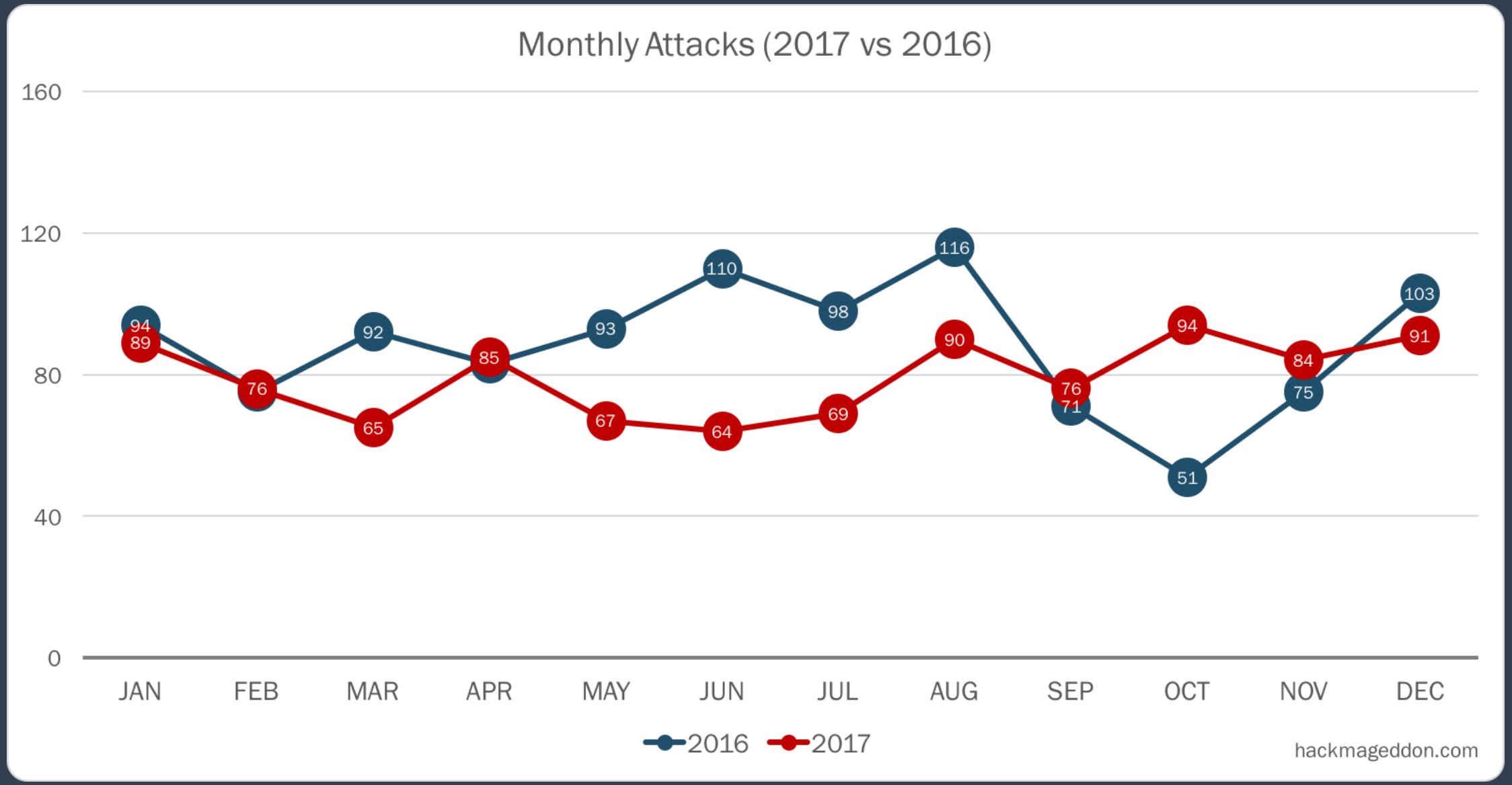
A look back at 2017

Taksati Consulting
Technical Security Services

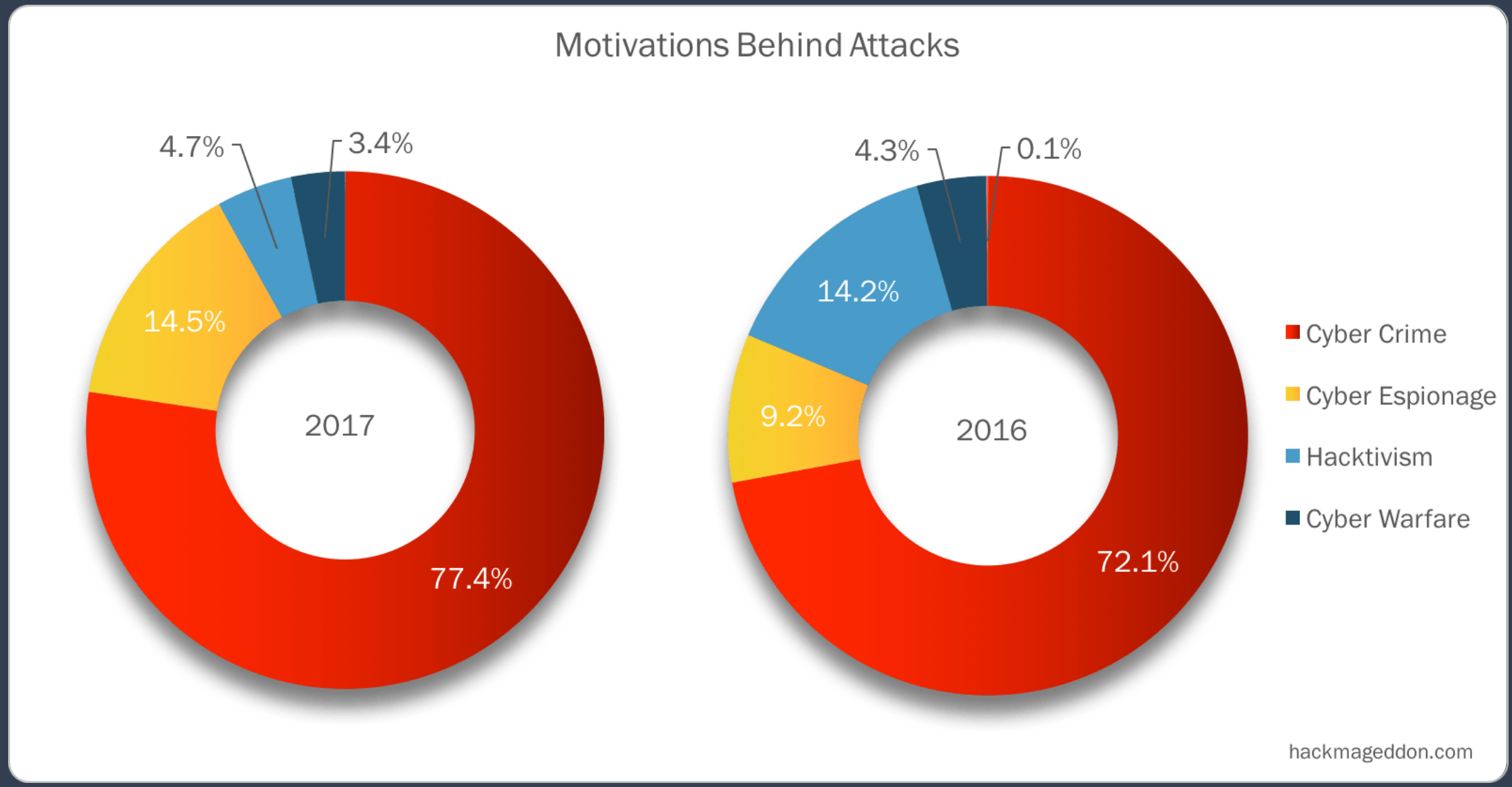
2017 Data Breach Victims

TAKSATI CONSULTING
TECHNICAL SECURITY SERVICES

Average >80 attacks per month



Attack Motivations



Cyber Crime Statistics

GAO's 2015 "Identity Theft and Tax Fraud" report says in 2013

- $24.2B of tax fraud was identified and prevented by IRS
- $5.8B was still paid out to criminals

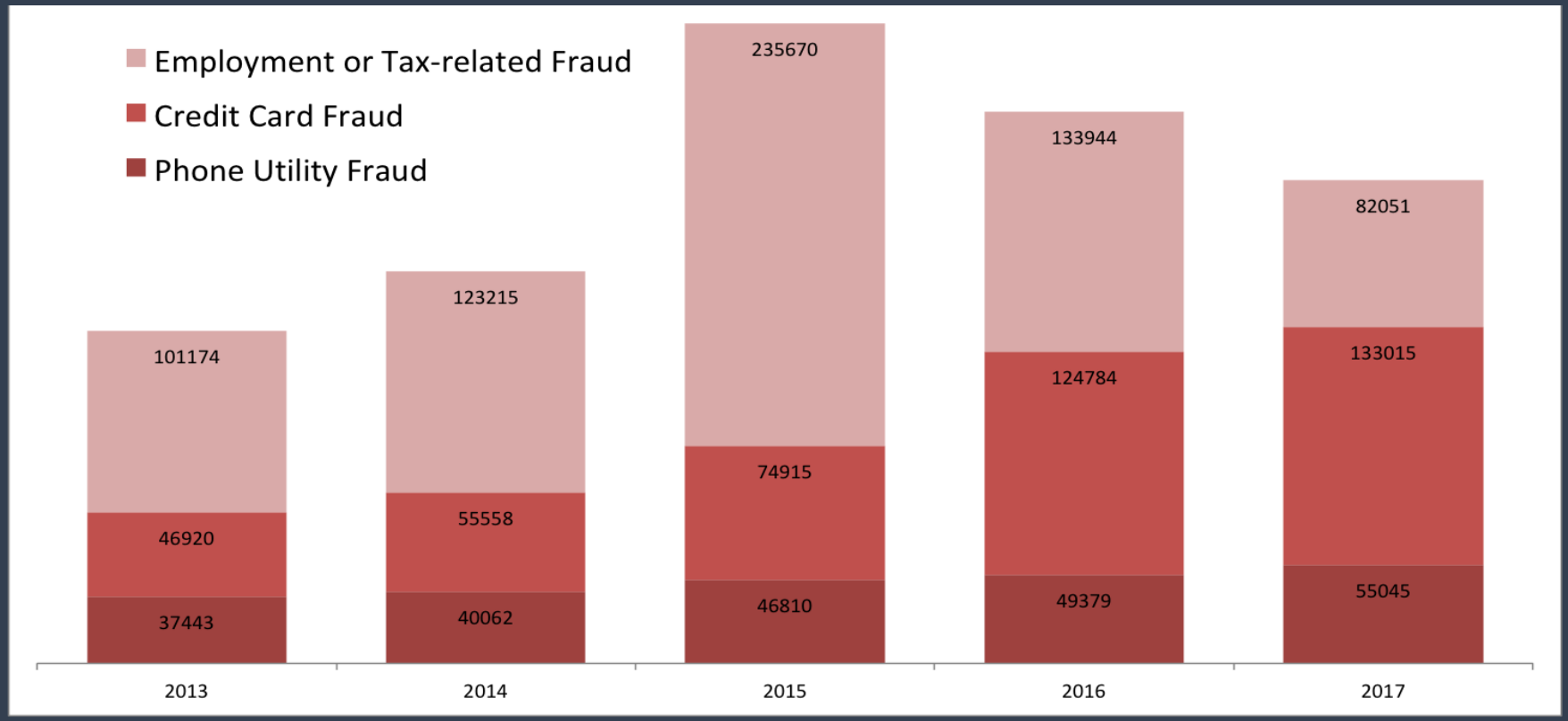
Source: GAO analysis of IRS data. | GAO-15-119

https://www.gao.gov/assets/670/667965.pdf

Cyber Crime Statistics

FTC's "2017 Consumer Sentinel Network Data Book"

- $904M in fraud losses in 2017



https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/main

Cyber Crime Statistics

McAfee/CSIS's 2018 "Economic Impact of Cybercrime" report says

- $445-$608B is total potential cost of cybercrime globally
- >6K criminal online marketplaces selling >45K different products
- 300K-1M new malware samples released every day
- A $60/day botnet can inflict as much as $720,000 in damages
- FBI reports >$5B stolen from >22K companies through BEC

https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

E-Sports Entertainment Association

ESEA hacked, 1.5 million records leaked after alleged failed extortion attempt

More than a million players have been affected by this incident

- January, 2017
- Breach exposed 1,503,707 customer records
  - including first and last name, email, city, state, zip code, phone number, username, password hash, registration date, last login, date of birth, website, Steam ID, Xbox ID, PSN ID – 90 fields in all
- Breach exposed some details of their game network configuration
- Attacker demanded ransom of $100k to NOT release or sell the data
  - They refused to pay it and instead notified the FBI
- Caused by exploit of an undisclosed vulnerability in custom software running their website registration database

https://www.csoonline.com/article/3155397/security/esea-hacked-1-5-million-records-leaked-after-alleged-failed-extortion-attempt.html

LeakedSource.com

- The ESEA data was released via LeakedSource.com
- This site aggregated breach data for easy searching and download
- Users could access raw breach data for a fee
- Ran by Jordan Evan Bloom (27), seen here ->
- Arrested by Canada's RCMP in Jan 2017
- Investigations are still ongoing
- Many find it suspicious that ESEA data was only available via this site

E-Sports Entertainment Association

Lesson Learned:

- Don’t pay ransom – there is no guarantee data won’t still be released
- Quality Breach Notification – ESEA was quick and clear in notification to users and published updates with just right amount of detail
- Notify the authorities

- Secure coding practices to close holes before they become problems
- Vulnerability scanning to identify problems asap

Equifax

Home > Newsroom > In the News > 2017

Massive Equifax Data Breach Could Affect Half of the U.S. Population

- September, 2017
- Breach exposed credit reports for 143 Million consumers
- Caused by exploit of an unpatched vulnerability in an Apache server
- Patch had been available for 4 months prior to date of exploit

https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686

Equifax


Equifax's massive 2017 data breach keeps getting worse

- Update from October 2017, 2.5M more consumers affected, 145.5M
- Update from March 2018, 2.4M more consumers affected, 147.9M

Equifax

Lesson Learned:

- Patches save lives!
- Good PR can make/break the reputational damage of an incident

Deep Root Analytics

Astonishing Level of Ineptitude Exposed in RNC Breach

NEWS ANALYSIS: Records of nearly every voter in the U.S. were found unprotected on the internet, freely exposing sensitive personal data to anyone.

- June, 2017
- Breach exposed detailed PII on 198M American voters, 3/5th population
- Data was compiled for Republican National Committee by Deep Root, TargetPoint, and Data Trust; hosted by Deep Root
- Data was stored in a **PUBLICLY ACCESSIBLE** AWS S3 BUCKET

- Just one of dozens of examples of private data found in public buckets

http://www.eweek.com/security/astonishing-level-of-ineptitude-exposed-in-rnc-breach

The Year of Living ~~Dangerously~~ Publicly

- …
- July, Dow Jones exposed 2.2M customers' data including PII, last four CC #, risk profiles
- July, WWE marketing data collected by 3rd-party firm exposed data of 3M fans
- August, Nice Systems exposed 6M Verizon customer service call records
- August, Groupize exposed hotel/air booking data, to include customer payment details
- September, Viacom MCS data exposed internal IT operational details
- September, Time Warner Cable exposed 600GB of data on 4M subscribers
- October, Accenture exposed 4 buckets with >140GB of customer data
- October, SVR Tracking exposed GPS tracks for >500k vehicles + passwords
- November, INSCOM stored Top Secret//NORFORN data publicly + private keys
- November, Australian Broadcasting Corp (ABC) kept stock photos, passwords, db
- …

https://news.google.com/news/?q=data+breach+public+s3

Other Public S3 Buckets

- HTTPCS conducted scan in Feb 2018 and
  - Discovered over 100k buckets
  - Of the discovered buckets, 10% were public
  - Of those public buckets, 58% were readable
  - Of those public buckets, 20% were writable
  - Of those writable buckets, 95% were not empty

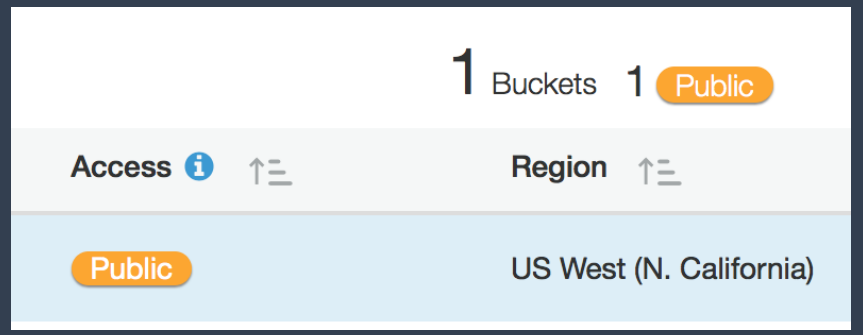
- This is AFTER a year of shaming public S3 in the news

Just Say No to Public S3 Buckets

Lesson Learned:

- Unless the goal is providing public download links,
- There is **NO** reason for data to be stored in publicly accessible buckets
- AWS S3 buckets have no connectivity by default
  - Someone specifically selected “I don’t care if the whole world reads this”

- AWS now displays warnings in console:



Uber

- Occurred in October, 2016; Disclosed in November, 2017
- Breach exposed contact details on 57M users, and DL# of 600K drivers
- Caused by gaining access to GitHub account; found username/pass to AWS in source code; accessed AWS to download data
- Paid $100k to the attackers
- No notification to users or drivers for over a year
  - New, incoming CEO disclosed it as part of cleanup of various scandals

Uber

Lessons Learned:

- Two-Factor Authentication on cloud apps
- Audit source code for credentials – avoid it!
  - Credentials in code should be encrypted, obfuscated, protected
- Not disclosing breach violated FTC rules, multiple state/federal laws
  - Soon GDPR will fine big for this
- Data Security and Breach Notification Act introduced in wake of this
  - Still waiting on a vote
  - Proposes jail time and fines for executives if no breach notification

Top Recommended Security Controls

1. Device and Software Inventory
   - You can’t secure what you don’t know
2. Patch Applications and Operating Systems
   - Apply all patches, updates, upgrades ASAP
3. Strong Authentication on Cloud Services
   - No publicly accessible data unless you mean for it to be public; two-factor auth is your friend
4. Limit Admin Access
   - As few local and domain admins as possible limits malware effects
5. Network Segmentation
   - Limit and control flow of network traffic to minimize impact of malware outbreak

Questions?

Chris Taylor

Taksati Consulting

https://taksati.org | info@taksati.org

Remember:

We can fight together, or you can die alone