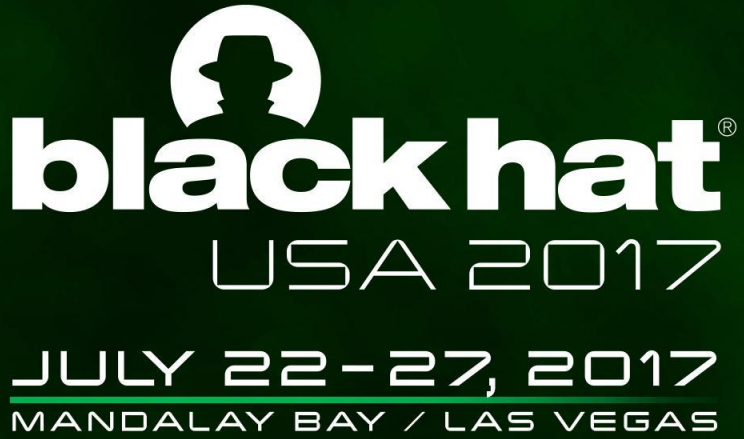


Delivering Javascript to World+Dog

Background

Enterprise SaaS Third party javascript Functional Spec

Include JS on site, increase biz

What could go wrong?

The Problem

Javascript - delivering code + data in one

Browser can’t always tell the difference

3rd party js - Hack once, pwn everywhere

Real-World Example

The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE **SECURITY** TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

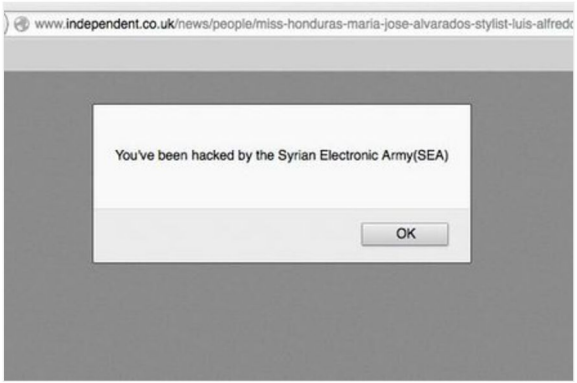
Security

20

Syrian Electronic Army in news site 'hack' POP-UP MAYHEM

Gigya redirect exploit blamed for pop-rageous ploy

By Jasper Hamill 27 Nov 2014 at 13:31 SHARE ▼



The Syrian Electronic Army has compromised a number of news websites – apparently through DNS redirects via Gigya, a customer identity management platform used by all the sites.

The Pro-Assad javascript popup appeared across several websites, including The Telegraph, The Independent, Forbes, Time Out, PC World and The Evening Standard.

Threat Model

Pwn any of these to have your Gigya moment

- Customer
- App admin
- App developer
- AWS Admin
- CDN developer or admin
- CDN
- DNS
- Staging
- Vuln in payload

Humans - the Weakest Link

Even after you get your shizz together, your customers won’t

Humans - the Weakest Link

Startup developers want to move fast, unencumbered by big company bureaucracy. They ship code daily. More access means less headaches getting their job done.

Least Privilege

Managing Secrets

Enterprise SaaS Authentication

Good- modern password best practices

Better - 2FA

Best - SAML SSO

Safely Creating Business Value

No custom js

Output encode everything

Building and Staging

Absolutely minimize attack surface

Log, publish HMAC of builds

HTTPS build fn

HTTPS to stage bucket

HTTPS to CDN

Third Party Library Management

CDN

HTTPS everywhere

Minimize admins

Logging

Change Management

SSO, 2FA

DNS

HTTPS everywhere

Have a backup ready

DNS CAA

Secure DNS?

TLS

Cert Transparency

Pinning

Pinning Preload

HTTP2

Server Push

SHA-2 certs

Update ciphersuites regularly

Browser

Cookies, HTML5 Local Storage

- Data **will** be scrutinized and tampered with
- Integrity checks first
- Don’t store sensitive data

Colliding with Performance

Load first on page

TLS latency

TLS tuning

Can’t break up javascript

Can’t break up data

HTTP2 - no need to bundle

Server Push

Long lived connections

CSP

Great idea

Least worst, allow unsafe

Hardly any customers ask for it

CSPv3?

Subresource Integrity

Integrity Check

Static

Ties your hands

Self Hosted

Not sustainable

Need rigorous agile release

See server side

Bug Bounty

What finds legit high severity bugs in the JS?

$1000 Bounty - Nope

$5000 Bounty - Nope

$10000 Bounty - ?

10k/1 week of a $300/hr consultant? Yup

Availability

Have backup:

- DNS
- CDN
- Origin
- Build
- Configuration

Looking Ahead

Anomaly detection

Privacy

Insurance?

For More

@kylerandolph

about.me/kylerandolph

Like this? Optimizely is Hiring!

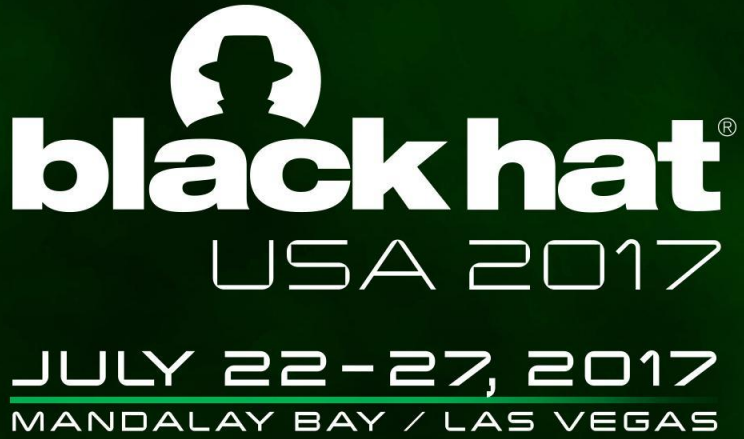
optimizely.com/careers

Black Hat Sound Bytes

TLS is essential

Javascript integrity must be ensured end-to-end

Don’t give your customers the opportunity to make insecure choices



Delivering Javascript to World+Dog