My Preciousss....

Holding on to Your Sensitive Data

Ofer MAOR
CTO
Quotium

@OferMaor

OWASP Israel
Sep 2014

Quotium

WWW.QUOTIUM.COM

Introduction

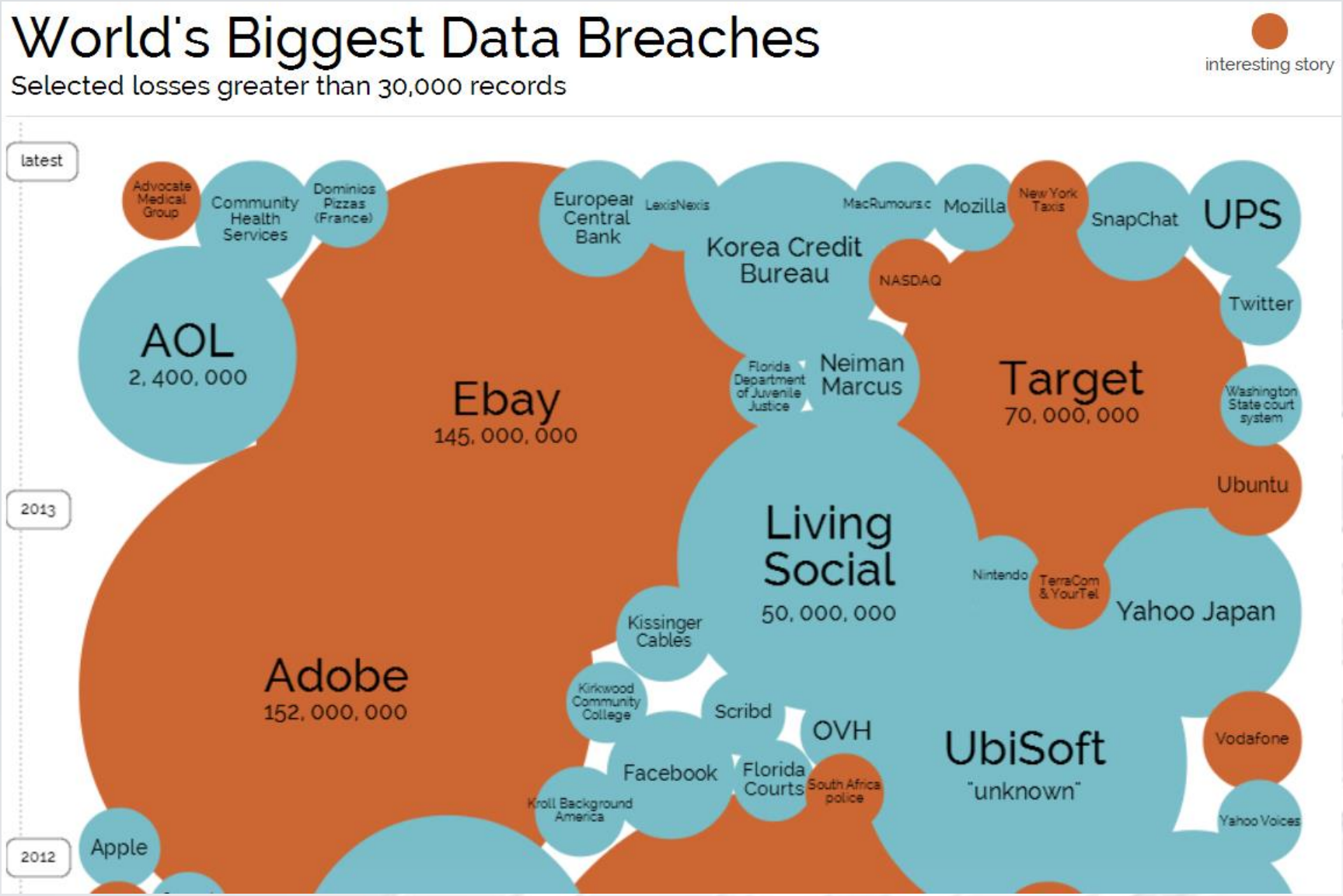
- Incidents
- The Problem
- Runtime Analysis / IAST
- DataHound™ - Free Tool
- Q&A

About Myself

- 20 years in information/application security
  (Over 10 years hands on penetration testing)
- Research, Development, Enhancement
  - Attack & Defense Techniques
  - WAF / AppSec Testing Products
- Regular Speaker in Security Conferences
- OWASP Member, Contributor & Leader

About Quotium/Seeker

- Agile Software Security
- IAST Pioneer - Runtime Analysis Engine
  - Analysis of application **data and code**
  - Exploit verification to classify **risk.**
- Data Oriented Approach
- Adaptive to the Development Process



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

South Korea Credit Card Data Theft Outrage

Legal action is being threatened after millions of South Koreans had their unencrypted credit card details stolen.

2:39pm UK, Tuesday 21 January 2014

Concerned bank customers queue up after the mass data theft was revealed

Thousands of concerned South Koreans have flocked to bank branches after the theft of data linked to 80 million credit cards.

There has been widespread public concern and anger after it was revealed that information including salaries, monthly card usage, credit rating and card numbers had been stolen from three major credit card firms.

sky NEWS

REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

EBay asks 145 million users to change passwords after cyber attack

BY JIM FINKLE, SOHAM CHATTERJEE AND LEHAR MA

BOSTON/BANGALORE Wed May 21, 2014 4:25pm EDT

12 COMMENTS | Tweet Share Sha

ebay™

EBay faces class action suit over data breach

John Ribeiro
@Johnribeiro

Jul 24, 2014 4:44 AM

EBay faces a class action suit in a U.S. federal court over a security breach earlier this year.

The consumer privacy class action lawsuit, filed Wednesday by Collin Green, a citizen of the state of Louisiana, alleged that the security breach was the result of eBay's inadequate security in regard to protecting identity information of its millions of customers.

"The thieves had access to, and reportedly copied, customer names, encrypted passwords, email addresses, physical addresses, phone numbers, and dates of birth, at a minimum," according to the lawsuit filed in the U.S. District Court for the Eastern District of Louisiana.

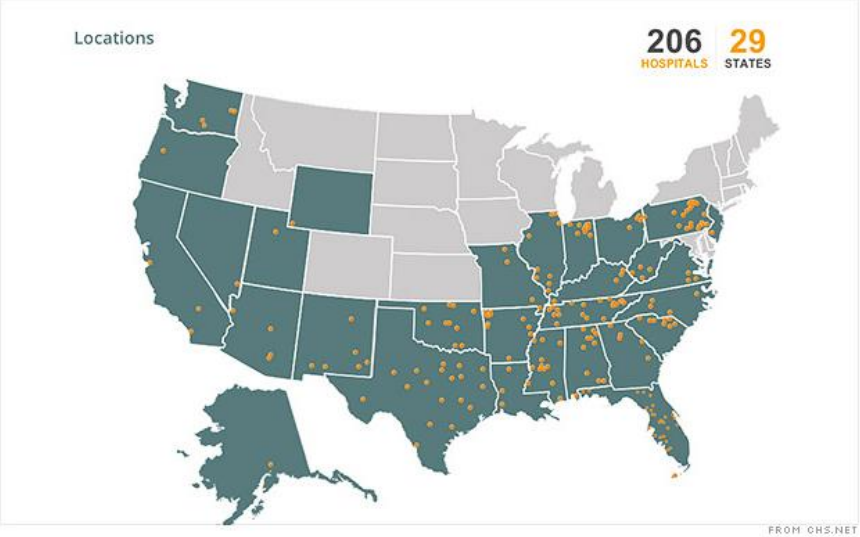
CNN Money

Home | Business | Markets | Investing | Economy | Tech | Personal Finance

The Cybercrime Economy

Hospital network hacked, 4.5 million records stolen

By Jose Pagliery @Jose_Pagliery August 18, 2014: 3:25 PM ET



Hackers have taken 4.5 million Social Security numbers from patients who attended any one of Community Health Systems' 206 hospitals this year.

NEW YORK (CNNMoney)

Community Health Systems, which operates 206 hospitals across the United States, announced on Monday that hackers recently broke into its computers and stole data on 4.5 million patients.

Hackers have gained access to their names, Social Security numbers, physical addresses, birthdays and telephone numbers.

theguardian

News › Technology › Adobe

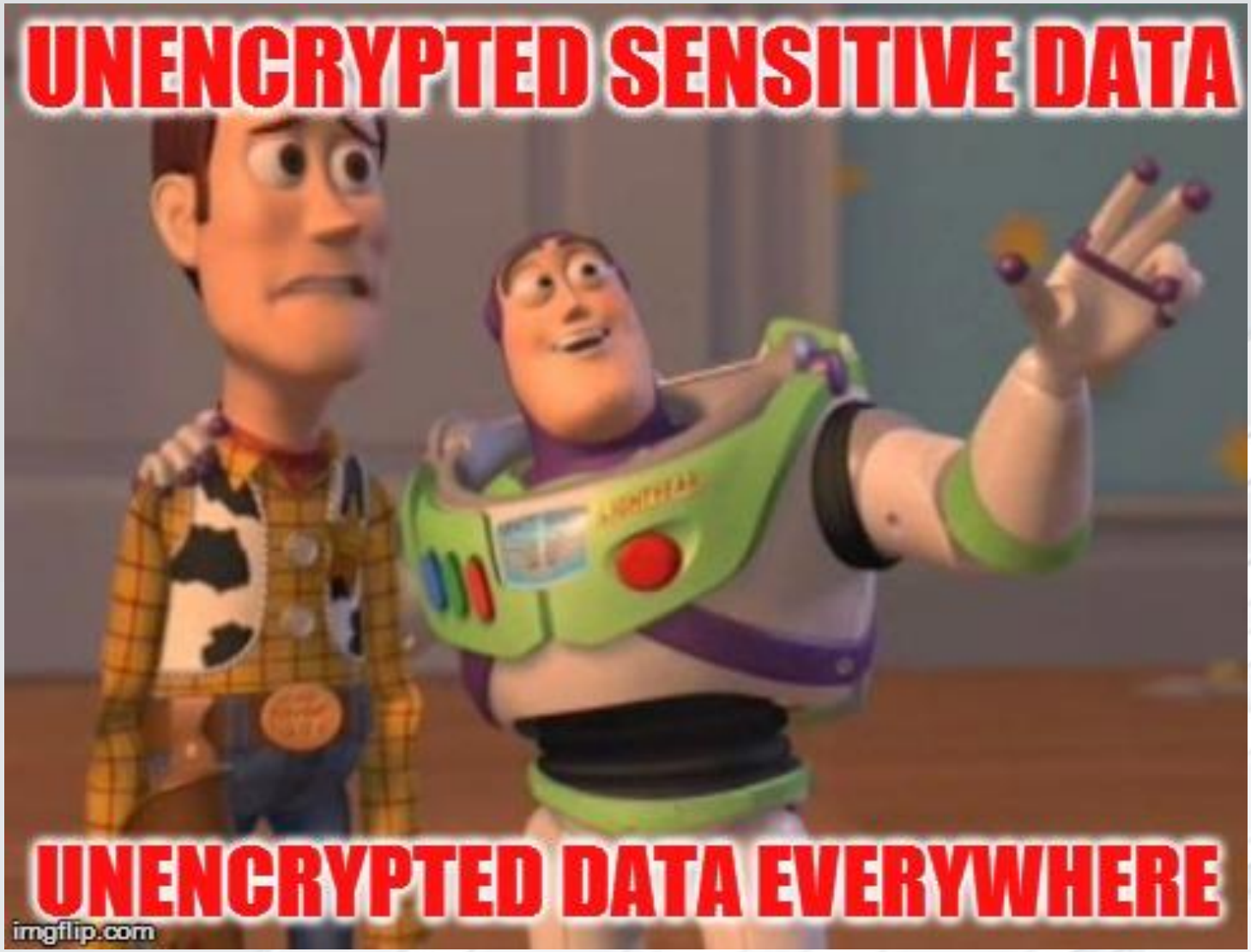
Did your Adobe password leak? Now you and 150m others can check

Leak is 20 times worse than the company initially revealed, and could put huge numbers of peoples' online lives at risk

Alex Hern

Adobe's HQ. The company leaked over 100m users' details. Photograph: PAUL SAKUMA/ASSOCIATED PRESS

Nearly 150 million people have been affected by a loss of customer data by Adobe, over 20 times more than the company admitted in its initial statement last week.


UNENCRYPTED SENSITIVE DATA
UNENCRYPTED DATA EVERYWHERE
imgflip.com

roughly 25 million UCard users, about the breach because it couldn't rule out the possibility that their personal information was among the data removed from its servers.

The bank typically keeps the personal information of its customers encrypted or scrambled, as a security precaution. However, during the course of the breach, personal data belonging to those customers had temporarily appeared in plain text in files the computers use to log activity.

Bad Luck?

Not Really…

The Data Tracking Challenge

- One of the biggest challenges described by information security managers
  - Understanding how data moves in their systems
  - What happens to user data from the moment it enters the application?
- PCI 3.0 also addresses this need for greater understanding of what is happening

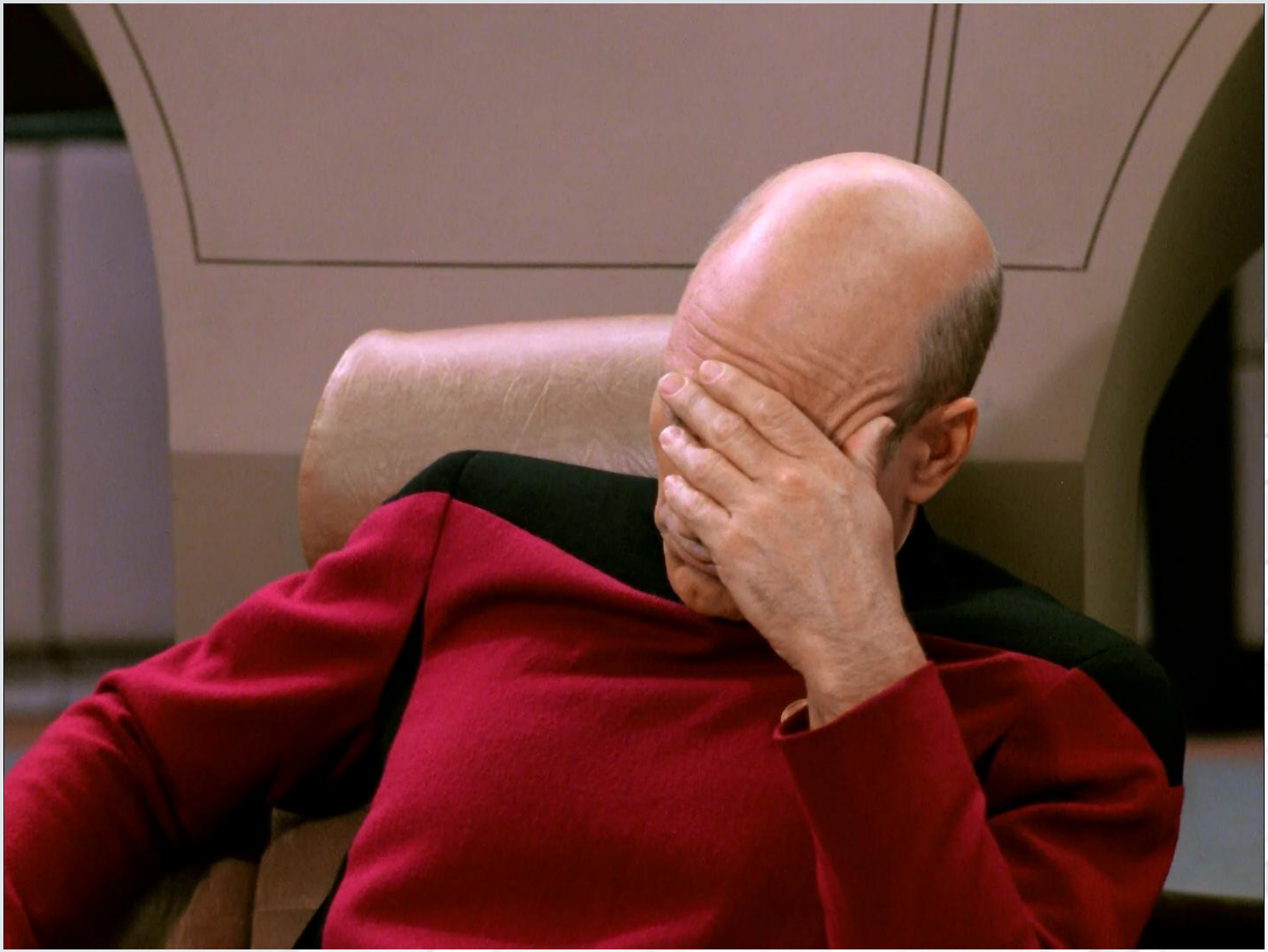
Data Leakage Coding Mistakes

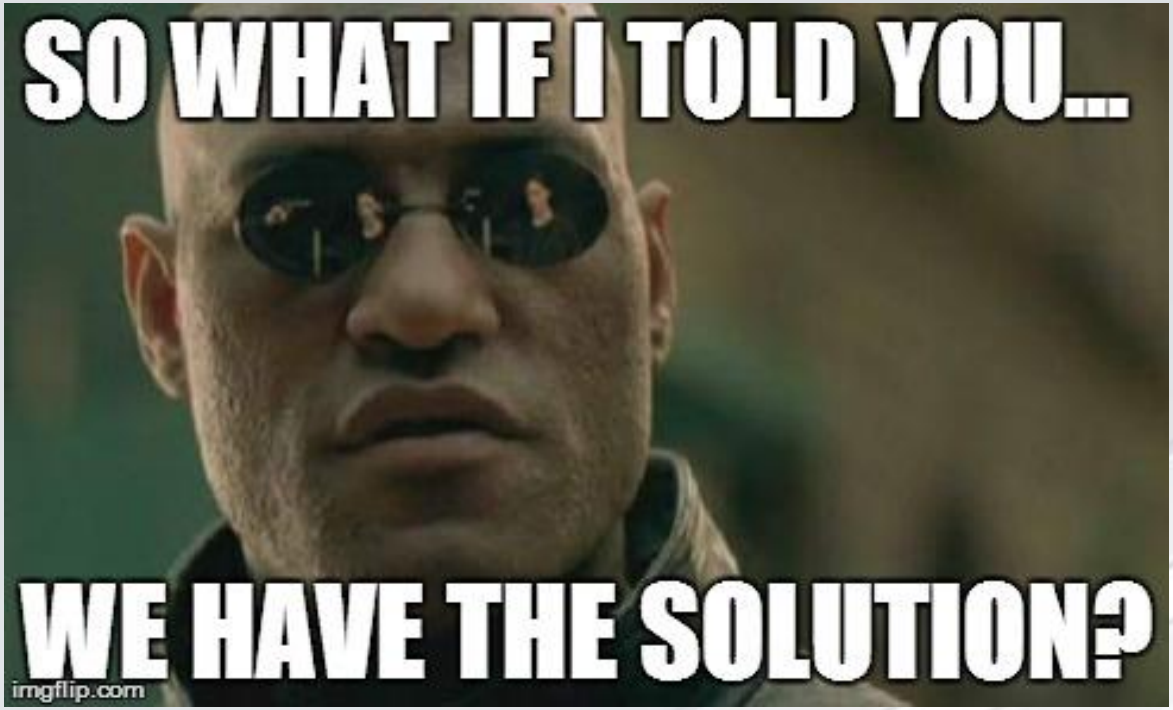
- The Basics – Unencrypted DB/File Storage
  - Passwords
  - Credit Cards
  - Personally Identifiable Information (PII)

    Name, Address, Phone Number, ID Number, SSN, Date of Birth, Place of Birth, Driver's License Num, Vehicle Registration Num, Biometric Info (Fingerprint, Portrait Photo, Handwriting, etc.) Email Address, Username, Nickname/Handle, Digital Identity, etc.
  - Medical Records
  - Financial Information
  - Etc…

Data Leakage Coding Mistakes

- And All the Rest…
  - Unsalted Password Hashing (REALLY?!?!?!)
  - Poor Encryption
  - Cleartext Storage of Encryption Keys / Salt
  - Response Writing
  - Log Files or DB Entries
  - Temporary Files or DB Entries
  - Debug Information Writing
  - Sending to 3rd Party (Intentional / Unintentional)
  - *Storing Unencrypted in Memory (Tricky…)*
  - More…



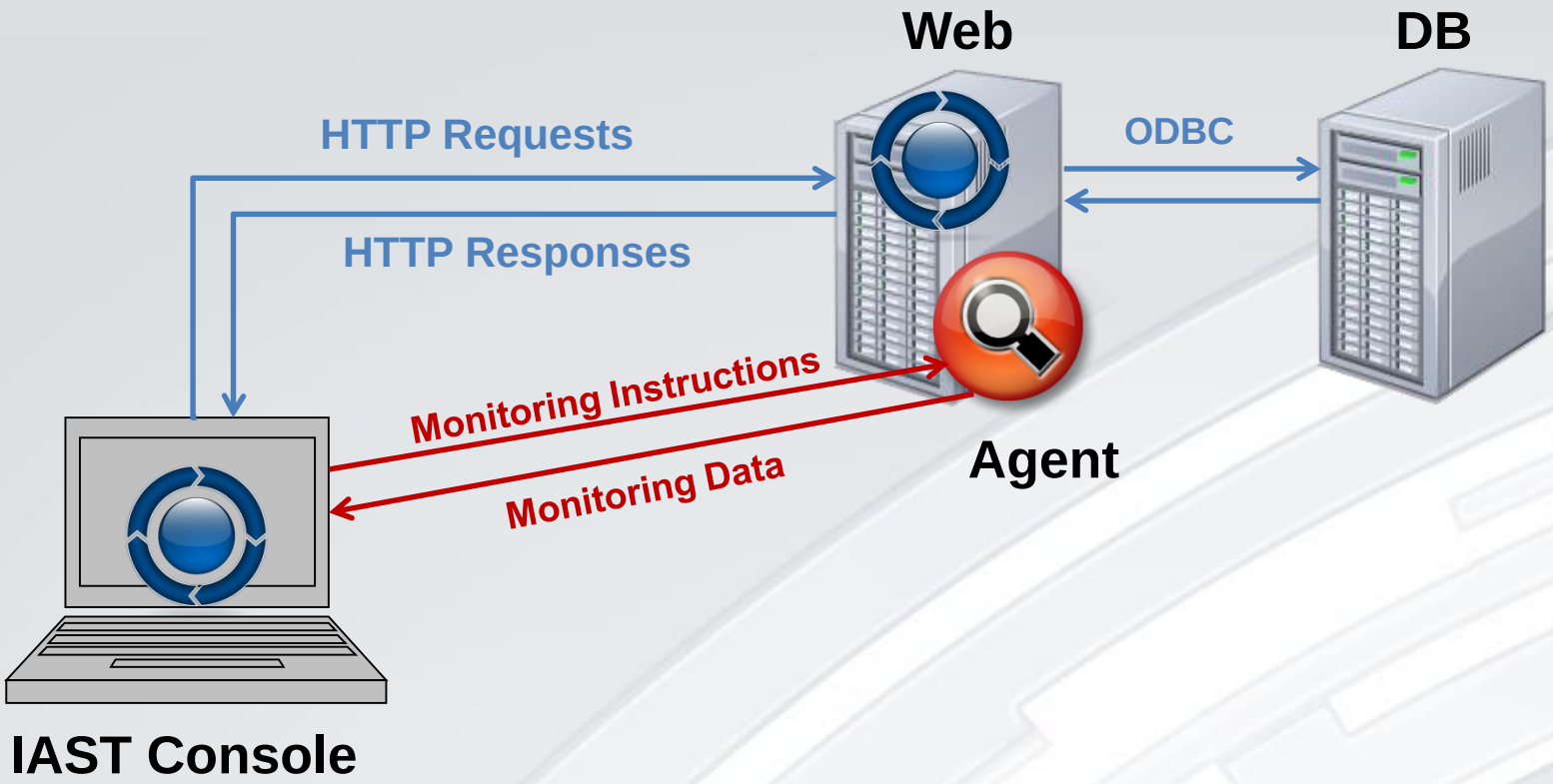


Runtime Data Tracking

Runtime Analysis (IAST) 101

- IAST: Interactive Application Security Testing: Runtime Code (& Data) Analysis Technology
- Analysis of Actual Executed Code
- Can Provide High Visibility to Data
- Observes Code Behavior During HTTP Req/Res

Basic IAST Architecture



IAST Agent Monitoring

- What can be monitored?
  - HTTP Requests End-to-End
  - Parameters Propagation
  - HTTP Response Writing
  - Database/Directory Calls & Responses
  - File System Calls
  - String Manipulations
  - Memory (Like a Watch…)
  - Usage of 3rd party libraries
  - Calls to external applications
  - More…

IAST Agent Monitoring

- How is it monitored?
  - Instrumentation *(No need for source code)*
  - Debugging *(No need for source code)*
  - Modify Runtime Env *(No need for source code)*
  - Aspect Oriented
  - Recode/Recompile
  - Other….
- What can be monitored?
  - Anything… But easier with parsed/partially compiled (.NET/Java/PHP/Stored Procedures/etc.)

Basic IAST

- Focused on tainted input tracking
  - SQL Injections
  - File/OS Injections
  - XSS (Reflected)
  - etc…
- Show vulnerable source code (or reflection)
- Show relevant query/response/etc.
- Coverage monitoring/enhancement
- Interactive Iterative Testing *(Sometimes)*

Example – SQL Injection

- URL

```
/SearchBranch.aspx?p_address=Athens
```

- Source Code:

Assembly Path:C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\luftbank\d5391338\716bda9a\assembly\dl3\36cb53c6\00dde867_5965cb01\Luft.General.DLL

Pseudo source code of execution from Luft.General.GeneralDB.searchBankBranch :

```
        {
                text += " and ";
        }
        text = text + " Address like '%" + p_address + "%'";
    }
    DbCommand sqlStringCommand = database.GetSqlStringCommand(text);

    return database.ExecuteDataSet(sqlStringCommand);

}
```

Example – SQL Injection

- Query Generated (Normal Conditions)

```
SELECT ID,Name,Address FROM Dyn_Branch
WHERE  Address like '%Athens%'
```

- Attack

```
/SearchBranch.aspx?p_address=Athens' and 7 = 8 union select 1,name, 'zFw03'
from (select top 20  name from sysobjects order by name) xxx --
```

- Query Generated under Attack

```
SELECT ID,Name,Address FROM Dyn_Branch
WHERE  Address like '%Athens' and 7 = 8 union select 1,name,'zFw03' from
(select top 20  name from sysobjects order by name) xxx--%'
```

Advanced IAST

End-to-End Data Analysis & Tracking

- **Track Sensitive Data in Application**
- Test Application, not just Code
- Correlation of Separate Code Segments
  - n-Tier Environments
  - Multi-Step Operations
- Data Sensitivity/Accessibility Classification
- Identify Data-Related “Logical” Vulnerabilities

Tracking Sensitive Data

- Monitor All Data Write Operations
  - DB, File, Directory, etc.
- Optional: Monitor All Read Operations
- Track Data Through String Manipulations
- Identify Poor Encryption
- Passive/Interactive
  - Passive: Identify Data by Format (RegEx)
  - Interactive: Also Identify Unformatted Data (Send specific data to be tracked…)
- Show Vulnerable Code

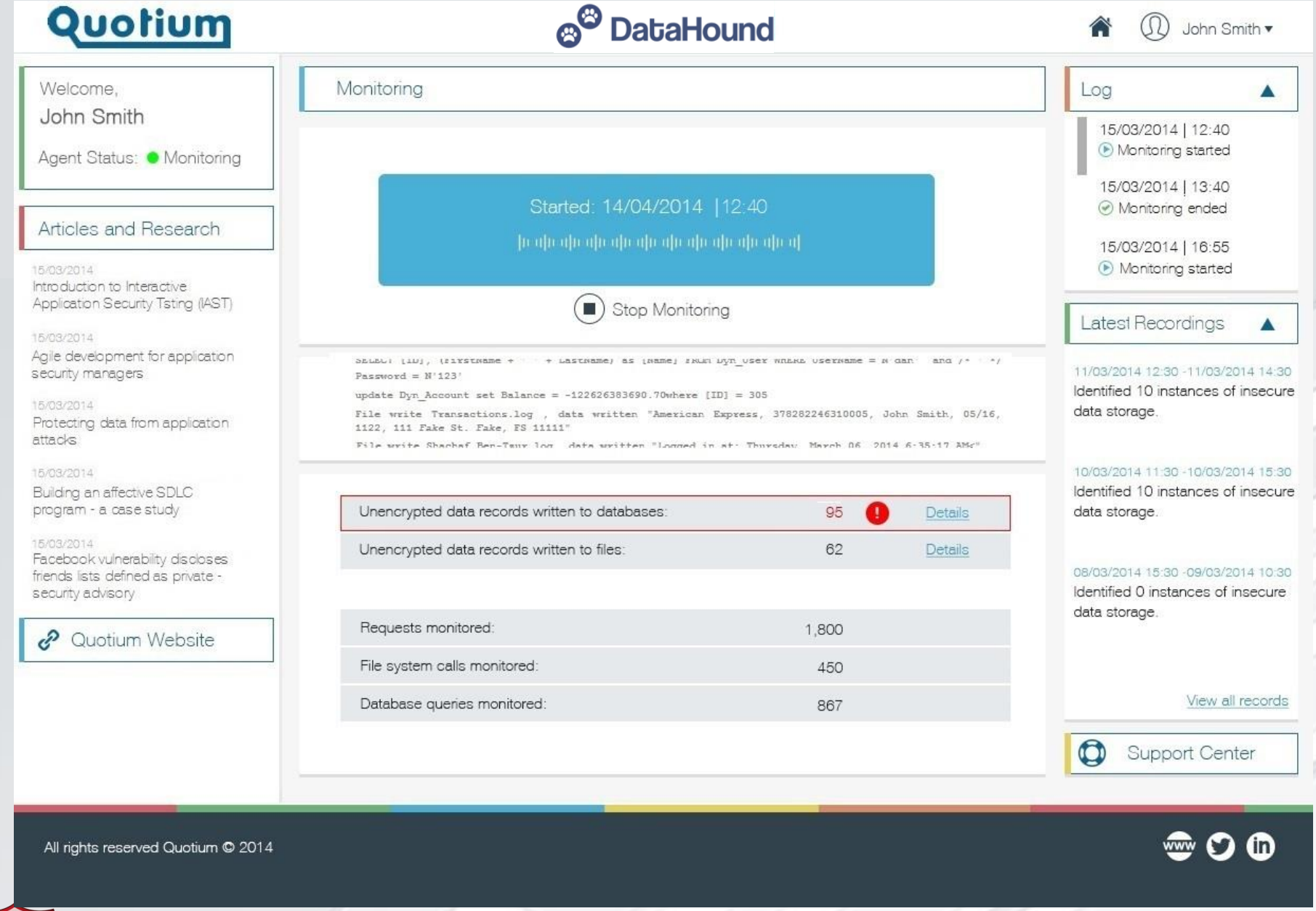
DataHound

By Quotium

DataHound™

- **FREE** Data Tracking IAST Tool
- Identifies Insecure Storage of Sensitive Data
- Shows Relevant Code & Data for Each Breach
- Easy to Use – Download, Install, Run
- Runs in the Background
- Supports .NET & Java
- Tracks Common Types of Sensitive Data

Credit Cards	SSN
Email	Phone Numbers
*Usernames**	*Passwords**


Quotium
DataHound
John Smith
Welcome,
John Smith
Agent Status: Monitoring
Articles and Research
15/03/2014
Introduction to Interactive Application Security Tsting (IAST)
15/03/2014
Agile development for application security managers
15/03/2014
Protecting data from application attacks
15/03/2014
Building an affective SDLC program - a case study
15/03/2014
Facebook vulnerability discloses friends lists defined as private - security advisory
Quotium Website
Monitoring
Started: 14/04/2014 |12:40
Stop Monitoring
Password = N'123'
update Dyn_Account set Balance = -122626383690.70where [ID] = 305
File write Transactions.log , data written "American Express, 378282246310005, John Smith, 05/16, 1122, 111 Fake St. Fake, FS 11111"
Unencrypted data records written to databases: 95 Details
Unencrypted data records written to files: 62 Details
Requests monitored: 1,800
File system calls monitored: 450
Database queries monitored: 867
Log
15/03/2014 | 12:40
Monitoring started
15/03/2014 | 13:40
Monitoring ended
15/03/2014 | 16:55
Monitoring started
Latest Recordings
11/03/2014 12:30 -11/03/2014 14:30
Identified 10 instances of insecure data storage.
10/03/2014 11:30 -10/03/2014 15:30
Identified 10 instances of insecure data storage.
08/03/2014 15:30 -09/03/2014 10:30
Identified 0 instances of insecure data storage.
View all records
Support Center
All rights reserved Quotium © 2014

DEMO

DataHound

By Quotium

Prevent Data Breaches Before They Happen

www.quotium.com/DataHound

Thank You!

Questions?

Ofer Maor
ofer@quotium.com

@OferMaor

Quotium

WWW.QUOTIUM.COM