Sysadministrivia

Linux, Lagers, and Late Nights

S1E3: "Fuzzy-Wuzzy Was a Bugbear (Was He?)"

Posted 2016-03-28 04:14
Modified 2017-01-28 14:22
Comments 0

Navigation

Previous Episode	Next Episode
S1E2: "hunter2"	S1E4: "A Challenger Appears!"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-03-17 02:26:50	2016-03-28 04:14:43	aaron k.

Verification

Format	SHA256	GPG	Audio File
MP3	4c60282ca1c128126dbf77930b3e488a2cbce9de4afabddea507b5978409e94d	click	click
OGG	81e6c31f01f062bc67ceae0f8470c06d4c9277c1c676dd0386a74eb9cdefef3f	click	click

Quicklisten:

Windows auto-updating, fuzzing, git (yes, again), and more of the ongoing Apple vs. FBI case. We also talk about BYOD (Bring Your Own Devices).

- News
- Notes
- Errata
- Music

News

Starts at **00m32s**.

- Several major websites were hit by ransomware.
  - The Fortune rag says it might be China. I typically disagree with these sort of things...
  - But there is some compelling evidence supporting it.
  - We talk a bit more about ransomware back in S1E1, and how you should really start implementing backups (that are RO at rest!).
- There's also a git vulnerability. We talk more about it in the notes.
- Windows 7, 8 etc. are auto-upgrading to Windows 10. We talk more about this in notes.

Notes

Starts at **1m30s**.

I was drinking a PBR (yes, I know. Again.), Paden was drinking Buckeye Vodka, and Jthan was drinking Upslope Pale Ale.

- I'm pretty sure the "free upgrade" to Windows 10 was a precursor to the nigh-forced upgrade.
  - We touch upon some reasons why this is actually a bad idea, despite our hard-on for keeping software updated.
  - Mac OS X does this but on a policy level. This is an example of the packaging changes I talk about.
- Fuzzing is fun! **(8m40s)**
  - There are a *lot* of fuzzers out there. AFL is a nice one. Keyfuzz is a keyboard driver fuzzer! Wfuzz is a fuzzer for websites. ZZUF is a generic input fuzzer for applications, etc. There are a lot of fuzzers out there. For testing netkit, though, I'd definitely start with the BlackHat preso on it.
  - Of course, just doing a `netcat somebox.with.telnet.open 23 < /dev/urandom` is always fun- see how long it takes before the thing crashes (or the target severs the connection)!
  - The beginner's guide to fuzzing is here.
- Git is awesome **(15m00s)**
  - Jthan's $dayjob is switching from gitolite to GitLab.
  - Git's CVEs are CVE-2016-2324 and CVE-2016-2315.
  - If you're a heavy user of git (and/or GitHub), you may find this pretty useful.
  - I mention some severe issues with using GitHub.
  - Use the Git daemon if you want to share code.
  - If you need to totally remove a file from your git repository, this is handy.

- The FBI vs. Apple case is still a big deal. **(20m48s)**
  - This is what happens when enforcement agencies want protection circumvented for them.
  - It's not legal to force Apple to write a backdoor.
- "Bring Your Own Devices" can be an issue **(29m15s)**
  - There are multiple cases of USB sticks used as a vector.

Errata

- I state that Tunnelblick is the "best" OpenVPN option for Mac OS X, but my boss (which I just found out listens to the show, apparently) mentioned Viscosity. It's a bit prettier and easier to use, and was definitely worth a mention. I had totally forgotten about it! Unlike Tunnelblick, however, it's not free/libre (9USD). They also, apparently, have a Windows port (which Tunnelblick does not- and the OpenVPN-provided GUI for Windows is atrocious). Another alternative is Shimo.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	The Curtain Rises	Kevin MacLeod	click	CC-BY 3.0
Outro	Allada	Kevin MacLeod	click	CC-BY 3.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories Season One

Comments

There are currently no comments on this article.