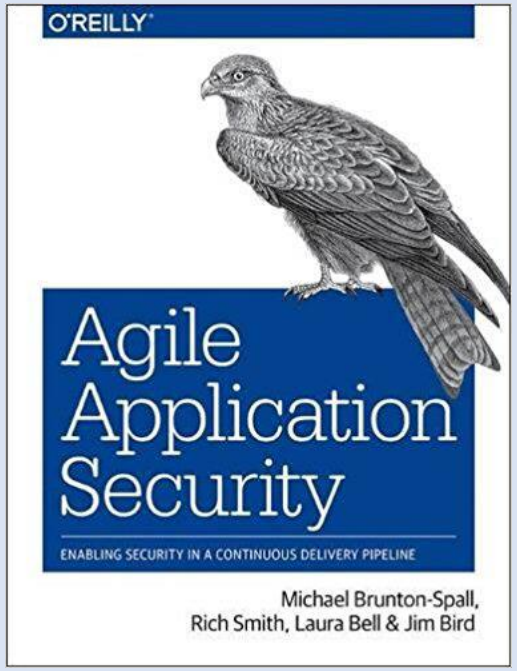
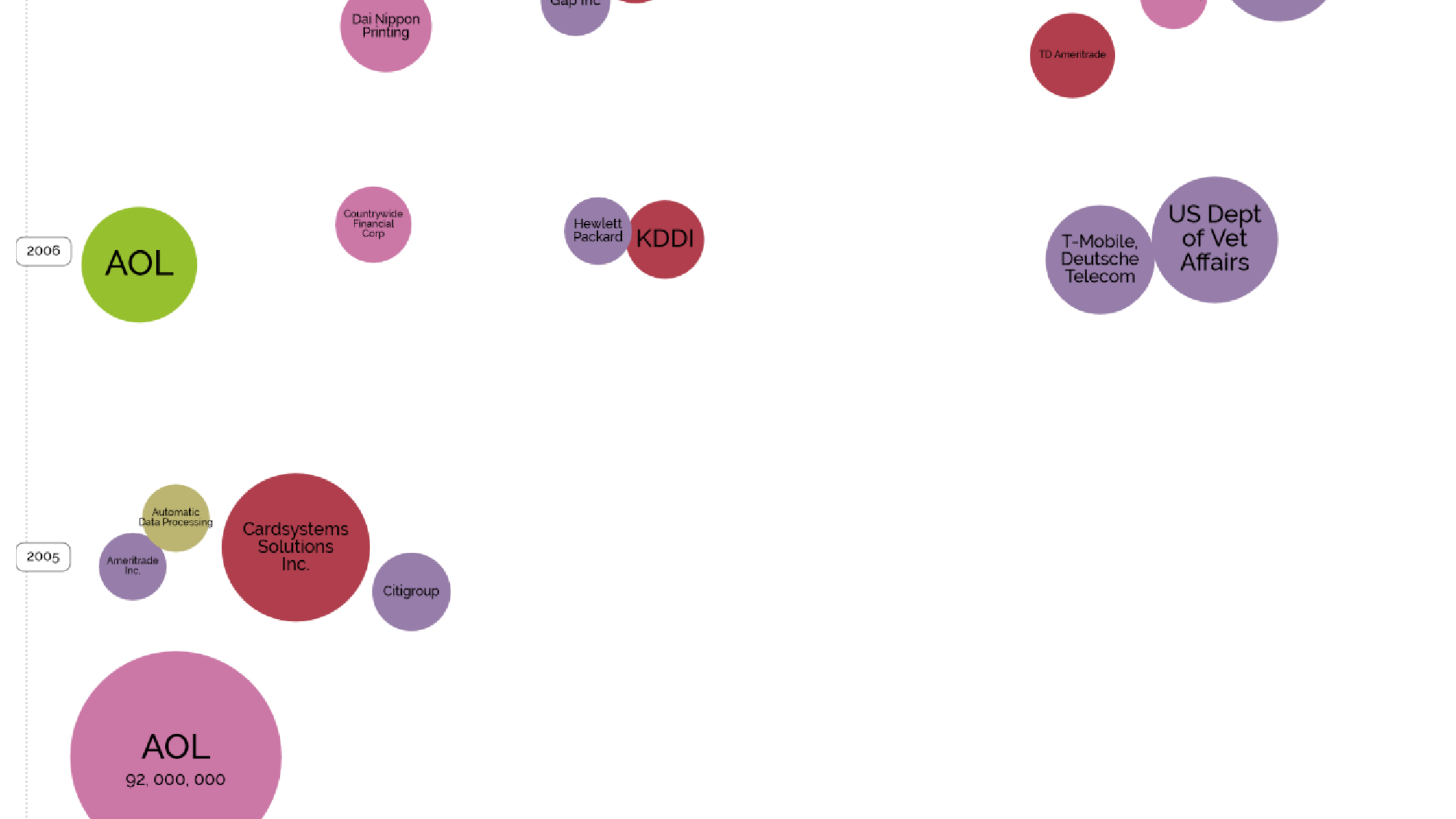
Attack Trees, Security modelling for Agile Teams

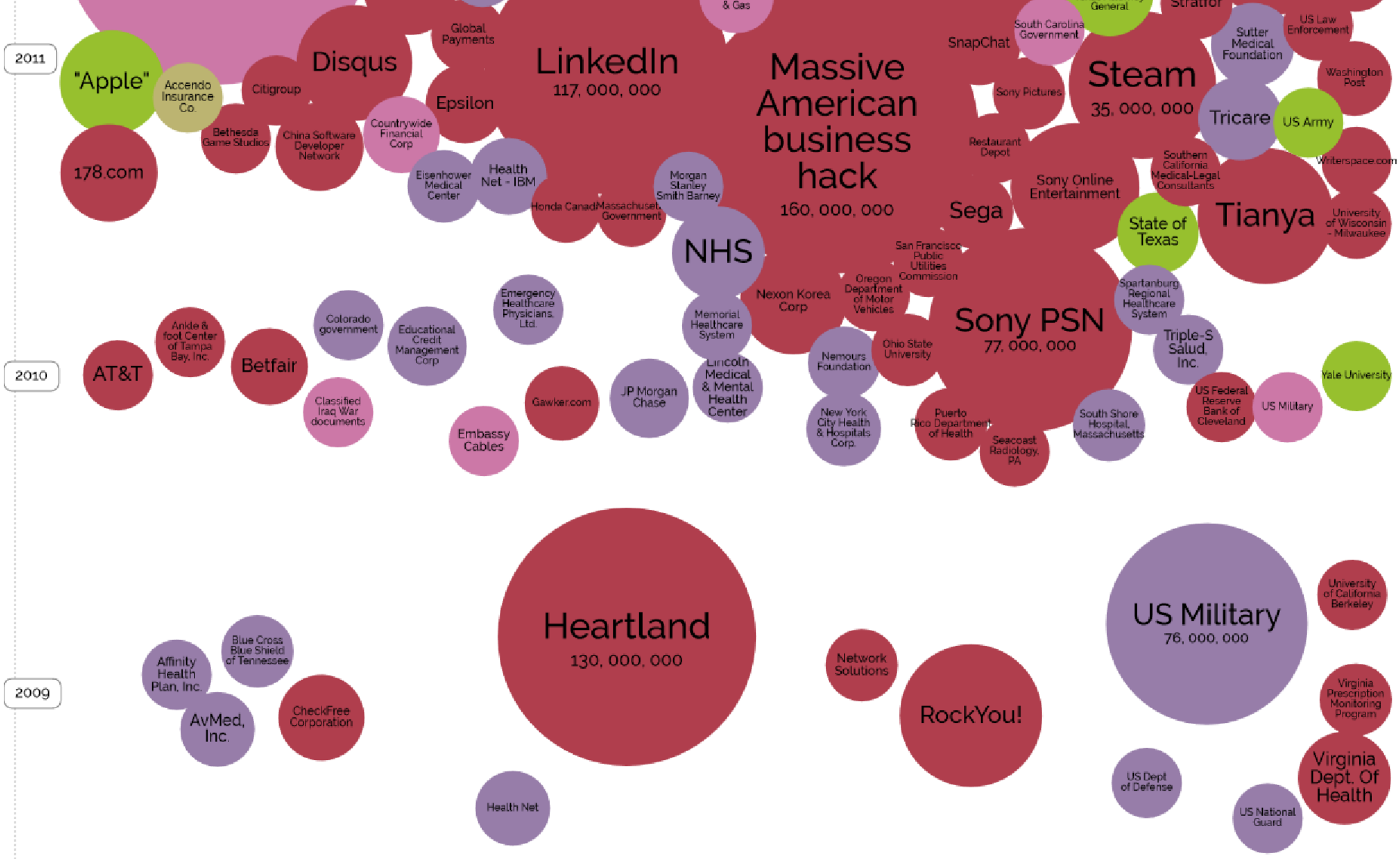
Michael Brunton-Spall **@bruntonspall**

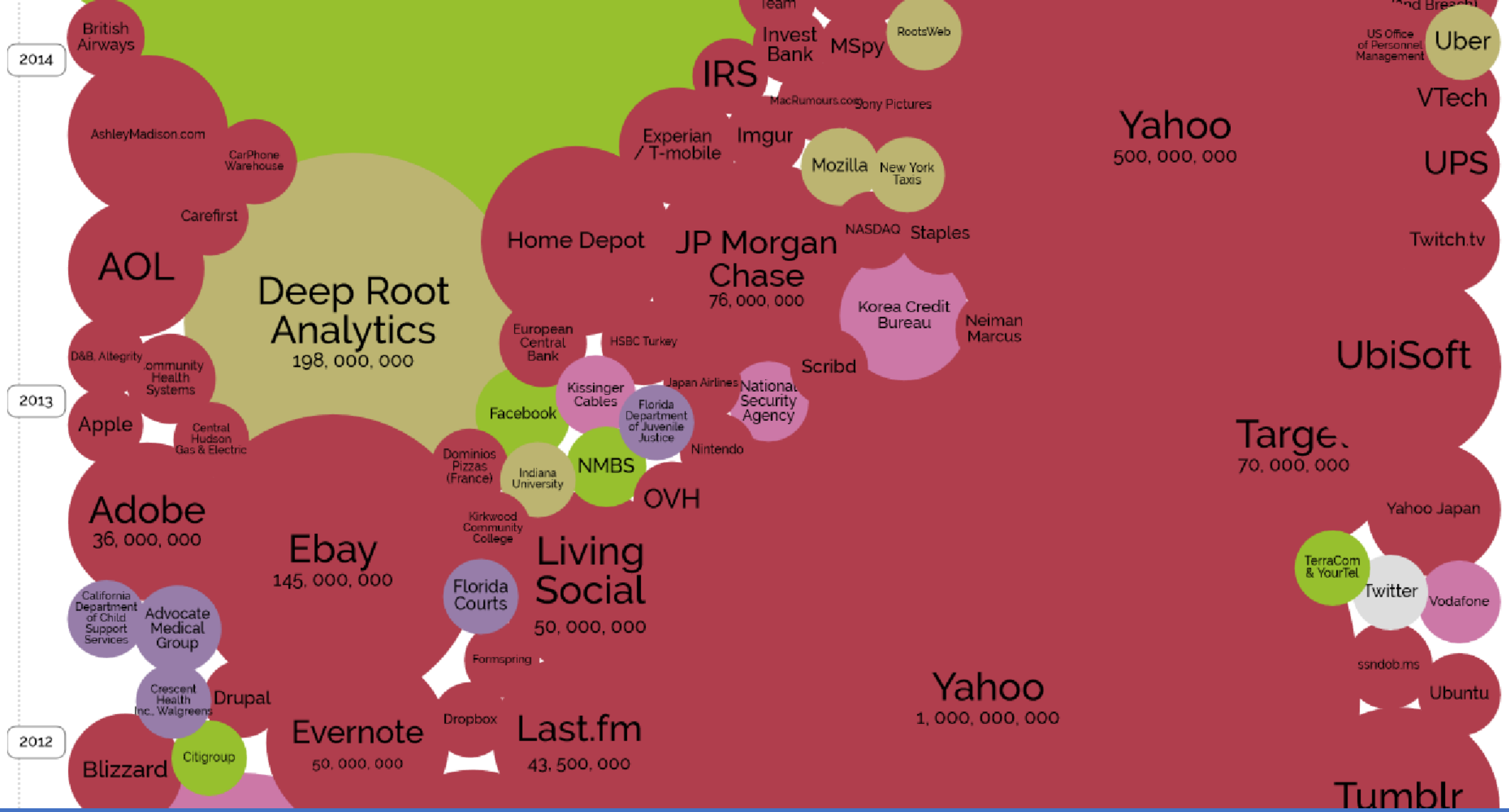


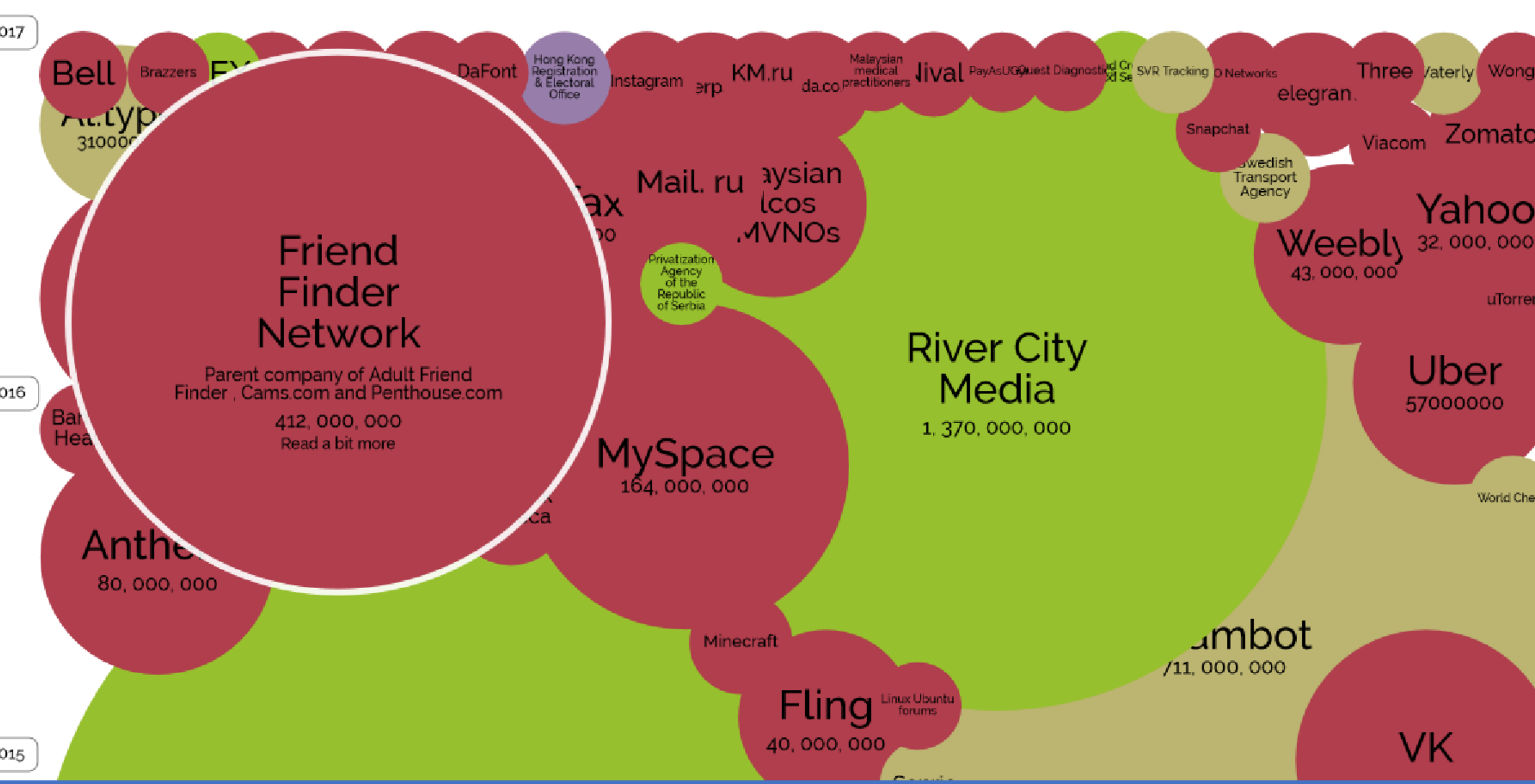
Michael Brunton-Spall
He/His/Him
Independent Cybersecurity Consultant

Why Security Matters


Dai Nippon Printing
Gap Inc
TD Ameritrade
2006
AOL
Countrywide Financial Corp
Hewlett Packard
KDDI
T-Mobile, Deutsche Telecom
US Dept of Vet Affairs
2005
Automatic Data Processing
Ameritrade Inc.
Cardsystems Solutions Inc.
Citigroup
AOL
92, 000, 000


2011
2010
2009
"Apple"
Accendo Insurance Co.
Citigroup
Disqus
Bethesda Game Studios
China Software Developer Network
Countrywide Financial Corp
178.com
Global Payments
Epsilon
Eisenhower Medical Center
Health Net - IBM
LinkedIn
117, 000, 000
Honda Canada
Massachusetts Government
Morgan Stanley Smith Barney
Massive American business hack
160, 000, 000
NHS
Emergency Healthcare Physicians, Ltd.
Memorial Healthcare System
Nexon Korea Corp
Oregon Department of Motor Vehicles
San Francisco Public Utilities Commission
Sega
SnapChat
South Carolina Government
Sony Pictures
Restaurant Depot
Sony Online Entertainment
Sony PSN
77, 000, 000
Nemours Foundation
Ohio State University
Lincoln Medical & Mental Health Center
New York City Health & Hospitals Corp.
Puerto Rico Department of Health
Seacoast Radiology, PA
South Shore Hospital, Massachusetts
Steam
35, 000, 000
Sutter Medical Foundation
US Law Enforcement
Washington Post
Tricare
US Army
Writerspace.com
Southern California Medical-Legal Consultants
Tianya
University of Wisconsin - Milwaukee
State of Texas
Spartanburg Regional Healthcare System
Triple-S Salud, Inc.
US Federal Reserve Bank of Cleveland
US Military
Yale University
AT&T
Ankle & foot Center of Tampa Bay, Inc.
Betfair
Colorado government
Classified Iraq War documents
Educational Credit Management Corp
Embassy Cables
Gawker.com
JP Morgan Chase
Heartland
130, 000, 000
Affinity Health Plan, Inc.
Blue Cross Blue Shield of Tennessee
AvMed, Inc.
CheckFree Corporation
Health Net
Network Solutions
RockYou!
US Military
76, 000, 000
University of California Berkeley
Virginia Prescription Monitoring Program
Virginia Dept. Of Health
US Dept of Defense
US National Guard


2014
2013
2012
British Airways
AshleyMadison.com
CarPhone Warehouse
Carefirst
AOL
D&B, Altegrity
Community Health Systems
Apple
Central Hudson Gas & Electric
Adobe
36, 000, 000
California Department of Child Support Services
Advocate Medical Group
Crescent Health Inc., Walgreens
Drupal
Blizzard
Citigroup
Deep Root Analytics
198, 000, 000
Ebay
145, 000, 000
Evernote
50, 000, 000
Dropbox
Last.fm
43, 500, 000
Team
Invest Bank
MSpy
RootsWeb
IRS
MacRumours.com
Sony Pictures
Experian / T-mobile
Imgur
Mozilla
New York Taxis
Home Depot
JP Morgan Chase
76, 000, 000
NASDAQ
Staples
Korea Credit Bureau
Neiman Marcus
European Central Bank
HSBC Turkey
Scribd
Kissinger Cables
Japan Airlines
National Security Agency
Facebook
Florida Department of Juvenile Justice
Nintendo
Dominios Pizzas (France)
Indiana University
NMBS
OVH
Kirkwood Community College
Florida Courts
Living Social
50, 000, 000
Formspring
Yahoo
1, 000, 000, 000
US Office of Personnel Management
Uber
VTech
Yahoo
500, 000, 000
UPS
Twitch.tv
UbiSoft
Targe.
70, 000, 000
Yahoo Japan
TerraCom & YourTel
Twitter
Vodafone
ssndob.ms
Ubuntu
Tumblr


017
016
015
Bell
Brazzers
DaFont
Hong Kong Registration & Electoral Office
Instagram
KM.ru
Malaysian medical practitioners
SVR Tracking
Three
Snapchat
Viacom
Swedish Transport Agency
Yahoo
32, 000, 000
Weebly
43, 000, 000
Mail. ru
Privatization Agency of the Republic of Serbia
Friend Finder Network
Parent company of Adult Friend Finder , Cams.com and Penthouse.com
412, 000, 000
Read a bit more
River City Media
1, 370, 000, 000
Uber
57000000
MySpace
164, 000, 000
Minecraft
Fling
40, 000, 000
Linux Ubuntu forums
VK

Criminal users on the internet

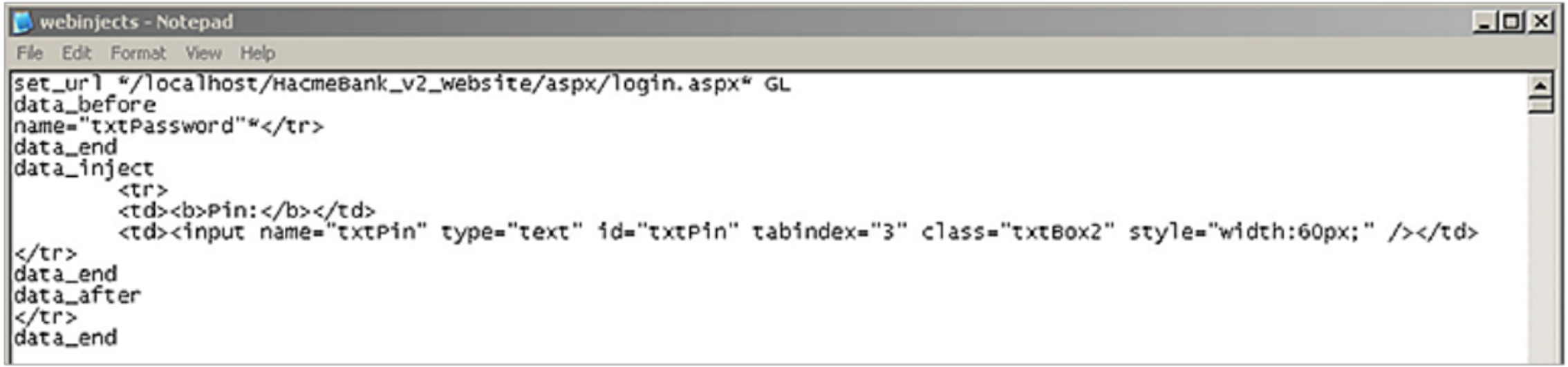
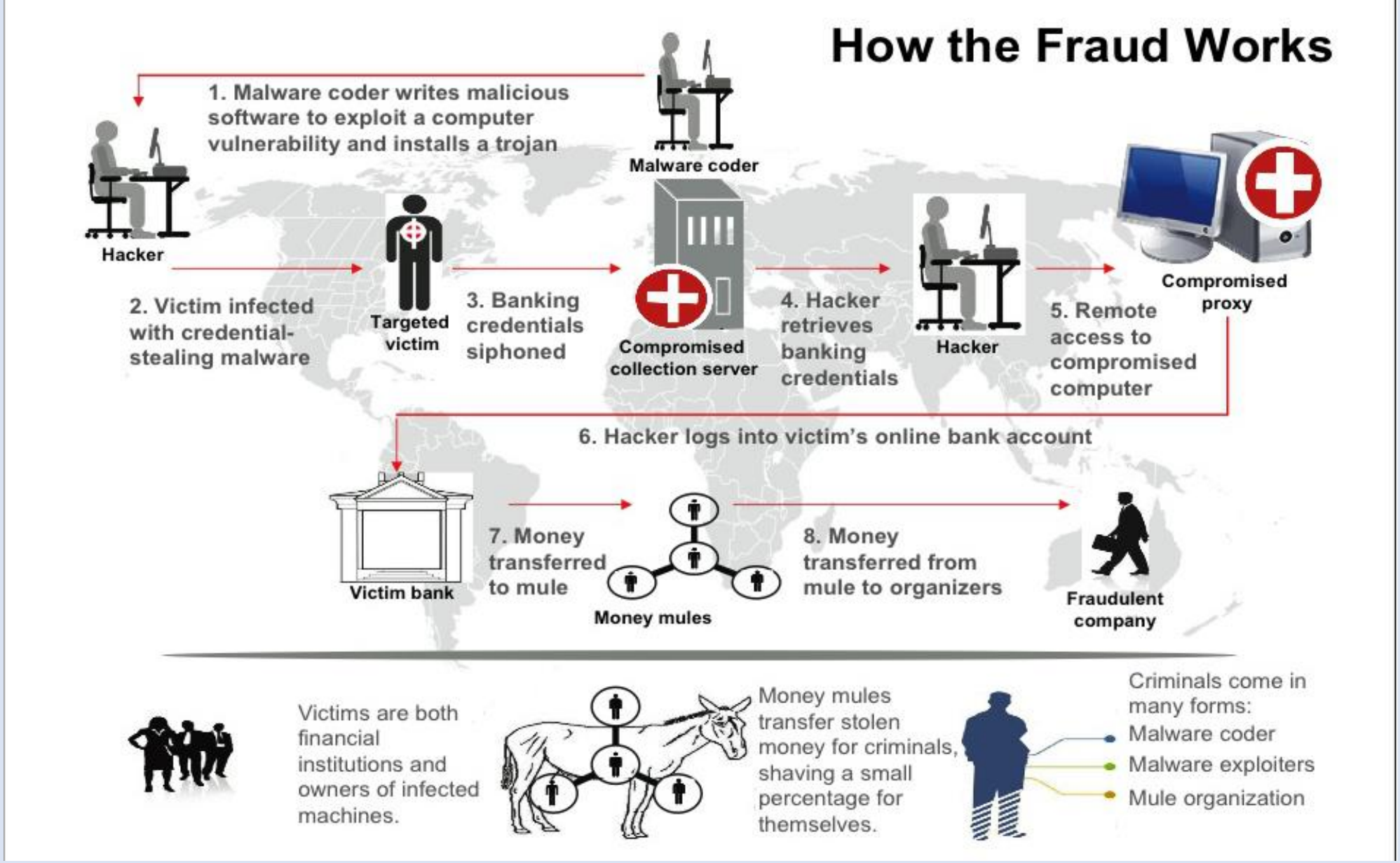


Figure 16: The webinject file is used by attackers to customize attacks for specific sites and applications

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



"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

Advanced Persistent Threats

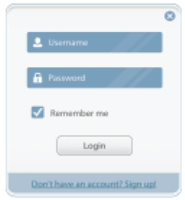
Michael Brunton-Spall **@bruntonspall**

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.

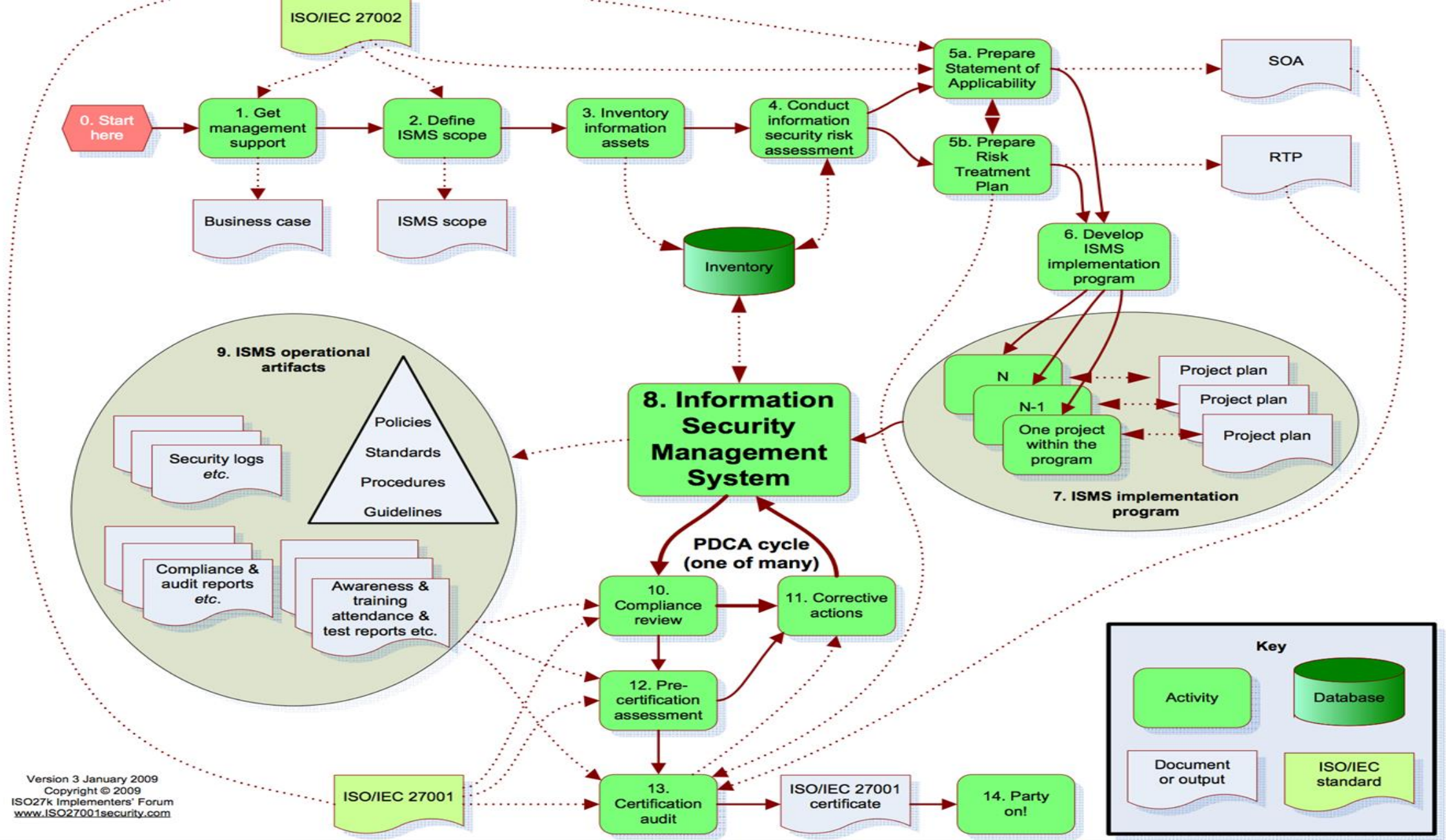
FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email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

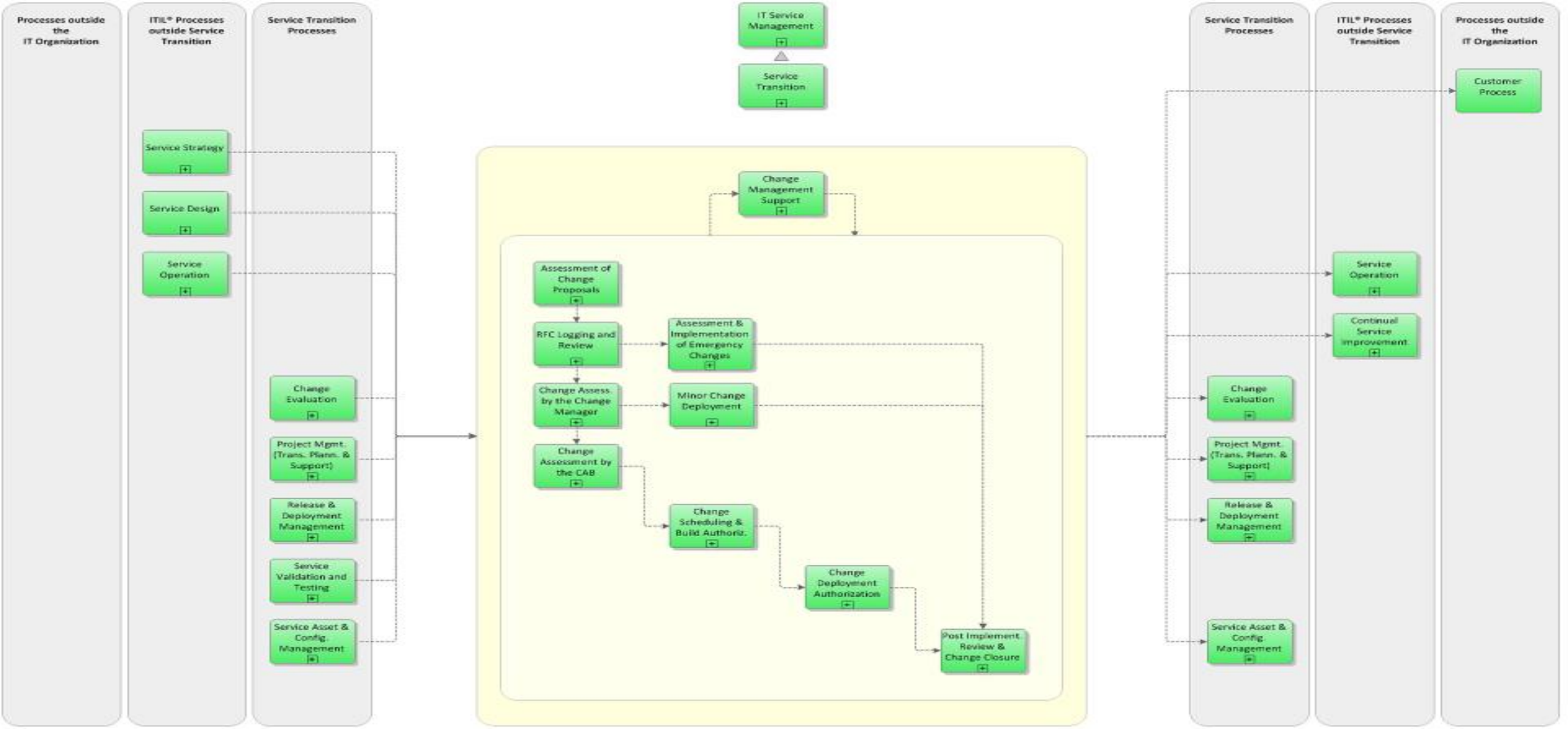

THE DARKHOTEL APT ATTACKS
DARK HOTEL
BACKDOOR
9.10pm
9.20pm
10pm
1 WI-FI
2
3 Done!
BACKDOOR
Documents
Secrets
Passwords
9.05pm

Security is not compliance

Certification
Accreditation
PCI
ISO27001


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
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
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Key
Activity
Database
Document or output
ISO/IEC standard
Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com

ITIL Change Management



Agile principles

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

Risk methodologies

Component based

IS1, ISO27005, NIST SP-800-30

System based

TOGAF, SABSA, Attack Trees

Michael Brunton-Spall **@bruntonspall**

Component Pro's
Thorough, Exhaustive, Objective

Systemic – Pro's
Subjective, Holistic, Interaction focused

Simple Systems – A bike

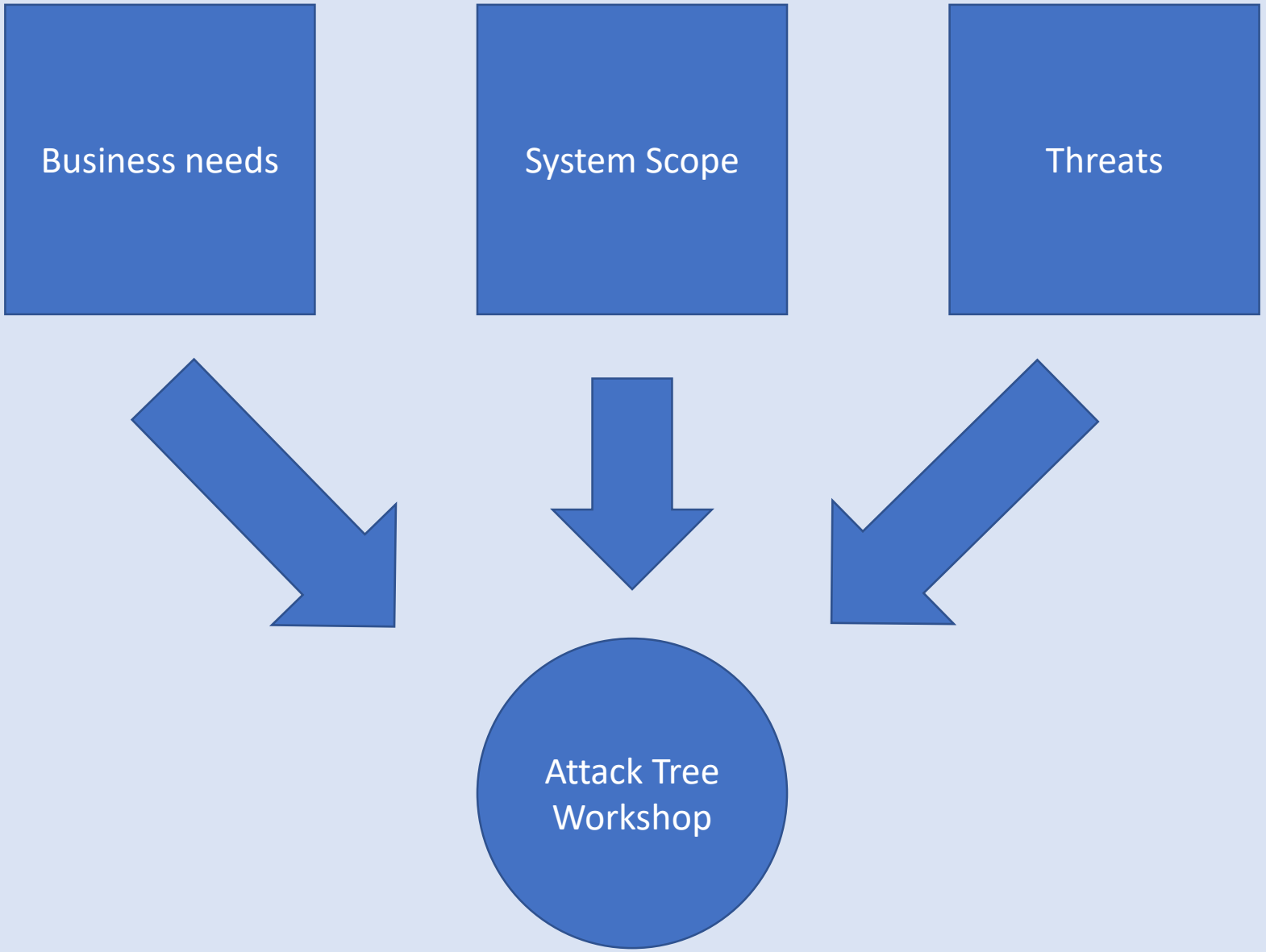
Complicated systems – A car

Complex Systems - Traffic

Michael Brunton-Spall **@bruntonspall**

We don’t solve motorway congestion by assuring tires

Attack trees


Business needs
System Scope
Threats
Attack Tree Workshop

Understand the business

Work out what’s in scope

Understand the threats

The Workshop

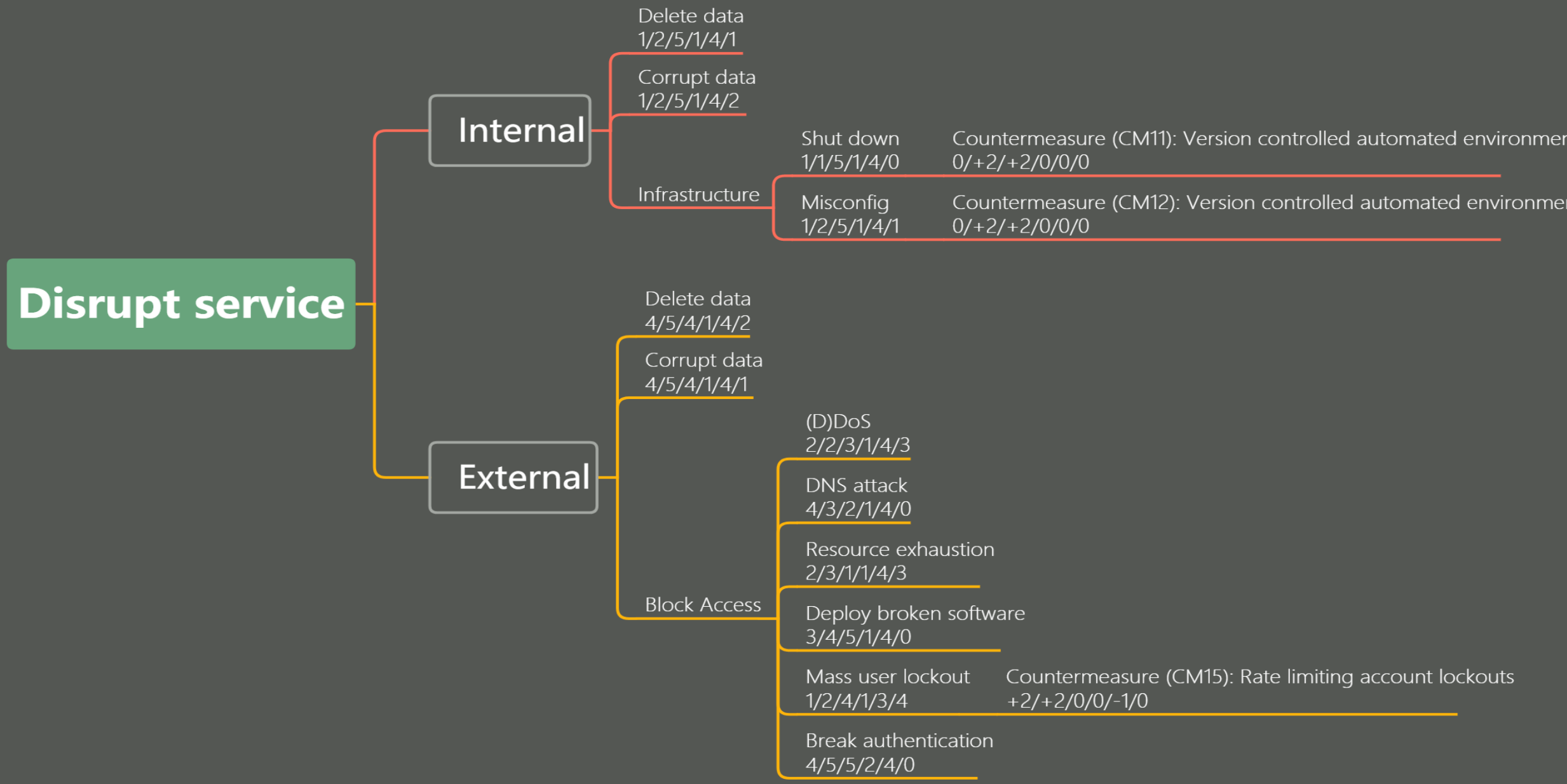
Who are the attackers?

What do they want?

How will they get it?

Workshop the attacks

Michael Brunton-Spall **@bruntonspall**


Disrupt service
Internal
Delete data
1/2/5/1/4/1
Corrupt data
1/2/5/1/4/2
Infrastructure
Shut down
1/1/5/1/4/0
Countermeasure (CM11): Version controlled automated environmer
0/+2/+2/0/0/0
Misconfig
1/2/5/1/4/1
Countermeasure (CM12): Version controlled automated environme
0/+2/+2/0/0/0
External
Delete data
4/5/4/1/4/2
Corrupt data
4/5/4/1/4/1
Block Access
(D)DoS
2/2/3/1/4/3
DNS attack
4/3/2/1/4/0
Resource exhaustion
2/3/1/1/4/3
Deploy broken software
3/4/5/1/4/0
Mass user lockout
1/2/4/1/3/4
Countermeasure (CM15): Rate limiting account lockouts
+2/+2/0/0/-1/0
Break authentication
4/5/5/2/4/0

Breadth first

Understand impact of attacks

Ranking 1-6, often order of magnitude increase

Cost to the attacker

Complexity of the attack

Consequences on the attacker

Reward to the attacker

Damage to the organisation

How often can it be repeated

Name	Cost	Complexity	Consequences	Reward	Damage	Replay	Risk	Countermeasures
» Malware Distribution » Email/Phish via password reset	3	2	2	3	3	4	MH **i**	
							MH **r**	
Get unauthorised access to relying party » Access to credentials » Bruteforce credentials » Guess email / password combo	1	2	2	3	3	3	MH **i**	
							MH **r**	
Get unauthorised access to relying party » Access to credentials » Bruteforce credentials » Guess password only	1	3	1	3	3	3	H **i**	
							MH	CM1:6

Post workshop

Determine countermeasures

In place and planned

Planned countermeasures go on the backlog

Repeat as needed

Fitting into the agile cycle

Workshop with whole team*

Visible outputs for walls

Threat Actor Personas

Misuse cases

Record decisions against stories

Record deferred security debt

Product Owner is in control

Attack Trees: System based risk methodology, for the whole team, iteratively updated

Any questions?

@bruntonspall
michael@brunton-spall.co.uk