Why Hackers Love Your Database

Michael Solomon
Solomon Consulting Inc.

PUG CHALLENGE EXCHANGE AMERICAS

Introduction

- Michael G. Solomon
- Solomon Consulting Inc.
  - OpenEdge, Roundtable, Security architecture
    - Since 1988 (Progress Version 4)
  - CyberSecurity Simulation attack team leader
    - Penetration testing, attack detection and response
- Emory University
  - Security and Privacy research
  - Private location proximity detection .

A few questions we'll cover

- What are hackers after?
- Why is your data so attractive?
- Why target databases?
- Who are the hackers anyway?
- Can you hide?
- What is the best defense? .

Setting the stage - few recent attacks

- Easy to find publicized data breaches
  - Starbucks
  - Target
  - IRS
  - Home Depot
    - Just filed to dismiss customer data breach case)
  - Evernote
  - Living Social
  - many, many more
- Most breaches involve databases
  - And the applications that access them .

http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html
https://www.ibtimes.co.uk/starbucks-customer-accounts-hacked-through-smartphone-apps-1501118
http://www.welivesecurity.com/2015/06/02/home-depot-calls-court-dismiss-consumer-data-breach-case/

Chronology of breaches

www.privacyrights.org/data-breach/new

PUG CHALLENGE AMERICAS EXCHANGE

http://www.privacyrights.org/data-breach/new

Extortion attack

- Dominos (2014)
- Attackers stole details of 650,000 customers
  - Belgium and France
  - Stolen data included PII
- Purpose was to extort around $40,000
- Failure to pay would result in posting all stolen data
- Dominos didn't pay .

https://nakedsecurity.sophos.com/2014/06/16/dominos-pizza-hacked-customer-database-held-to-ransom/#comments

More common attacks

- Credit card info
- Best place to find lots of people with good credit cards?
  - Hotels!
- 38% of credit card hacking occurs at hotels
- Most hotel attacks occur at point-of-sale or the database .

PUG CHALLENGE AMERICAS EXCHANGE

8

http://www.lockergnome.com/reflections/2010/07/06/hackers-love-to-attack-hotel-databases-to-grab-credit-card-info/

So what are they after?

- Criminals are criminals
  - Don't overthink this
  - All crime has motivating factors
- Primary motivations
  - Greed / financial need
  - Retaliation / inflict harm
  - Publicity / notoriety
  - Power
    - State actors
    - Industrial espionage .

It's getting worse

- Cost of breaches expected to rise to $2.1 trillion annually by 2019
- Average attack costs $6 million
- Some are more
  - Target $162 million
  - Sony Pictures $100 million
  - TJX $250 million
- What about time?
  - Average 170 days to detect an attack
  - Average 45 days to resolve an incident
- CyberTab - https://cybertab.boozallen.com/ .

PUGCHALLENGE AMERICAS EXCHANGE

http://www.computing.co.uk/ctg/news/2408344/the-cost-of-insecurity-usd21-trillion-every-year-by-2019
http://www.securityweek.com/cost-cyber-attacks-jumps-us-firms-study
https://cybertab.boozallen.com/

Why is your data so attractive?

- Personal information is currency to hackers
- Many consumers of PII
  - Identity thieves
  - Organized crime
  - Spammers
  - Botnet operators
- Value of PII
  - Less than 1 cent to over $1 for direct sale
    - Name or email address
    - Phishing, spam, outright identity theft, etc.
  - Pay-per-click for response to spam
  - Rental of botnets (thousands of dollars per hour) .

PUG CHALLENGE AMERICAS EXCHANGE

http://www.cio.com/article/2400064/security0/are-you-at-risk–what-cybercriminals-do-with-your-personal-data.html

Minimum valuable information

- How much information do hackers need to make money?
  - Email address
- Yep, that's it
- Anything else is "icing on the cake" .

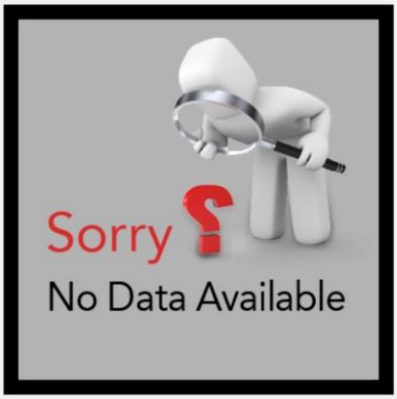
http://www.cio.com/article/2400064/security0/are-you-at-risk–what-cybercriminals-do-with-your-personal-data.html

Hackers leveraging data value

- Some data is more valuable to you than a hacker
- Basis for different types of attacks
  - Extortion / Ransom
  - Embarrassment / Loss of status / Loss of revenue
  - Damage to the organization
- Hacker motivation is generally for publicity or retaliation

- How much would it hurt if your database became unavailable?

- What is your RTO?
  - Recovery Time Objective .



Why target databases?

- Remember the first slide?
- Databases are easy pickings
  - In at least some cases
- Why?
  - All databases have at least one network access path
  - If Internet users can access the database, security becomes “interesting”
- The biggest reason for database attacks
  - Taken as a whole, attacking databases is easy! .

Another uncomfortable truth

- Our focus is all wrong
- For many years (and today), organizations focused on
  - Prevention
  - Protection
- A single successful exploit pierces most control layers
- Prevention and protection NOT ENOUGH!
- Progressive organizations understand the importance of
  - Detection
  - Response .

What hackers know

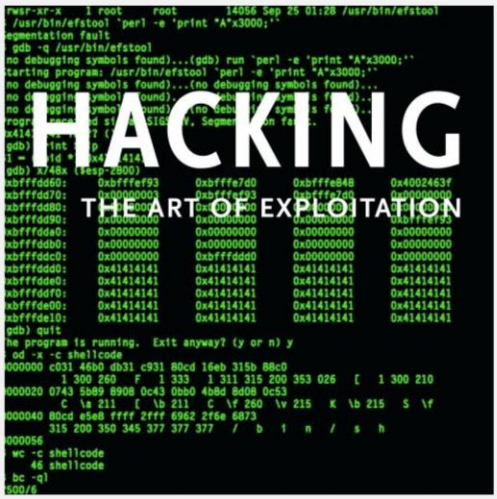
- Database applications are “target rich environments”
- Applications are written by development professionals
  - NOT security professionals

    (I’m sorry, but someone had to say it.)
- Applications routinely “need” hardcoded access to the database
- Hackers can hide data exfiltration in regular traffic
- Cloud databases can make it easier for hackers
  - Compromise your database WITHOUT having to compromise your network
    - Bordering on fear mongering .

http://www.cloudpro.co.uk/cloud-essentials/cloud-security/3639/databases-in-the-cloud-a-new-target-for-cyber-criminals

What hackers do

- Reconnaissance (start with Google, etc.)
  - What are you exposing?
  - OS / infrastructure / services
- Value assessment
  - What looks interesting and of some value
  - Hacker motivation is important here
  - Different for various threat vectors
- Vulnerability search
  - CVE vulnerability database (and others)
- Attack plan
  - How to exploit vulnerabilities
- Attack execution .



PUG CHALLENGE AMERICAS EXCHANGE

http://www.experian.com/blogs/data-breach/2011/09/06/how-hackers-find-their-targets/

Some common database attacks

- Top database attacks
  - Weak/exposed username/passwords
  - SQL (ABL) injection
  - Known vulnerabilities (unpatched)
  - Escalated privileges
  - Broken configuration management
    - Devices, DBMS, Application, etc.
  - Denial of Service (DoS)
  - Backup acquisition
- Many more, but these get us started .

http://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481
http://www.netlib.com/blog/data-protection/The-10-Most-Common-Database-Vulnerabilities.asp
https://www.exploit-db.com/search/

Don't forget about application vulnerabilities

- Applications are generally "trusted entities"
- Legacy user authentication may not be granular enough
- Easy to find stored credentials
  - Easy for .NET assemblies
    - http://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481
  - Easy for OpenEdge r-code …

http://www.codeproject.com/Articles/401220/Why-hackers-love-String-data-type

R-code doesn't mean encrypted!

Procedure Editor - C:\O

File Edit Search Buffer Compile Tools

```
/* dbconnect.p */

DEF VAR dbUserid   AS CHAR NO-UNDO.
DEF VAR dbPassword AS CHAR NO-UNDO.

ASSIGN
    dbUserid   = "appuser"
    dbPassword = "secret".

CONNECT myDB -U dbUserid -P dbPasswor

RUN runapp.p.
```

Proenv

```
C:\OpenEdgex86\WRK>strings dbconnect.r

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

001B00010005utf-8
00000038
MAIN .\dbconnect.p 1,,
ISO8859-1
PROGRESS
undefined
myDB
dbUserid
xH^
dbPassword
xH^
runapp.p
xH^
TXS
dbUserid
dbPassword
appuser
secret
dbUserid
dbPassword
.\dbconnect.p
```

Why is it so easy?

- The attack vectors are well publicized and understood
  - Lots of "Top n Database Attacks" lists
- Easy for even script kiddies to jump in
- Patching all of the holes is hard (costly and time consuming)
- As a result, many databases are soft
  - Unpatched vulnerabilities
  - Default usernames/passwords/services
    - scott / tiger
    - system / manager
  - Permissions are excessive .

http://rabidofficemonkey.com/protect-your-website-ten-things-hackers-look-for-in-a-potential-target/
http://www.abcarticledirectory.com/Article/Auditing-Tools—Why-do-we-need-database-security-/258201

Favorite attacks

- SQL/ABL injection
  - Yes, ABL is vulnerable too!
    - Exchange 2005: INNOV-09
    - "How to Keep Hackers Out of Your Web Application"
- Social engineering
  - Get someone else to do your dirty work
  - Lots of attacks depend on the goodness of people
- Lazy password management
  - Too many passwords to manage!!
  - We all get lazy sometimes
  - Watch out for OE SQL "No Authentication Check"
- Are any of your passwords on the list? …

http://www.hackersonlineclub.com/website-hacking
http://knowledgebase.progress.com/articles/Article/20143

Top 25 worst (most common) passwords

Here is a list of the 25 most common passwords:

1. password
2. 123456
3. 12345678
4. 1234
5. qwerty
6. 12345
7. dragon
8. puss
9. baseball
10. football
11. letmein
12. monkey
13. 696969
14. abc123
15. mustang
16. michael
17. shadow
18. master
19. jennifer
20. 111111
21. 2000
22. jordan
23. superman
24. harley
25. 1234567

Oops! - NSFW

PUG CHALLENGE AMERICAS EXCHANGE

http://www.techsupportalert.com/content/worst-passwords-use-these-and-hackers-will-love-you.htm

Who are the hackers anyway?

- **"If you know the enemy and know yourself, you will not fear the outcome of a hundred battles."**

  Sun Tzu, *The Art of War*

- Hackers have motivation and means to attack
  - Understanding both will allow you to defend
- Motivation (need)
  - Financial, Revenge, Power, Fame
- Means (how good are they)
  - Script kiddie to state player
- Opportunity
  - Internal attackers can be the toughest
- Has your organization conducted a threat analysis? .

http://www.brighthub.com/computing/enterprise-security/articles/5299.aspx

Can you hide?

- No
- Well, maybe a little
- Prepare for attacks from every threat
  - Yes, every threat
  - Risk management 101
- Reduce your attack surface
  - Expose as little as possible
  - Disable/remove unwanted services / close ports
  - Least privilege everywhere
  - Implement low visibility (don't advertise the jewels) .

What is the best defense?

- Industry best practices
  - SANS Critical Security Controls
  - http://www.sans.org/critical-security-controls/
- Plan for prevention and protection, BUT
  - Also plan for detection and response!!!
  - Fire Department responsibilities
- Regularly test your BCP and DRP
- Solid Risk Management
  - Risk assessment
  - Risk response .

http://www.sans.org/reading-room/whitepapers/securitytrends/critical-controls-prevent-red-team-p0wning-database-35397
http://www.sans.org/critical-security-controls/
http://www.computerweekly.com/news/4500247312/The-drivers-and-inhibitors-of-cyber-security-evolution

Takeaways

- Stay current
- Be aware of relevant attack trends
- Understand the value of your data
- Know your environment's attack surface
- Mount the best defense


time for questions


THANK
YOU!