Sysadministrivia

Linux, Lagers, and Late Nights

S6E11: "Ransom? Where?"

Posted 2021-07-18 23:59
Modified 2021-07-18 03:59
Comments 0

Navigation

Previous Episode	Next Episode
S6E10: "You Can't Scale a Fish"	

Log

Recorded (UTC)	Aired (UTC)	Editor
2021-07-08 02:39:17	2021-07-17 08:58:21	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`c5e04a7254633950600b6fbd66dca20ceef2abc0ca60c4b1ac922a7f12e27ddf`	click	click
OGG	`73d53e3dc4bceef558f216dbf9fabf13ce65fceae68e54590eba1a5c61bb60b3`	click	click

Quicklisten:

We talk about the increased (reporting) of ransomware attacks.

Goin' down to the dickotheque.

- Just the Tip
- Notes
- 15 Clams
- Errata
- Music

Just the Tip

- Paden wasn't able to join us this episode, so instead we talk about iterating in bash.
  - Specifically, Jthan wanted to iterate over a list of files. Rather than putting them into an array, I suggested that he use xargs (which he had no idea existed before).
  - You can find examples here.

Notes

Starts at **27m33s**.

I was drinking Shiner Bock. Jthan was drinking an old-fashioned (with the same bourbon as last episode).

- Ransomware prevention (and a bit of mitigation)
  - Jthan read in a Slashdot article (which reports that paying ransoms for ransomware may now be **tax-deductible**) that a very significant percentage of businesses hit by ransomware still pay…
    - Because they have "cyber insurance". Real thing, if you didn't know.
    - Cyber insurers need to **stop** paying out for ransomware attacks. This will never get better if not.
    - Ransomware will end if companies stop paying the ransoms. It will get worse if they do. **Stop paying the ransoms.**
  - Backups are **the key** to making ransomware attacks irrelevant.
    - Ideally, backups should be **append-only**. Clients should NOT be able to prune its own backups.
    - Keep a cold-spare ready, already imaged/prepped with your most recent backup, but keep it airgapped or off until needed. In the event of a compromise/ransomware attack/etc., replace the hot with that spare and reimage the hot with the known-good backup. The old hot then becomes the new cold spare or, alternatively, the cold spare can be used to provide services while you are preparing to restore your hot.
  - Educating users about phishing and having a "disposable OS install" (via config management, iPXE/PXE, and backups) approach will go MILES in preventing and recovering from a ransomware attack (attempt).

15 Clams

In this segment, Jthan shares with you a little slice of life. The title is a reference to this video. (2m16s in)

Starts at **1h05m44s**.

Audacity was bought a while back by Muse Group. They changed some privacy notices (likely to conform to GDPR requirements), and now people are calling Audacity “spyware”.

But don’t worry, that’s not really what’s going on.

Errata

- I didn’t out Jthan’s original quote in the shownotes! He (Jthan) originally (I want to say somewhere in season 3?) claimed he was “young, dumb, and full of cum”.
- I may have been thinking of something else, because Allagash does not have wine. (Their beer is fantastic, though.)
- I try to point out to Jthan that most ransomware attacks **don’t occur as a result of 0days**, but rather dumb everyday shit like phishing emails and downloading and running nasty shit. Ransomware infections are primarily due to user/staff error, not a targeted attack.
- Jthan, the scammers do not give a shit about emotionally manipulating you to scam you. You **must not** shy away from these in your training/testing phish campaigns.
- Jthan, the seed can still be generated locally and uniquely across multiple devices and allow for multiple simultaneous devices. Typically, the user is not interactively/manually creating the seed so unless that client software is opensourced and you’ve read through the code, you don’t know where that seed is being actually generated; the entire point is it’s transparent to the user whether local or remote.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Me And You	Crennwiick	click	CC-BY-NC-ND 4.0
Outro	Irie Transmission	Dub Cmd	click	CC-BY-NC-ND 4.0

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

Author r00t^2
Categories Season Six

Comments

There are currently no comments on this article.

Published with Textpattern CMS