Sysadministrivia

Linux, Lagers, and Late Nights

S2E9: "Fileswatter"

Posted 2017-06-19 03:59
Modified 2017-06-19 02:29
Comments 0

Navigation

Previous Episode	Next Episode
S2E8: "Why do Bids Suddenly Appear?"	S2E10: "Free AS IN Beer, Not FREE BEER"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-06-09 03:36:11	2017-06-18 18:09:28	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`70fba1eb27bb9c240d1ded96e054a936fdc6da6788ce116745c6a80914b8e1a8`	click	click
OGG	`c2895e08b22006f4f071cd4026e18a25be2e82c0612bda0d984dce93bf003881`	click	click

Quicklisten:

In this episode we discuss some ways of permanently erasing content. It's not quite as easy as you might think!

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- British Airways has had some trouble lately.
- The Supreme Court is considering whether a warrant is needed for local law enforcement to search your mobile device
- China discovered a massive underground network of Apple employees selling personal data and PII of consumers.

Notes

Starts at **13m14s**.

I was drinking whiskey (same Bulleit 10 as before). Paden was drinking Stella Artois. Jthan was drinking Alaskan Summer Ale again.

- Securely destroying data (see S2E8 for more in-depth discussion on why this is important)
  - Deleting a single file can be challenging, especially with journaled filesystems (e.g. EXT3/4, BTRFS, ZFS, NTFS, etc.)
    - We mention shred
    - …and wipe for secure **file** deletion
  - Deleting contents off an entire drive/filesystem, however, can be more daunting.
    - dwipe is the "guts" behind DBAN (Darik's Boot And Nuke) (previously opensource)
    - nwipe is a fork of dwipe that remains opensource and supports newer hardware/technologies and other features.
  - Because there are tools that can recover data "underneath" reformats (see S0E14), you need to be careful when wiping disks.
  - You'll also want to probably physically destroy the media, if possible. This can be done commercially (via a company such as SSI) or in-house (via equipment from companies such as SEM, Ameri-Shred, and Allegheny Shredders).
  - Platter disks should/can be degaussed
  - But degaussing doesn't work for SSDs.
    - Basically you need to EMP them…
    - Which, strangely enough, doesn't work as well for platter drives due to their construction. So if you use platter and solid-state, you'll need/want access to BOTH degaussing and EMP. (Sadly I'm having trouble tracking down equipment for EMP generation and Paden's under NDA, so you're on your own for this.)
    - SSDs also require a little extra work to do a software wipe of.
  - Paden thought I was referring to GPartEd but I was actually referring to GNU parted, which can be used to recover a lost/wiped partition table (but not lost data on wiped inodes). For a more detailed scan/recovery, you'll want to use Testdisk.
  - Paden talks about some videos on physical destruction of platter disks. Some **really great** (and hilarious) DEF CON talks on this can be found here: How I Lost my Eye (with Shane Lawson, Deviant Ollam – whom you may remember from S1E14, and Bruce Potter) and How I Lost my Other Eye (by Zoz). Seriously, watch them. They're both great talks.
  - For optical media, you can even get cheap in-house shredders that should do the job. Make sure you further obliterate the remains, though –

optical media is easier to reconstruct since it's less densely packed.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(43m30s)**

- A company didn't document their onboarding process well, which led to a new hire frying their production DB.

Note that this Baddie is for the **company**, the person who wrote the documentation/runs operations/etc. and **not** the new hire.

Errata

- Paden was at SELF (Southeast Linux Fest) and Jthan was off-site from his normal recording rig, so the sound quality for their tracks may not be ideal.
- "Deducer" and "surmiser" are both not words, Jthan. (And "suspic" as a verb is not a real word either.)
- Irrecoverable is, indeed, a word.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	A Dark Blue Arc Instrumental	Pipe Choir	click	CC-BY 4.0
Outro	Turtle Island	Todd W. Emmert	click	CC-BY-NC-SA 3.0

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

Author r00t^2
Categories Season Two

Comments

There are currently no comments on this article.