Cabinet Office

Michael Brunton-Spall
Technical Architect
Government Digital Service
@bruntonspall

Building secure software and keeping it secure in the face of changing requirements

Michael Brunton-Spall GDS

This guidance is in alpha

I am a civil servant

I work for the Government Digital Service

Publishing

Transactions

API's

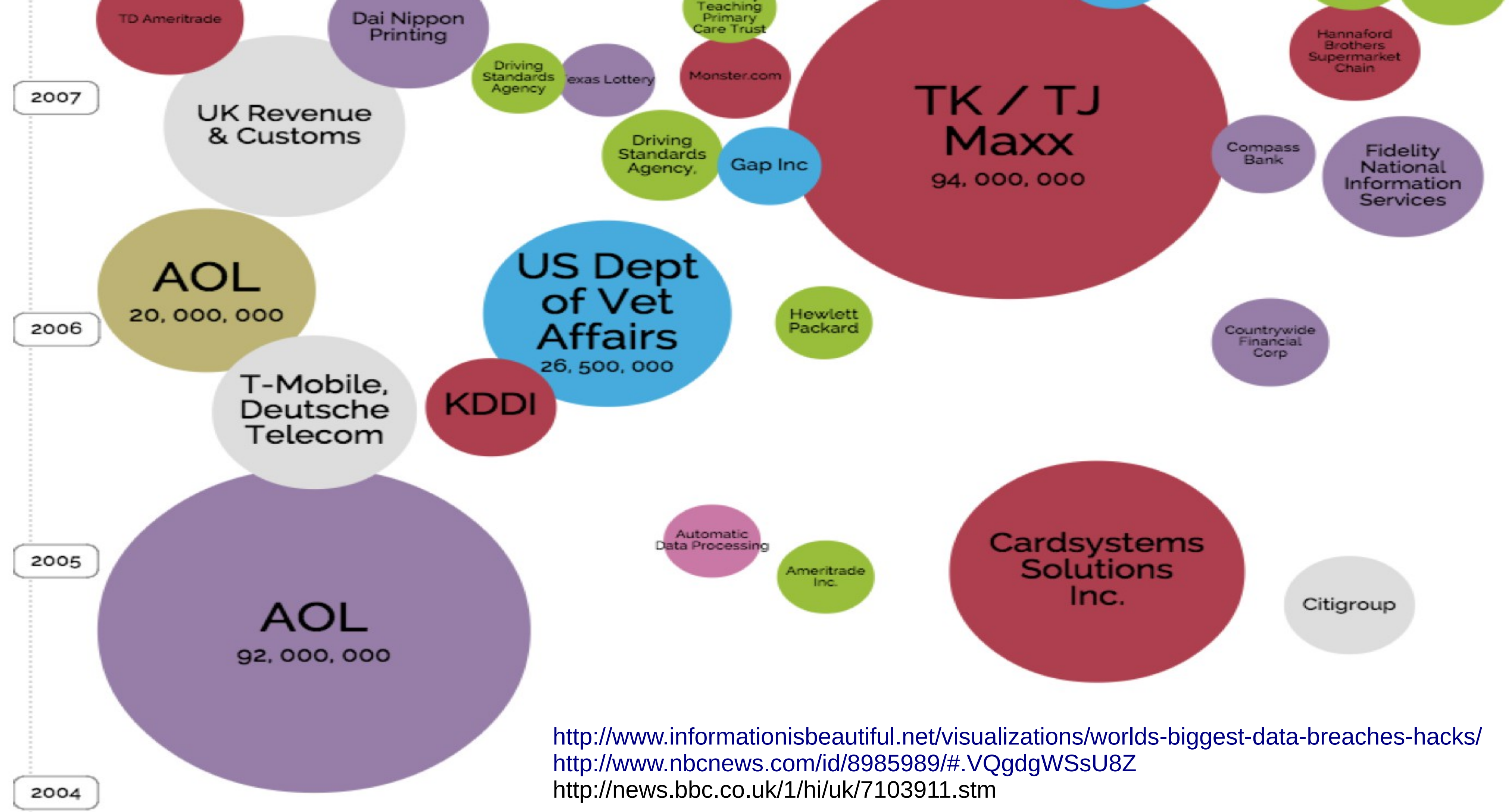
Agile

Security vs Information Risk

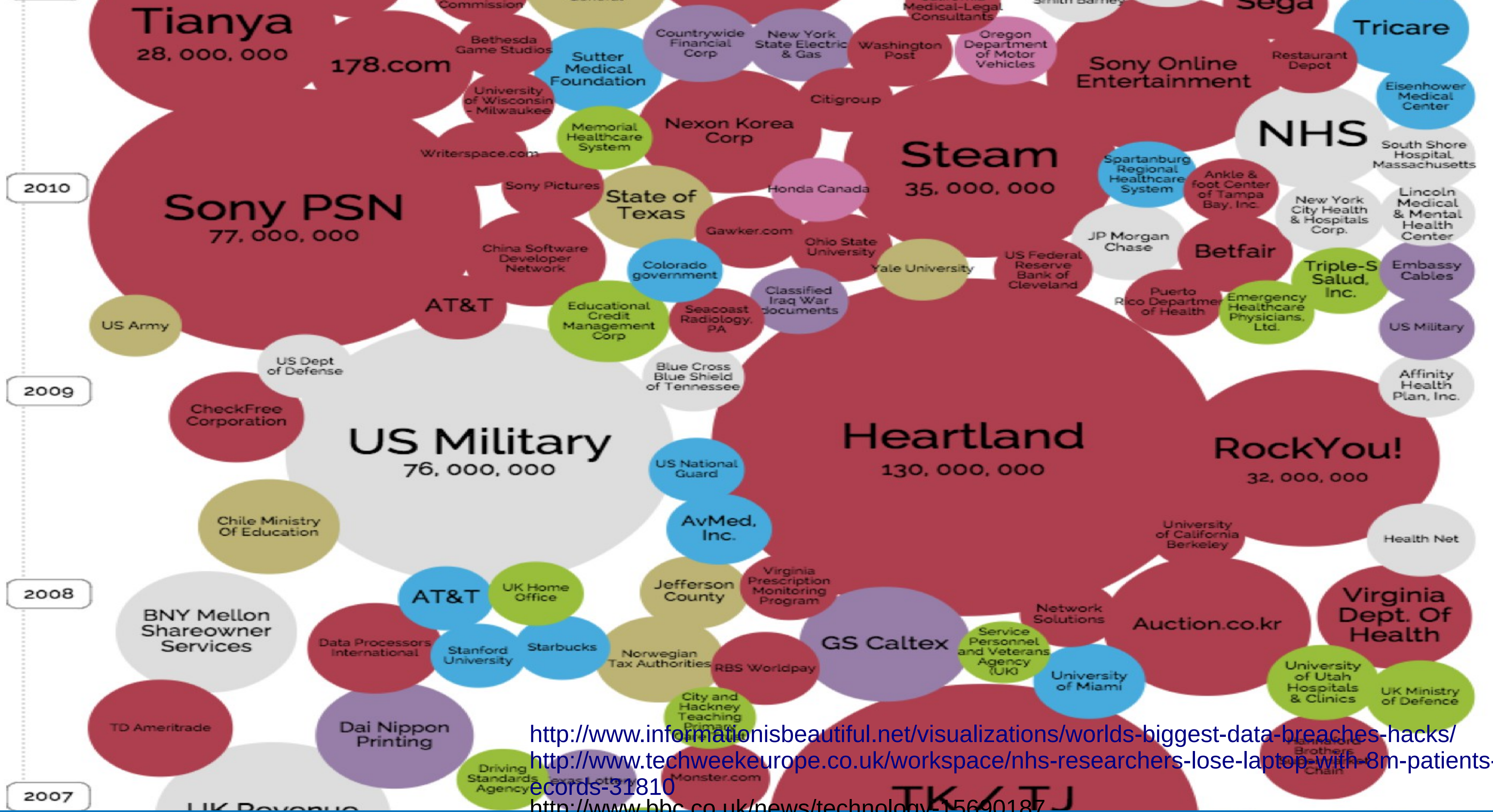
Why bother?

What are the threats?

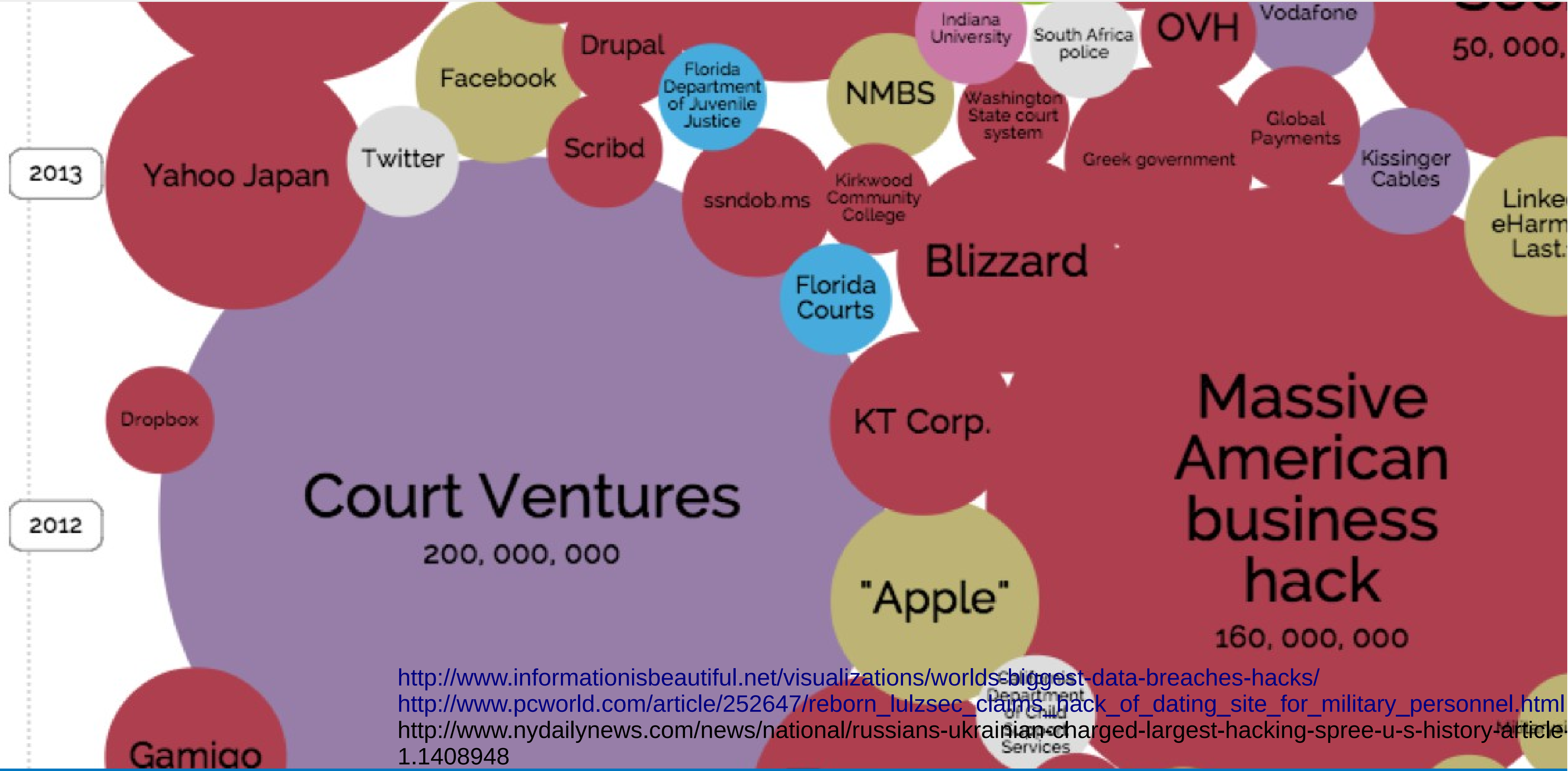
Data loss and theft



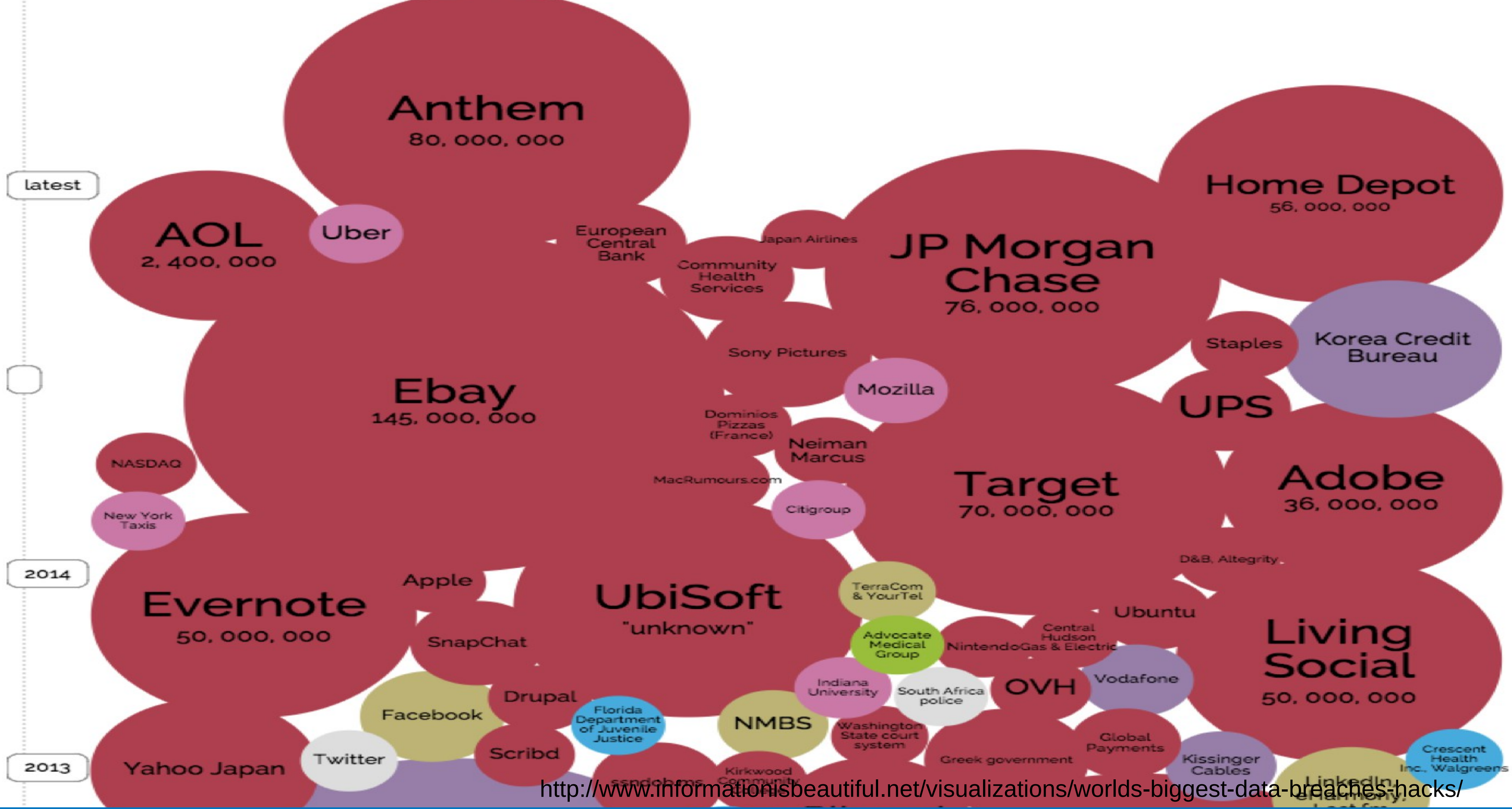
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
http://www.nbcnews.com/id/8985989/#.VQgdgWSsU8Z
http://news.bbc.co.uk/1/hi/uk/7103911.stm



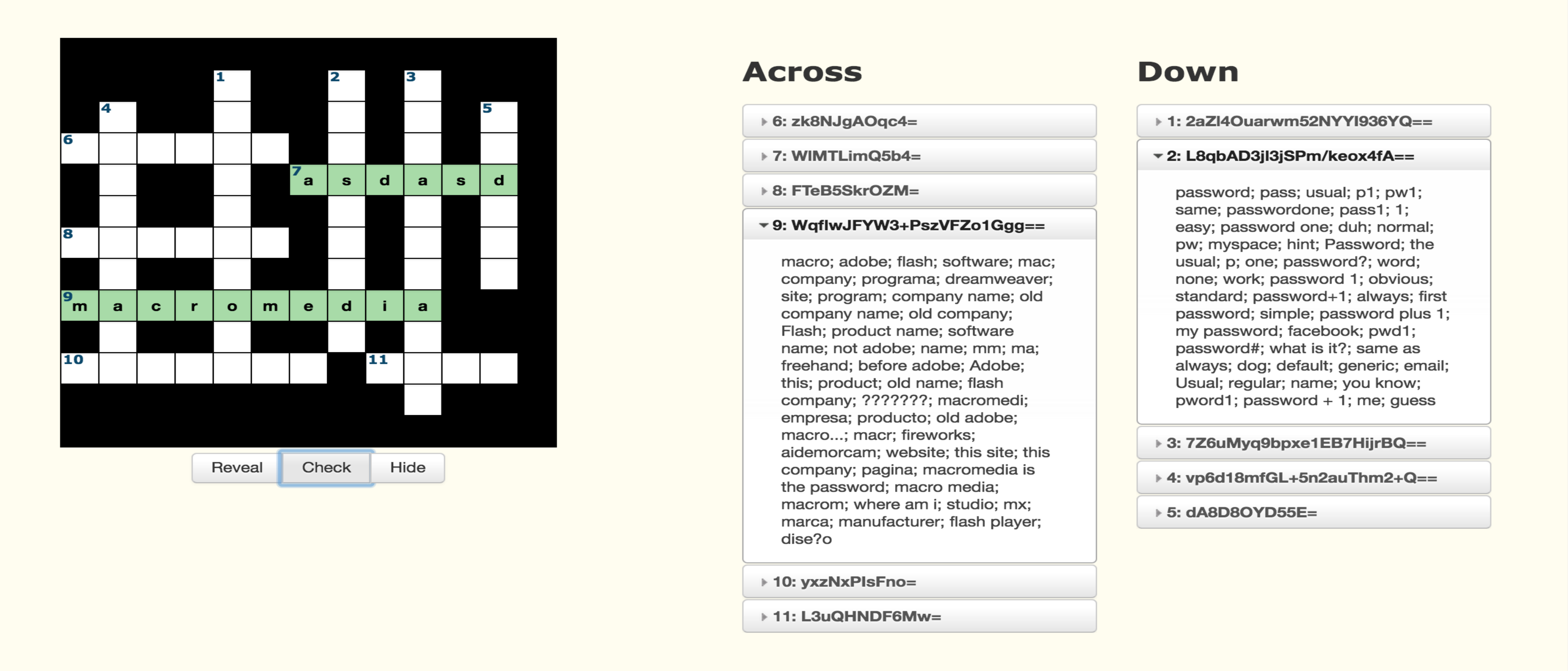
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
http://www.techweekeurope.co.uk/workspace/nhs-researchers-lose-laptop-with-8m-patients-records-31810
http://www.bbc.co.uk/news/technology-15690187



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
http://www.pcworld.com/article/252647/reborn_lulzsec_claims_hack_of_dating_site_for_military_personnel.html
http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948



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



Across

- 6: zk8NJgAOqc4=
- 7: WIMTLimQ5b4=
- 8: FTeB5SkrOZM=
- 9: WqflwJFYW3+PszVFZo1Ggg==

macro; adobe; flash; software; mac; company; programa; dreamweaver; site; program; company name; old company name; old company; Flash; product name; software name; not adobe; name; mm; ma; freehand; before adobe; Adobe; this; product; old name; flash company; ???????; macromedi; empresa; producto; old adobe; macro...; macr; fireworks; aidemorcam; website; this site; this company; pagina; macromedia is the password; macro media; macrom; where am i; studio; mx; marca; manufacturer; flash player; dise?o

- 10: yxzNxPIsFno=
- 11: L3uQHNDF6Mw=

Down

- 1: 2aZI4Ouarwm52NYYI936YQ==
- 2: L8qbAD3jI3jSPm/keox4fA==

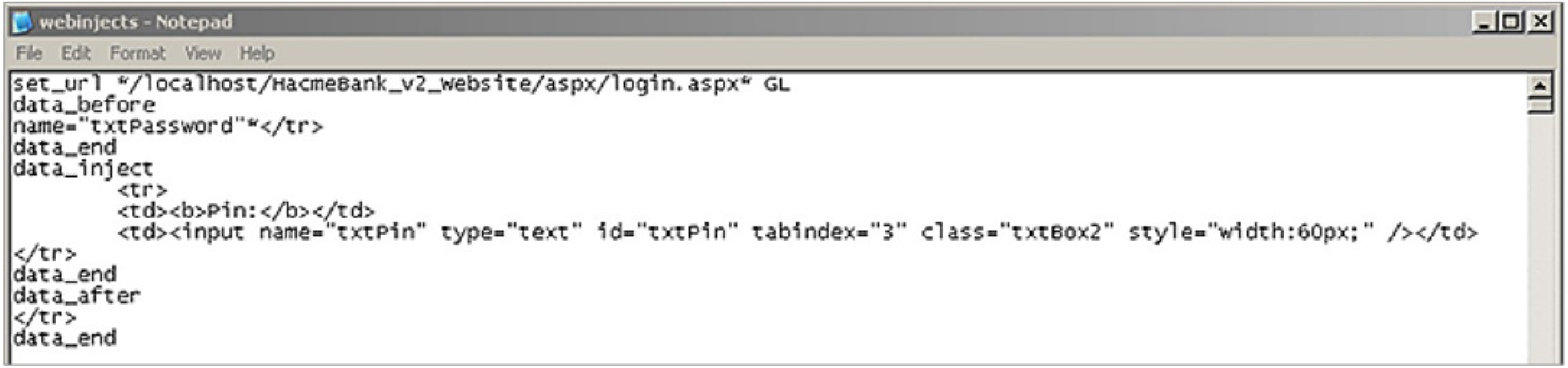
password; pass; usual; p1; pw1; same; passwordone; pass1; 1; easy; password one; duh; normal; pw; myspace; hint; Password; the usual; p; one; password?; word; none; work; password 1; obvious; standard; password+1; always; first password; simple; password plus 1; my password; facebook; pwd1; password#; what is it?; same as always; dog; default; generic; email; Usual; regular; name; you know; pword1; password + 1; me; guess

- 3: 7Z6uMyq9bpxe1EB7HijrBQ==
- 4: vp6d18mfGL+5n2auThm2+Q==
- 5: dA8D8OYD55E=

http://zed0.co.uk/crossword/

Criminal users on the internet

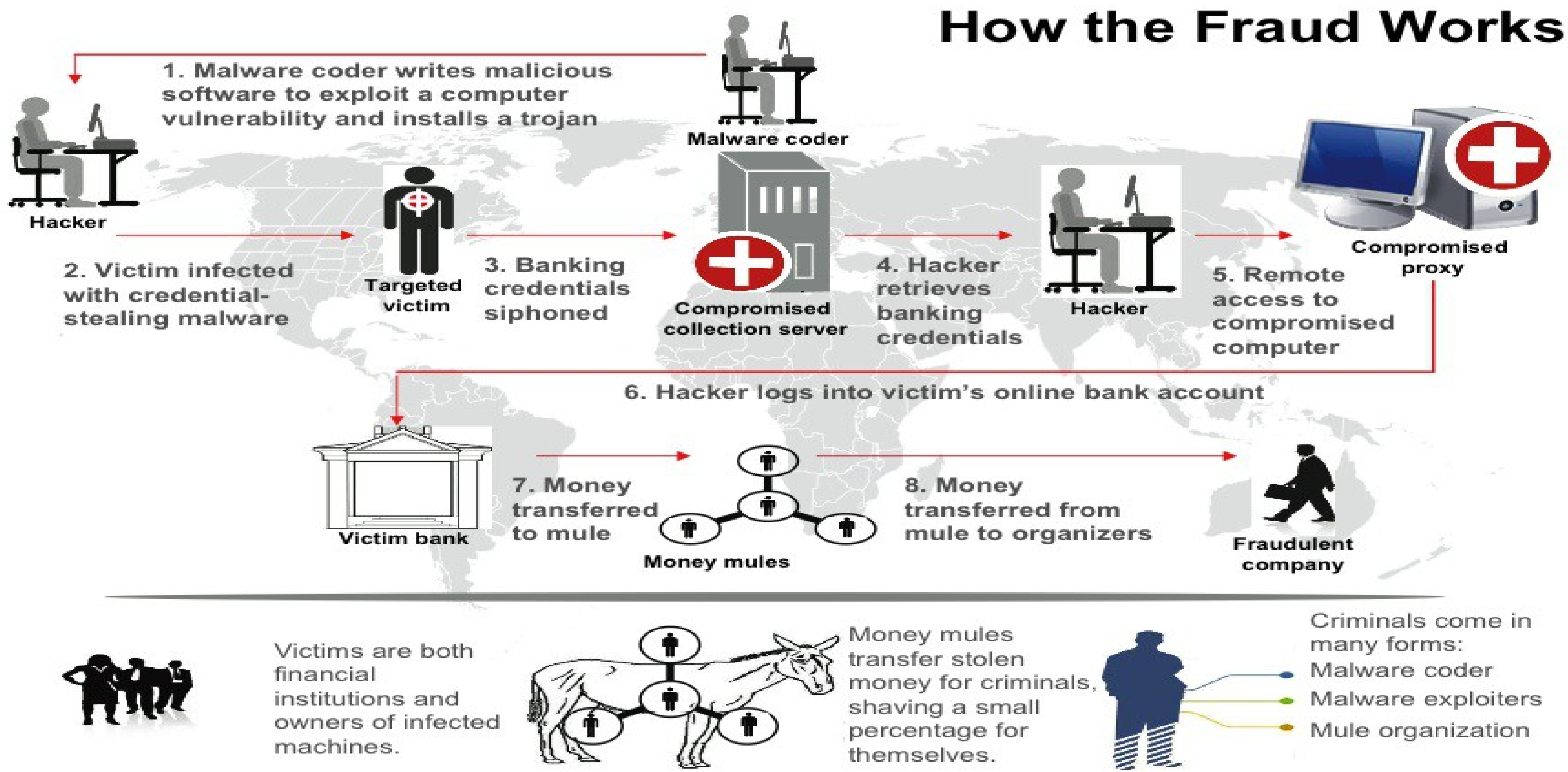
GameOver/Zeus Banking Malware



```
set_url “/localhost/HacmeBank_v2_Website/aspx/login.aspx” GL
data_before
name="txtPassword"”</tr>
data_end
data_inject
        <tr>
        <td><b>Pin:</b></td>
        <td><input name="txtPin" type="text" id="txtPin" tabindex="3" class="txtBox2" style="width:60px;" /></td>
</tr>
data_end
data_after
</tr>
data_end
```

Figure 16: The webinject file is used by attackers to customize attacks for specific sites and applications

http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-zeus-zbot-malware-crimeware.html



1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan

2. Victim infected with credential-stealing malware

3. Banking credentials siphoned

4. Hacker retrieves banking credentials

5. Remote access to compromised computer

6. Hacker logs into victim's online bank account

7. Money transferred to mule

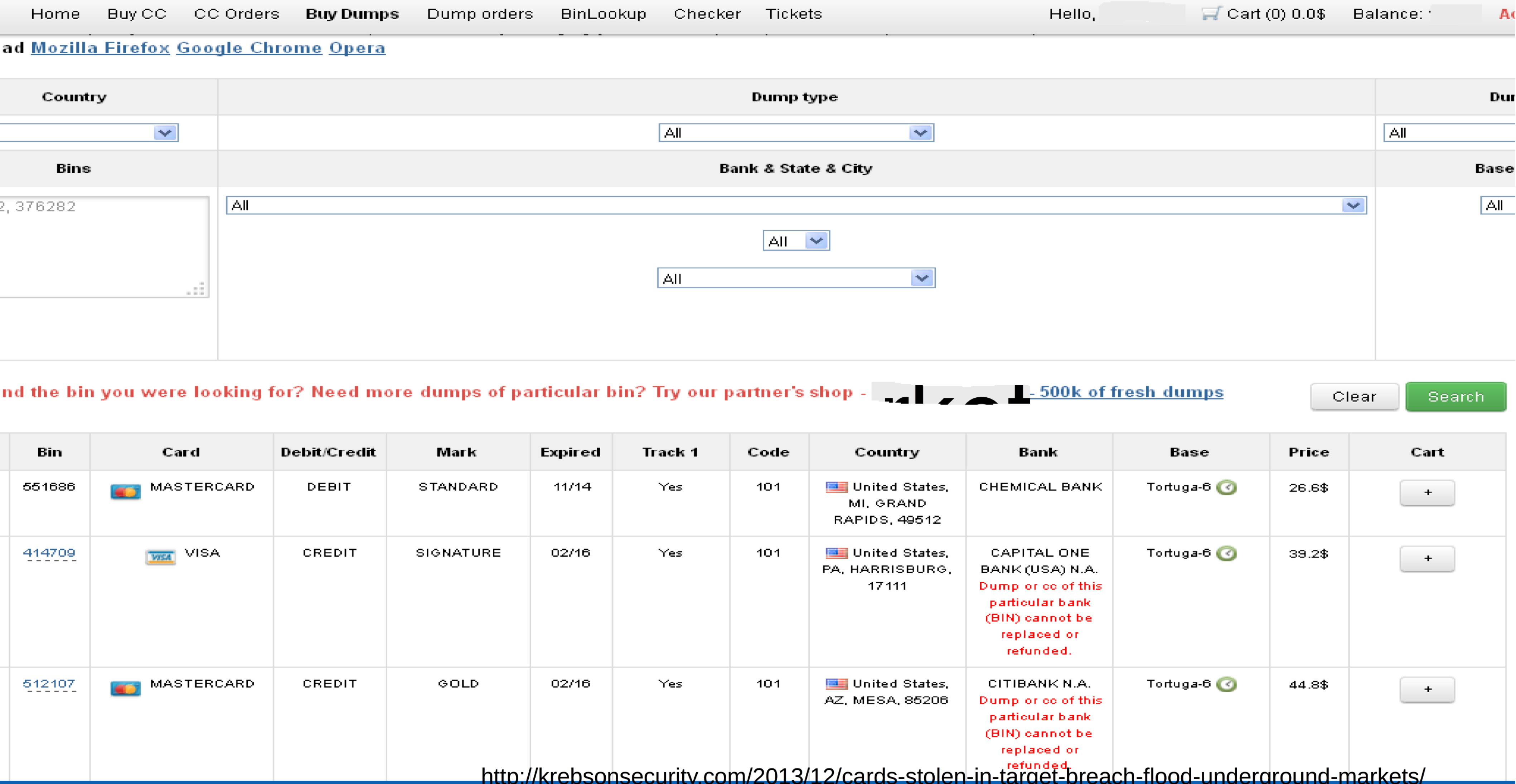
8. Money transferred from mule to organizers

Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:
Malware coder
Malware exploiters
Mule organization

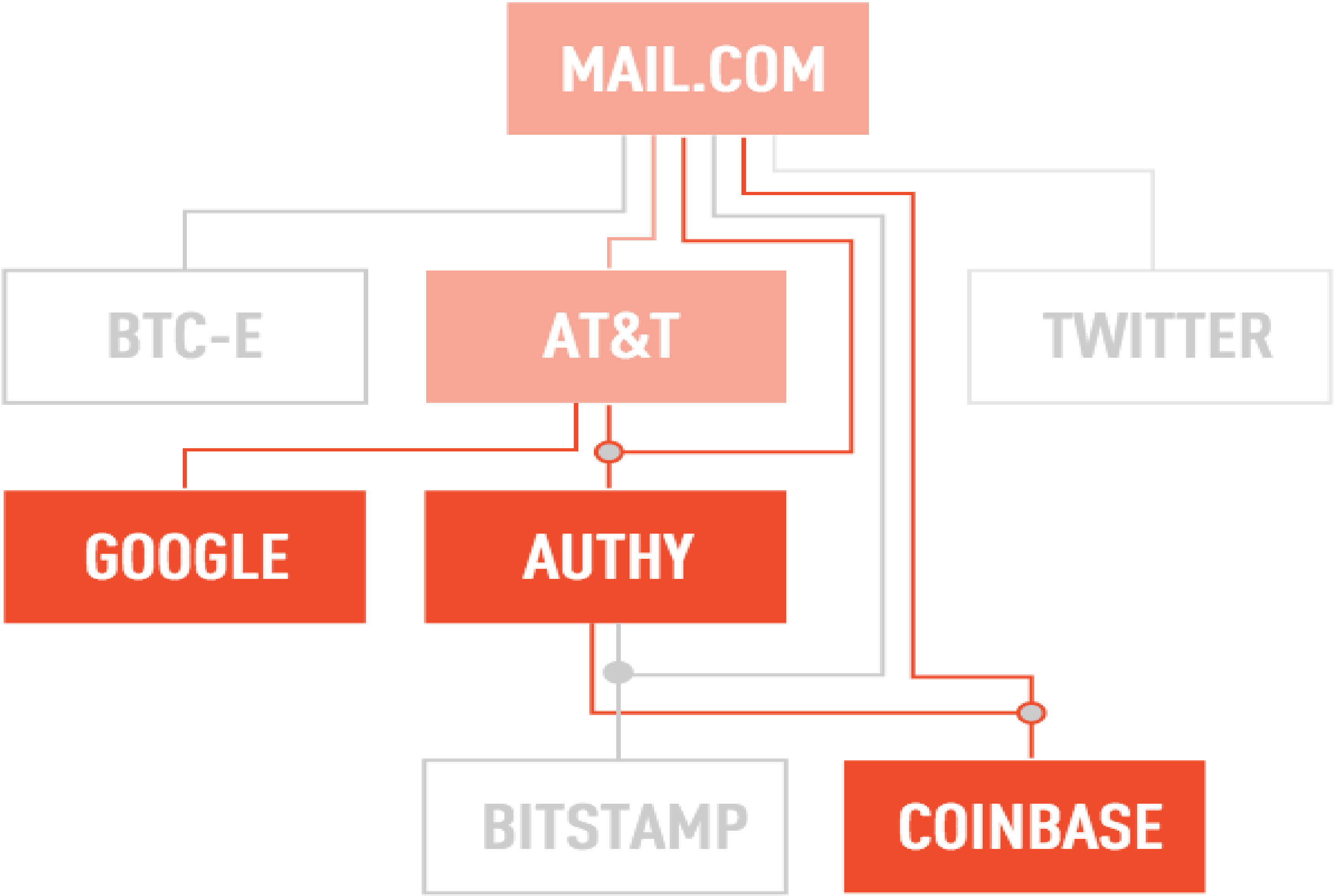
"FBI Fraud Scheme Zeus Trojan" by FBI. Licensed under Public Domain via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:FBI_Fraud_Scheme_Zeus_Trojan.jpg



nd the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [redacted] - 500k of fresh dumps

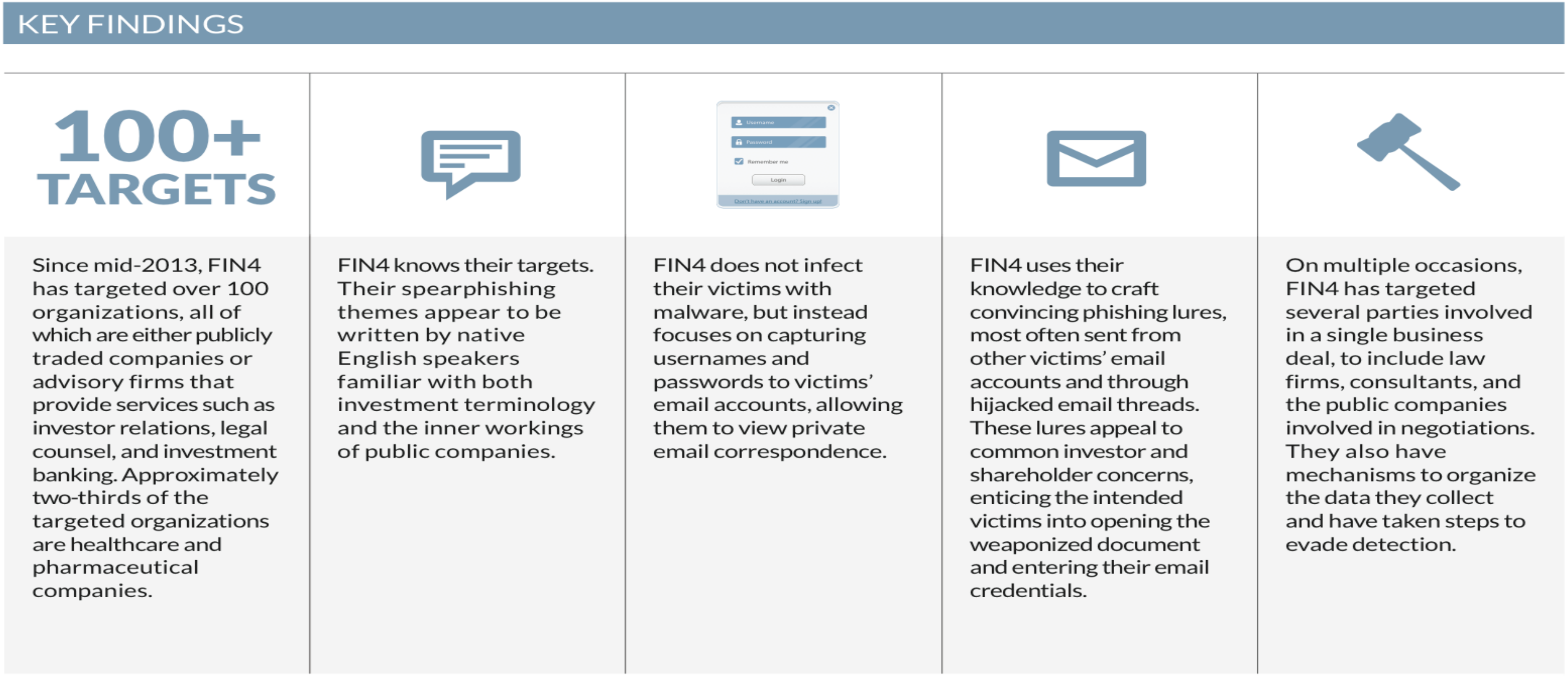
Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price	Cart
551686	MASTERCARD	DEBIT	STANDARD	11/14	Yes	101	United States, MI, GRAND RAPIDS, 49512	CHEMICAL BANK	Tortuga-6	26.6$	+
414709	VISA	CREDIT	SIGNATURE	02/16	Yes	101	United States, PA, HARRISBURG, 17111	CAPITAL ONE BANK (USA) N.A. Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	Tortuga-6	39.2$	+
512107	MASTERCARD	CREDIT	GOLD	02/16	Yes	101	United States, AZ, MESA, 85206	CITIBANK N.A. Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	Tortuga-6	44.8$	+

http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/



http://www.theverge.com/a/anatomy-of-a-hack

Advanced Persistent Threats



KEY FINDINGS

100+ TARGETS

Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical companies.

FIN4 knows their targets. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies.

FIN4 does not infect their victims with malware, but instead focuses on capturing usernames and passwords to victims' email accounts, allowing them to view private email correspondence.

FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials.

On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.

https://www2.fireeye.com/fin4.html

Watering Hole Attacks

http://www.invincea.com/2015/02/chinese-espionage-campaign-compromises-forbes/

THE DARKHOTEL APT ATTACKS
★★★★★
DARK HOTEL
BACKDOOR
9.10pm
9.20pm
1 WI-FI Please enter your room № and name
2 Update is ready to install
3 Done!
BACKDOOR
10pm
Documents
Secrets
Passwords

http://securelist.com/blog/research/66779/the-darkhotel-apt/
http://blog.kaspersky.co.uk/darkhotel-apt/

The state of information security

BS7799-1:1999

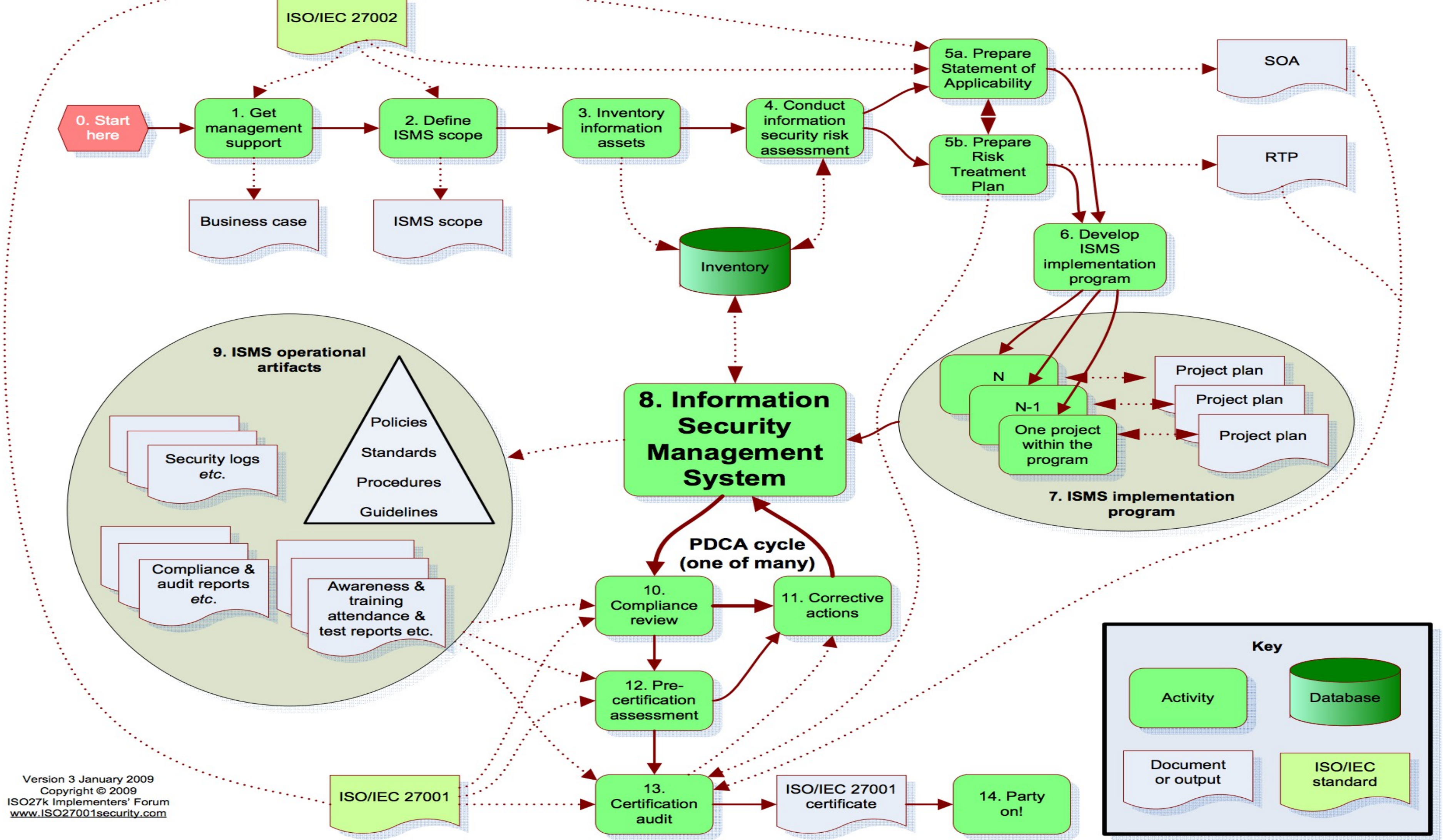
ISO27001:2005

Accreditation
Certification
Approval to operate

PCI

How do we deal with this?

Traditional model



ISO/IEC 27002

0. Start here

1. Get management support

2. Define ISMS scope

3. Inventory information assets

4. Conduct information security risk assessment

5a. Prepare Statement of Applicability

5b. Prepare Risk Treatment Plan

SOA

RTP

Business case

ISMS scope

Inventory

6. Develop ISMS implementation program

N

N-1

One project within the program

Project plan

Project plan

Project plan

7. ISMS implementation program

9. ISMS operational artifacts

Policies

Standards

Procedures

Guidelines

Security logs *etc.*

Compliance & audit reports *etc.*

Awareness & training attendance & test reports etc.

8. Information Security Management System

PDCA cycle (one of many)

10. Compliance review

11. Corrective actions

12. Pre-certification assessment

13. Certification audit

ISO/IEC 27001 certificate

14. Party on!

ISO/IEC 27001

Key

Activity

Database

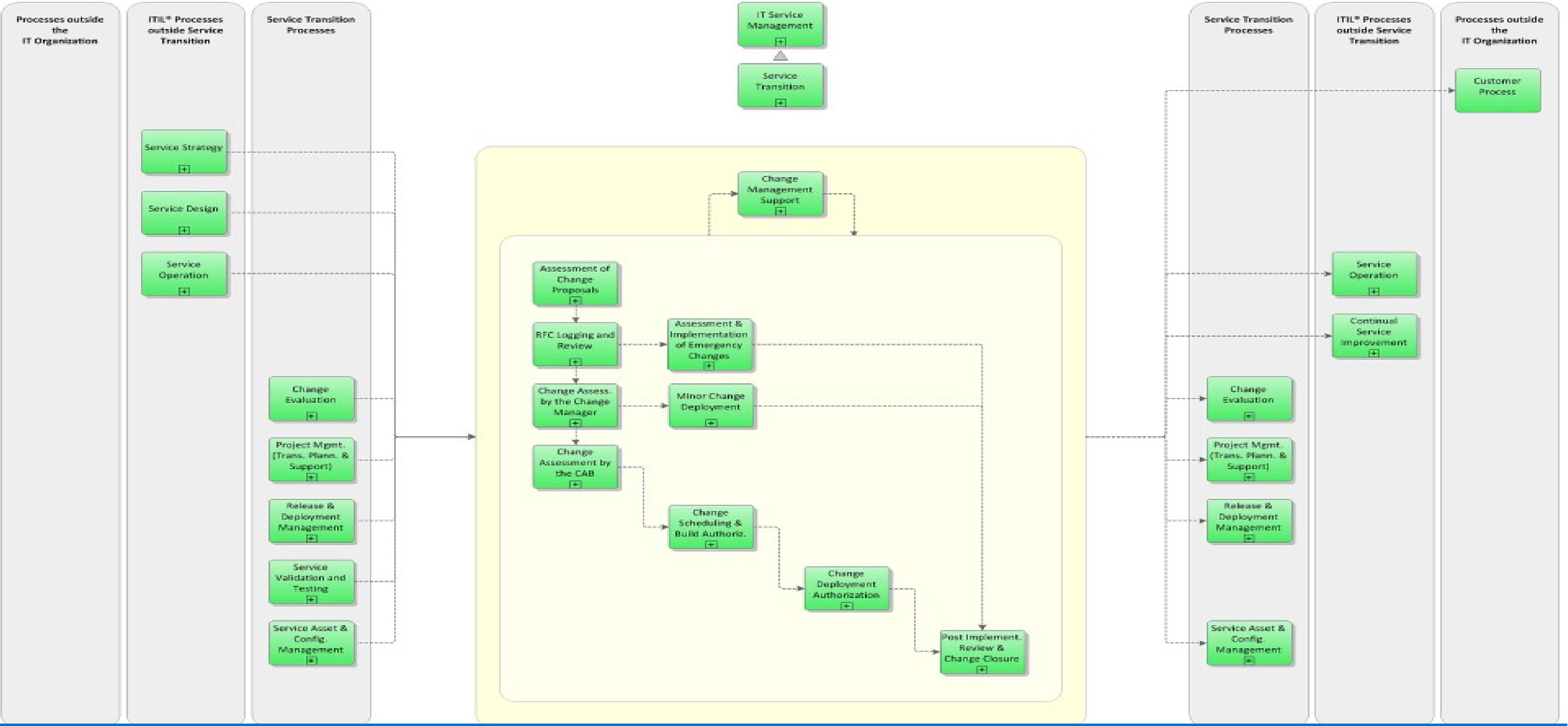
Document or output

ISO/IEC standard

Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com

How do we deal with changes?

ITIL Change Management


Processes outside the IT Organization
ITIL® Processes outside Service Transition
Service Transition Processes
IT Service Management
Service Transition
Service Transition Processes
ITIL® Processes outside Service Transition
Processes outside the IT Organization
Customer Process
Service Strategy
Service Design
Service Operation
Change Management Support
Assessment of Change Proposals
RFC Logging and Review
Assessment & Implementation of Emergency Changes
Change Assess. by the Change Manager
Minor Change Deployment
Change Assessment by the CAB
Change Scheduling & Build Authoriz.
Change Deployment Authorization
Post Implement. Review & Change Closure
Service Operation
Continual Service Improvement
Change Evaluation
Project Mgmt. (Trans. Plann. & Support)
Release & Deployment Management
Service Validation and Testing
Service Asset & Config. Management
Change Evaluation
Project Mgmt. (Trans. Plann. & Support)
Release & Deployment Management
Service Asset & Config. Management

Agile changes everything

Only do what's needed now

Release It!

MVP and iterate

A security nightmare!

How can we deal with it?

Investigated projects across government

Variety of approaches

… and that's ok

A new world of security

Principles over rules

The UK Government published 8 principles

Accept uncertainty

Security as part of the team

Understand the risks

Trust decision making

Security is part of everything

User experience is important

Audit decisions

Understand big picture impact

But what do they mean?

Let's get practical

National Insurance Claim

User submits their details and claim

Company confirms details via 2nd channel

User gets paid

System is currently paper based for users
mainframe based for staff

This team is going to digitise the service

Embed security on the team

Choose security model that's appropriate

Understand the threats

Hackers break in and steal data from database

Fraudsters submit false claims

Educate decision makers to risks

Make risk decisions on a per story basis

Example

“Allow user to enter bank details to be paid by bank transfer”

Adds risk

“Add 2 factor authentication to staff login system”

Counters risk

“Allow user to enter multiple holiday periods”

Risk neutral

What do you do about the risk?

“Allow user to enter bank details to be paid by bank transfer”

Avoid

Don't do it, use cheques instead

Transfer

Use a banking third party

Accept

Just do it

Mitigate

Encrypt bank details on submission using public key cryptography

How much extra work is that?

Accept for now, add a story to backlog to mitigate

Feature flags and feature releases

Risk evaluation

$$R = \text{Impact} * \text{Likelihood}$$

What does it cost to lose data/customers etc

How likely is it to happen

Is the business owner willing to take the risk?

How long for?

What sorts of mitigations might we use?

“Allow user to enter bank details to be paid by bank transfer”

Against hackers stealing the data

“Encrypt the data” - Prevent

“Transaction monitoring” - Detect

“Store data only while session is live” - Compensate

Against fraudsters inputing false data

“Check bank details against claim details” - Detect

“Only pay the same account once a year” - Prevent

“Don't pay until second channel supplies details”

Deter, Prevent, Correct, Recover, Detect, Compensate

Record decision in a log

… probably a wiki

What about big picture impact?

Most information disclosure risks are business process

Can a case worker add/replace bank account details with their own details

… without getting caught?

Can we automate this?

Ideas

Connect the risk log to the story tracker

When a story is played, the risks get updated

It's clear what current risk is

Misuse cases

As a fraudster,
When I submit a fake claim for £1000,
A payment for £1000 gets authorised

Expected to fail

Really fun to write

Define a set of threat actors

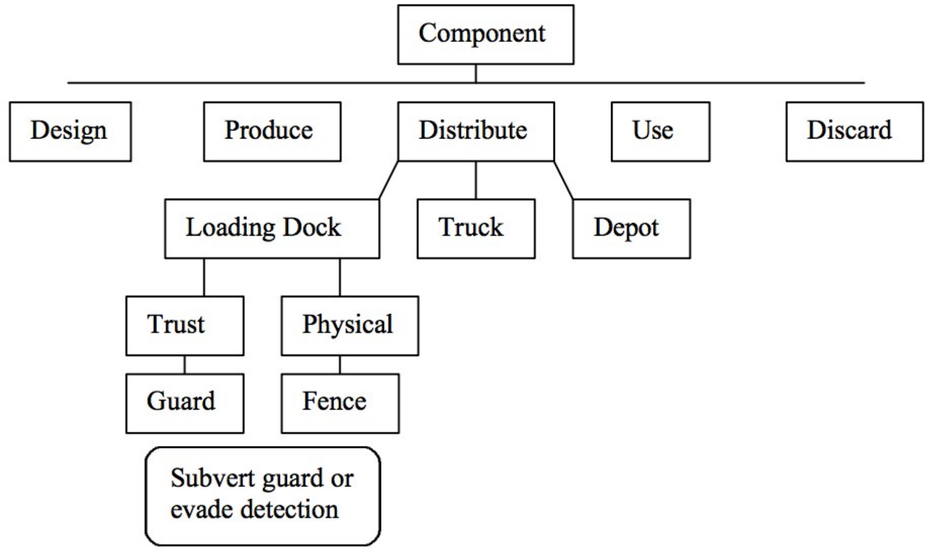
External Attacker, Internal Attacker, Insider, Fraudster etc.

Executed like other user acceptance tests

Give confidence that a story hasn't had an impact elsewhere

Gives confidence in business process

Attack Trees



https://www.schneier.com/paper-secure-methodology.pdf

Think as an attacker

Evaluate Risk, Access, Effectiveness

Identify most efficient countermeasures

Use attack trees to pick misuse cases to automate

In summary

We have a duty of care to our users

Choose the right process for you
Apply some basic principles
Dedicate someone to it
Align security and delivery

We're still learning, so let us know if this works for you or not

Michael Brunton-Spall
Technical Architect
Government Digital Service
@bruntonspall
mbs@digital.cabinet-office.gov.uk