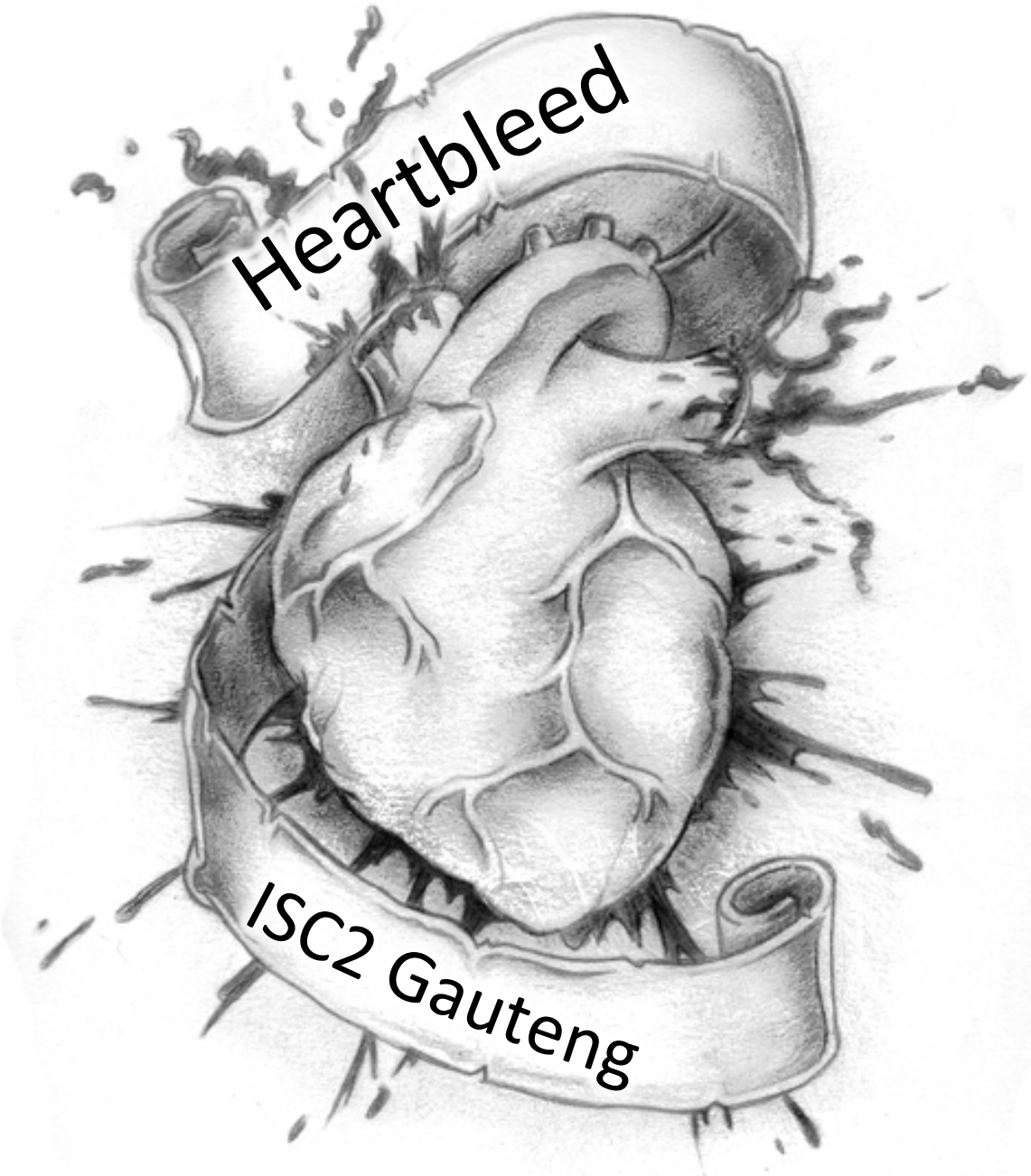
sensepost



whoami

Dominic White
CTO @ SensePost

We
Hack | Build | Train | Scan
Stuff

@singe / @sensepost

dominic@sensepost.com
info/research/job @sensepost.com

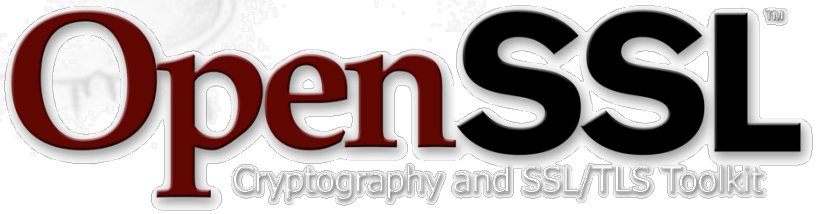
sensepost

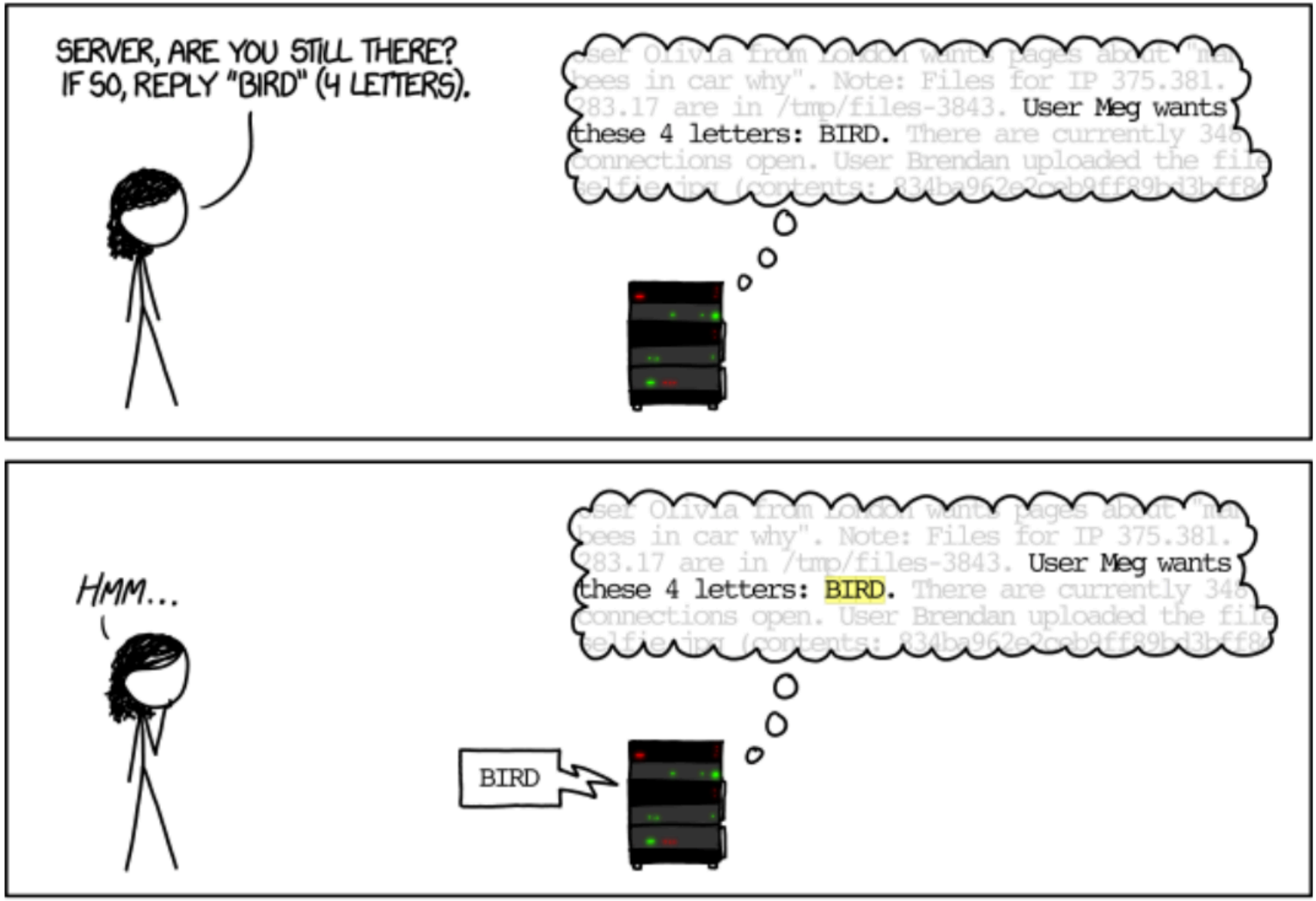
What Happened

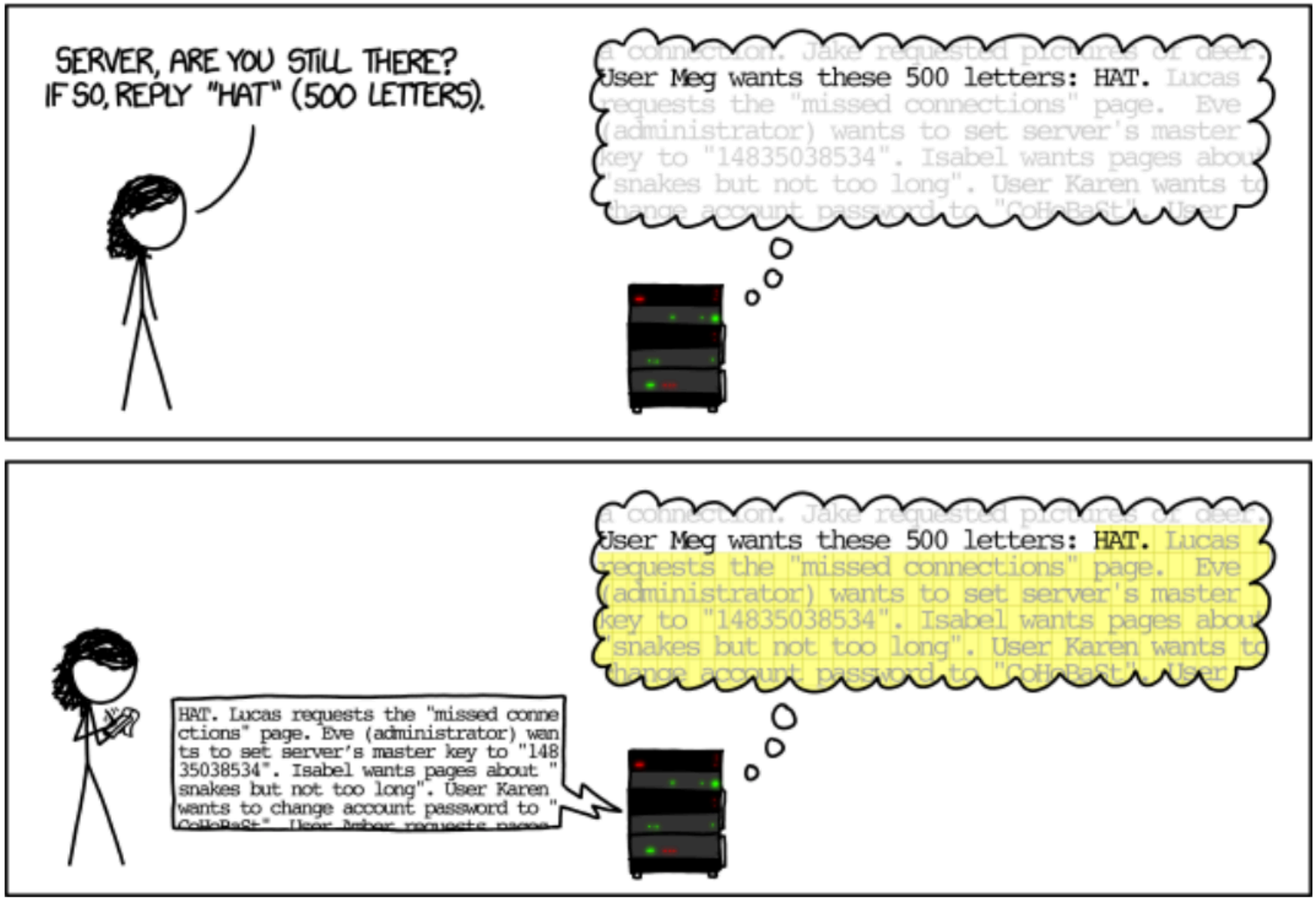
- **7 April 2014** – Vulnerability announced to the world with a website, **OpenSSL** vulnerability announcement and new code release (1.0.1g)
  - Found by two groups; Google Security Team (Neel Mehta & Condenomicon)
- Told that **private keys** to SSL certificates could be exposed – uh oh
- Operating systems had not packaged the new release, so **many were vulnerable**
- Many big name companies were vulnerable; Big Tech names, Banks, Law Enforcement, Intelligence Agencies
- Online testers appeared, and were quickly swamped
- **But** ….

What is it?

- Vulnerability in a widely used **cryptographic** library
  - i.e. lots of Unix things use this to do encryption
- Vulnerability specific to SSL **Heartbeats**
  - RFC 6520 https://tools.ietf.org/html/rfc6520
- Introduced on Dec 31 **2011** by Dr Stephen Henson
- Allows you to read parts of a program **memory**
  - Buffer Over Read

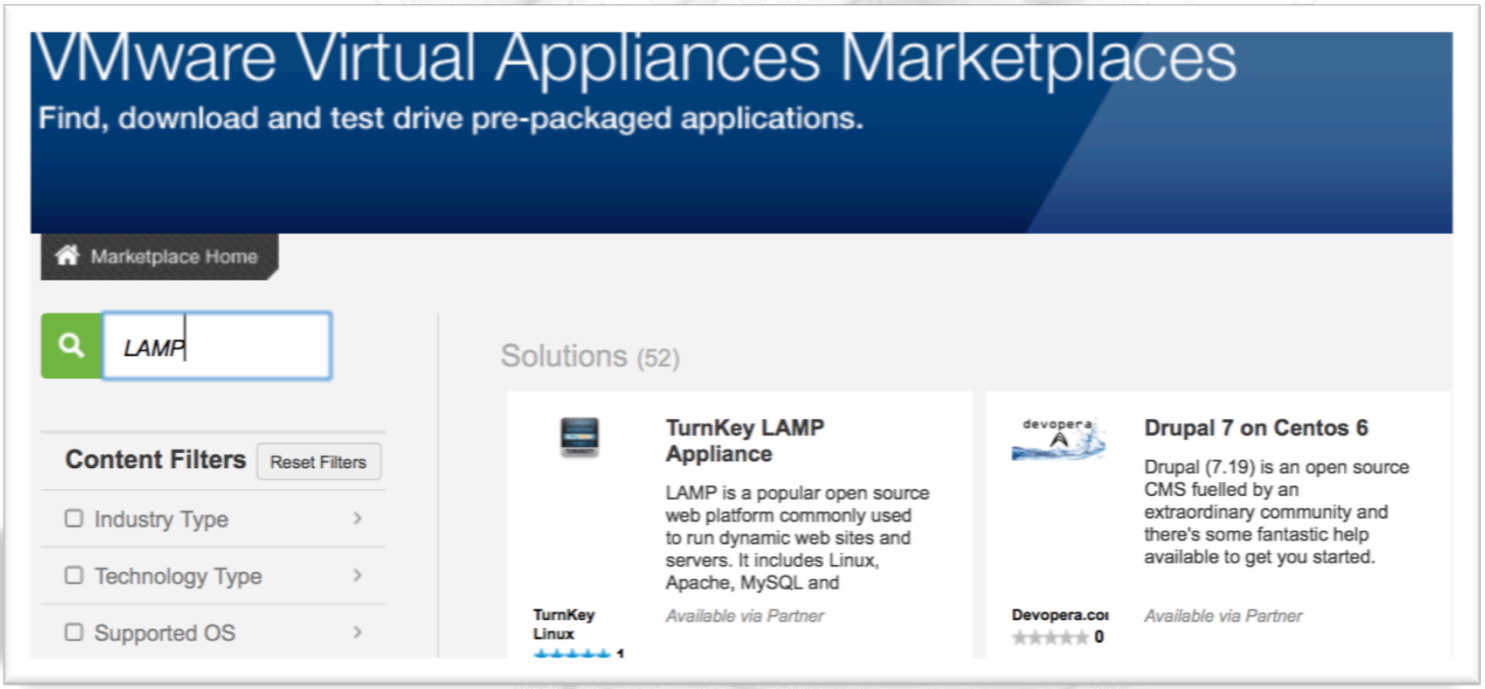



SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
HMM...
User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
User Meg wants these 500 letters: HAT.
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "

Demo

- Extracting cookies & private SSL keys from a vulnerable server



sensepost

Why does it work

- OpenSSL is just the library, the actual process is something like Apache, Nginx, Dovecot, Exim etc.
- These processes have a HEAP, in which data used by the process is stored.
  - If the process is active, it changes a lot
- Certificate private keys are made up of two large prime numbers; we can find these if they were used recently

The slow path to enlightenment

- Initial testers looked for vanilla SSL on port 443 using TLS v1.1
  - Most famous and first PoC by Jared Stafford; ssltest.py
- But:
  - SSL runs on **non-standard ports**
  - Some servers didn't support **TLS v1.1**
  - SSL can be invoked on clear-text ports with **STARTLS**
    - STARTTLS is different for different protocols
  - **Clients** are vulnerable too!
  - Lots of debate about whether **keys** could be grabbed
    - CloudFlare challenge cleared that up
  - **IDS** signatures were quickly defeated

Meanwhile ….

- #heartbleedvirus
- Bruce Schneier
  - "On the scale of 1 to 10, this is an 11."
- I'm not Vulnerable, the scanner said so!
- Claims of NSA backdoor bogey men
- EVERYBODY CHANGE ALL YOUR PASSWORDS!
  - NO WAIT, CHANGE THEM AGAIN!

How Bad Was It?

- Masscan (Robert Graham)
  - 615 268 / 28 581 134
  - After one month 318 239

- Our clients
  - 1.8% when it broke
  - Offered free “complete” scan
  - 24 / 224 186

sensepost

Tactical Defence

Fix the Vuln

- Patch it
  - OpenSSL >= 1.0.1g
  - Old versions < 1.0.1 unaffected
- Disable it
  - Firewall, VPN?
- Reconfigure it
  - Disable heartbeats
  - Enable Perfect Forward Secrecy
- IDS it?
  - Do not rely on this

Cleanup

- Change certificates
  - Revoke the old ones
- Reset sessions
  - i.e. invalidate all cookies
- Change passwords
  - Only affected user-stores

sensepost

Defence in Depth

- One 0day shouldn't ruin your day
  - But this one was tricky

1. Early alerting
2. Response procedures (IR)
3. Ability to act quickly (devsecops)
4. Avoid heterogeneity/monocultures?

sensepost

The State of OpenSSL's Future

- Massive amount of legacy code
- Incredibly complex to maintain
  - 2 people effectively doing most of it
- C considered harmful today
  - Pointer arithmetic makes problems
- FIPS certification dangerous
  - Certifies bad crypto & bad implementations
- OpenBSD's OpenSSL rampage -> LibreSSL
- OpenSSL just got a ton of funding

sensepost

Eye Openers

- We thought OpenSSL was okay
  - Ok, lots didn't, but nobody did anything about it
  - We think lots of other things are ok
  - ESR's Linus' Law: "Given enough eyeballs, all bugs are shallow"
- But!
  - We found the bug
  - People actually patched it
- Others
  - The rise of the branded bug
  - The trail of fakes
- Media still drives reactions

sensepost

Thanks & References

- Hackerfantastic
  - Tool & Presentation
- Erratarob
  - Tool/s & blogs
- XKCD
  - Comics!
- Elpartydiablo & xnvx.com
  - Background