

Offset	Topic
00:17	<ul style="list-style-type: none"> ● Intro <ul style="list-style-type: none"> ● Star Wars exhibit at the Franklin <ul style="list-style-type: none"> ● Smaller than I expected ● Enjoyed getting a close look at designs ● Took plenty of photos ● Kids showed no bias between two trilogies ● Adults mostly favored original trilogy ● Recorded some audio for Voice of Free Planet X ● http://planetx.libsyn.com ● Probably had more fun at The Franklin as a whole, spending time with friends
05:08	<ul style="list-style-type: none"> ● Listener Feedback <ul style="list-style-type: none"> ● Dave LaMorte <ul style="list-style-type: none"> ● Teaching for the Future podcast ● http://www.teachingforthefuture.com/ ● Weighing in on the editing vs. timeliness question ● Disagreeing with multimode
08:29	<ul style="list-style-type: none"> ● Security Alerts
08:48	<ul style="list-style-type: none"> ● Kraken surprises Storm worm in size at over 400K affected PCs <ul style="list-style-type: none"> ● http://go.theregister.com/feed/www.theregister.co.uk/2008/04/07/kraken_botnet_menace/ ● 400K PCs infected, including ones within 50 Fortune 500 companies ● Only 20% of PCs were accurately detecting the worm ● Low recognition apparently due to Kraken's ability to change its own code ● Talked about evolutionary, changing code in the past ● Far and away the biggest example of malware using this trick ● Apparently alters itself when the payload is activated ● Even in the original file is detected, can re-infected from altered file on disk ● Doubles odds of escaping detection ● Also receive updates through command channel once PC is infected ● Infected machines sending high volumes of spam ● As much as 500K per machine by some measurements ● Royal at security firm Damballa thinks it may grow up to 600K ● No one is sure why it remains so elusive, infectious ● http://blog.washingtonpost.com/securityfix/2008/04/kraken_creates_a_clash_of_the.html ● More details, including the accuracy behind Damballa's numbers

Offset

Topic

13:31

- Kraken uses DynDNS, as do others
- Includes code to identify new control sites in case host, domain names are yanked
- Damballa reversed some of the code in Kraken
- Registered the names ahead of the infection, create sinkholes
- Claims no traffic is going back out to infected nodes reporting to them
- Does give them a good idea of rate of infection, other details
- Still keep the kimono closed on how they pulled this off
- Looks like Damballa has re-classified a pre-existing baddy, Bobax
- Points out problems in classifying, standardizing recognition, names
- An alternate analysis identifies Kraken as Bobax, only at 185K PCs
- Security researcher develops Trojan counter hack
 - <http://feeds.wired.com/~r/wired/topheadlines/~3/268656293/researcher-demo.html>
 - Work by Joel Eriksson, at Swedish firm Bitsec
 - Reverse engineers hacking software, looking for exploitable security holes
 - Sort of like using phages against super bacteria
 - In particular targets the control software for trojans on remote client
 - Demoed his technique at RSA conference on Friday
 - Leverages the same mistakes, short cuts programmers of all stripes commits
 - Eriksson has demonstrated his technique a few times before
 - Even yielded a security patch, not effective, in one case
 - May be a bit legally dubious but effective when traditional approaches are losing ground
 - What would make this legally sustainable?
 - Keeping it to just investigation, identification to be followed by arrest, prosecution?

15:49

• News

16:03

- Gmail being throttled, blocked by some antispam vendors
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/265413535/20080406-gmail-being-throttled-blocked-by-some-anti-spam-vendors.html>
 - Talked about spammer's cracking Google's captcha
 - http://thecommandline.net/2008/03/02/news_133/
 - Success ratio was small, but apparently enough to have an effect
 - Ars has verified that anti-spam vendors are recommending slowing, blocking Gmail
 - On vendor, MessageLabs, is trying to be surgical
 - Attempting to block only relays from which spam is being sent
 - Affected relays change as spammers move around
 - Delays vary between none, to between 4 and 24 hours

18:54

- Doesn't affect client side, Bayesian filters
- Postini, acquired by Google recently, also unaffected
- Really only impacts IP based back lists
- This mostly means anti-spam services that mail providers use
- Pressure is on for Google to deal directly with captcha problems
- Ars did not talk to Google, apparently
- Couldn't find any press release, other materials from Google on the issue
- Google spends a good deal of time blogging about technology
- Even launched a public policy blog some time ago
- Why do they not have a security blog?
- Google application hosting
 - <http://arstechnica.com/news.ars/post/20080408-analysis-google-app-engine-alluring-will-be-hard-to-escape.html>
 - Contrasts to Amazon's services which are loosely coupled
 - App Engine is a one stop shop
 - Details direct from Google
 - <http://code.google.com/appengine/docs/whatisgoogleappengine.html>
 - Free accounts available initially
 - Ability to purchase more space, bandwidth to follow
 - Only supports Python but looking to add more languages
 - Some limits on Python standard libs, some additional Google specific libs
 - Includes Django but doesn't use a relational data store
 - Notes this may make some Django components harder to use
 - Provides some help to work with Django
 - Other frameworks should work
 - Provides own framework, webapp
 - Wonder how they can make promises of scalability when the app code could technically prevent that?
 - Use a sandbox security model, limit access to underlying OS
 - Data store is transactional, sounds like an object database
 - Uses optimistic locking
 - Initial language choice may be a huge limiter
 - In my experience, hackers either love or hate Python
 - Lock-in is another concern
 - This is not standardized web app hosting, with simple database, language support
 - No clean way to port code in or out
 - By Google's language, they seem to expect people to start, stay
 - Have to admit despite Ars' objections that Google's ability to scale infrastructure is attractive

Offset

25:15

Topic

- Google may be banking on that
- Also don't know the premium price point yet, may be very competitive
- How introversion may lead to reluctance about tech even among geeks
 - <http://db.tidbits.com/article/9544>
 - Author examines self as a geek who favors tech, disfavors IM
 - Avoids a diatribe against IM as evil
 - Willing to consider it is a personal, psychological question
 - Is it a consequence of a certain temperament?
 - Acknowledges IM is an important tool many use for communication
 - Clearly a self aware exercise to reconcile with IM
 - Admits to being an introvert
 - Explains it is not lack of social skill but choice, preference for asocial activity
 - Affects choice in social setting, is not itself a choice
 - Gives some good background
 - Jung's definition of introversion, extroversion as a continuum
 - Gives a good, short bibliography for further reading
 - Looks at specific traits of introverts and how they don't mesh well with IM
 - For example, introverts don't deal well with distraction, multitasking
 - Contrasts the experience of IM, Twitter interrupting with email
 - Can take time for responses, doesn't demand immediate attention
 - Makes a good point about that and voice mail making interruptions manageable
 - Genuinely has tried to find ways to make IM workable
 - Clearly concedes its usefulness and integral part of online norms
 - Find the Twitter conundrum less compelling
 - Description admits this is more of a social concern
 - Good suggestions for introverts to work with IM, Twitter
 - Overall, makes me more sympathetic to more introverted friends
 - Allowed me to recognize the online habits of some friends as introversion
 - Reminder that as generally positive some progress may be, benefit not always spread evenly
- Recent court decisions eroding ISP liability protection
 - http://www.news.com/8301-10784_3-9911501-7.html?tag=nefd.led
 - At risk is section 230 of the 1996 Telecommunications Act
 - Immunizes site operators from many complaints
 - One form of safe harbor
 - Article gives a brief background
 - Listen to episodes 9, 10 of Rules for the Revolution for more on 230

29:25

Offset

Topic

- <http://www.rulesfortherevolution.com/2007/03/20/episode-009-section-230/>
- <http://www.rulesfortherevolution.com/2007/04/20/episode-010-section-230-continued/>
- Kurt Opsahl of the EFF is the guest in these two episodes
- First case involved an operator of a variety of dating sites
- Complaint was over a bogus, sexually explicit profile
- Judge dismissed most of complaints, except for issues around rights of publicity
- Seems like rights of publicity coming more into question
- Think back to the Virgin Mobile case
- Sites, services encourage more info, which may be attractive for ads, press
- Not a privacy question, per se, or even an IP question, where copyright is waived or CC is used
- CDT's Sophia Cope concerned that this could be used to reframe defamation complaints
- Cope admits there is not much case law on publicity
- A potential loophole, doesn't mean generally weakening of 230, per se
- Defending lawyer optimistic about appeal, though
- Roommates.com the other case
- Allegations it violated fair house act with questionnaire
- Successfully defended but circuit court divided on appeal
- Is the site an "information provider", except from section 230?
- Structure, presuppositions of questions seem to be the core issue
- Also ability to search, filter specifically on preset answers
- Open ended questions, where users could say anything, allowed since questions were deemed neutral
- May narrow 230 but may also stall critics
- Also not sure that this ruling applies broadly, given the specifics of the case
- Even for another operator with a questionnaire, merits, biases of questions need to be decided, then only if complaint is raised

34:20

- **tail -f**

34:39

- Another museum joins Flickr commons project
 - <http://creativecommons.org/weblog/entry/8190>
 - The Commons was started in collaboration with LoC
 - Talked about this on the 1/20 news show from this year
 - Goals are to share, invite collective tag, annotation
 - At the time it was announced, Smithsonian immediately showed interest
 - Powerhouse Museum in Sydney, Australia
 - First museum to participate

Offset

Topic

36:11

- Contributing 200 photos from its Tyrell Collection, publicly held photos
- Will continue to add photos from this almost 8K collection
- Carriers to argue P4P means regulation unnecessary
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/268086748/20080410-big-isps-push-p4p-as-substitute-for-fcc-regulation.html>
 - In latest filings from Comcast, AT&T to the FCC, argue P4P lessens need to regulation
 - Original work published was with Verizon's participation
 - Pando, only developer of P4P, has since broadened to include AT&T, Comcast, others
 - Still following other arguments about abuse by P2P users, definitions of reasonable network management
 - Problem is Pando is the only implementation
 - Until we see competitors able to use the same underlying protocol, then skepticism is due
 - An open P4P with many clients, competitors, but working with carriers cooperatively may lessen argument for regulation
 - It is way too early to seriously consider this point

38:21

- **Outro**
 - Contact me
 - Email to feedback@thecommandline.net
 - Web site at <http://thecommandline.net/>
 - IM to command.line@skype
 - Listener comment line is 240-949-2638
 - del.icio.us tag is "for:cmdln"
 - <http://twitter.com/cmdln>
 - I'd like to thank libsyn.com for AAC hosting and Wouter de Bie for MP3 hosting
 - These notes and the show audio and music are covered by a Creative Commons license
 - <http://creativecommons.org/licenses/by-nc-sa/3.0/us/>
 - Attribution, non-commercial, share alike