The Last Month in InfoSec July 2015 Edition

Joe T. Sylve, M.S.

NOLASec

July 15, 2015

Disclaimer

- The views expressed during this talk (and in general after drinks) are mine alone and do not necessarily reflect those of Blackbag Technologies or 504ENSICS Labs.
- They may or may not also be shared by Vico and Andrew (but who cares what those guys think?)

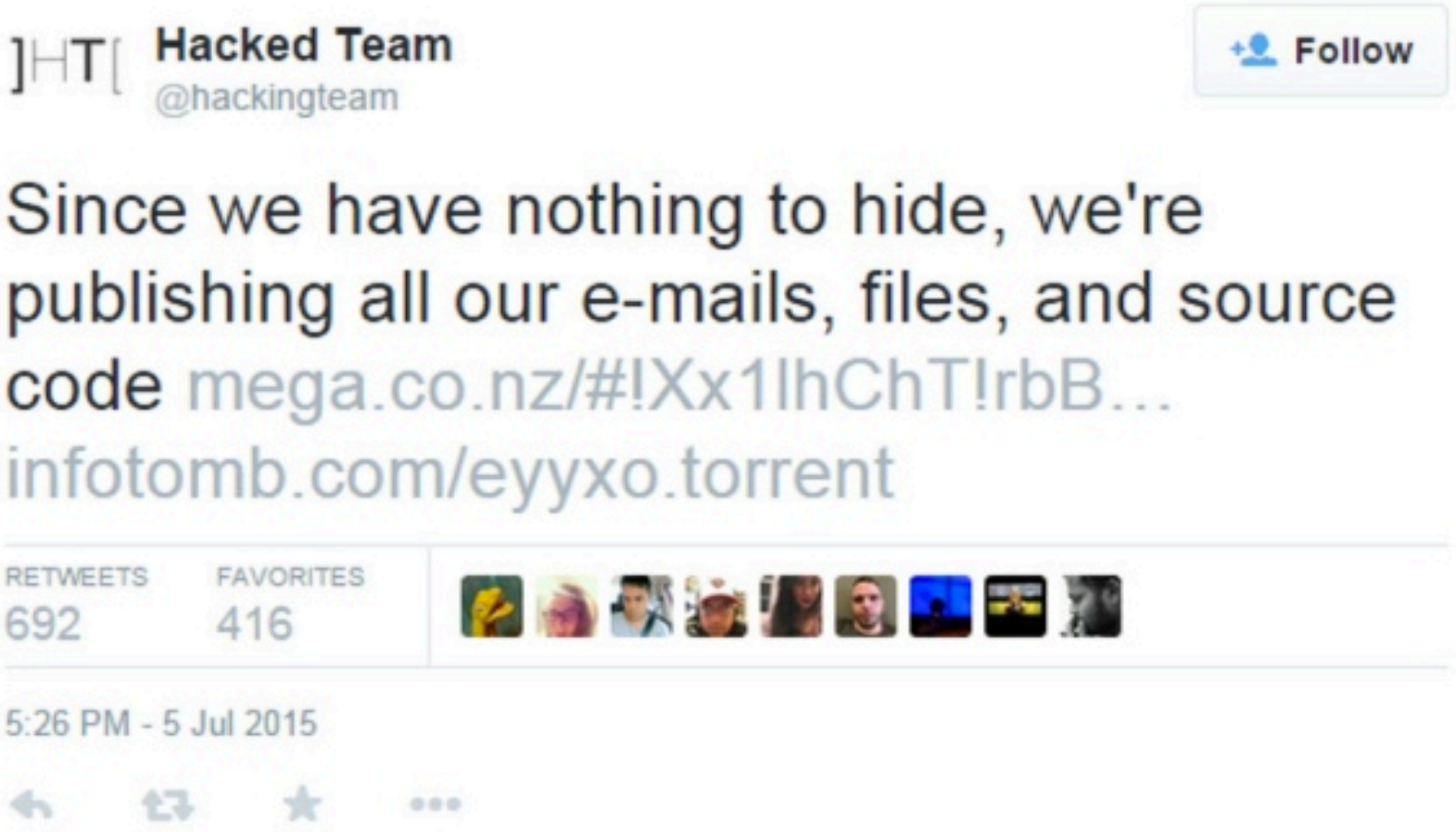
Grab a Copy of These Slides

https://github.com/jtsylve/slides

So many goodies…

HACKING TEAM

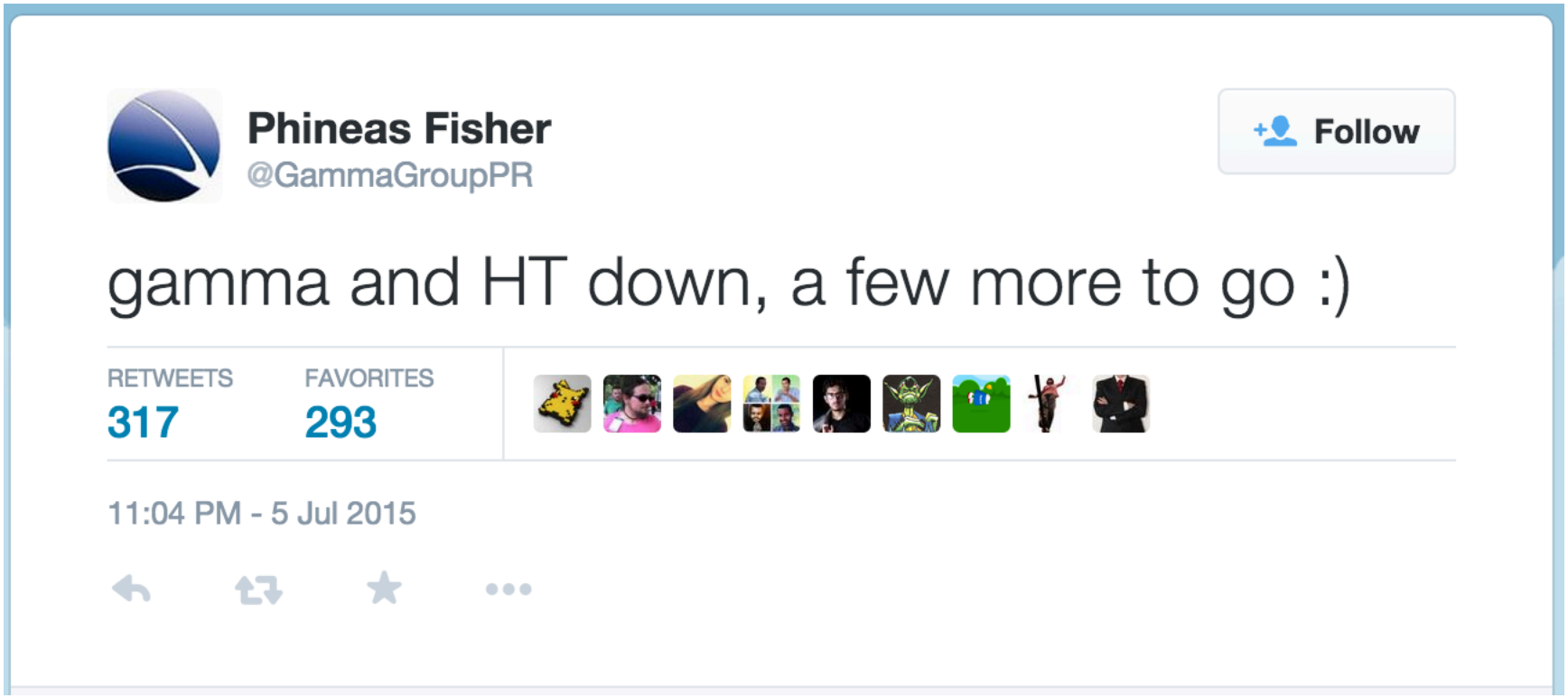
Hacking Team Hacked



Hacking Team Hacked

- University of Toronto Report (July 2014)
  - https://goo.gl/a0J8gC
- Over 400 GB of Data Released
  - https://infotomb.com/eyyxo.torrent
  - https://github.com/hackedteam
  - https://wikileaks.org/hackingteam/emails

Hacking Team Hacked



Hacking Team Hacked

- Several 0day have already been discovered and are actively being used in the wild
  - Flash (more than one)
  - IE 11
  - Office
  - Java
- There will be more…

Hacking Team Hacked

- UEFI Rootkit Used for Persistence
  - Rootkit: https://goo.gl/kCLdGS
  - Powerpoint: https://goo.gl/j7sOqF
  - Intel Write-up: https://goo.gl/iQqrDp

… but wait there’s more!

IN OTHER NEWS

In Other News

- Another High Severity OpenSSL bug found
  - https://goo.gl/fO8NBH
- FBI is still lobbying Congress to mandate encryption backdoors
  - Full Senate Hearing: http://goo.gl/JB3zUX
    - No SSL link available (Thanks senate.gov!)
  - Experts Outline Risks: https://goo.gl/kVDa3s
  - Bruce's Thoughts: https://goo.gl/KyHkD5

In Other News

- Amazon releases new TLS library: s2n
  - Only 6,000 LoC
  - Annoucement: https://goo.gl/nBhaQG
  - Source: https://github.com/awslabs/s2n
- RIPv1 DDoS Attack
  - Outdated Routing Protocol
  - Akamai Advisory: https://goo.gl/pZiuJo

In Other News

- Many Cisco Appliances Use Default Hardcoded SSH Keys
  - https://goo.gl/PV0Kau
  - They're not the only ones…
    - https://github.com/rapid7/ssh-badkeys

That's All for Now!

- Thoughts?
- Questions?
- Comments?

joe.sylve@gmail.com

@jtsylve

https://github.com/jtsylve/slides