goto; copenhagen

Does agile make us less secure?

Michael Brunton-Spall

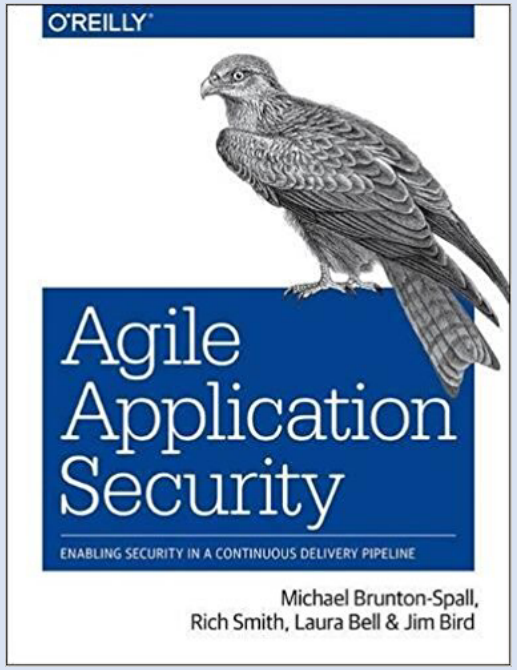
Follow us @gotocph

goto; copenhagen

GOTO Copenhagen 2019
Conference Nov. 18 - 20

Click ‘Rate Session’ to rate session and ask questions.

Follow us @gotocph



O'REILLY

Agile Application Security

ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE

Michael Brunton-Spall,
Rich Smith, Laura Bell & Jim Bird

Michael Brunton-Spall
He/His/Him

https://tinyletter.com/cyberweekly

Does agile make us less secure?

What is agile?

Individuals and Interactions over process and tools

Working software over comprehensive documentation

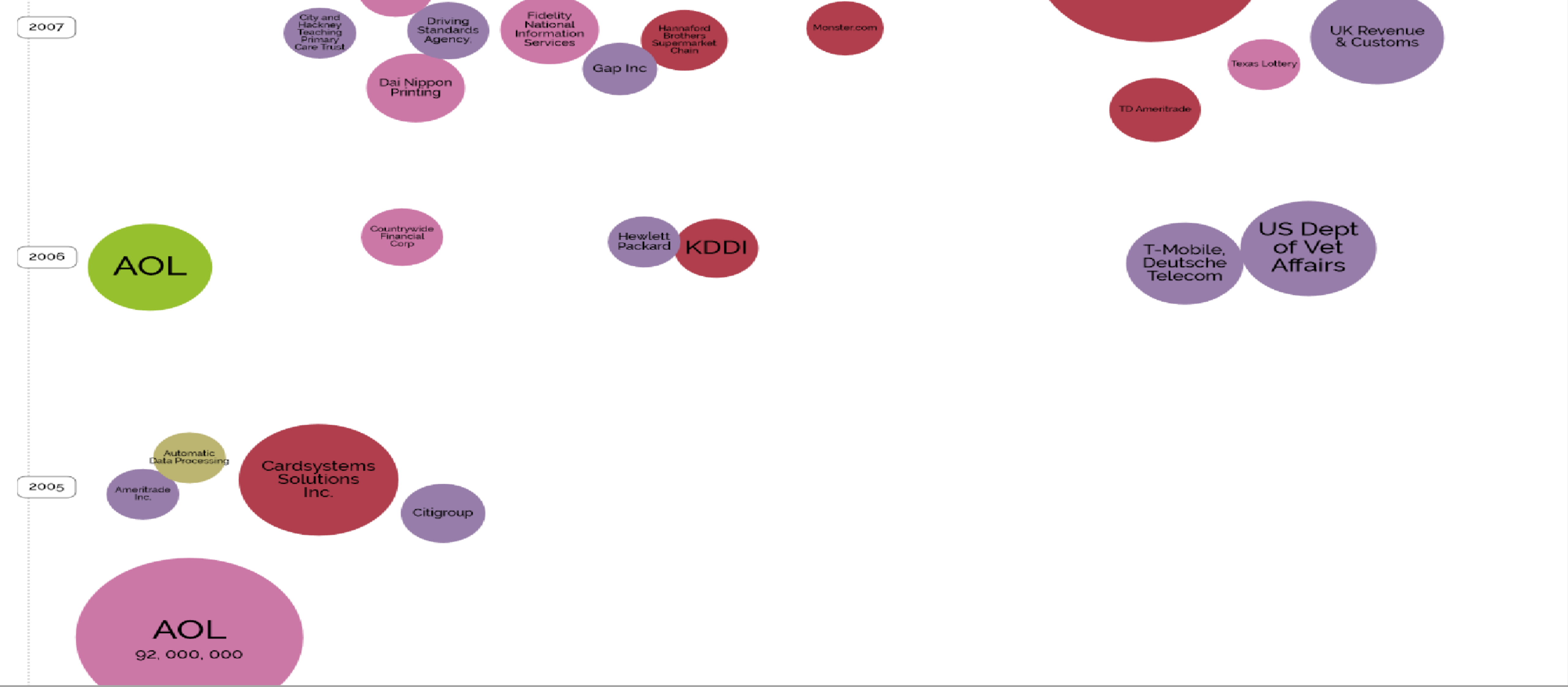
Customer collaboration over contract negotiation

Responding to change over following a plan

What is Security?

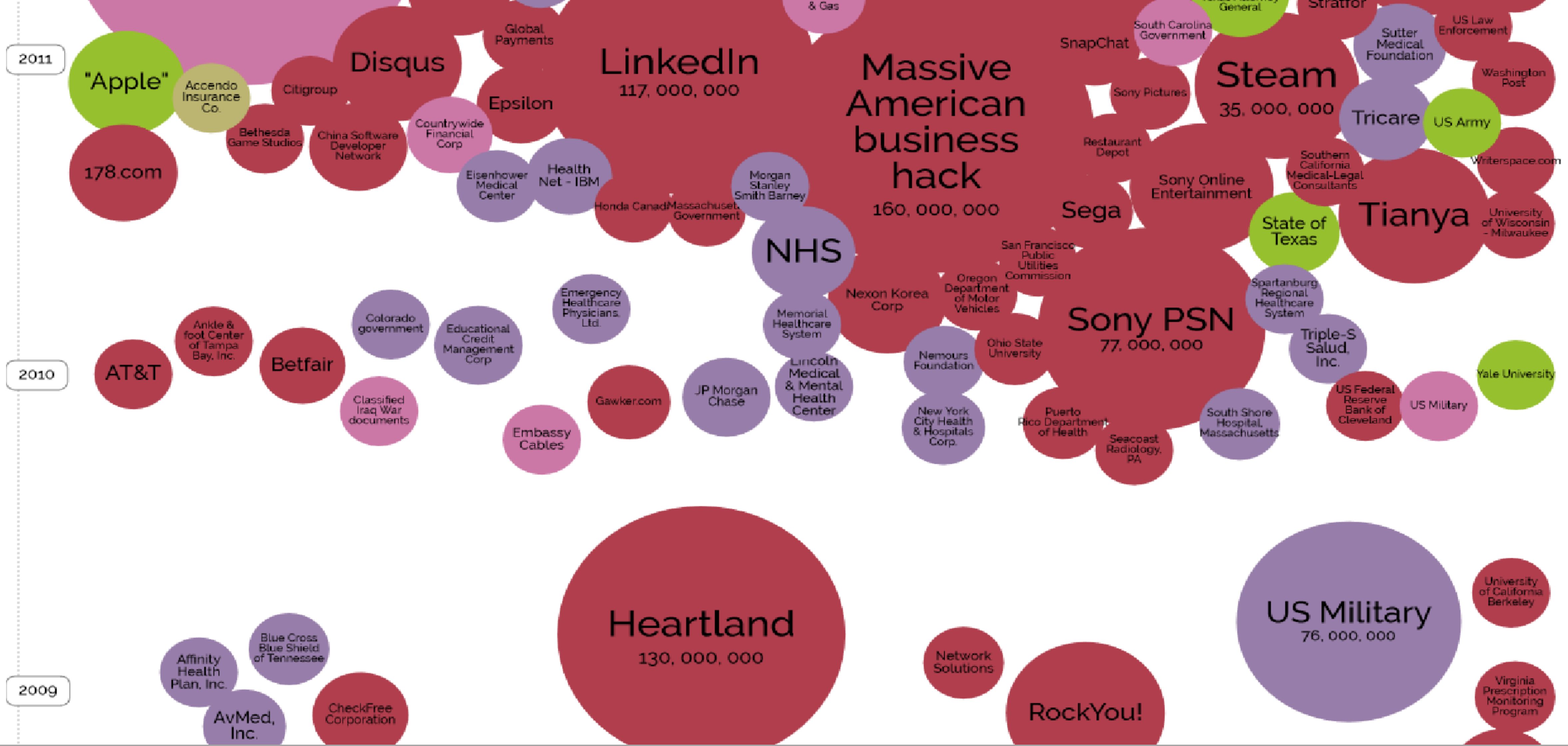
A process for assuring the preservation of confidentiality, integrity and availability of information

Security, in its current form, does not actually work



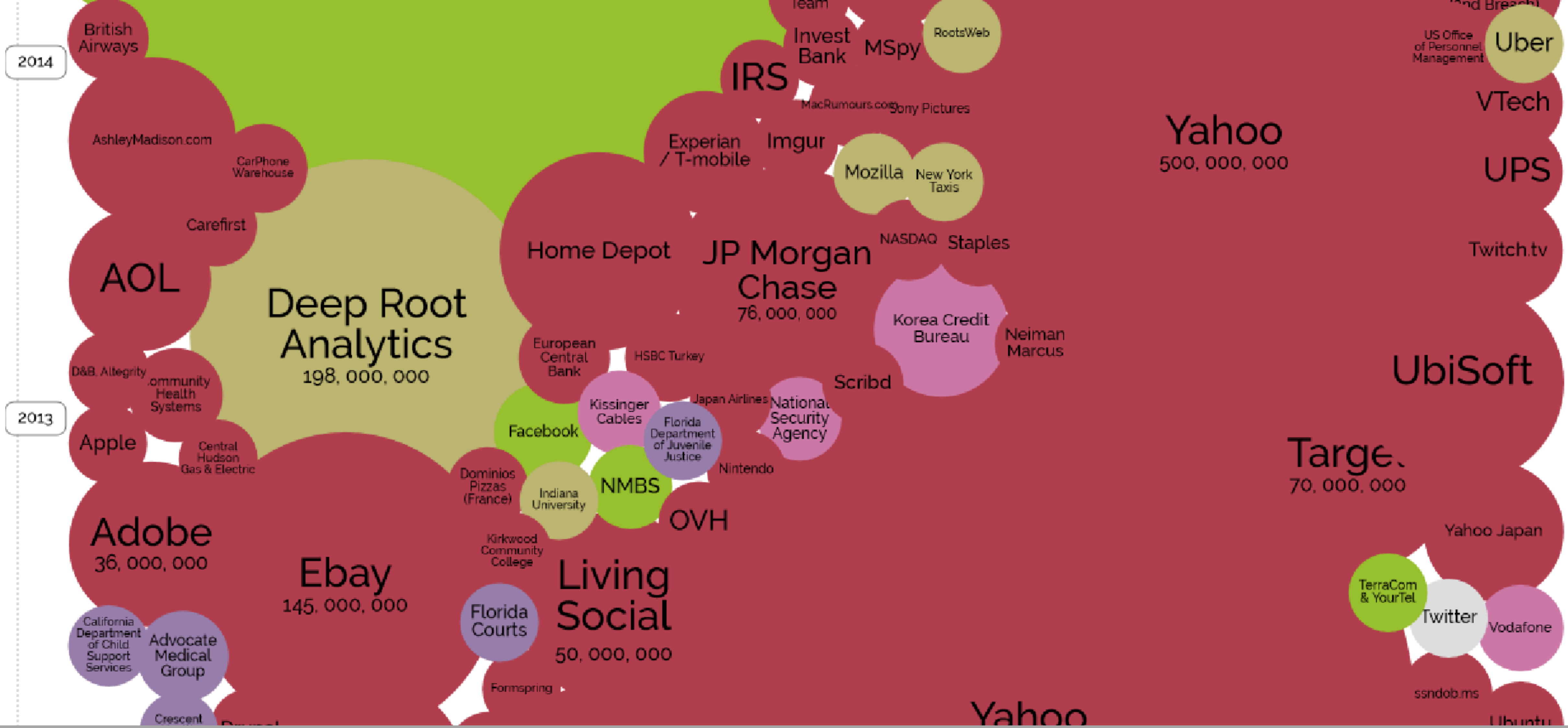
2006

Michael Brunton-Spall @bruntonspall



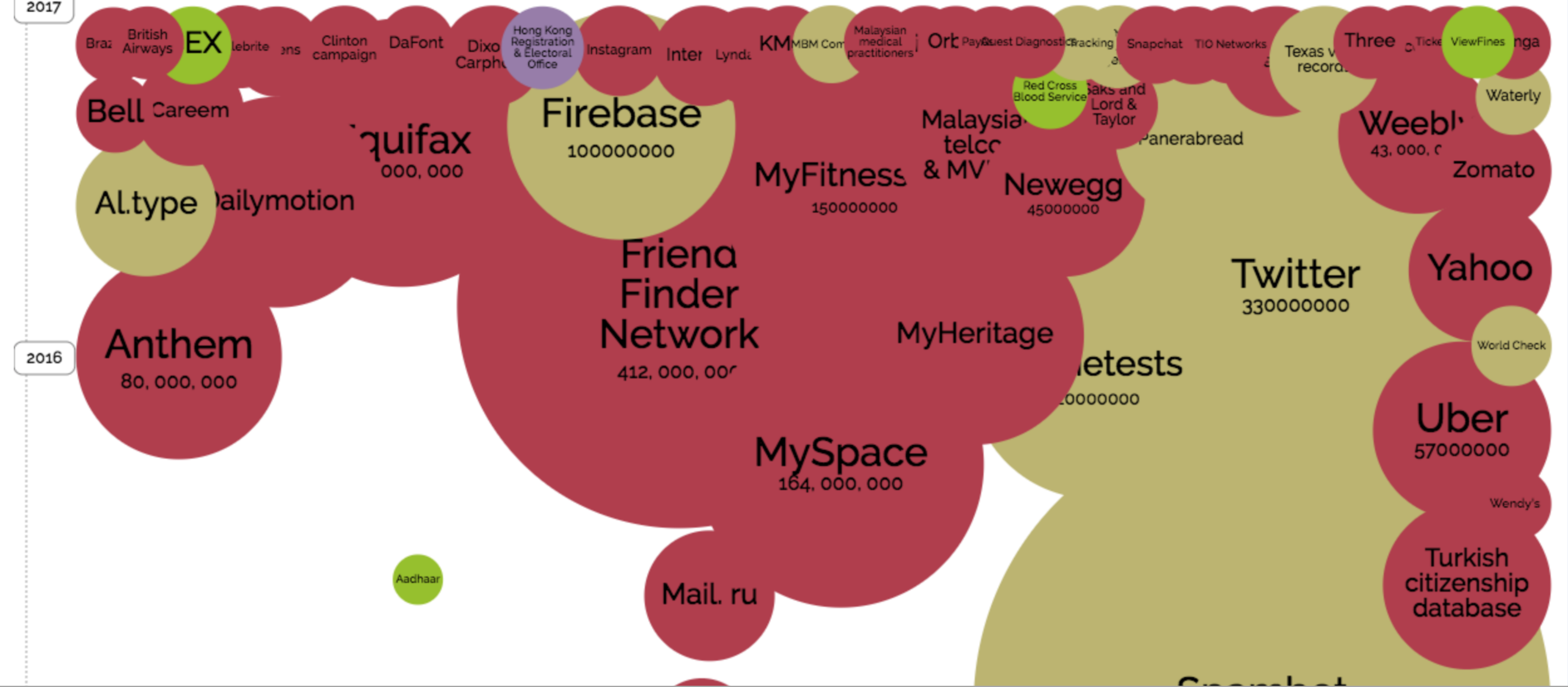
2010

Michael Brunton-Spall @bruntonspall



2013

Michael Brunton-Spall @bruntonspall

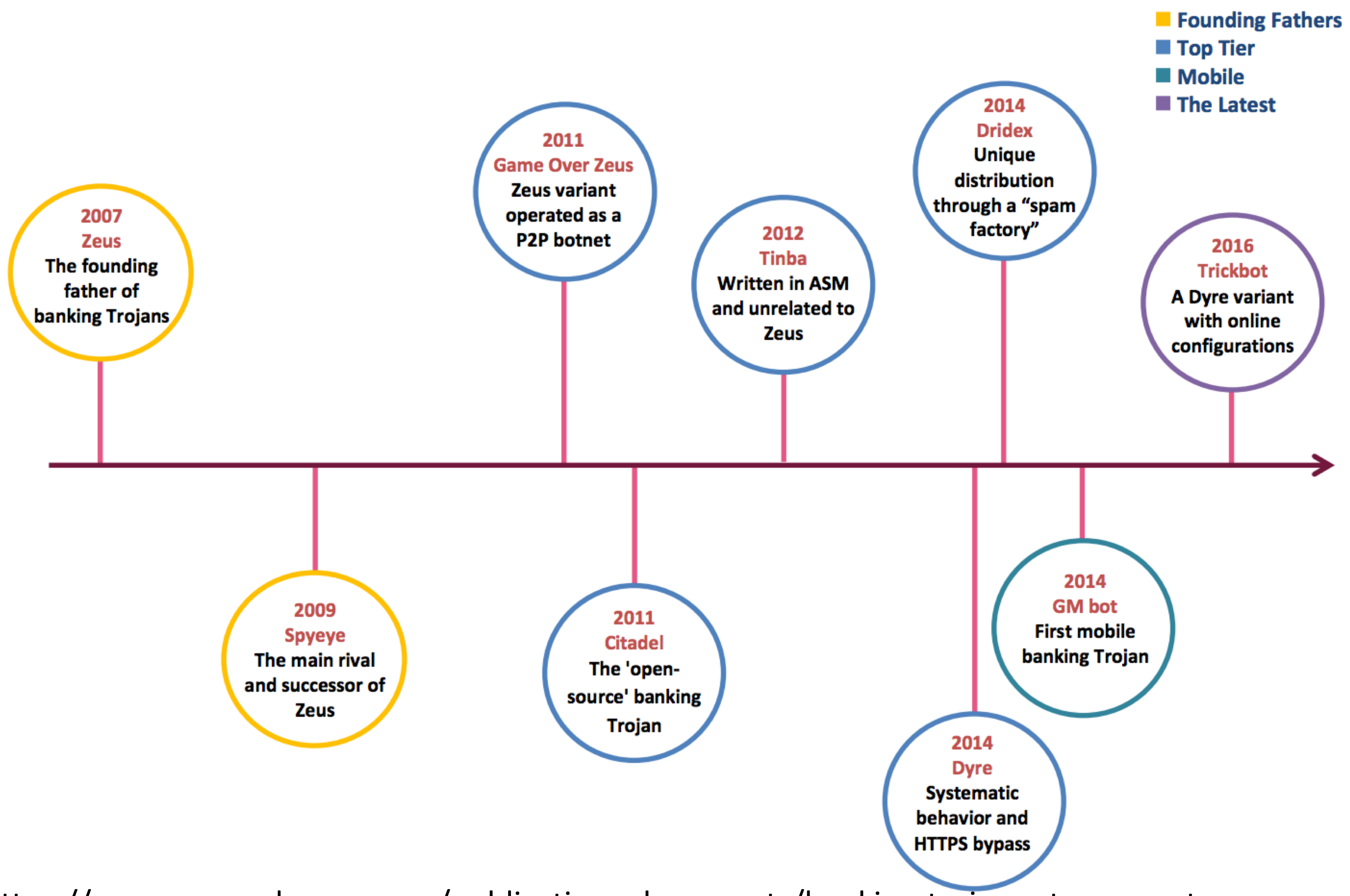

2017
2016
Braz
British Airways
EX
lebrite
ons
Clinton campaign
DaFont
Dixo Carph
Hong Kong Registration & Electoral Office
Instagram
Inter
Lynda
KM
MBM Com
Malaysian medical practitioners
Ork
Pay
Quest Diagnostics
Tracking
Snapchat
TIO Networks
Texas v record
Three
Ticke
ViewFines
nga
Red Cross Blood Service
Saks and Lord & Taylor
Waterly
Bell
Careem
quifax
000, 000
Firebase
100000000
Malaysia telco & MV
Panerabread
Weebl
43, 000, 0
Zomato
AI.type
Dailymotion
MyFitness
150000000
Newegg
45000000
Friend Finder Network
412, 000, 00
Twitter
330000000
Yahoo
MyHeritage
etests
0000000
World Check
Anthem
80, 000, 000
Uber
57000000
MySpace
164, 000, 000
Wendy's
Aadhaar
Mail. ru
Turkish citizenship database
Snapchat

2018

Criminal users on the internet

At least $1.5t a year

https://www.bromium.com/resource/into-the-web-of-profit/#



🟨 Founding Fathers
🟦 Top Tier
🟩 Mobile
🟪 The Latest

2007
Zeus
The founding father of banking Trojans

2009
Spyeye
The main rival and successor of Zeus

2011
Game Over Zeus
Zeus variant operated as a P2P botnet

2011
Citadel
The 'open-source' banking Trojan

2012
Tinba
Written in ASM and unrelated to Zeus

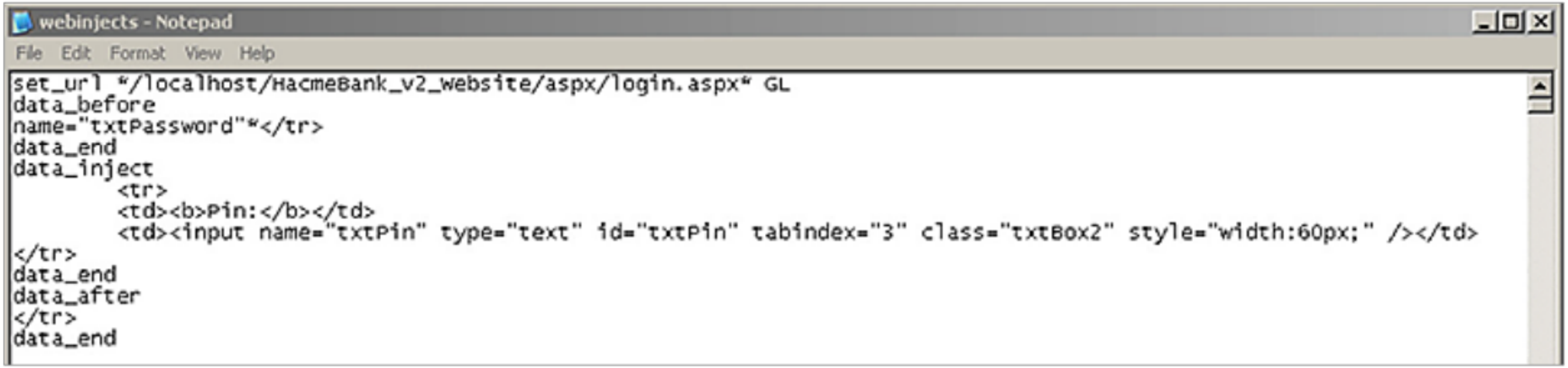
2014
Dyre
Systematic behavior and HTTPS bypass

2014
Dridex
Unique distribution through a "spam factory"

2014
GM bot
First mobile banking Trojan

2016
Trickbot
A Dyre variant with online configurations

https://www.europol.europa.eu/publications-documents/banking-trojans-stone-age-to-space



```
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
```

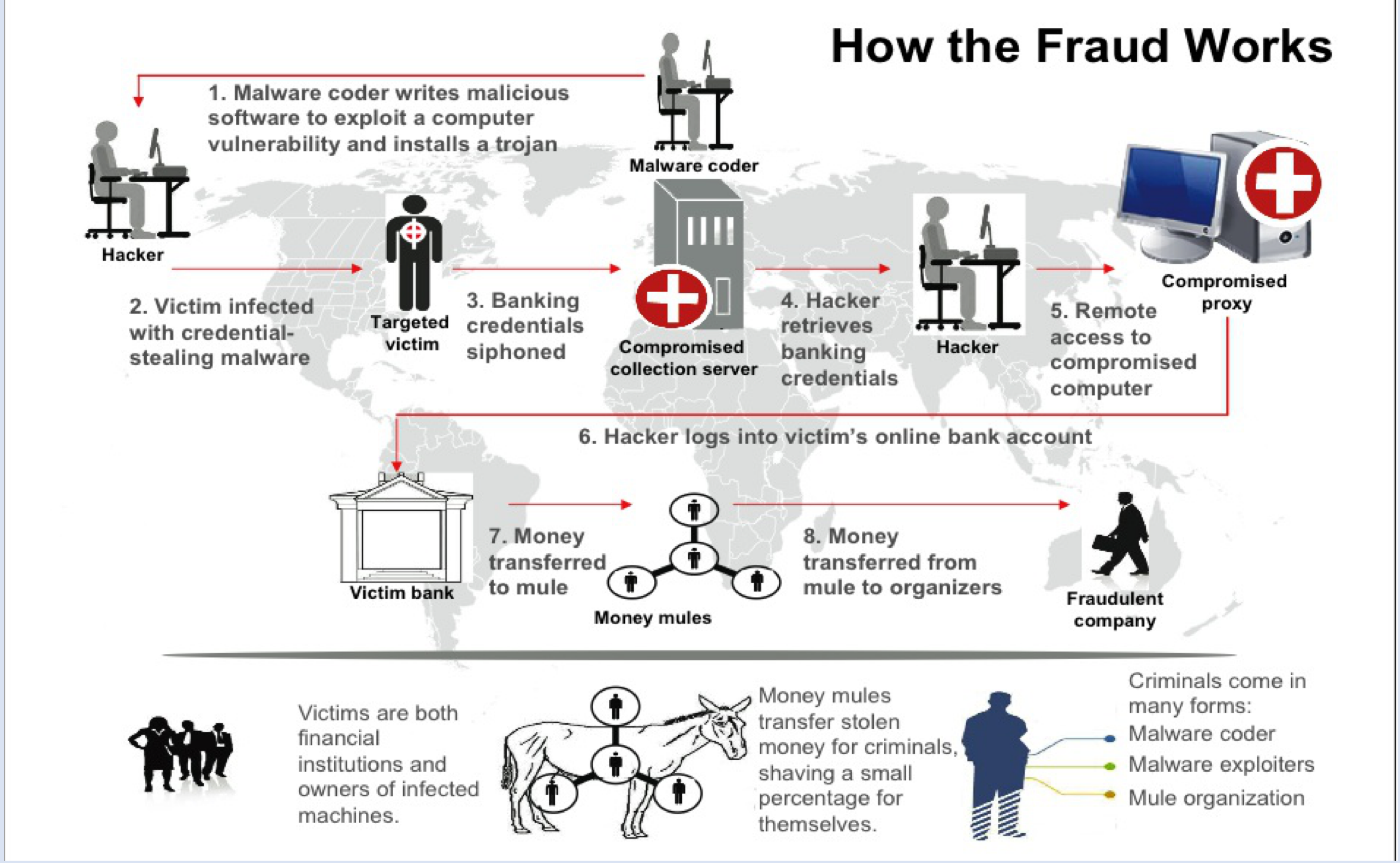
Figure 16: The webinject file is used by attackers to customize attacks for specific sites and applications

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

Platform Capitalism

Cybercrime as a service

https://www.bromium.com/resource/into-the-web-of-profit/#



How the Fraud Works

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

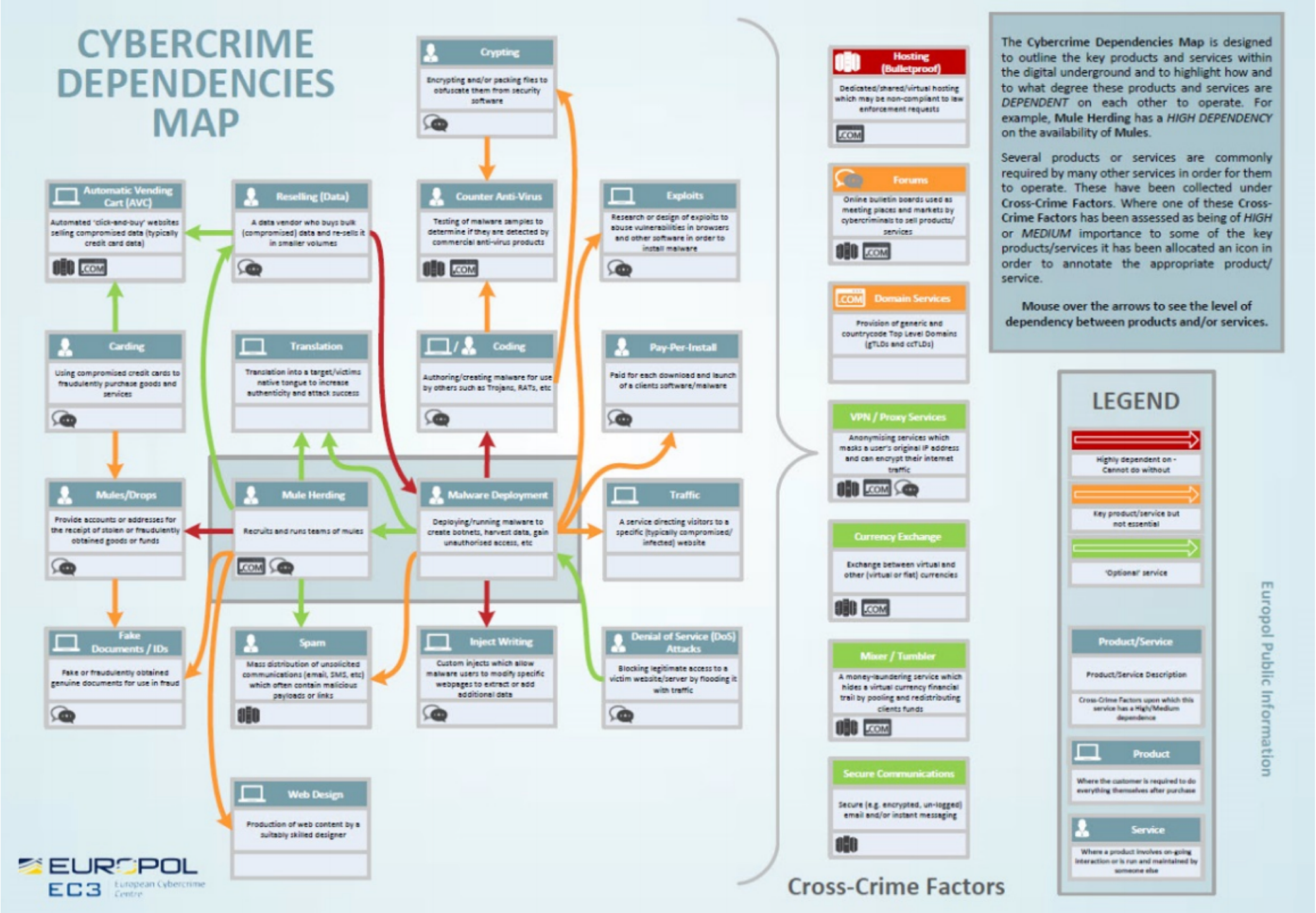
8. Money transferred from mule to organizers

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



CYBERCRIME DEPENDENCIES MAP

Crypting
Encrypting and/or packing files to obfuscate them from security software

Automatic Vending Cart (AVC)
Automated 'click-and-buy' websites selling compromised data (typically credit card data)

Reselling (Data)
A data vendor who buys bulk (compromised) data and re-sells it in smaller volumes

Counter Anti-Virus
Testing of malware samples to determine if they are detected by commercial anti-virus products

Exploits
Research or design of exploits to abuse vulnerabilities in browsers and other software in order to install malware

Carding
Using compromised credit cards to fraudulently purchase goods and services

Translation
Translation into a target/victims native tongue to increase authenticity and attack success

Coding
Authoring/creating malware for use by others such as Trojans, RATs, etc

Pay-Per-Install
Paid for each download and launch of a clients software/malware

Mules/Drops
Provide accounts or addresses for the receipt of stolen or fraudulently obtained goods or funds

Mule Herding
Recruits and runs teams of mules

Malware Deployment
Deploying/running malware to create botnets, harvest data, gain unauthorised access, etc

Traffic
A service directing visitors to a specific (typically compromised/infected) website

Fake Documents / IDs
Fake or fraudulently obtained genuine documents for use in fraud

Spam
Mass distribution of unsolicited communications (email, SMS, etc) which often contain malicious payloads or links

Inject Writing
Custom injects which allow malware users to modify specific webpages to extract or add additional data

Denial of Service (DoS) Attacks
Blocking legitimate access to a victim website/server by flooding it with traffic

Web Design
Production of web content by a suitably skilled designer

EUROPOL
EC3 European Cybercrime Centre

Cross-Crime Factors

Hosting (Bulletproof)
Dedicated/shared/virtual hosting which may be non-compliant to law enforcement requests

Forums
Online bulletin boards used as meeting places and markets by cybercriminals to sell products/services

Domain Services
Provision of generic and countrycode Top Level Domains (gTLDs and ccTLDs)

VPN / Proxy Services
Anonymising services which masks a user's original IP address and can encrypt their internet traffic

Currency Exchange
Exchange between virtual and other (virtual or fiat) currencies

Mixer / Tumbler
A money-laundering service which hides a virtual currency financial trail by pooling and redistributing clients funds

Secure Communications
Secure (e.g. encrypted, un-logged) email and/or instant messaging

The **Cybercrime Dependencies Map** is designed to outline the key products and services within the digital underground and to highlight how and to what degree these products and services are *DEPENDENT* on each other to operate. For example, **Mule Herding** has a *HIGH DEPENDENCY* on the availability of **Mules**.

Several products or services are commonly required by many other services in order for them to operate. These have been collected under **Cross-Crime Factors**. Where one of these **Cross-Crime Factors** has been assessed as being of *HIGH* or *MEDIUM* importance to some of the key products/services it has been allocated an icon in order to annotate the appropriate product/service.

Mouse over the arrows to see the level of dependency between products and/or services.

LEGEND

🟥 Highly dependent on - Cannot do without

🟧 Key product/service but not essential

🟩 'Optional' service

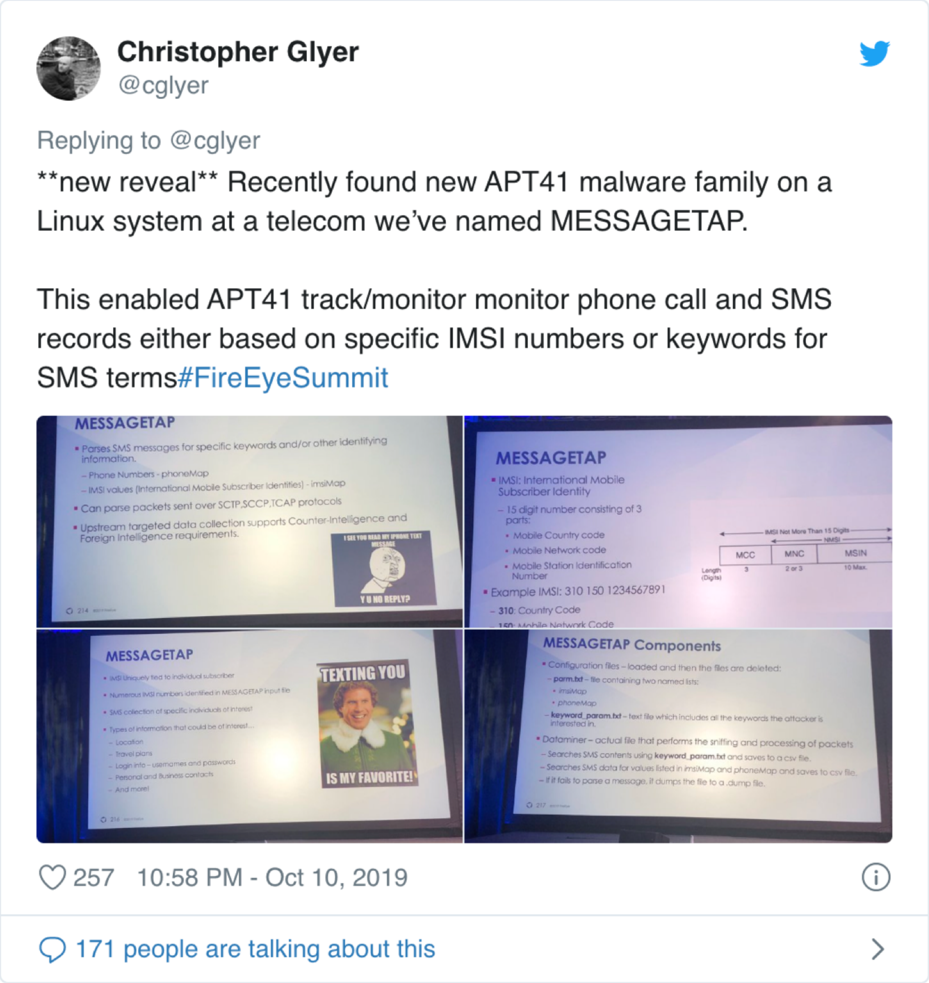
Product/Service
Product/Service Description
Cross-Crime Factors upon which this service has a High/Medium dependence

Product
Where the customer is required to do everything themselves after purchase

Service
Where a product involves on-going interaction or is run and maintained by someone else

Europol Public Information

Advanced Persistent Threats



Christopher Glyer
@cglyer

Replying to @cglyer

new reveal Recently found new APT41 malware family on a Linux system at a telecom we've named MESSAGETAP.

This enabled APT41 track/monitor monitor phone call and SMS records either based on specific IMSI numbers or keywords for SMS terms#FireEyeSummit

MESSAGETAP

- Parses SMS messages for specific keywords and/or other identifying information.
  - Phone Numbers - phoneMap
  - IMSI values (International Mobile Subscriber Identities) - imsiMap
- Can parse packets sent over SCTP,SCCP,TCAP protocols
- Upstream targeted data collection supports Counter-Intelligence and Foreign Intelligence requirements.

MESSAGETAP

- IMSI: International Mobile Subscriber Identity
  - 15 digit number consisting of 3 parts:
    - Mobile Country code
    - Mobile Network code
    - Mobile Station Identification Number
- Example IMSI: 310 150 1234567891
  - **310**: Country Code
  - 150: Mobile Network Code

MESSAGETAP

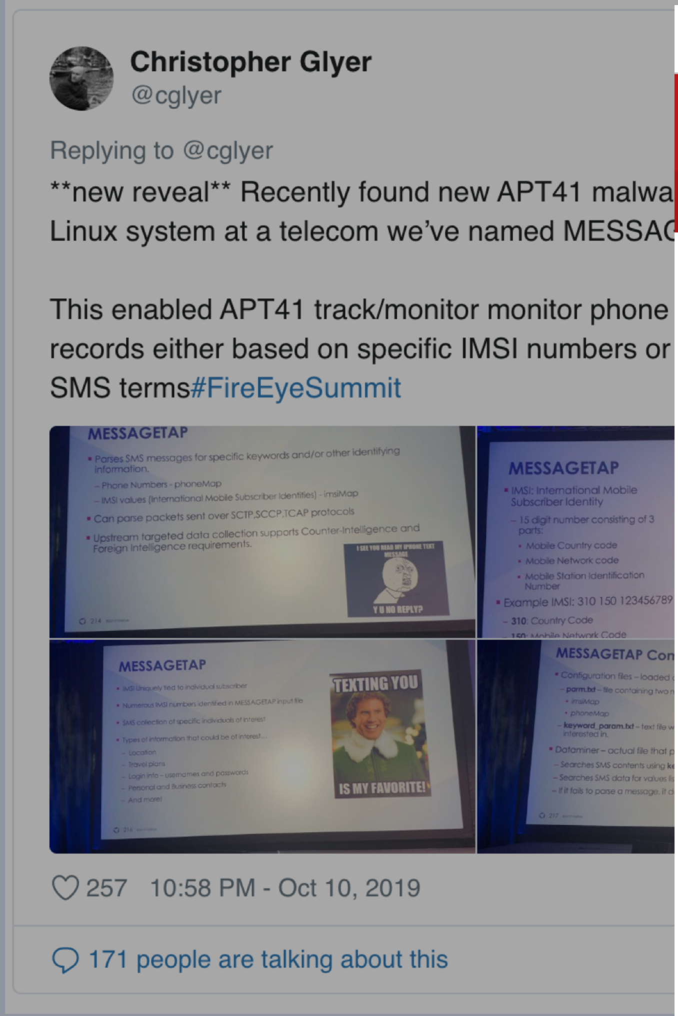
- IMSI Uniquely tied to individual subscriber
- Numerous IMSI numbers identified in MESSAGETAP input file
- SMS collection of specific individuals of interest
- Types of information that could be of interest...
  - Location
  - Travel plans
  - Login info – usernames and passwords
  - Personal and Business contacts
  - And more!

MESSAGETAP Components

- Configuration files – loaded and then the files are deleted:
  - **parm.txt** – file containing two named lists:
    - *imsiMap*
    - *phoneMap*
  - **keyword_param.txt** – text file which includes all the keywords the attacker is interested in.
- Dataminer – actual file that performs the sniffing and processing of packets
  - Searches SMS contents using **keyword_param.txt** and saves to a csv file.
  - Searches SMS data for values listed in *imsiMap* and *phoneMap* and saves to csv file.
  - If it fails to parse a message, it dumps the file to a .dump file.

257 10:58 PM - Oct 10, 2019

171 people are talking about this



Christopher Glyer
@cglyer

Replying to @cglyer

new reveal Recently found new APT41 malwa
Linux system at a telecom we've named MESSAG

This enabled APT41 track/monitor monitor phone
records either based on specific IMSI numbers or
SMS terms#FireEyeSummit

MESSAGETAP
- Parses SMS messages for specific keywords and/or other identifying information.
  - Phone Numbers - phoneMap
  - IMSI values (International Mobile Subscriber Identities) - imsiMap
- Can parse packets sent over SCTP,SCCP,TCAP protocols
- Upstream targeted data collection supports Counter-Intelligence and Foreign Intelligence requirements.

214

MESSAGETAP
- IMSI: International Mobile Subscriber Identity
  - 15 digit number consisting of 3 parts:
    - Mobile Country code
    - Mobile Network code
    - Mobile Station Identification Number
- Example IMSI: 310 150 123456789
  - 310: Country Code
  - 150: Mobile Network Code

MESSAGETAP
- IMSI Uniquely tied to individual subscriber
- Numerous IMSI numbers identified in MESSAGETAP input file
- SMS collection of specific individuals of interest
- Types of information that could be of interest...
  - Location
  - Travel plans
  - Login info – usernames and passwords
  - Personal and Business contacts
  - And more!

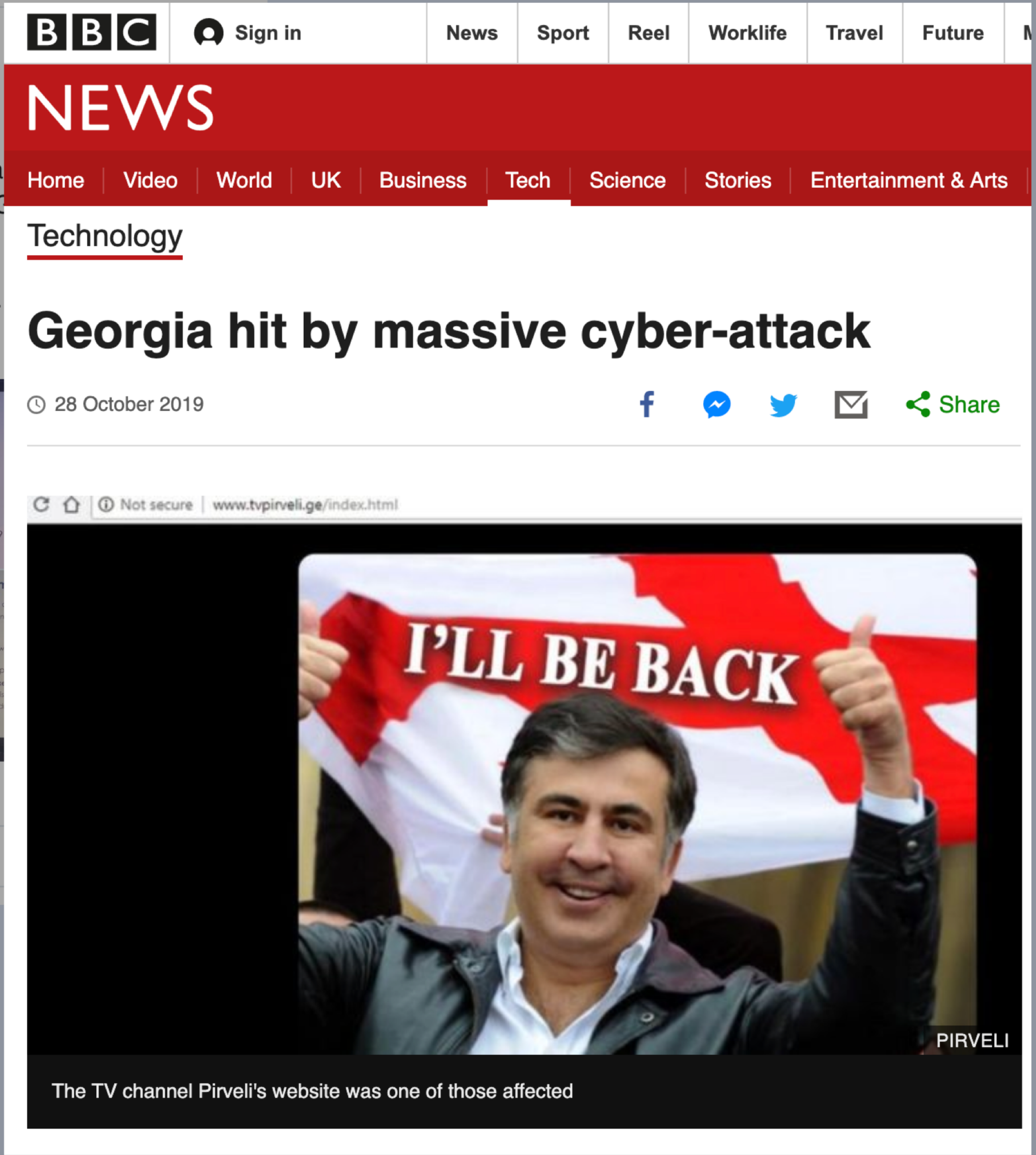
216

MESSAGETAP Con
- Configuration files – loaded
  - parm.txt – file containing two
    - imsiMap
    - phoneMap
  - keyword_param.txt – text file w interested in.
- Dataminer – actual file that p
  - Searches SMS contents using ke
  - Searches SMS data for values lis
  - If it fails to parse a message, it d

217

257 10:58 PM - Oct 10, 2019

171 people are talking about this



NEWS

Technology

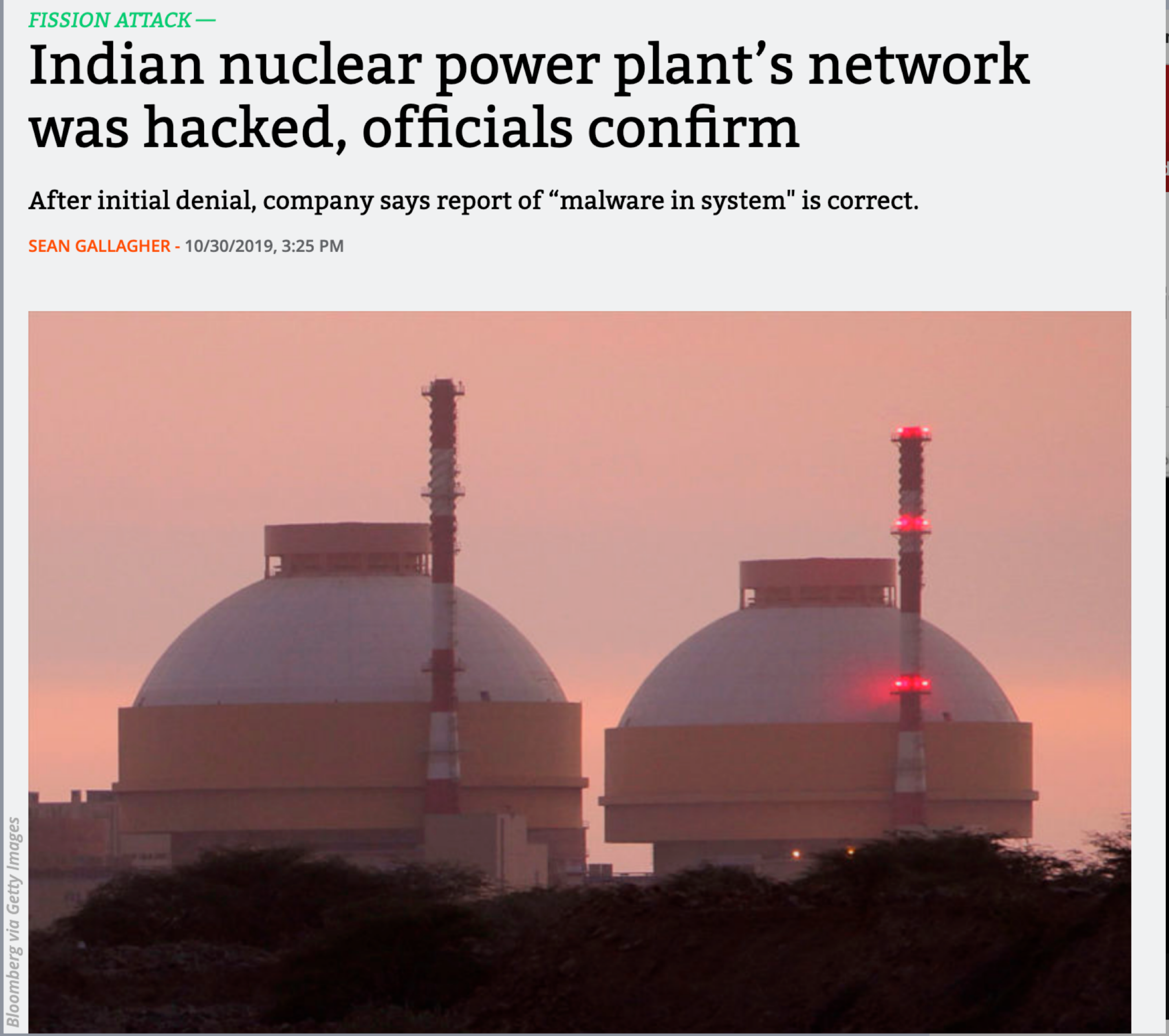
Georgia hit by massive cyber-attack

28 October 2019

Not secure | www.tvpirveli.ge/index.html

PIRVELI

The TV channel Pirveli's website was one of those affected



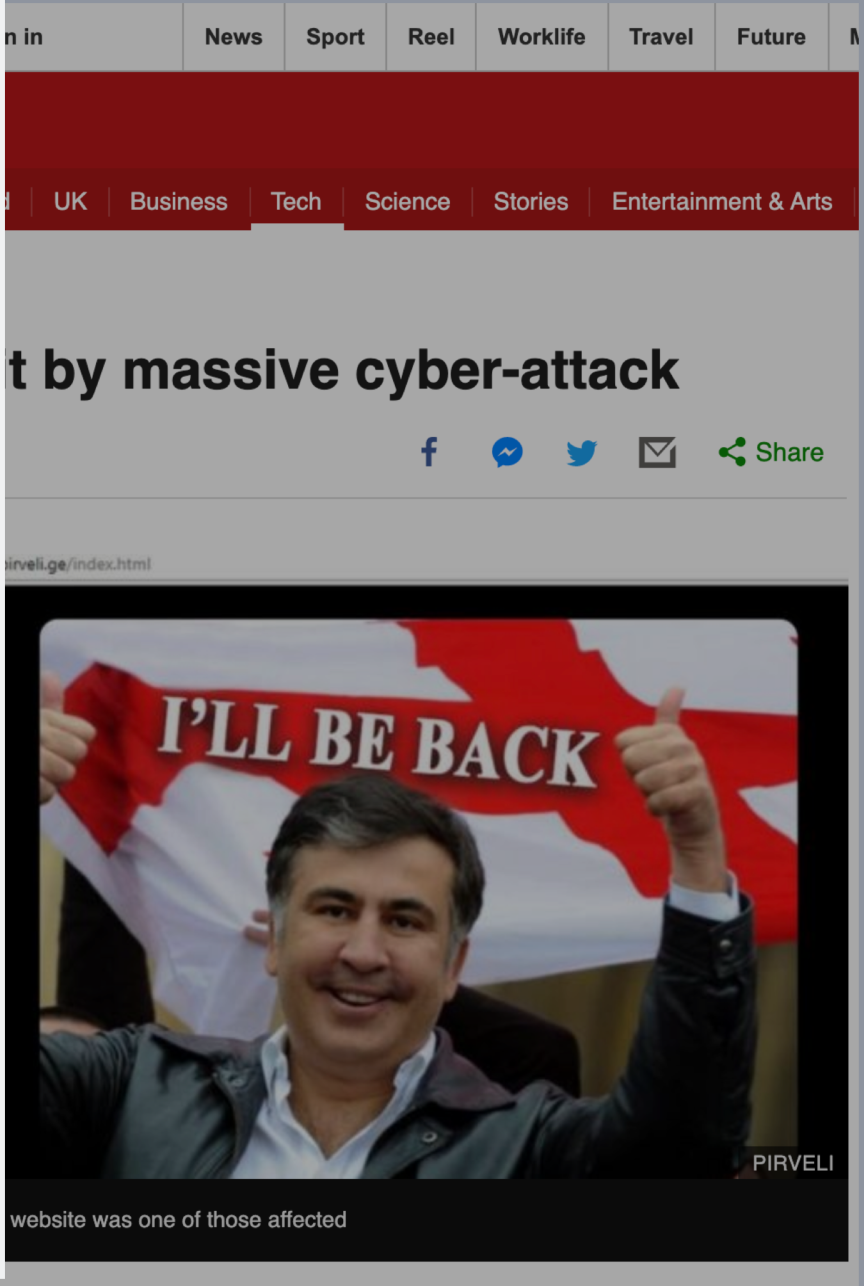
FISSION ATTACK —

Indian nuclear power plant's network was hacked, officials confirm

After initial denial, company says report of "malware in system" is correct.

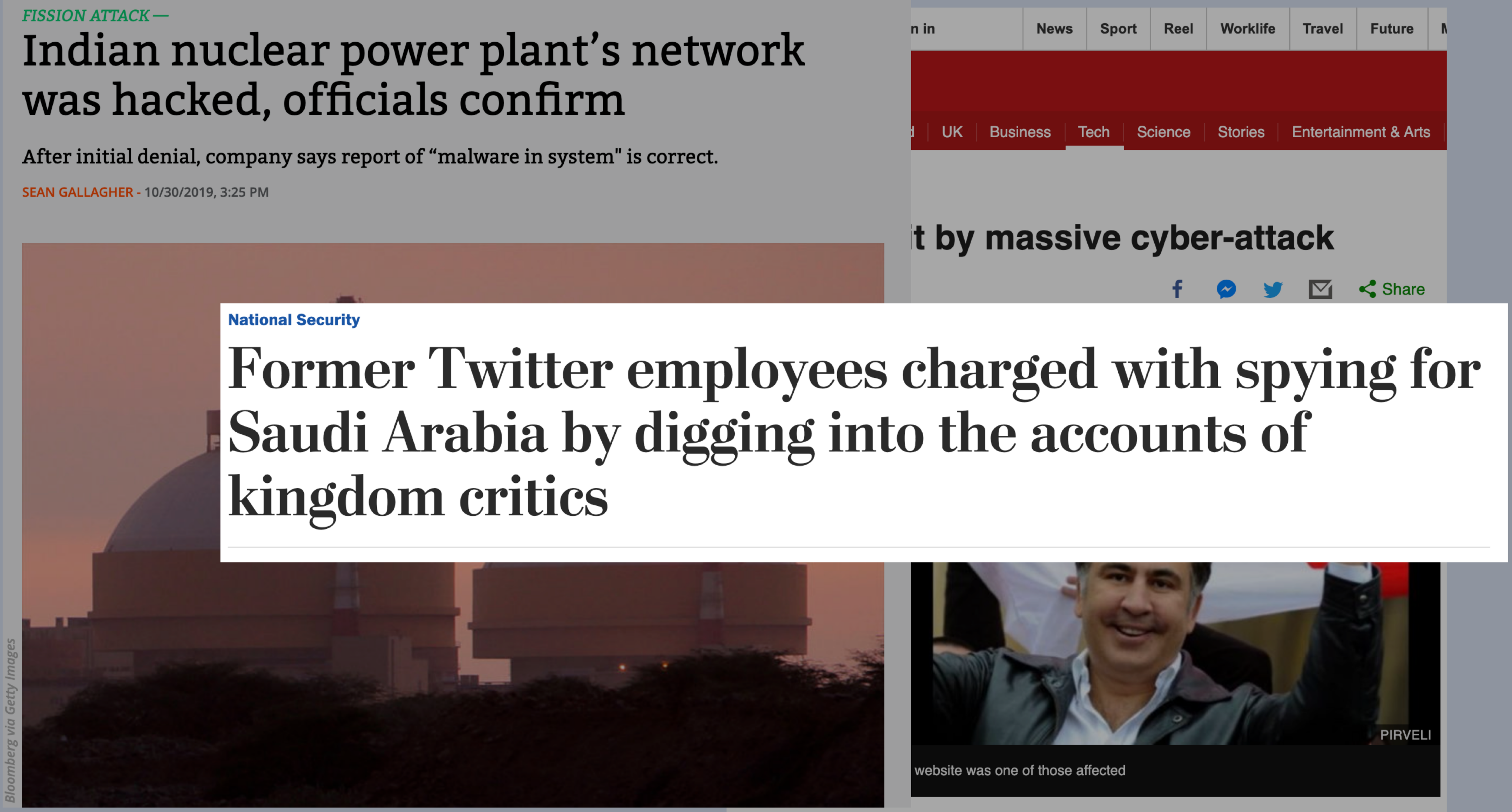
SEAN GALLAGHER - 10/30/2019, 3:25 PM

Bloomberg via Getty Images



t by massive cyber-attack

website was one of those affected



FISSION ATTACK —

Indian nuclear power plant’s network was hacked, officials confirm

After initial denial, company says report of “malware in system" is correct.

SEAN GALLAGHER - 10/30/2019, 3:25 PM

Bloomberg via Getty Images

n in | News | Sport | Reel | Worklife | Travel | Future | M

UK | Business | Tech | Science | Stories | Entertainment & Arts

t by massive cyber-attack

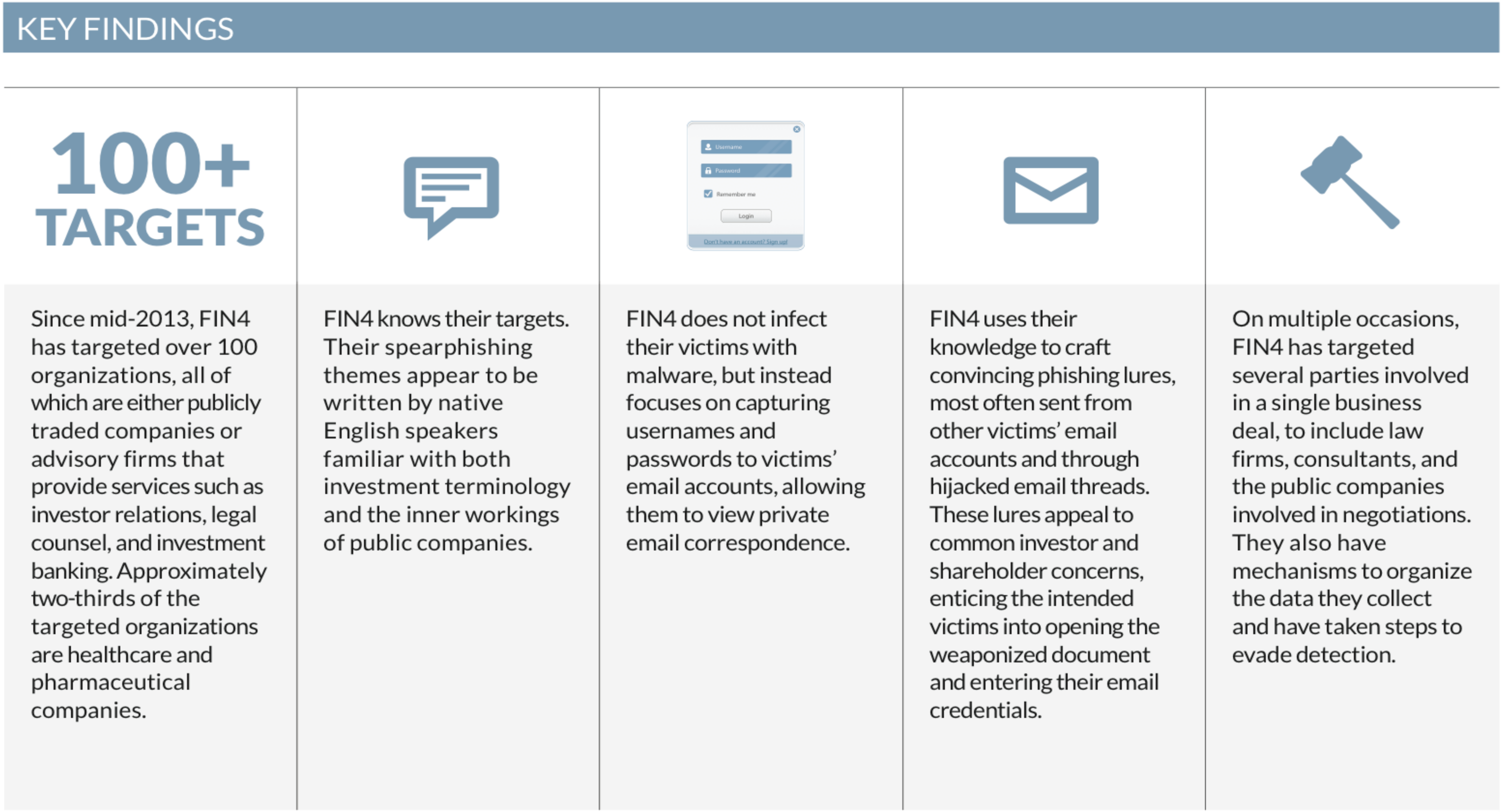
Share

PIRVELI

website was one of those affected

National Security

Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics



Username
Password
Remember me
Login
Don't have an account? Sign up!

KEY FINDINGS

100+ TARGETS

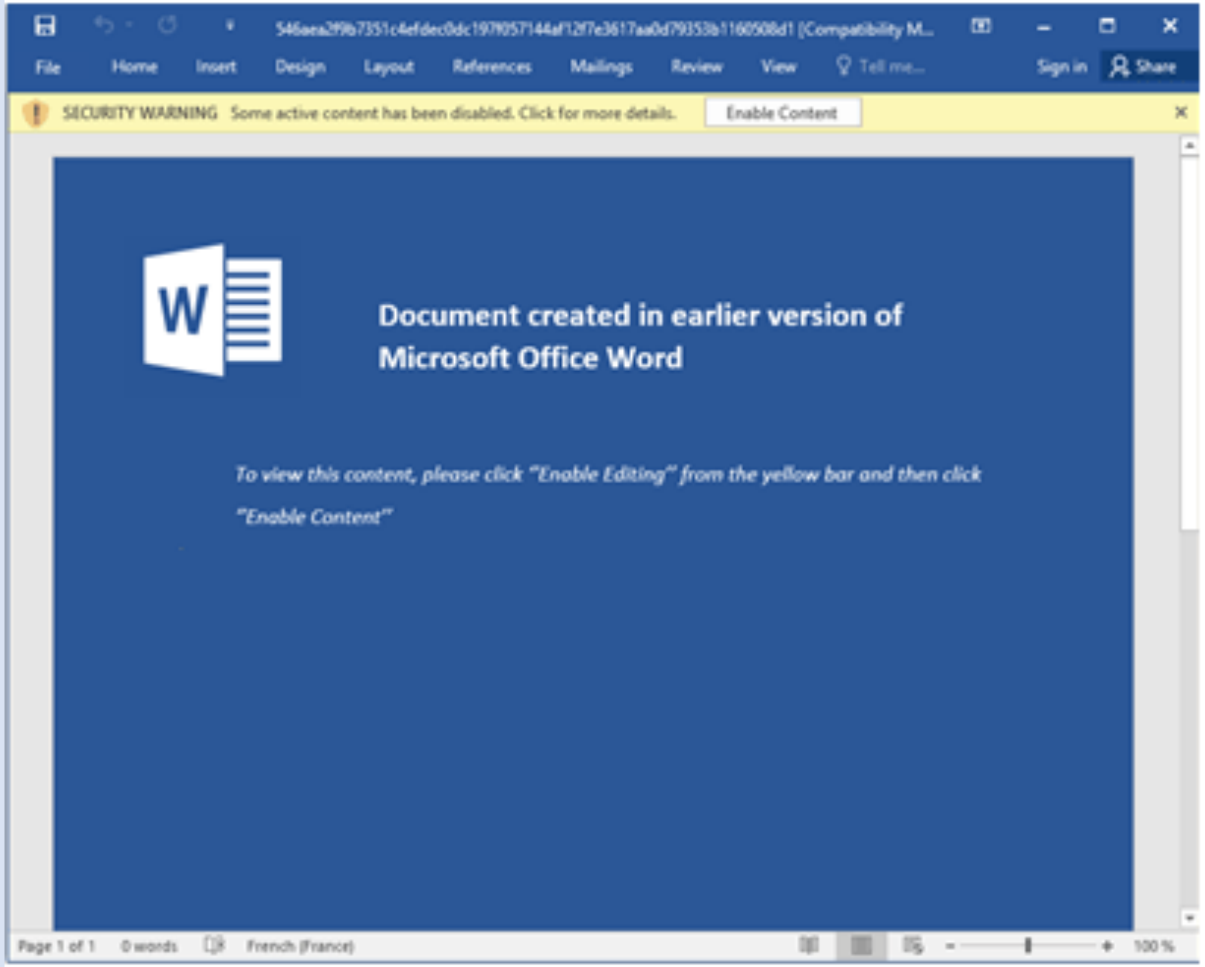
Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical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

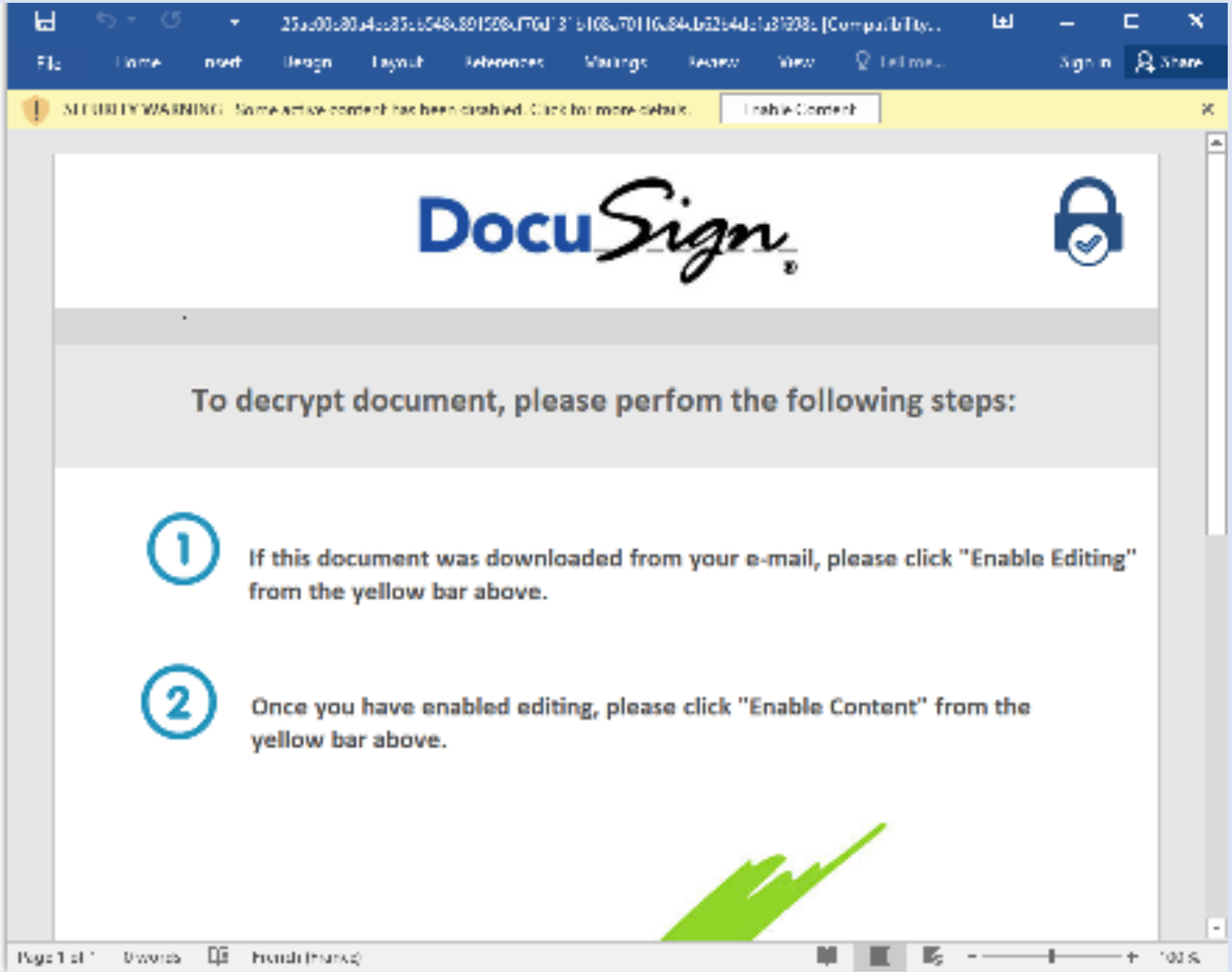
On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.



SECURITY WARNING Some active content has been disabled. Click for more details.

Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"



SECURITY WARNING Some active content has been disabled. Click for more details.

To decrypt document, please perfom the following steps:

1. If this document was downloaded from your e-mail, please click "Enable Editing" from the yellow bar above.

2. Once you have enabled editing, please click "Enable Content" from the the yellow bar above.

What is our defense?

Certification

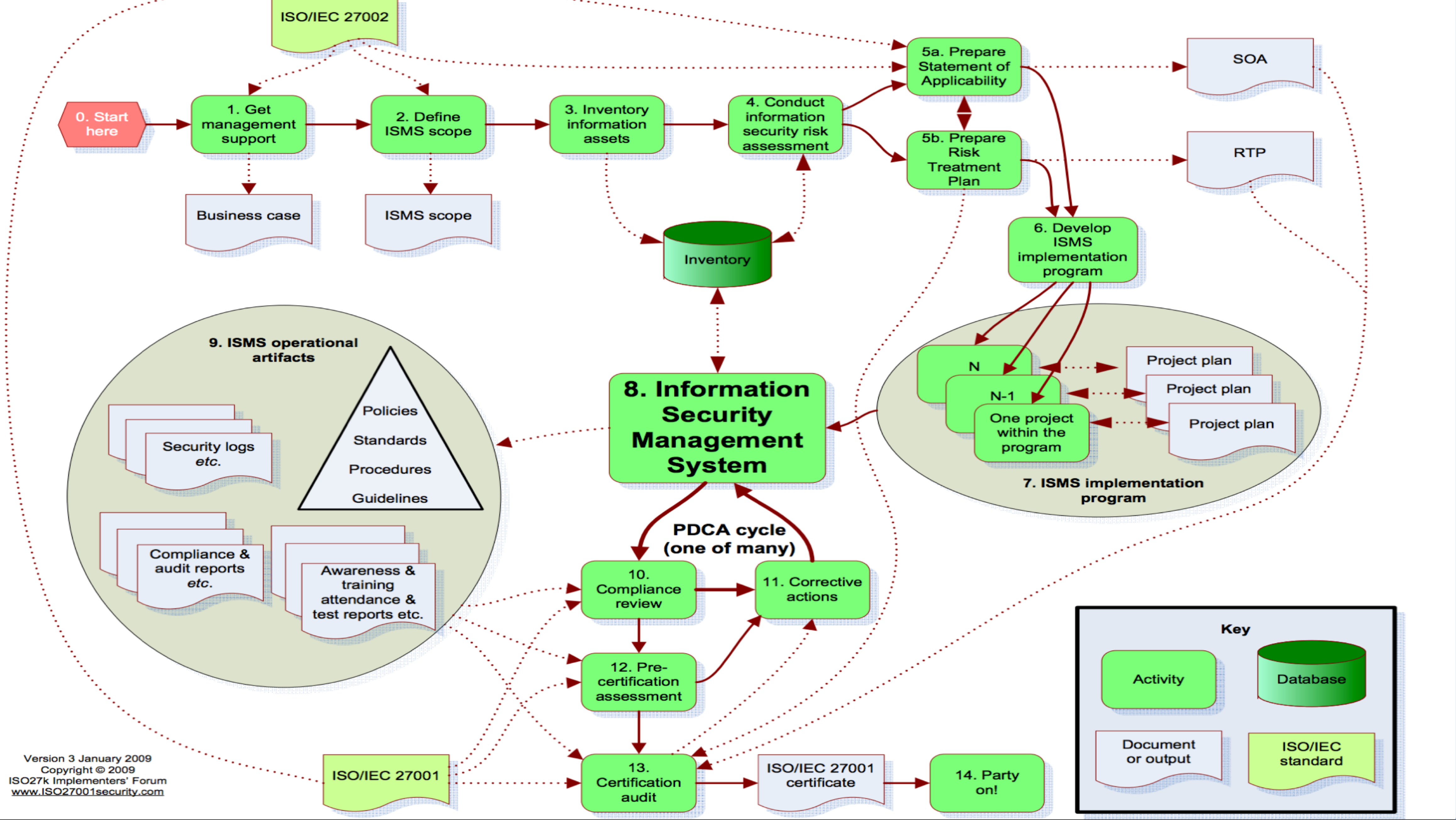
Certification
Accreditation

Certification

Accreditation

PCI

Certification
Accreditation
PCI
ISO27001

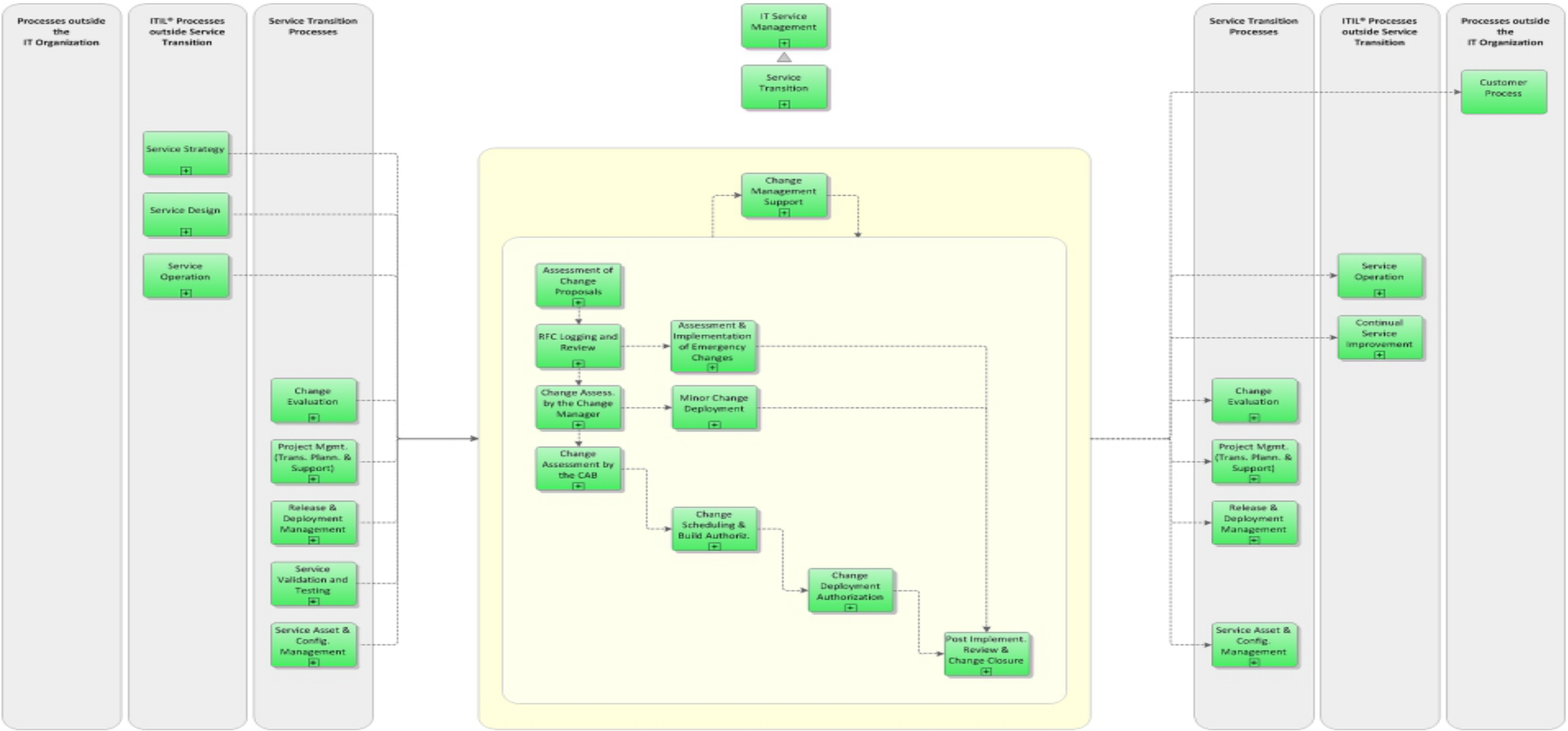

ISO/IEC 27002
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Conduct information security risk assessment
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
ISMS scope
Inventory
6. Develop ISMS implementation program
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 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

Michael Brunton-Spall @bruntonspall

Change control

ITIL Change Management

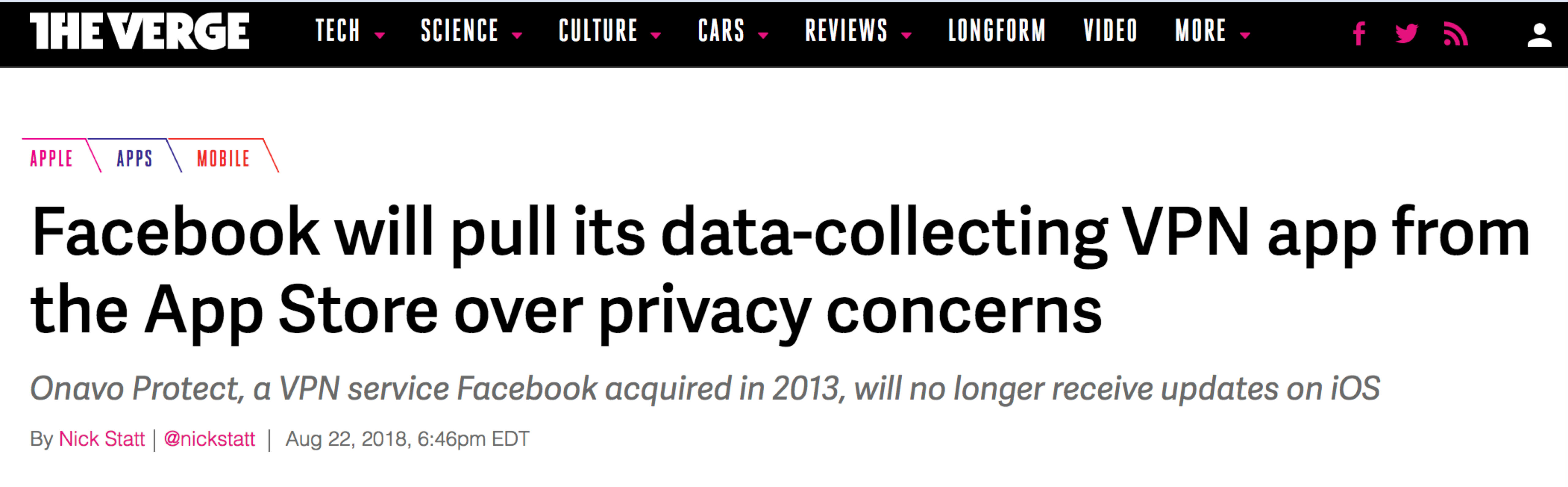

Processes outside the IT Organization
ITIL® Processes outside Service Transition
Service Transition Processes
IT Service Management
Service Transition
Service Transition Processes
ITIL® Processes outside Service Transition
Processes outside the IT Organization
Customer Process
Service Strategy
Service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

Who does this?

Large Organisations?

Security Organisations?

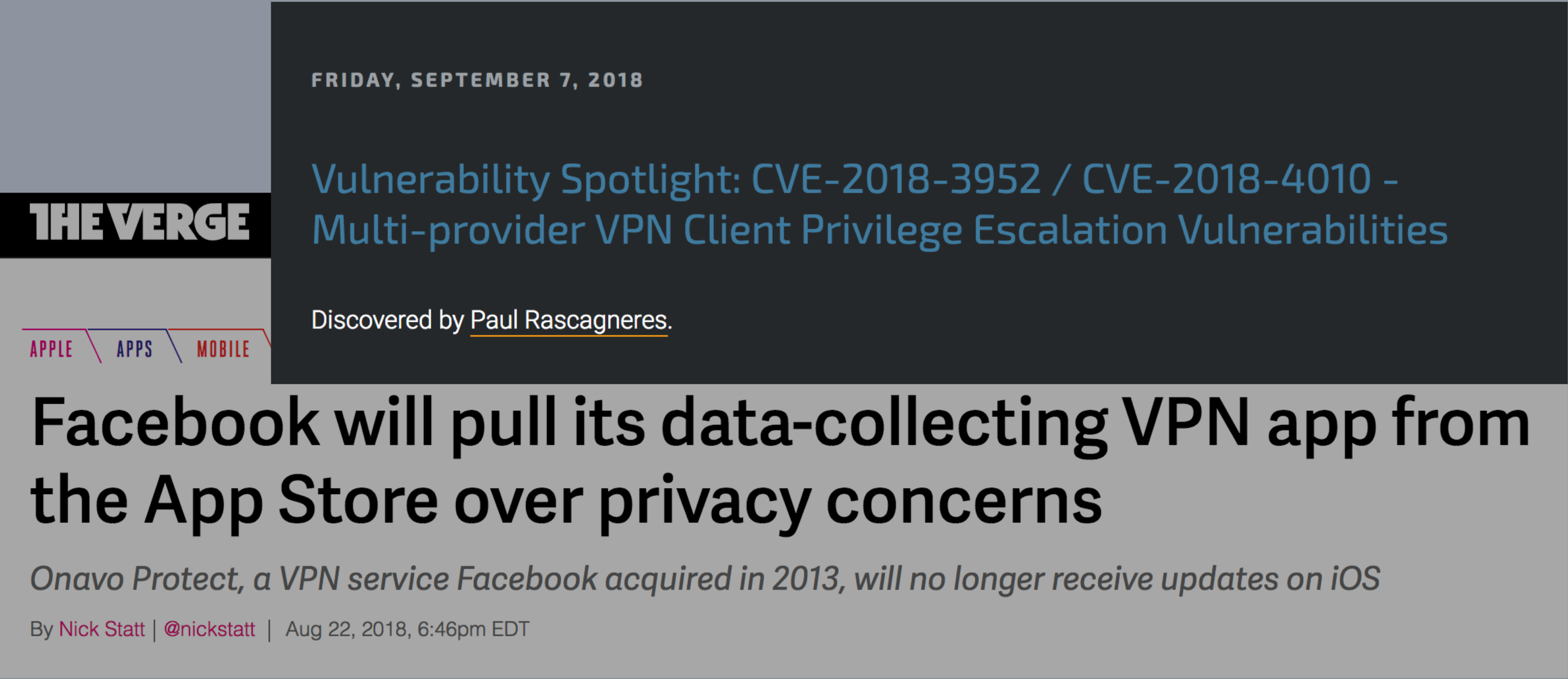
People with big budgets?



Facebook will pull its data-collecting VPN app from the App Store over privacy concerns

Onavo Protect, a VPN service Facebook acquired in 2013, will no longer receive updates on iOS

By Nick Statt | @nickstatt | Aug 22, 2018, 6:46pm EDT



FRIDAY, SEPTEMBER 7, 2018

Vulnerability Spotlight: CVE-2018-3952 / CVE-2018-4010 - Multi-provider VPN Client Privilege Escalation Vulnerabilities

Discovered by Paul Rascagneres.

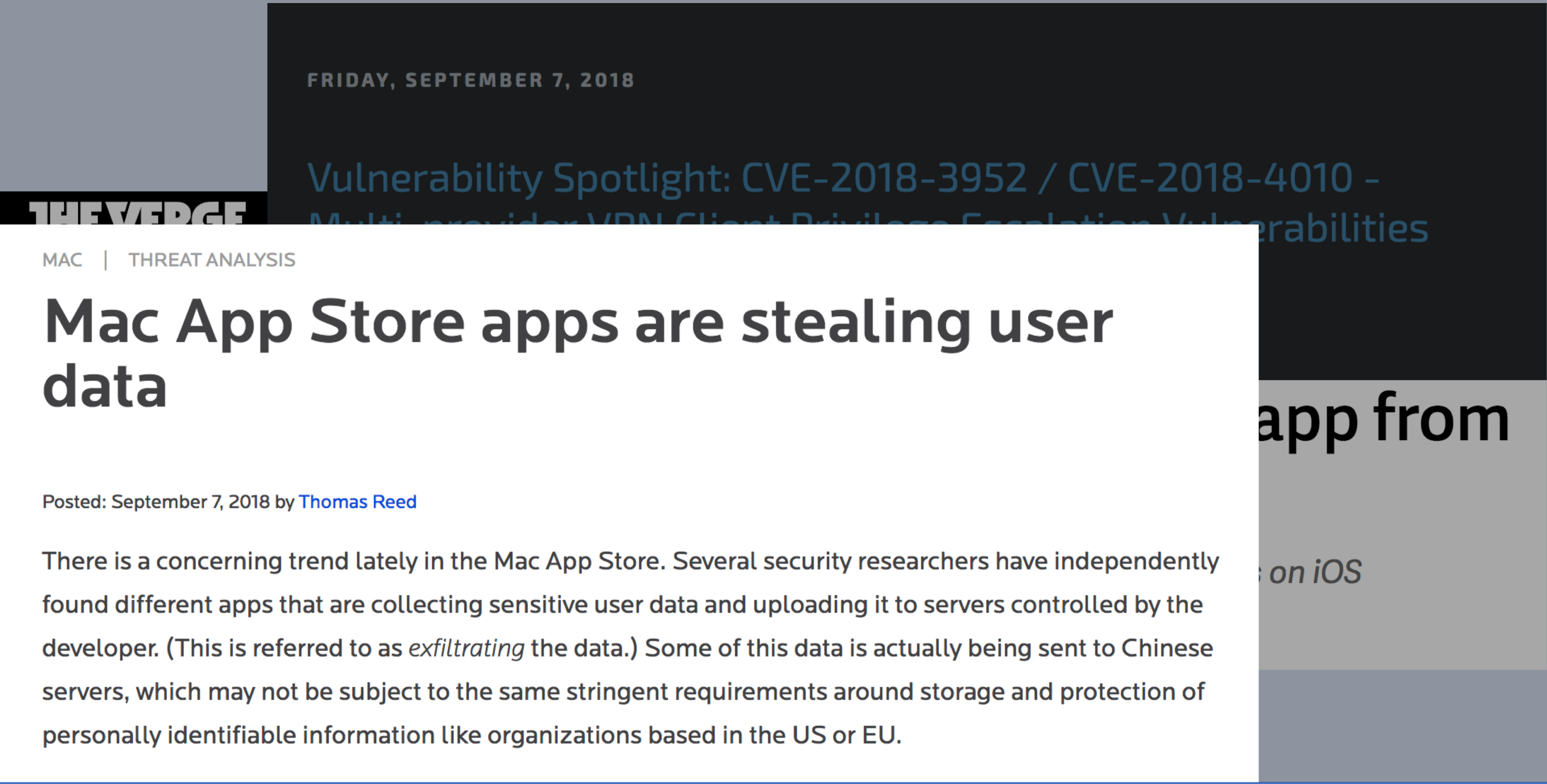
THE VERGE

APPLE \ APPS \ MOBILE

Facebook will pull its data-collecting VPN app from the App Store over privacy concerns

Onavo Protect, a VPN service Facebook acquired in 2013, will no longer receive updates on iOS

By Nick Statt | @nickstatt | Aug 22, 2018, 6:46pm EDT



FRIDAY, SEPTEMBER 7, 2018

Vulnerability Spotlight: CVE-2018-3952 / CVE-2018-4010 - Multi-provider VPN Client Privilege Escalation Vulnerabilities

THE VERGE

app from

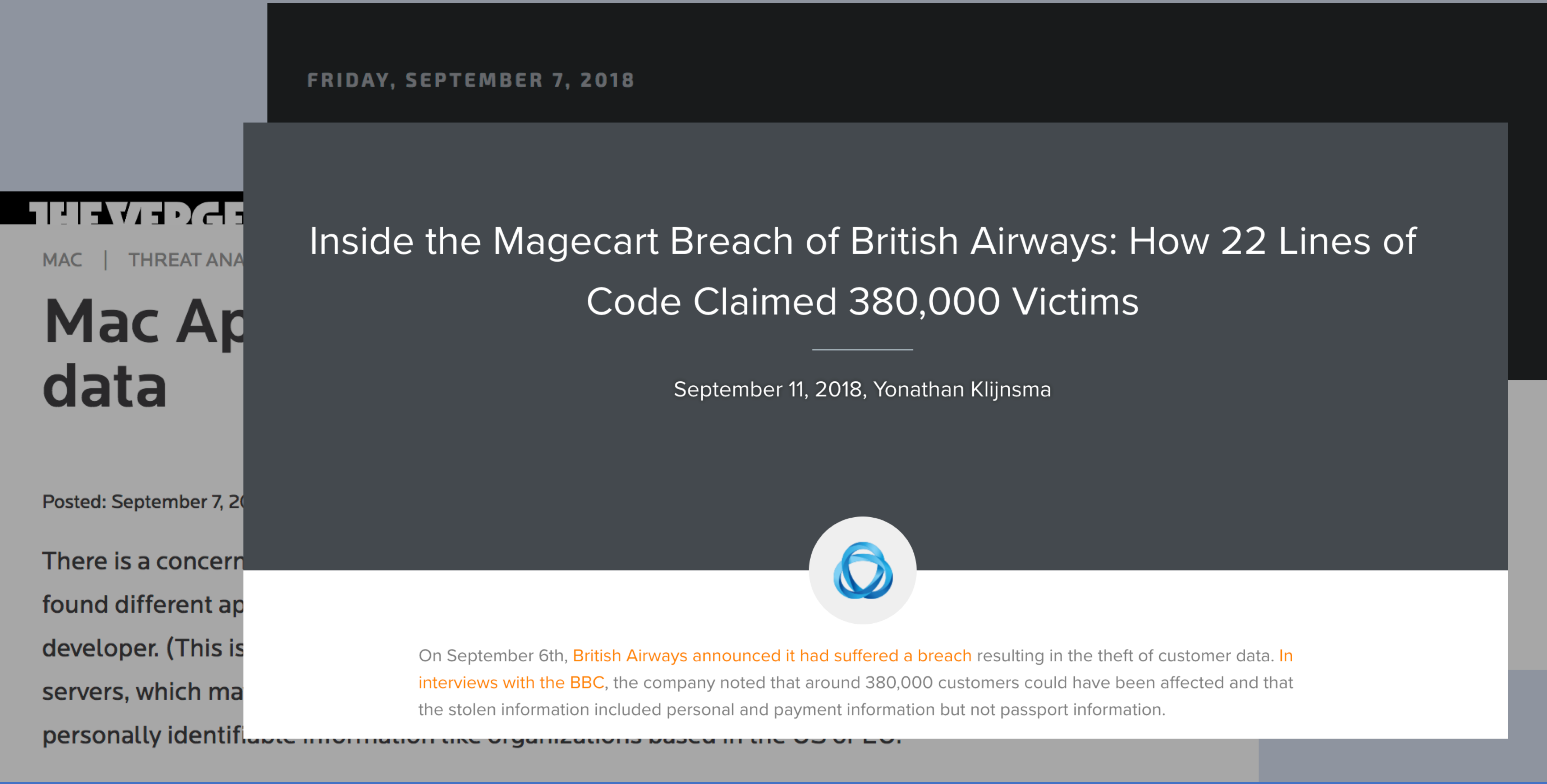
on iOS

MAC | THREAT ANALYSIS

Mac App Store apps are stealing user data

Posted: September 7, 2018 by Thomas Reed

There is a concerning trend lately in the Mac App Store. Several security researchers have independently found different apps that are collecting sensitive user data and uploading it to servers controlled by the developer. (This is referred to as *exfiltrating* the data.) Some of this data is actually being sent to Chinese servers, which may not be subject to the same stringent requirements around storage and protection of personally identifiable information like organizations based in the US or EU.



FRIDAY, SEPTEMBER 7, 2018

THE VERGE

MAC | THREAT ANA

Mac Ap
data

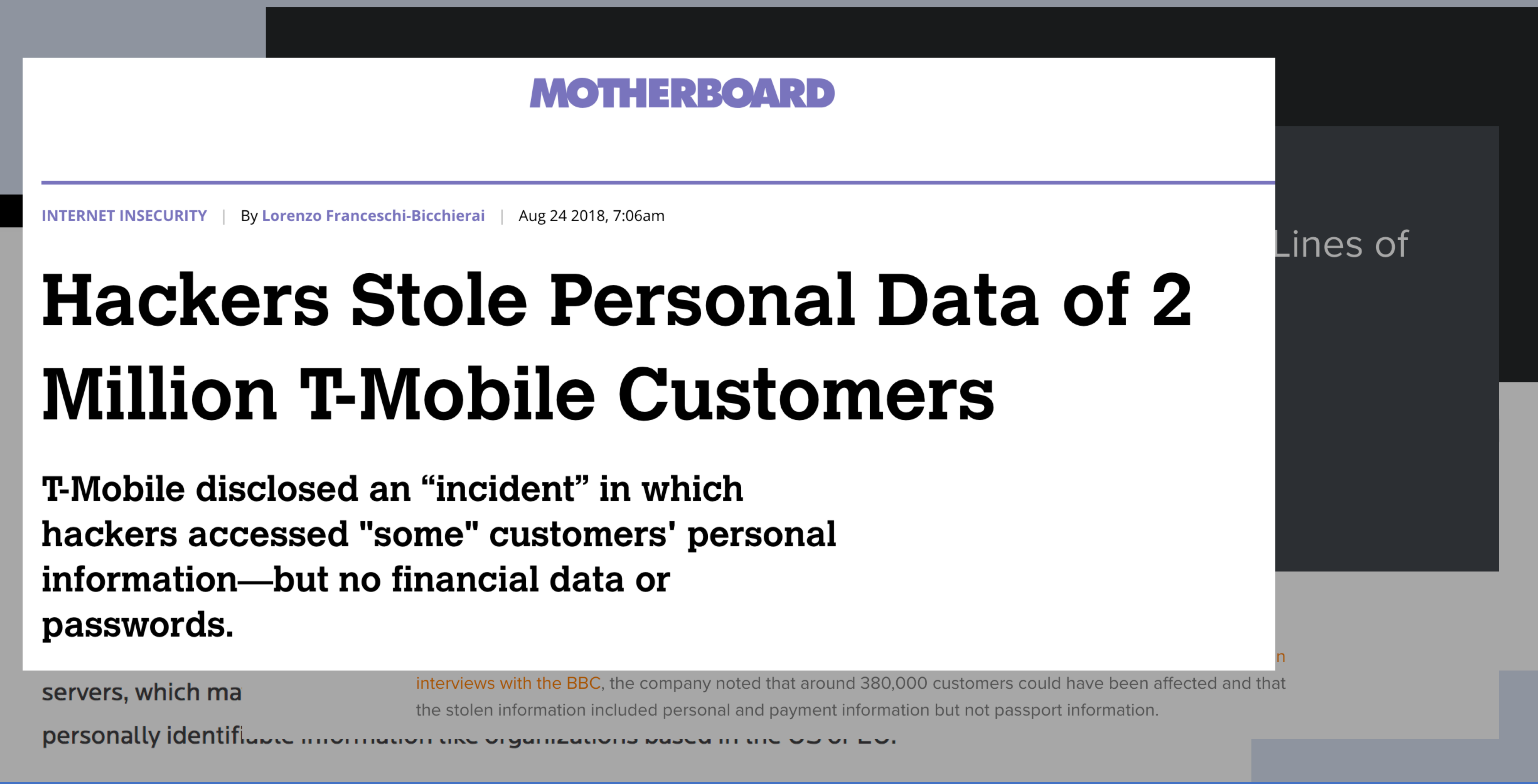
Posted: September 7, 2(

There is a concern
found different ap
developer. (This is
servers, which ma
personally identifi

Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims

September 11, 2018, Yonathan Klijnsma

On September 6th, British Airways announced it had suffered a breach resulting in the theft of customer data. In interviews with the BBC, the company noted that around 380,000 customers could have been affected and that the stolen information included personal and payment information but not passport information.



MOTHERBOARD

INTERNET INSECURITY | By Lorenzo Franceschi-Bicchierai | Aug 24 2018, 7:06am

Hackers Stole Personal Data of 2 Million T-Mobile Customers

T-Mobile disclosed an “incident” in which hackers accessed "some" customers' personal information—but no financial data or passwords.

Lines of

n

interviews with the BBC, the company noted that around 380,000 customers could have been affected and that the stolen information included personal and payment information but not passport information.

servers, which ma

personally identifi

Simple systems are more secure

Complexity theory

Simple Systems – A bike

Complicated systems – A car

Complex Systems - Traffic

We don’t solve motorway congestion by assuring tires

Microservices and security

"Software that can fit in my head"
James Lewis

Small systems focused on one business domain

Business based

Own their own data

Contracts for communication

Simple services with clear boundaries

Security must be an enabler for the team

The unit of delivery is the team

The unit of decision making is the team

“Appoint a suitably senior and empowered decision maker”

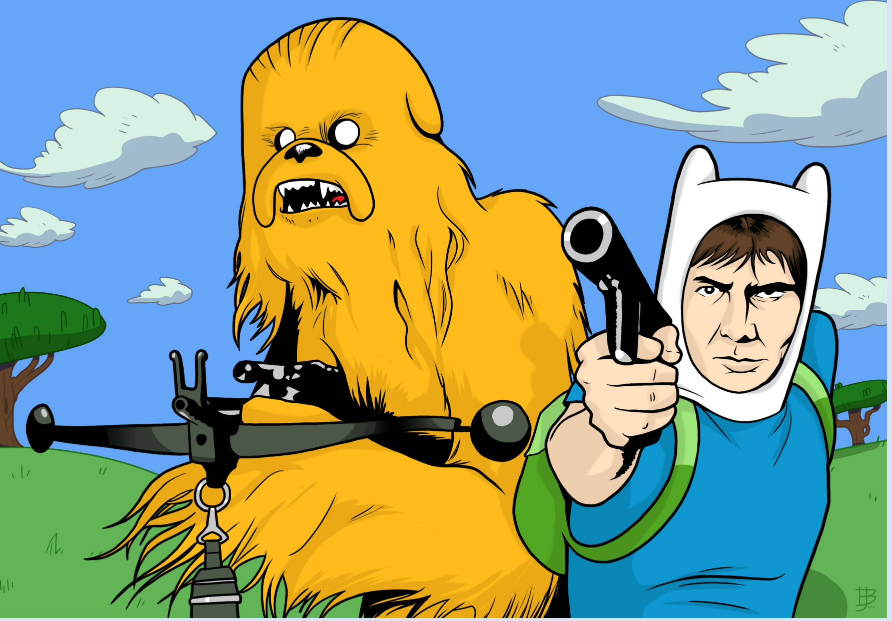
Workshop with whole team

Workshop with whole team*

Michael Brunton-Spall @bruntonspall

Visible outputs for walls

AntiPersonas



Han Solo

Motivation

Han Solo is motivated primarily by money, but also works with the rebel alliance.

Han is capable of using common tools as well as modifying existing tools on the fly

Han doesn’t want to be caught and so takes an effort to avoid head on confrontations

Capabilities

Resources: 2/5

Capability: 4/5

Bravery: 2/5

Criminal connections: 3/5

Connections

Rebel Alliance, Hutts

Misuse cases

Understand the riskier stories

Applying ISO27001 controls in agile

4 mechanisms: Avoid, Mitigate, Transfer, Accept

6 Controls: Deter, Prevent, Correct, Recover, Detect, Compensate

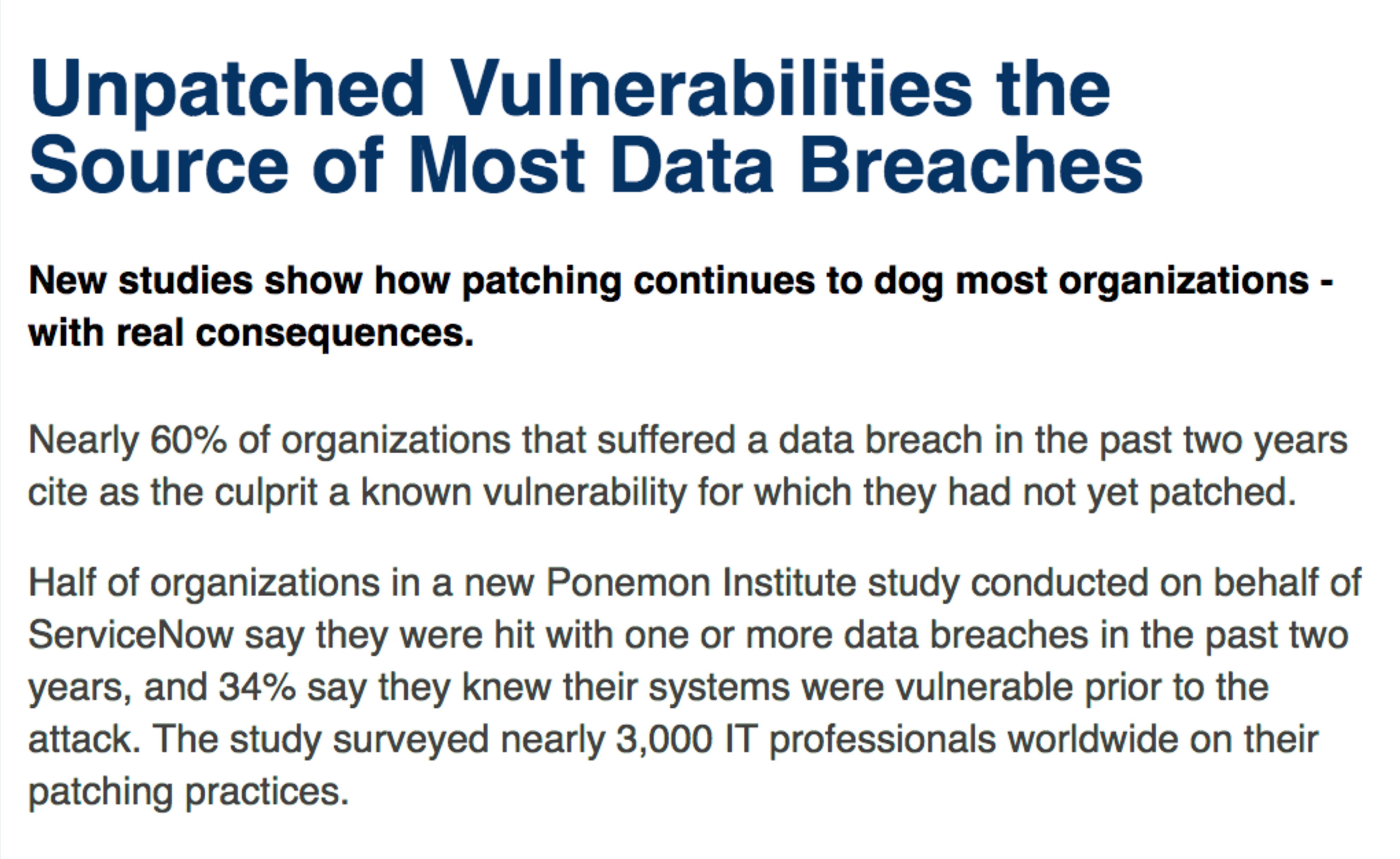
Record decisions against stories

Record deferred security debt

Security bugs are not evenly distributed

Product Owner/Service Manager is in control

Regular releases reduces risk

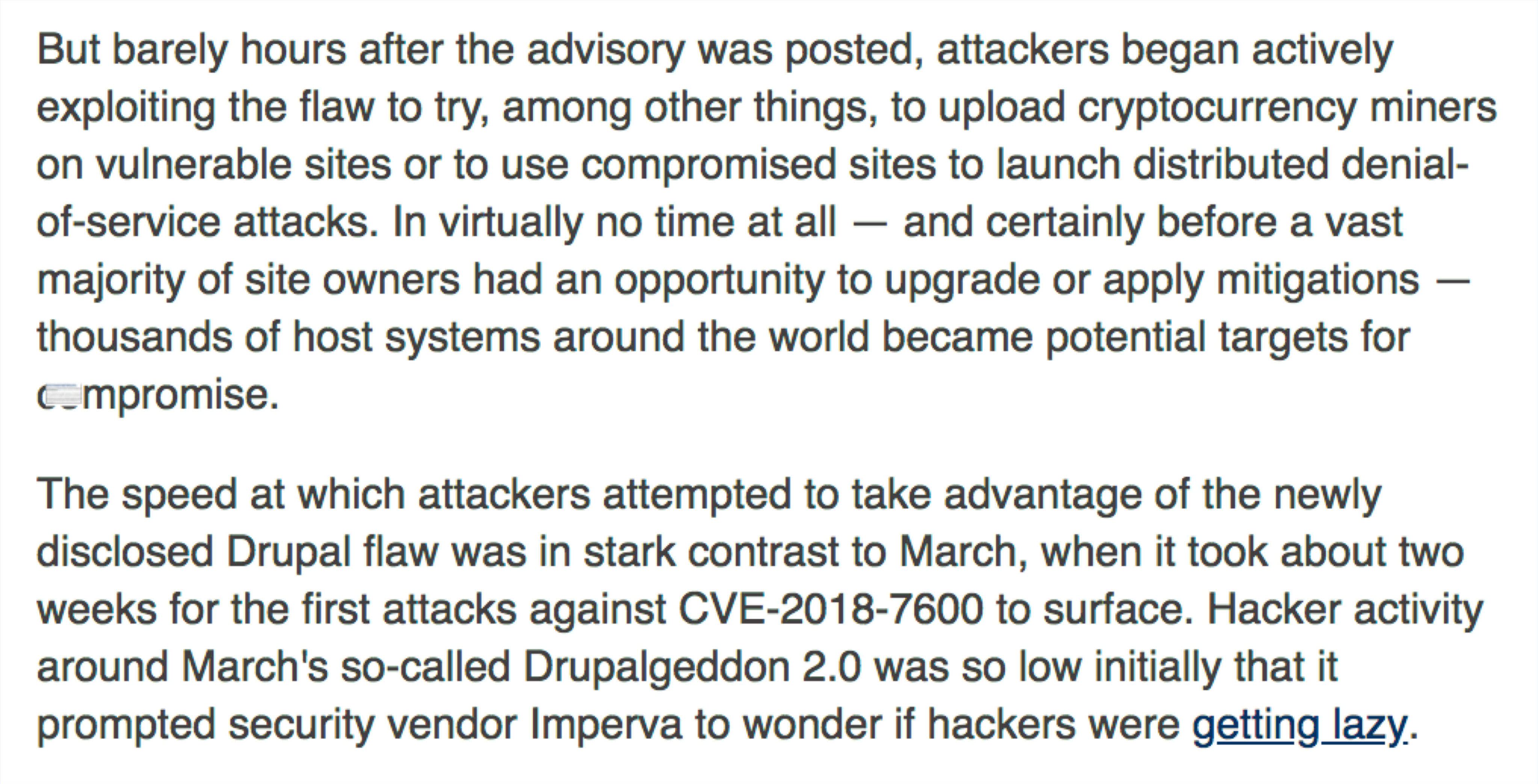


Unpatched Vulnerabilities the Source of Most Data Breaches

New studies show how patching continues to dog most organizations - with real consequences.

Nearly 60% of organizations that suffered a data breach in the past two years cite as the culprit a known vulnerability for which they had not yet patched.

Half of organizations in a new Ponemon Institute study conducted on behalf of ServiceNow say they were hit with one or more data breaches in the past two years, and 34% say they knew their systems were vulnerable prior to the attack. The study surveyed nearly 3,000 IT professionals worldwide on their patching practices.



But barely hours after the advisory was posted, attackers began actively exploiting the flaw to try, among other things, to upload cryptocurrency miners on vulnerable sites or to use compromised sites to launch distributed denial-of-service attacks. In virtually no time at all — and certainly before a vast majority of site owners had an opportunity to upgrade or apply mitigations — thousands of host systems around the world became potential targets for compromise.

The speed at which attackers attempted to take advantage of the newly disclosed Drupal flaw was in stark contrast to March, when it took about two weeks for the first attacks against CVE-2018-7600 to surface. Hacker activity around March's so-called Drupalgeddon 2.0 was so low initially that it prompted security vendor Imperva to wonder if hackers were getting lazy.

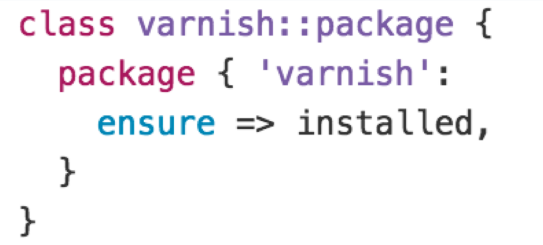
GOV.UK fixed Heartbleed within approx 2 hours

https://insidegovuk.blog.gov.uk/2014/04/11/govuk-and-the-heartbleed-openssl-bug/

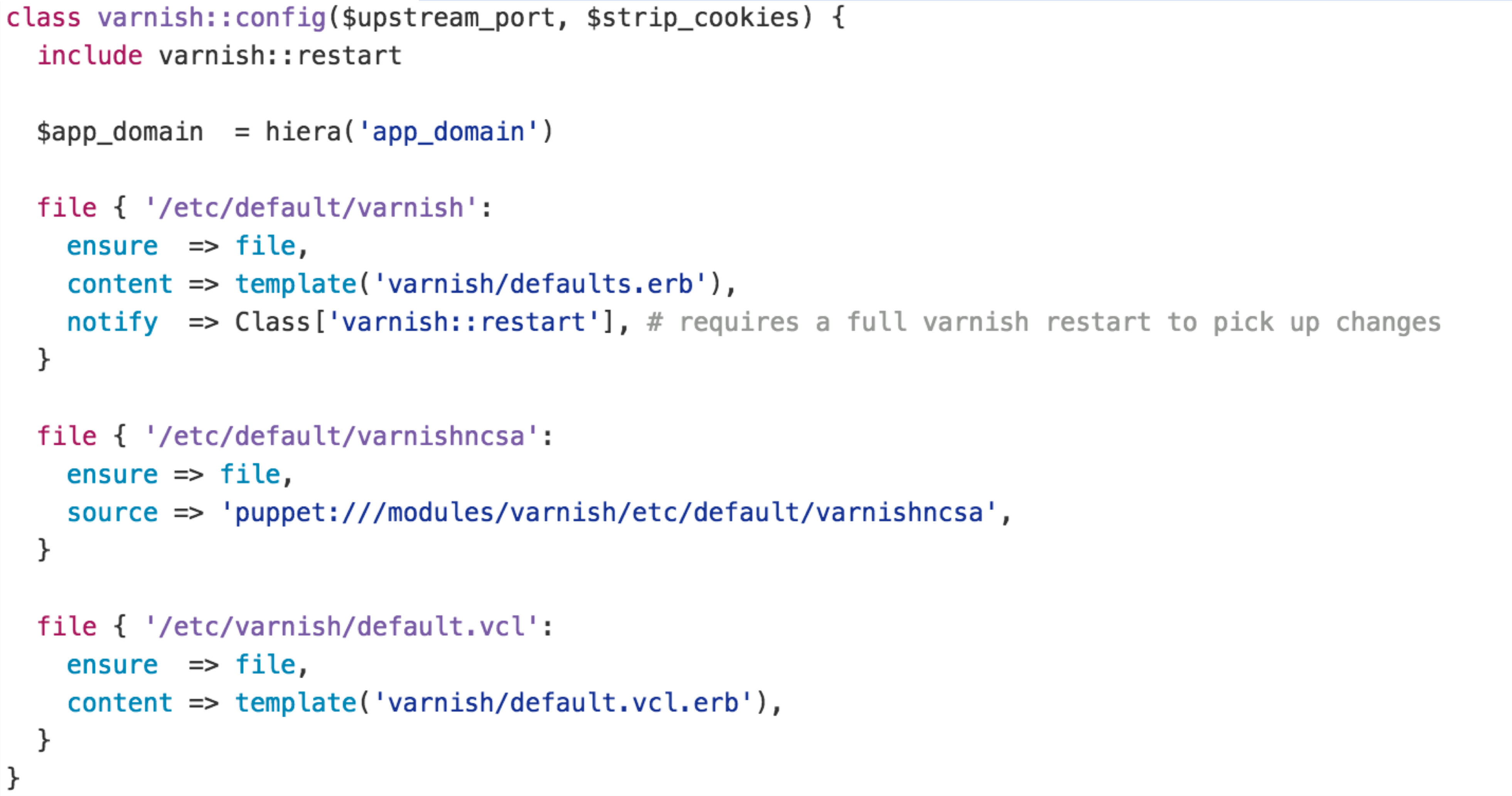
AWS fixed entire AWS estate within 1 hour and scanned customers to inform them

https://threadreaderapp.com/thread/1114944298246660100.html

Infrastructure as code

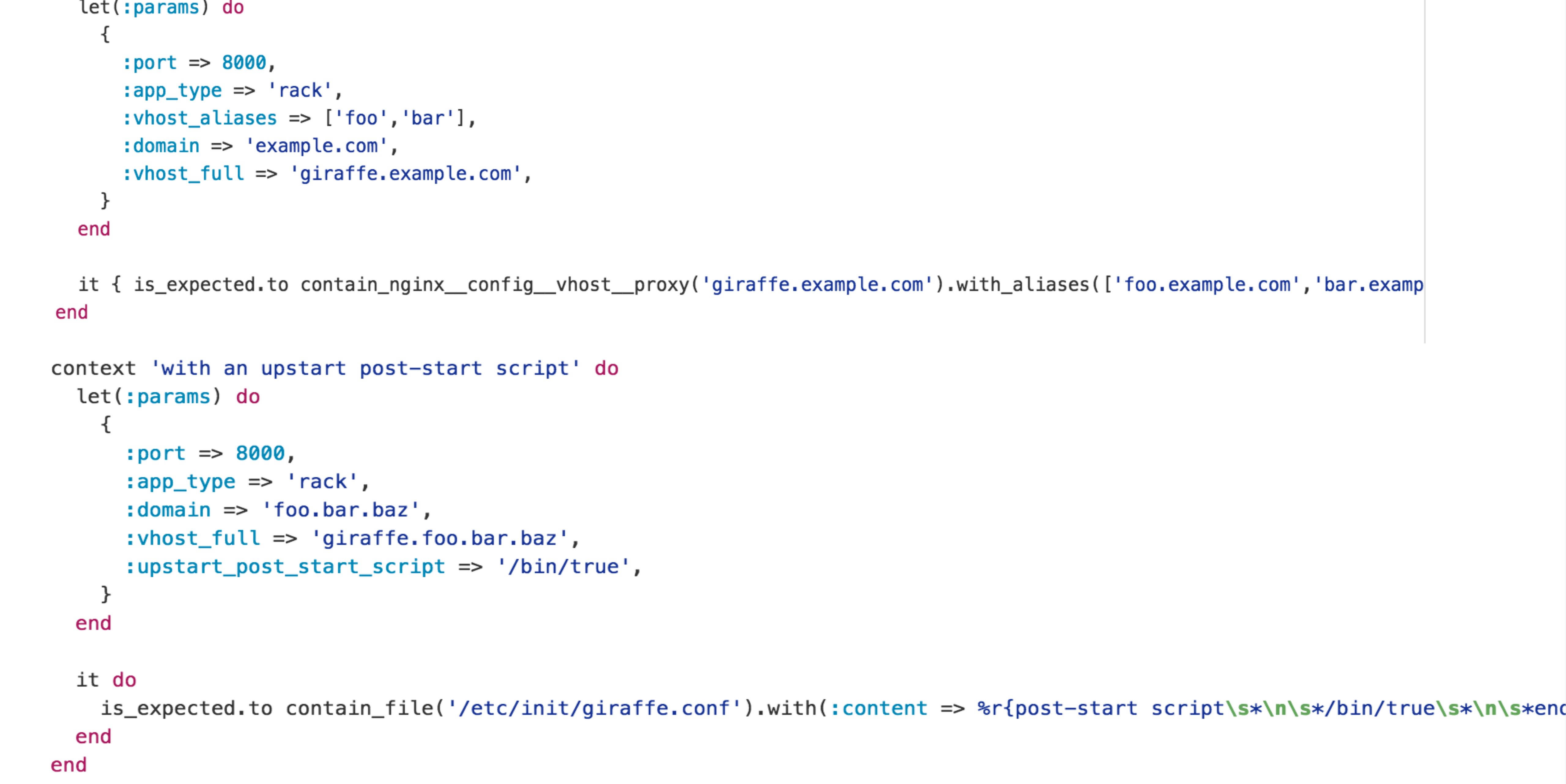


```
class varnish::package {
  package { 'varnish':
    ensure => installed,
  }
}
```

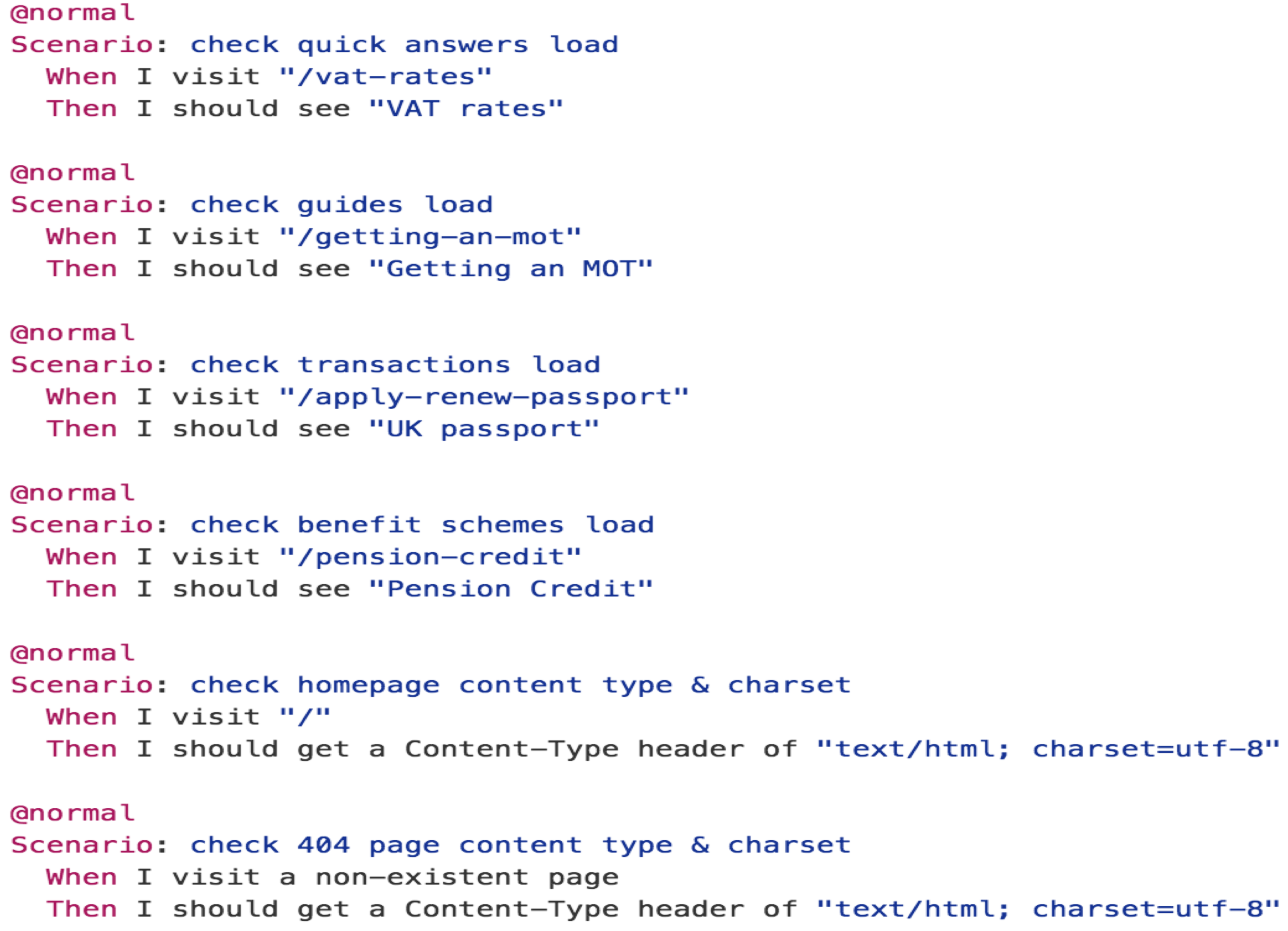


```
class varnish::config($upstream_port, $strip_cookies) {
  include varnish::restart

  $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



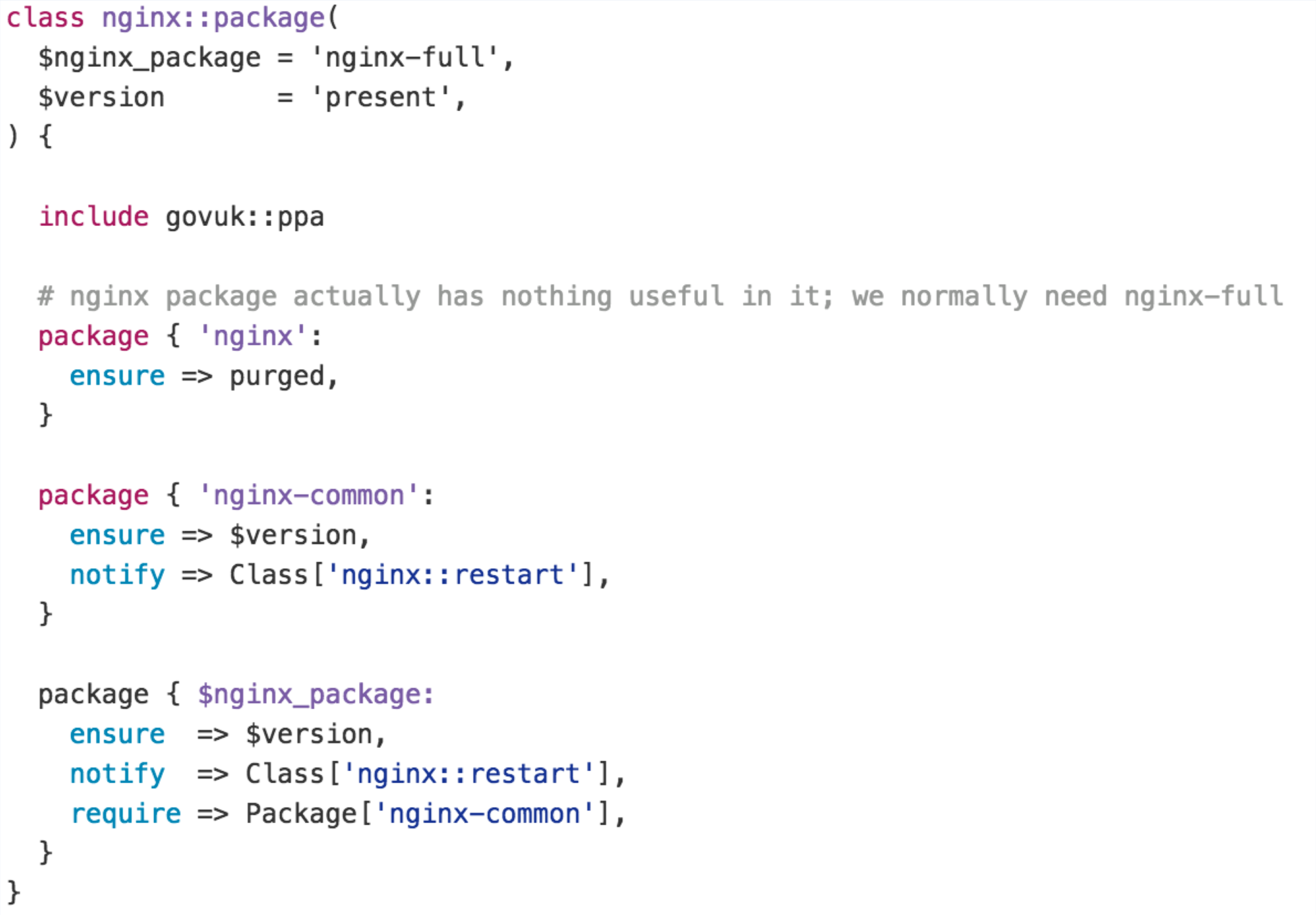
```
    let(:params) do
      {
        :port => 8000,
        :app_type => 'rack',
        :vhost_aliases => ['foo','bar'],
        :domain => 'example.com',
        :vhost_full => 'giraffe.example.com',
      }
    end

    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*\n\s*en
    end
  end
```



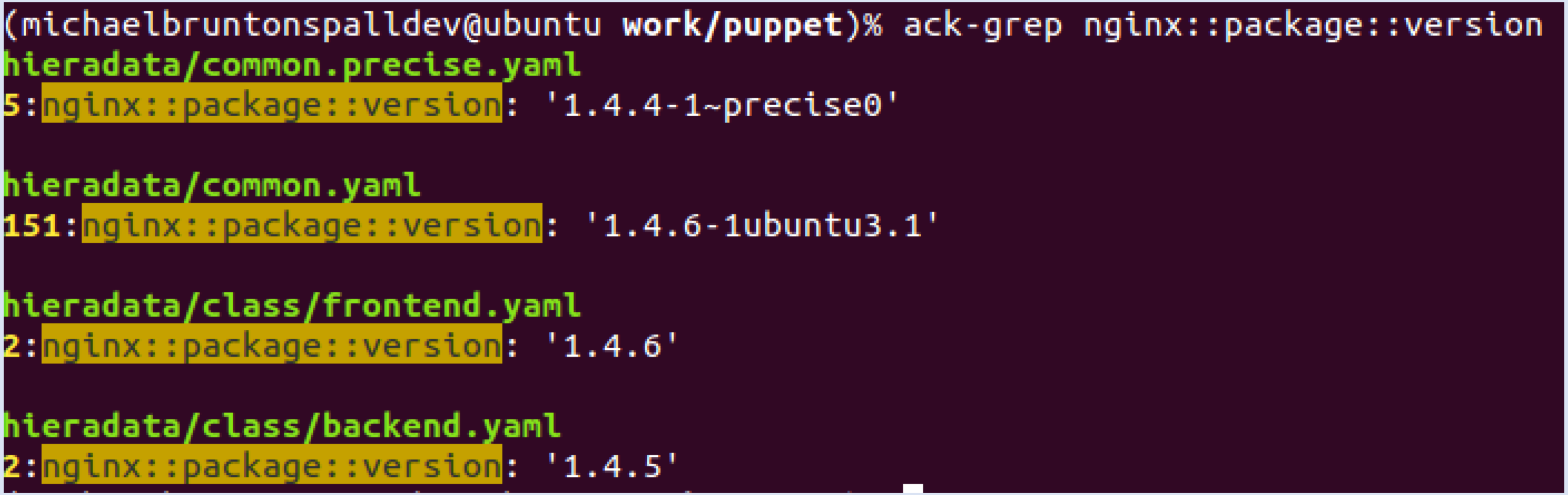
```
@normal
Scenario: check quick answers load
  When I visit "/vat-rates"
  Then I should see "VAT rates"

@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 "/"
  Then I should get a Content-Type header of "text/html; charset=utf-8"

@normal
Scenario: check 404 page content type & charset
  When I visit a non-existent page
  Then I should get a Content-Type header of "text/html; charset=utf-8"
```

Dealing with patches

What machines are affected?

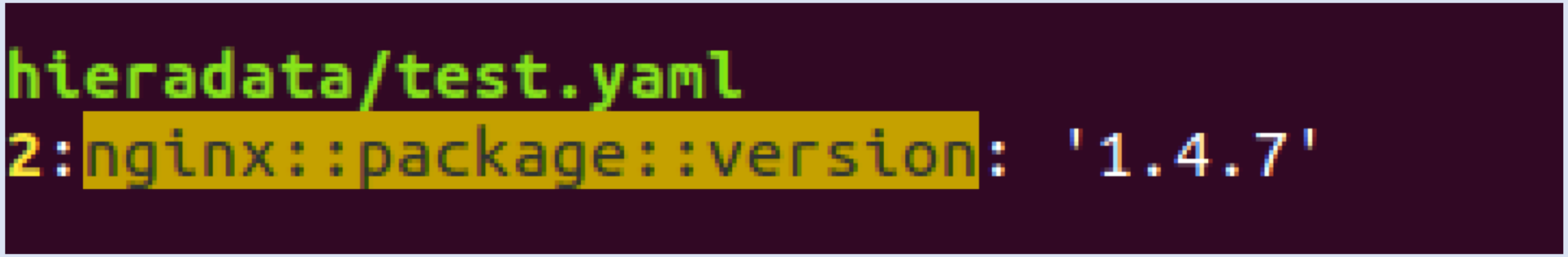


```
class nginx::package(
  $nginx_package = 'nginx-full',
  $version       = 'present',
) {

  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'],
  }
}
```



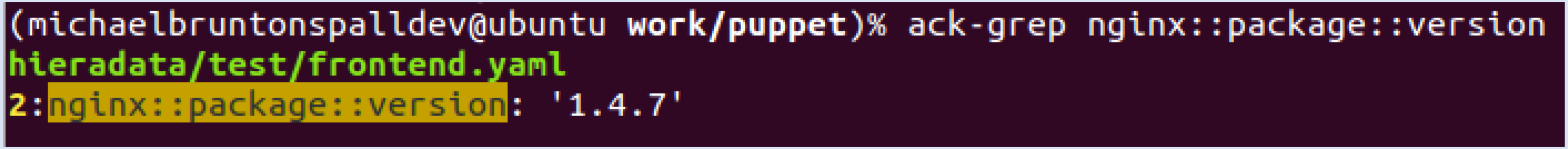
```
(michaelbruntonspalldev@ubuntu work/puppet)% ack-grep nginx::package::version
hieradata/common.precise.yaml
5:nginx::package::version: '1.4.4-1~precise0'

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



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

Just some machines?



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

Repeat in production

One Government service released code once every 6 months

GOV.UK released around 8 times per day

1 day = 4 years of practice

Summary

Security in its current form does not work

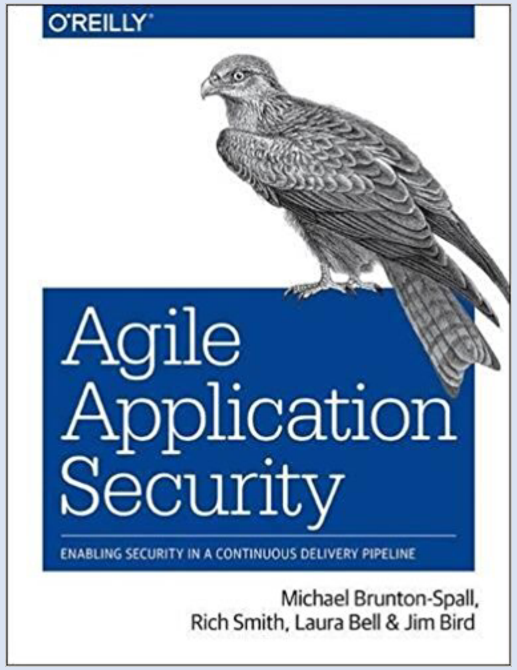
Simple systems are more secure

Security must be an enabler for the team

Regular releases reduces risk

Agile doesn’t make us less secure

Agile makes us **more** secure



O'REILLY

Agile Application Security

ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE

Michael Brunton-Spall,
Rich Smith, Laura Bell & Jim Bird

Michael Brunton-Spall

michael@brunton-spall.co.uk

https://tinyletter.com/cyberweekly

goto; copenhagen

GOTO Copenhagen 2019

Conference Nov. 18 - 20

Please

Remember to rate this session

Thank you!

Follow us @gotocph