2012 – In Review

Rob Vinson – Information Security & Policy Office

Announcements

- **SSH border block** to be implemented **March 1st**
- Have Java installed? Don't use it? Uninstall it!

  At least disable it in the browser…

Agenda

- Flame
- Pwnies
- Legislation
- Flashback
- Linux/SSH Compromise
- ISPO Stats

Flame

- Large malware (on disk)
- Stuxnet related
- MITM of Microsoft Update. Fake update is signed with a Microsoft Code-signing cert…. wait… whaaat?

Pwnies

- http://pwnies.com/
- Best Client-Side Bug: Pinkie Pie's/Sergey Glazunov's Pwnium Exploit
- Best Privilege Escalation Bug: Windows Kernel Exception Handler Vuln (CVE-2011-2018)
- Best Server-Side Bug: MySQL Authentication Bypass
- Most Epic FAIL: F5 Static Root SSH Key

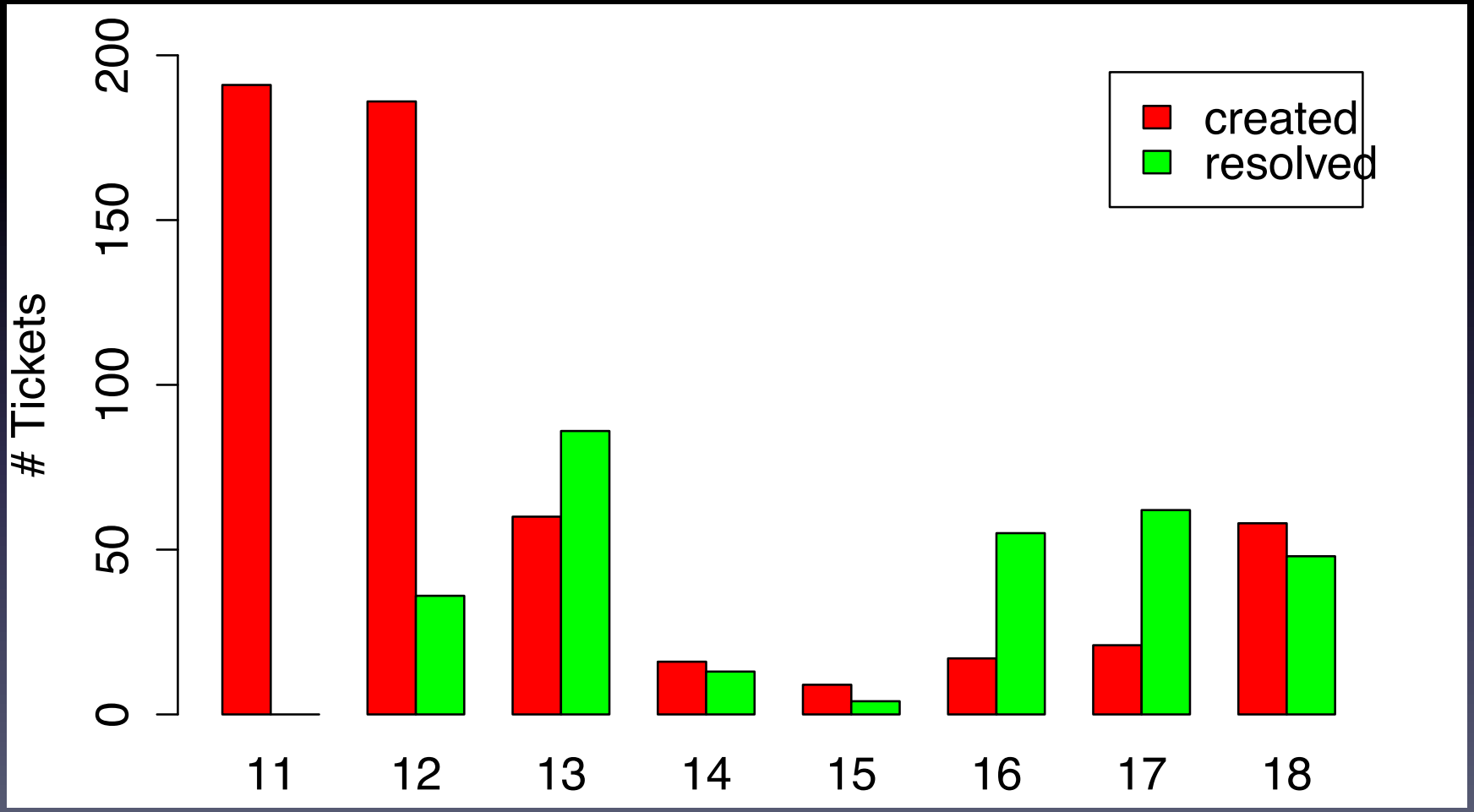
Legislation

- Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA)
- Cyber Intelligence Sharing & Protection Act (CISPA)

Flashback

- Java vulns, yay!
- OS 10.5 didn't get the update off the bat.

Flashback Tickets

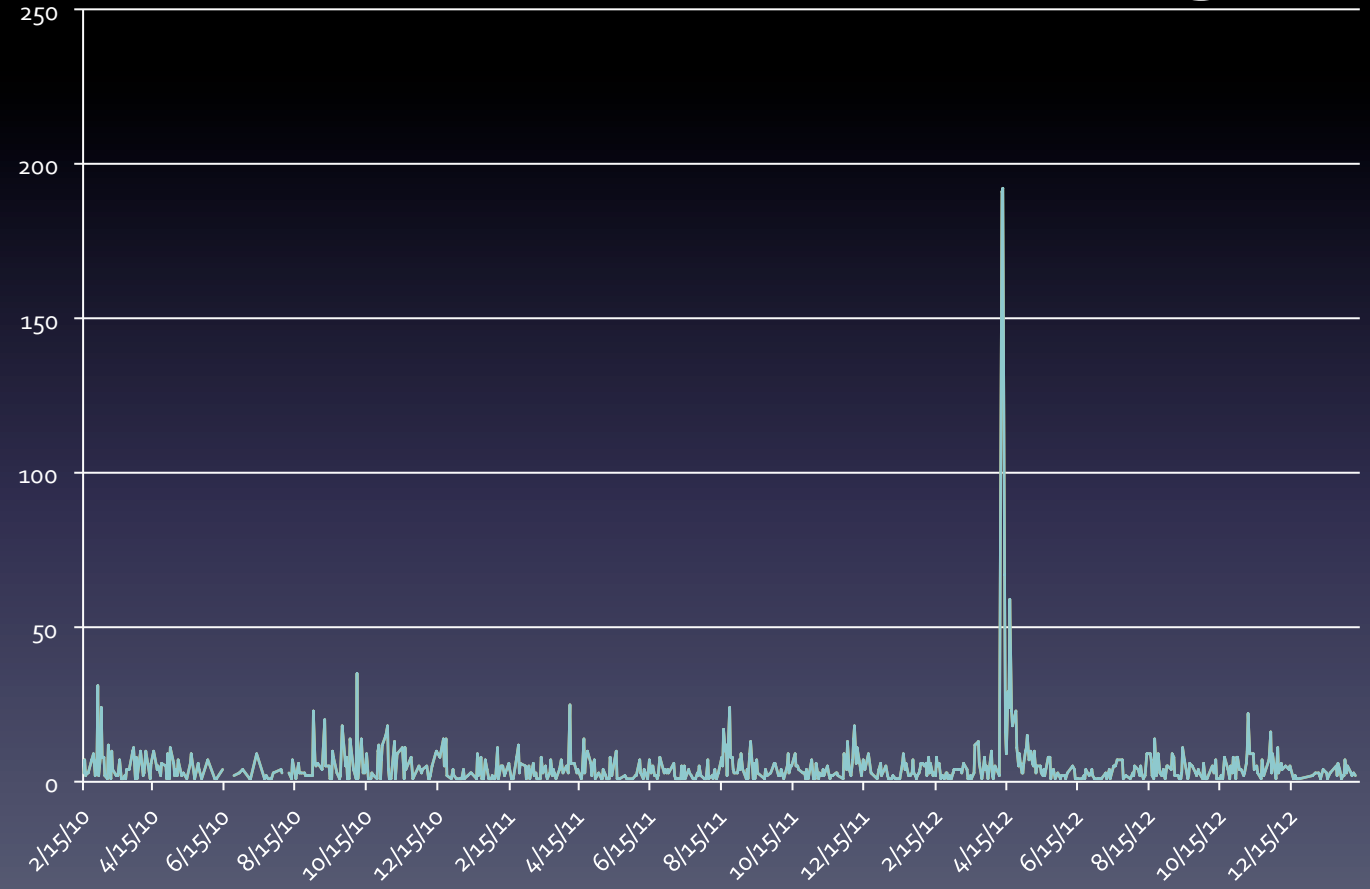


Linux/SSH Compromise

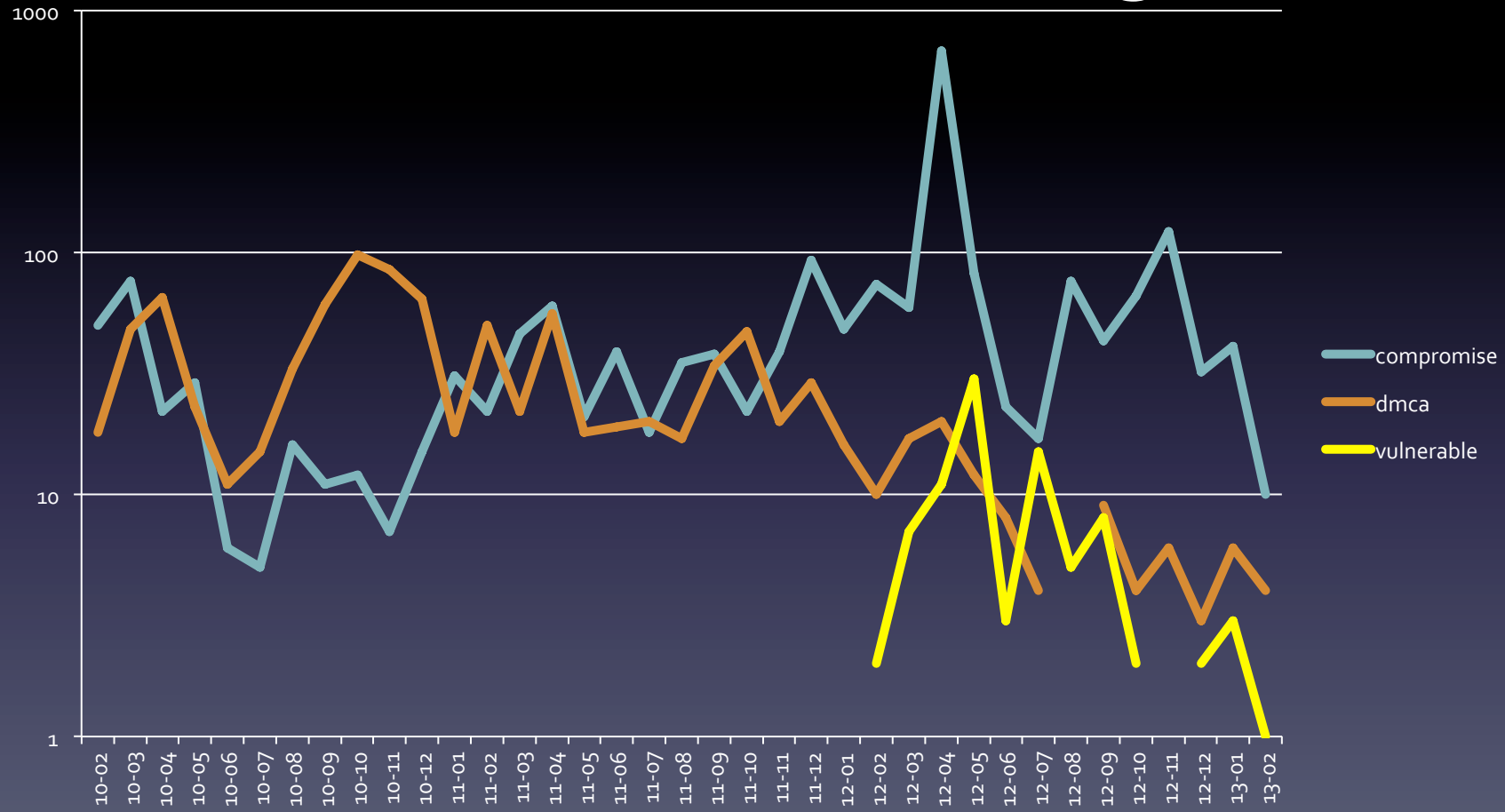
- It all starts with one weak password

ISPO STATS

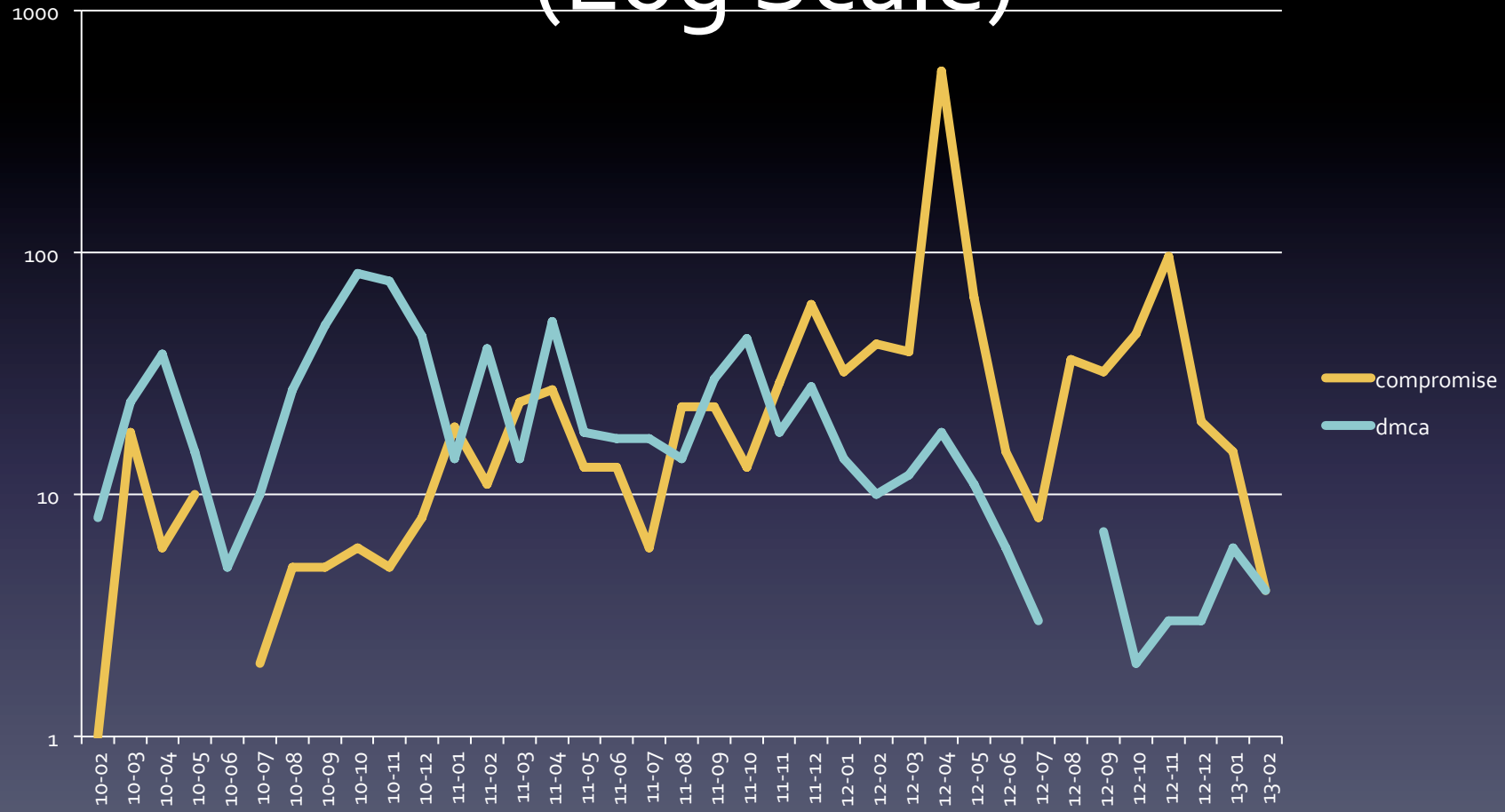
Tickets Created / Day 02/2010 – 02/2013



Tickets Created - Log Scale 02/2010 – 02/2013



Wireless – Tickets Created (Log Scale)



Wired – Tickets Created (Log Scale)