Agile Security

Build Stuff 2016

Michael Brunton-Spall

GDS

Michael Brunton-Spall
He/His/Him

Head of cybersecurity

I'm from the Government, and I'm here to help

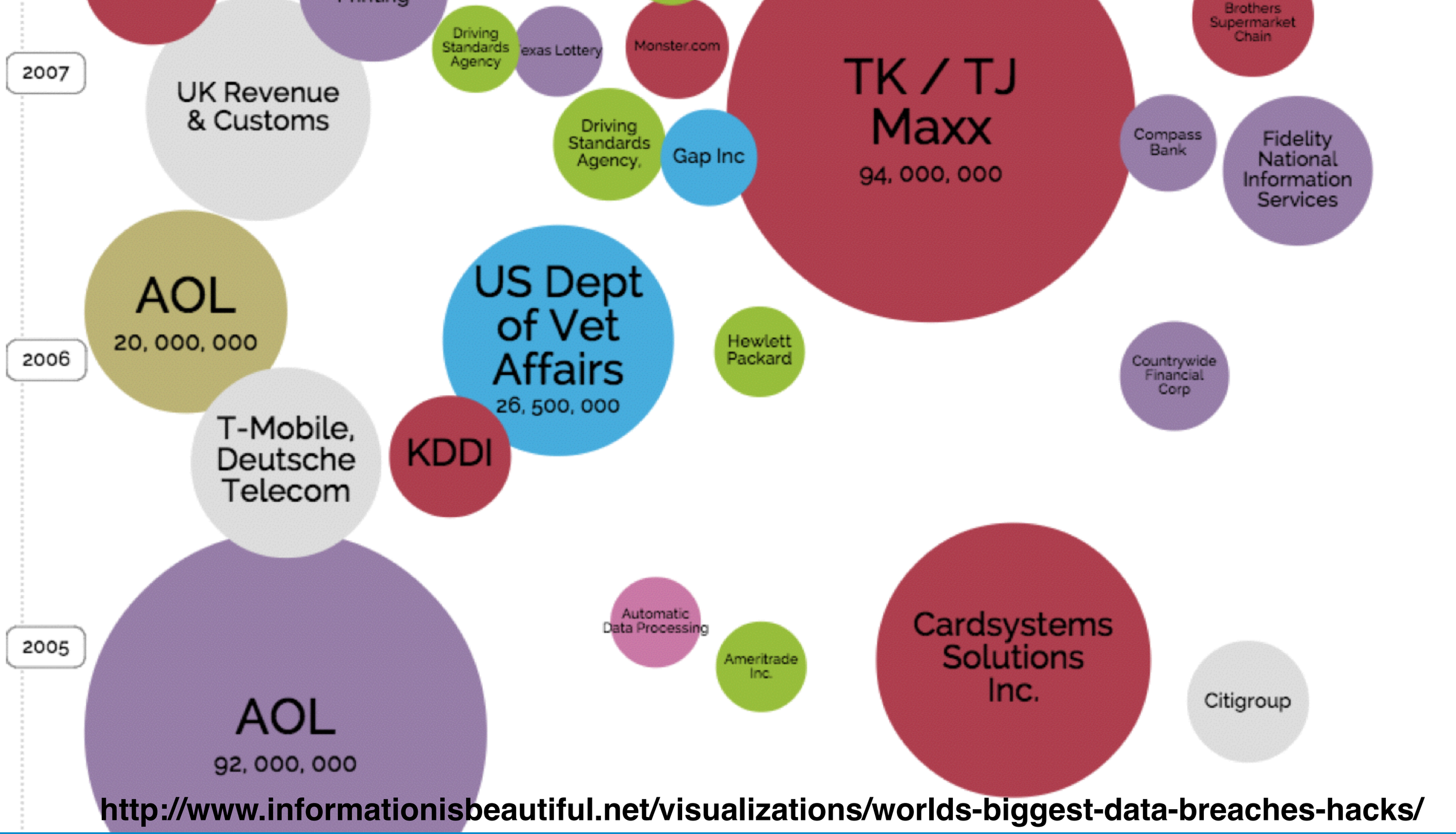
Michael Brunton-Spall GDS

I'm from security, and I'm here to help

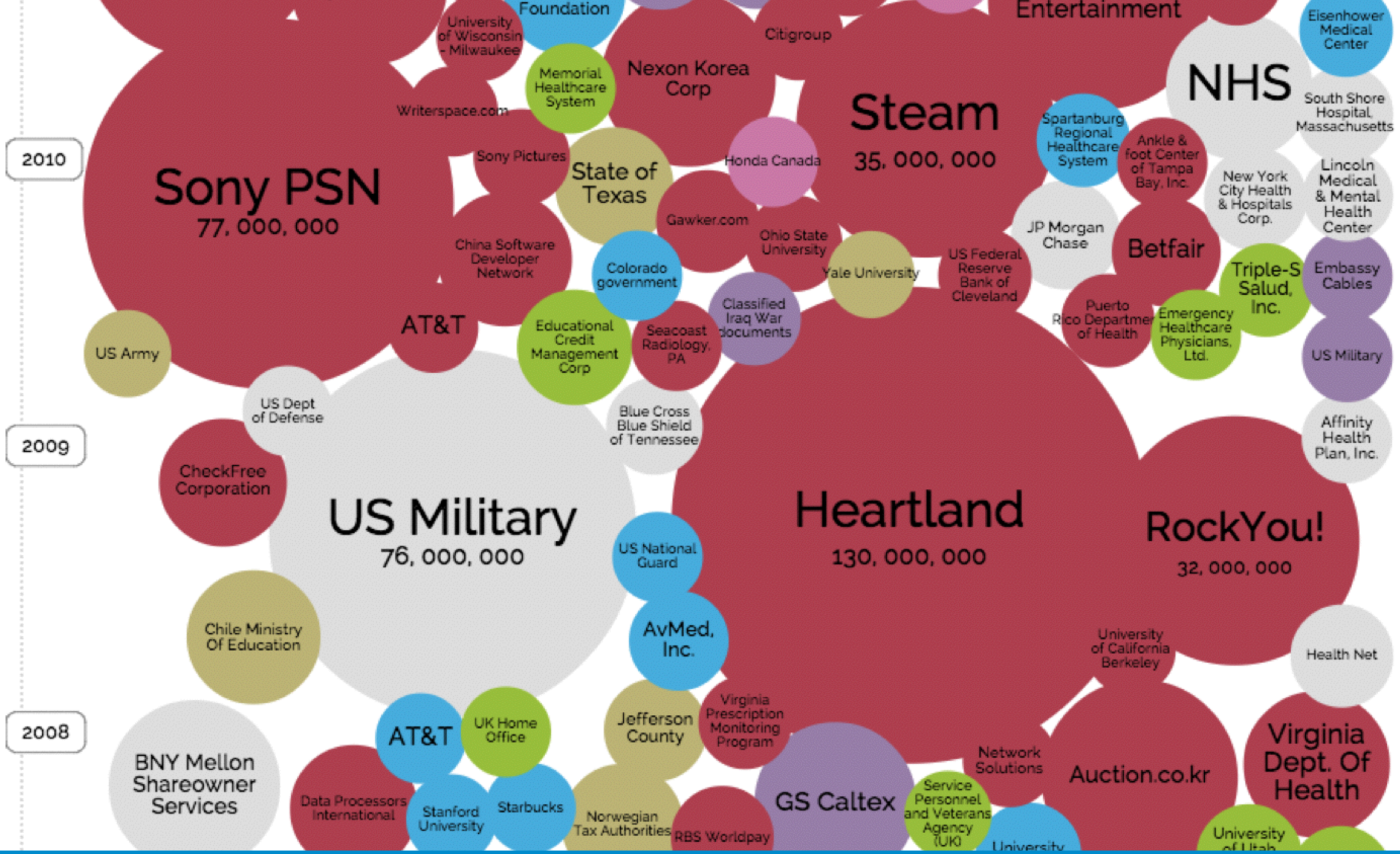
The state of security

Michael Brunton-Spall

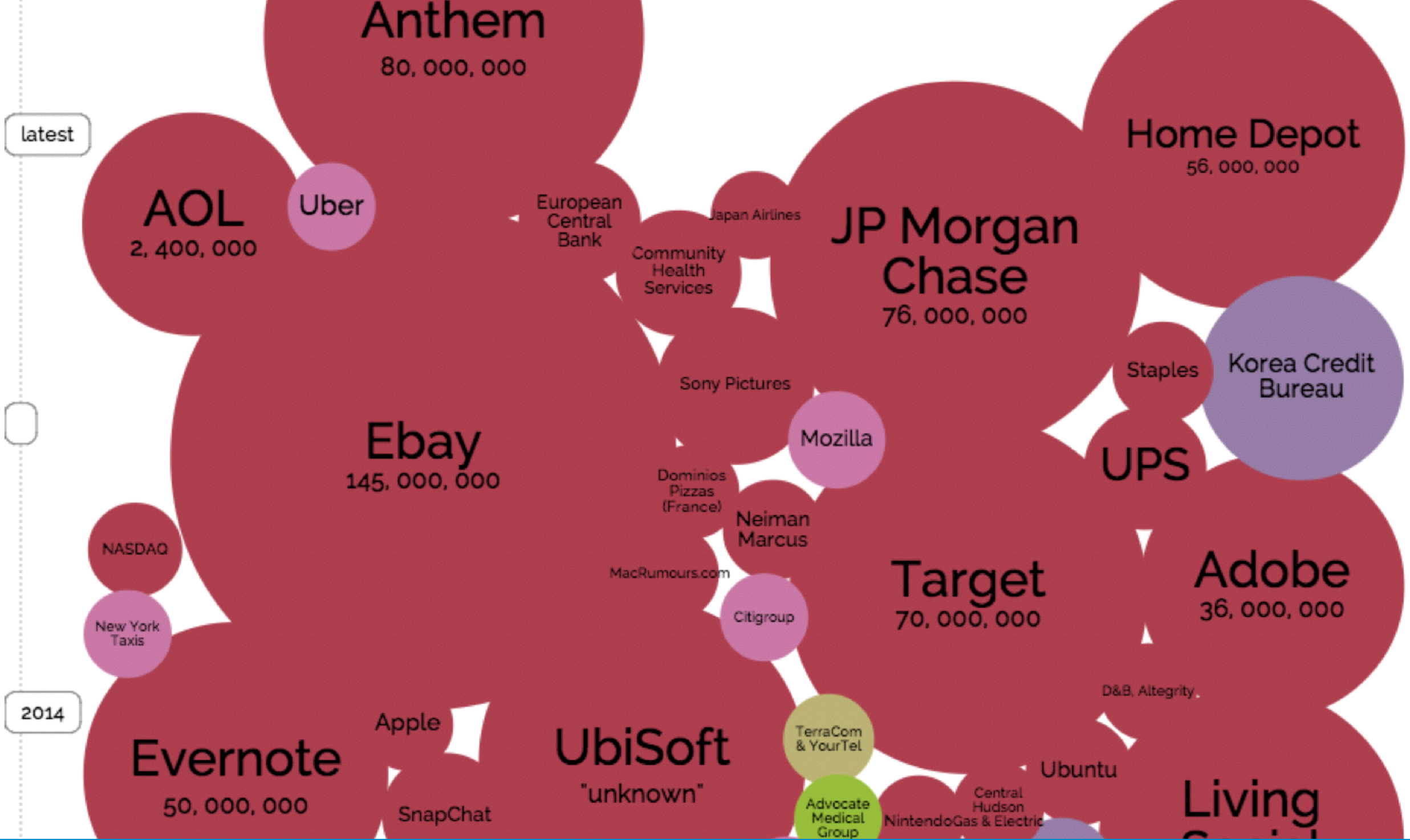
GDS



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


2010
2009
2008
Sony PSN
77, 000, 000
Foundation
University of Wisconsin - Milwaukee
Citigroup
Entertainment
Eisenhower Medical Center
NHS
South Shore Hospital, Massachusetts
Memorial Healthcare System
Nexon Korea Corp
Writerspace.com
Steam
35, 000, 000
Spartanburg Regional Healthcare System
Ankle & foot Center of Tampa Bay, Inc.
Sony Pictures
State of Texas
Honda Canada
New York City Health & Hospitals Corp.
Lincoln Medical & Mental Health Center
Gawker.com
Ohio State University
JP Morgan Chase
Betfair
China Software Developer Network
Colorado government
Yale University
US Federal Reserve Bank of Cleveland
Triple-S Salud, Inc.
Embassy Cables
Puerto Rico Department of Health
Emergency Healthcare Physicians, Ltd.
AT&T
Classified Iraq War documents
US Army
Educational Credit Management Corp
Seacoast Radiology, PA
US Military
US Dept of Defense
Blue Cross Blue Shield of Tennessee
Affinity Health Plan, Inc.
CheckFree Corporation
US Military
76, 000, 000
Heartland
130, 000, 000
RockYou!
32, 000, 000
US National Guard
AvMed, Inc.
Chile Ministry Of Education
University of California Berkeley
Health Net
BNY Mellon Shareowner Services
AT&T
UK Home Office
Jefferson County
Virginia Prescription Monitoring Program
Virginia Dept. Of Health
Network Solutions
Auction.co.kr
Data Processors International
Stanford University
Starbucks
Norwegian Tax Authorities
RBS Worldpay
GS Caltex
Service Personnel and Veterans Agency (UK)
University of Utah

Indiana University
South Africa police
OVH
Vodafone
50, 0
Drupal
Facebook
Florida Department of Juvenile Justice
NMBS
Washington State court system
Global Payments
Kissinger Cables
Twitter
Scribd
ssndob.ms
Kirkwood Community College
Greek government
Li
eH
L
Blizzard
Florida Courts
KT Corp.
Massive American business hack
160, 000, 000
Court Ventures
200, 000, 000
"Apple"
California Department


latest
2014
Anthem
80, 000, 000
AOL
2, 400, 000
Uber
European Central Bank
Japan Airlines
Community Health Services
JP Morgan Chase
76, 000, 000
Home Depot
56, 000, 000
Staples
Korea Credit Bureau
Sony Pictures
Mozilla
Ebay
145, 000, 000
Dominios Pizzas (France)
UPS
Neiman Marcus
NASDAQ
MacRumours.com
Target
70, 000, 000
Adobe
36, 000, 000
New York Taxis
Citigroup
D&B, Altegrity.
Apple
TerraCom & YourTel
Evernote
50, 000, 000
UbiSoft
"unknown"
Ubuntu
Central Hudson
Advocate Medical Group
NintendoGas & Electric
SnapChat
Living

Criminal users on the internet

Michael Brunton-Spall GDS

GameOver/Zeus Banking Malware

Michael Brunton-Spall GDS

webinjects - Notepad

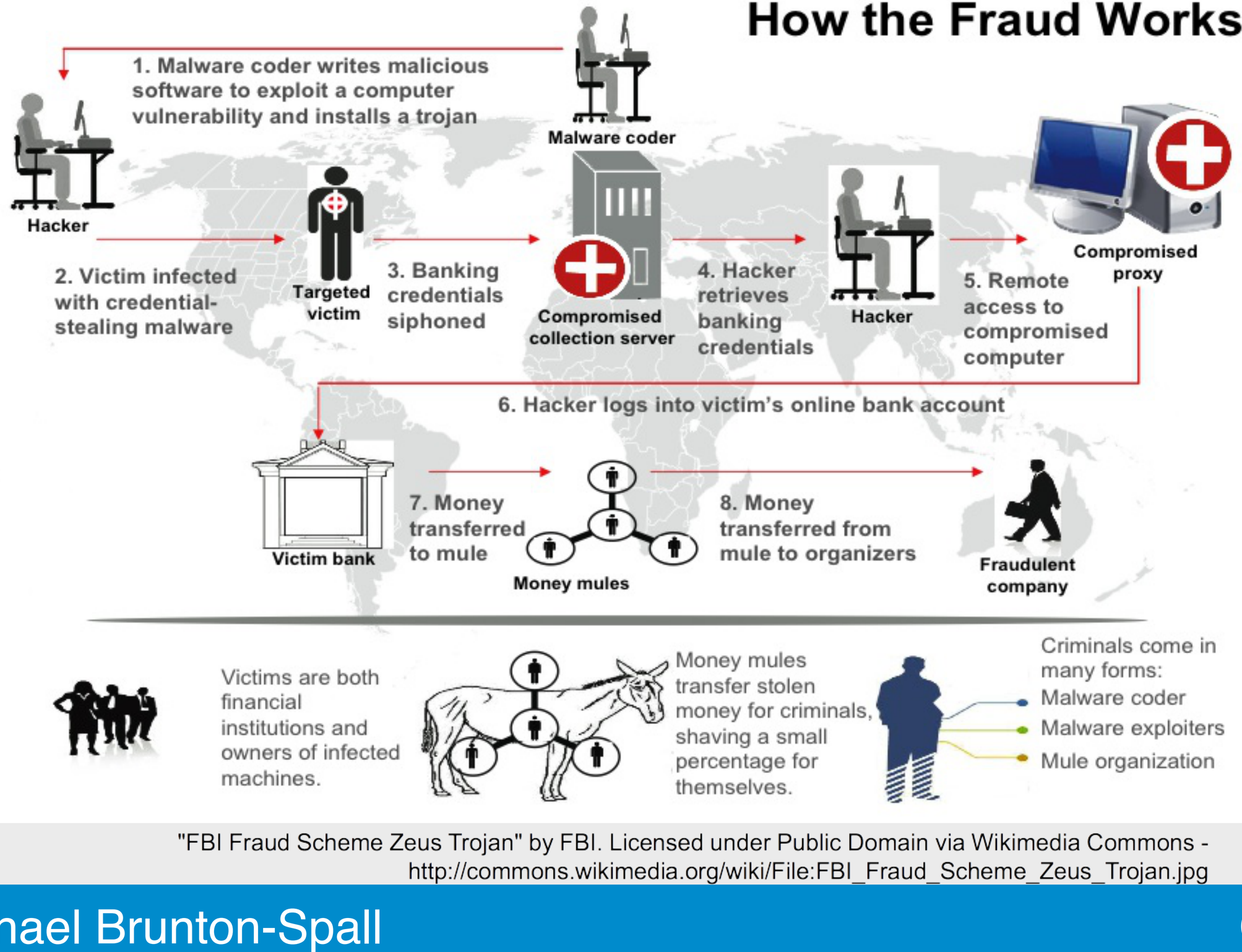
File Edit Format View Help

```
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

How the Fraud Works



"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

Home Buy CC CC Orders **Buy Dumps** Dump orders BinLookup Checker Tickets Hello, Cart (0) 0.0$ Balance: Add money Replace policy Logout

oad Mozilla Firefox Google Chrome Opera

Country	Dump type	Dump mark	Debit/Credit
	All	All	All

Bins	Bank & State & City	Base and other	Additional
2, 376282	All	All	Expired 12/13
	All		Track1
	All		Exp. date (1312)
			Last 4 Digits
			Select code

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

Clear Search

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	Tortuga-6	44.8$	+

Michael Brunton-Spall GDS

Advanced Persistent Threats

Michael Brunton-Spall

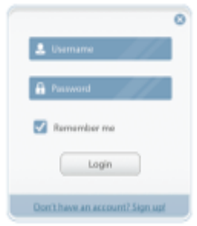
GDS

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.

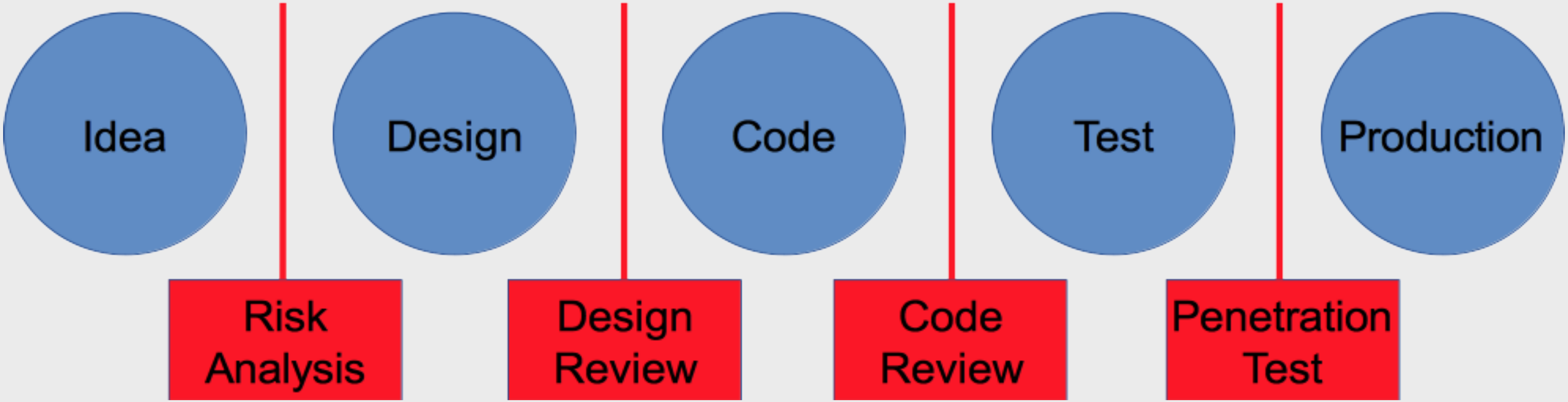

THE DARKHOTEL APT ATTACKS
DARK HOTEL
BACKDOOR
9.10pm
9.20pm
10pm
9.05pm
1 WI-FI
Please enter your room N° and name
2
Update is ready to install
3 Done!
BACKDOOR
Documents
Secrets
Passwords

What does security do?

Certification Accreditation

PCI ISO27001

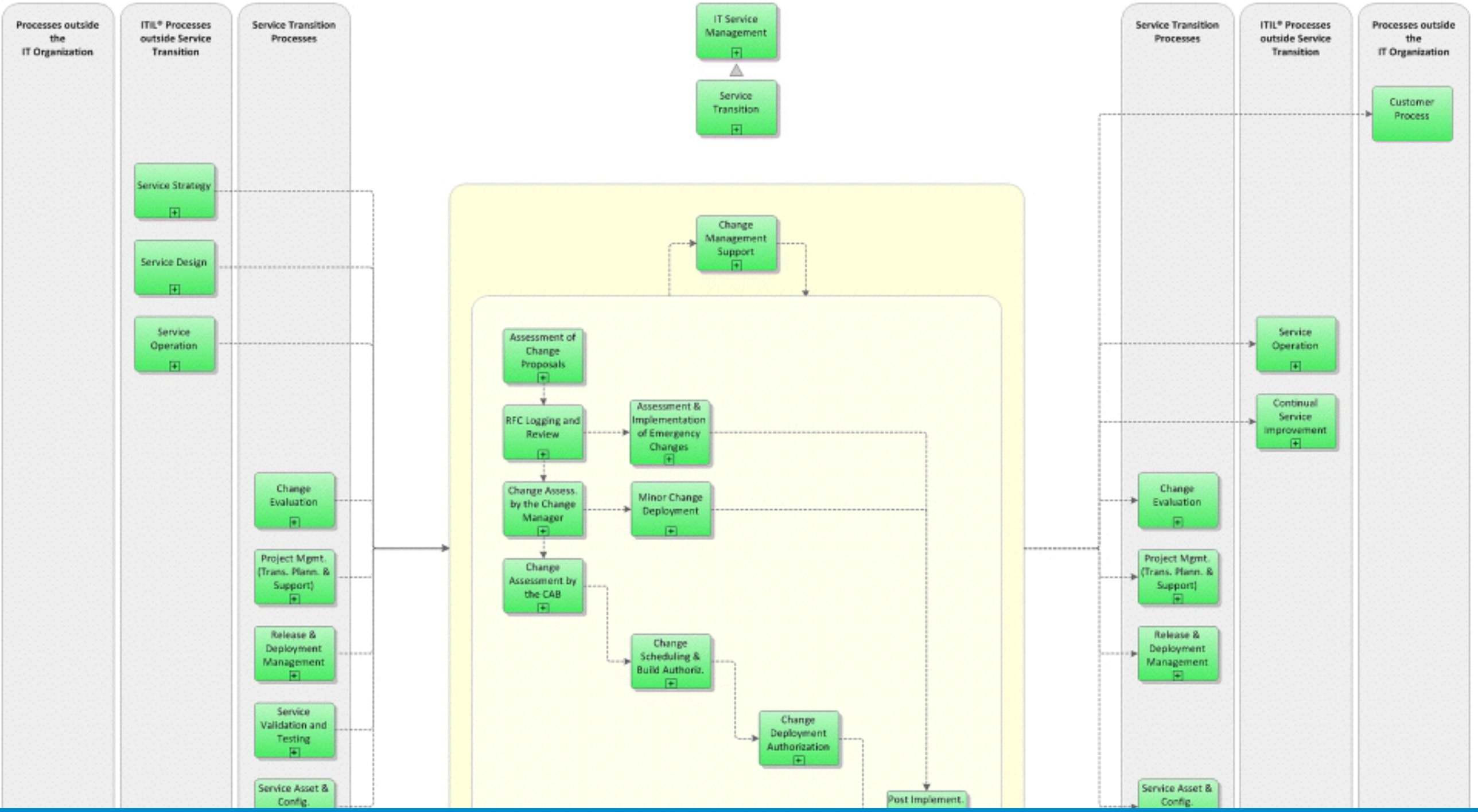
Michael Brunton-Spall GDS


Idea
Design
Code
Test
Production
Risk Analysis
Design Review
Code Review
Penetration Test

Change control boards

Michael Brunton-Spall

GDS


Processes outside the IT Organization
ITIL® Processes outside Service Transition
Service Transition Processes
IT Service Management
Service Transition
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.
Change Evaluation
Project Mgmt. (Trans. Plann. & Support)
Release & Deployment Management
Service Validation and Testing
Service Asset & Config.
Service Transition Processes
ITIL® Processes outside Service Transition
Processes outside the IT Organization
Customer Process
Service Operation
Continual Service Improvement
Change Evaluation
Project Mgmt. (Trans. Plann. & Support)
Release & Deployment Management
Service Asset & Config.

Agile changes everything

Michael Brunton-Spall GDS

What is agile?

Michael Brunton-Spall

GDS

We are uncovering better ways of developing
software by doing it and helping others do it.
Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on
the right, we value the items on the left more.

While the things on the right have value

The things on the left have more value

Michael Brunton-Spall GDS

Individuals and interactions over processes and tools

Michael Brunton-Spall GDS

Working software over comprehensive documentation

Michael Brunton-Spall GDS

Responding to change over following a plan

Michael Brunton-Spall

GDS

Customer collaboration over contract negotiation

Michael Brunton-Spall GDS

Contracts, Planning, Documentation, Processes and Tools

Michael Brunton-Spall GDS

Collaboration, Change, Deliverables, People

Michael Brunton-Spall GDS

Building software together

Michael Brunton-Spall

GDS

Support and trust

Michael Brunton-Spall

GDS

Simplicity

Michael Brunton-Spall

GDS

Maximising work not done

Michael Brunton-Spall GDS

"Minimising the lead time for delivering business value" @tastapod

What does this mean today?

Minimum viable product or service

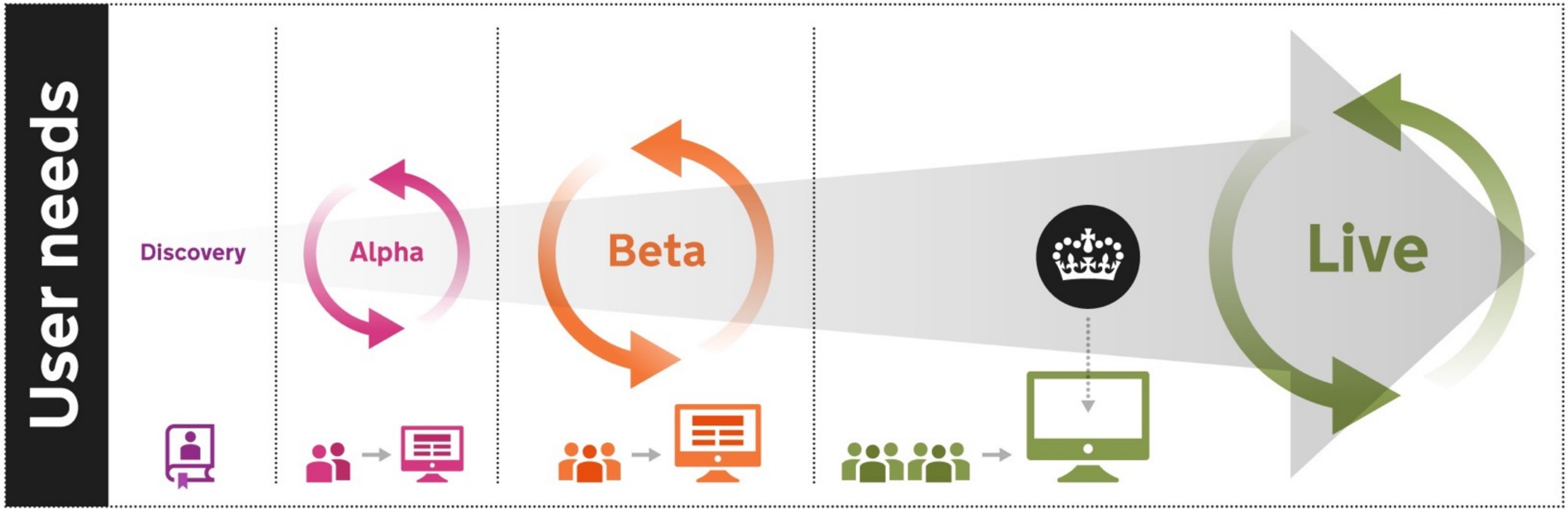
Michael Brunton-Spall GDS

Iterate

Michael Brunton-Spall GDS

Release early, release often

Michael Brunton-Spall GDS


User needs
Discovery
Alpha
Beta
Live

Principles

Michael Brunton-Spall

GDS

Protect personal data

https://www.cesg.gov.uk/guidance/protecting-bulk-personal-data

Security design principles

https://www.cesg.gov.uk/guidance/security-design-principles-digital-services-0

Michael Brunton-Spall GDS

8 Principles of risk management

https://www.gov.uk/government/publications/principles-of-effective-cyber-security-risk-management

Accept uncertainty
Security as part of the team
Understand the risks

Michael Brunton-Spall GDS

Trust decision making
Security is part of everything
User experience is important

Michael Brunton-Spall GDS

Audit decisions

Understand big picture impact

Michael Brunton-Spall GDS

How does agile help?

Continual delivery of business value

Michael Brunton-Spall GDS

Continual acceptance of risk

Michael Brunton-Spall

GDS

Secure Agile Development

Michael Brunton-Spall

GDS

Security must be an enabler of the team

Michael Brunton-Spall GDS

Safety engineering and security engineering

Michael Brunton-Spall GDS

The unit of delivery is the team

Michael Brunton-Spall

GDS

The unit of decision making is the team

Michael Brunton-Spall GDS

Software bugs are not evenly distributed

Michael Brunton-Spall GDS

Risk

Michael Brunton-Spall

GDS

Educate the team to the threats

Michael Brunton-Spall GDS

Keep a running risk log

Michael Brunton-Spall

GDS

Apply risk decisions per story

Michael Brunton-Spall

GDS

Apply controls per story

Michael Brunton-Spall

GDS

Security debt

Michael Brunton-Spall

GDS

Microservices and security

Michael Brunton-Spall

GDS

"Software that can fit in my head"

James Lewis

Michael Brunton-Spall GDS

Small systems focused on one business domain

Michael Brunton-Spall GDS

Business based

Michael Brunton-Spall GDS

Own their own data

Michael Brunton-Spall

GDS

Contracts for communication

Michael Brunton-Spall GDS

Simple systems are more secure

Michael Brunton-Spall GDS

Simple
Complicated
Complex

Michael Brunton-Spall

GDS

Security concerns aren't evenly distributed

Michael Brunton-Spall GDS

Secure Agile Operations

Michael Brunton-Spall

GDS

Infrastructure as code

Michael Brunton-Spall

GDS

```
class varnish::package {
  package { 'varnish':
    ensure => installed,
  }
}
class varnish::config($upstream_port, $strip_cookies) {
  include varnish::restart

  $app_domain  = hiera('app_domain')

  file { '/etc/default/varnish':
    ensure  => file,
    content => template('varnish/defaults.erb'),
    notify  => Class['varnish::restart'], # requires a full varnish restart to pick up changes
  }

  file { '/etc/default/varnishncsa':
    ensure => file,
    source => 'puppet:///modules/varnish/etc/default/varnishncsa',
  }

  file { '/etc/varnish/default.vcl':
    ensure  => file,
    content => template('varnish/default.vcl.erb'),
  }
}
```

Infrastructure as testable code

Michael Brunton-Spall GDS

```
context 'with aliases' do
  let(:params) do
    {
      :port => 8000,
      :app_type => 'rack',
      :vhost_aliases => ['foo','bar'],
      :domain => 'example.com',
      :vhost_full => 'giraffe.example.com',
    }
  end

  it { is_expected.to contain_nginx__config__vhost__proxy('giraffe.example.com').with_aliases(['foo.example.com','bar.examp
end

 context 'with an upstart post-start script' do
   let(:params) do
     {
       :port => 8000,
       :app_type => 'rack',
       :domain => 'foo.bar.baz',
       :vhost_full => 'giraffe.foo.bar.baz',
       :upstart_post_start_script => '/bin/true',
     }
   end

   it do
     is_expected.to contain_file('/etc/init/giraffe.conf').with(:content => %r{post-start script\s*\n\s*/bin/true\s*\
   end
end
```

```
@normal
Scenario: check quick answers load
  When I visit "/vat-rates"
  Then I should see "VAT rates"

@normal
Scenario: check guides load
  When I visit "/getting-an-mot"
  Then I should see "Getting an MOT"

@normal
Scenario: check transactions load
  When I visit "/apply-renew-passport"
  Then I should see "UK passport"

@normal
Scenario: check benefit schemes load
  When I visit "/pension-credit"
  Then I should see "Pension Credit"

@normal
Scenario: check homepage content type & charset
  When I visit "/"
```

Dealing with patches

Michael Brunton-Spall

GDS

What machines are affected?

Michael Brunton-Spall GDS

```
class nginx::package(
  $nginx_package = 'nginx-full',
  $version       = 'present',
) {

  include govuk::ppa

  # nginx package actually has nothing useful in it; we normally need nginx-full
  package { 'nginx':
    ensure => purged,
  }

  package { 'nginx-common':
    ensure => $version,
    notify => Class['nginx::restart'],
  }

  package { $nginx_package:
    ensure  => $version,
    notify  => Class['nginx::restart'],
    require => Package['nginx-common'],
  }
}
```

```
(michaelbruntonspalldev@ubuntu work/puppet)% ack-grep nginx::package::version
hieradata/common.precise.yaml
5:nginx::package::version: '1.4.4-1~precise0'

hieradata/common.yaml
151:nginx::package::version: '1.4.6-1ubuntu3.1'

hieradata/class/frontend.yaml
2:nginx::package::version: '1.4.6'

hieradata/class/backend.yaml
2:nginx::package::version: '1.4.5'
```

Updating machines in test

Michael Brunton-Spall

GDS

```
hieradata/test.yaml
2:nginx::package::version: '1.4.7'
```

Just some machines?

Michael Brunton-Spall GDS

```
(michaelbruntonspalldev@ubuntu work/puppet)% ack-grep nginx::package::version
hieradata/test/frontend.yaml
2:nginx::package::version: '1.4.7'
```

Repeat in production

Michael Brunton-Spall GDS

What does Agile and DevOps give you?

Michael Brunton-Spall

GDS

Automated Testing

Michael Brunton-Spall GDS

Infrastructure as code

Michael Brunton-Spall

GDS

Fast repeatable deploys

Michael Brunton-Spall

GDS

Audit logs

Michael Brunton-Spall

GDS

Code review of infrastructure changes

Michael Brunton-Spall GDS

Confidence!

Michael Brunton-Spall GDS

Why does that matter?

Australian Signals Directorate

http://www.asd.gov.au/publications/protect/top_4_mitigations.htm

Application whitelisting

Michael Brunton-Spall

GDS

Patching

Michael Brunton-Spall

GDS

Patching (again)

Michael Brunton-Spall

GDS

Minimise administrative controls

Michael Brunton-Spall GDS

Done well, agile development means more secure

Michael Brunton-Spall GDS

Cabinet Office

Michael Brunton-Spall

Head of cybersecurity

Government Digital Service

@bruntonspall