Sysadministrivia

Linux, Lagers, and Late Nights

S2E8: "Why do Bids Suddenly Appear?"

Posted 2017-06-05 03:59
Modified 2017-06-05 02:44
Comments 0

Navigation

Previous Episode	Next Episode
S2E7: "Projecting Insecurities"	S2E9: "Fileswatter"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-05-26 02:50:01	2017-06-02 06:48:34	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`db8855ea211c3718d39bf6e1d3e48bc48fab87f2cab1890f7d001f5d46c938e3`	click	click
OGG	`72f824c44c45d6424eccb1ab125a6f60ceb90f390c194a069d1f90d90ca078f0`	click	click

Quicklisten:

We give some tips and tricks on buying older/used hardware, and recount two very silly reactions to “cyber attacks”.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- The NSA-originated, NHS-spread ransomware “WannaCry” goes global
  - Dear intelligence agencies: this is why you do not need to develop offensive tools or hoard vulnerabilities/exploits. Or shouldn’t, rather.
- Apple is seeing a rise in requests pertaining to “national security”
- A Sydney airport was brought down by malware
- Related to WannaCry, there’s an SMB attack that uses 7 NSA-originated/hoarded vulnerabilities/exploits (WannaCry just had two)
- Florida’s database of Concealed Carry permits/licenses has been leaked

Notes

Starts at **15m12s**.

I was drinking Bulleit bourbon 10-year again. Paden was drinking Pyrat rum. Jthan was drinking Kimbao Pinot Noir.

- How to purchase used equipment properly
  - Always go with new storage. Always. Because things like this and this exist.
    - And if you’re decommissioning equipment yourself, make sure you wipe your disks securely and don’t sell them!
  - Sometimes you need actual extra equipment! (e.g. RS-232 with a null modem etc.)
  - Make sure you try to get any original install discs, licenses, maintenance records, etc.
  - Jthan has only gotten used stuff from UnixSurplus; others have offered donations
    - Others worth mentioning include (no, we aren’t being sponsored):
      - ServerMonkey
      - STI
      - XByte
  - Make sure you know what sort of testing, refurbishment, etc. processes the vendor goes through to “certify” the equipment
  - How do you verify the integrity of the hardware? With memtest86+, a burn-in test and other methods. I’d also recommend the Phoronix test suite (system builders, take note- that’s useful for not only doing a hardware check but also benchmarking performance)
    - Many CompTIA A+ study guides have instructions for testing a PSU with a multimeter
  - The cabinet I was going to recommend for Paden is here.
  - For used managed switches, make sure you reset to the default configuration!
  - For used UPSes, you’ll want to get a new battery no matter what.

- “Things you should never say after a cyber attack” (thanks, Skip!) **(37m37s)**
  - “There is no evidence that patient data has been compromised.”
  - “We can’t send you/release logs because it contains IP addresses”
    - Pro-tip: all this tells me is that you don’t know how to scrub/anonymize logs, which is like… system administration 101.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(58m28s)**

It seems that an untested patch brought down an AU hospital.

Errata

- Paden, sic has nothing to do with tyranny – it’s a preposition/pronoun/etc. (depending on context). “Semper fidelis” isn’t actually a grammatically complete sentence otherwise.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Extreme Fight	Marcos H. Bolanos	click	CC-BY-NC-SA 4.0
Outro	The Gifted House	Greg Atkinson	click	CC-BY 4.0

(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.