Sysadministrivia

Linux, Lagers, and Late Nights

S0E7: "The Isolation Chamber (pt. 1)"

Posted 2015-05-17 06:53
Modified 2017-01-28 08:46
Comments 0

Navigation

Previous Episode	Next Episode
S0E6: "Backups and Beatdowns"	S0E8: "Something Old, Something New, Something Broken, Something Due"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-05-24 17:25:44	2015-05-17 06:53:13	brent s.

Verification

Format	SHA256	GPG	Audio File
MP3	d7e050a4d109fa1b0626a55db10f9a84854117d176d27c7c38cf5d109e7f2eba	click	click
OGG	aac7a75a4f417d43cab81c684270e5fc97cd0c418b46bed39167b4a6dd9e491d	click	click

Quicklisten:

This episode, I go solo because Jthan is lame.

- Notes
- Errata
- Music

Notes

- VENOM's page is here. CVE is here. PoC is here.
  - It affects QEMU / KVM and Xen
  - Linode says they are not vulnerable (but their KVM beta program was, and has been patched per the comments of that article).
- You can find more real-time interaction with us via our twitter or IRC (details/webchat client on our contact page).
  - As for live-streaming, we're still looking into solutions on this. If you know of something that hooks into Mumble/Murmur server-side and spits out something like an RTSP stream, let us know!
    - When we have something worked out for live-streaming, we'll announce it on our twitter.
- As far as documentation via a wiki goes, I prefer MediaWiki (in case you couldn't tell by viewing this in the wiki itself!).
  - For generating static documentation (and exporting to PDF), I like LibreOffice.
  - Encrypting plaintext files for e.g. credentials can be hard. I like Pass. It uses GPG to encrypt, and you can specify multiple people who have access to a given password store by simply adding their public key.
  - PHBs, or Pointy-Haired Bosses, is a reference to Dilbert.
  - For a great example of documentation, check out TLDP's Howtos with LinuxDoc and the LDP Author Guide.
- Making people care about security is probably a futile effort, but you know what they say about the weakest link in a chain.
  - For details as to why I don't like it when people refer to attackers, crackers, thieves, etc. as "hackers", see the Jargon File's entry. File it under any use of the word "cyber".
  - It's not like banks getting compromised is a regular thing or anything.
    - And especially not via the users…
    - And they TOTALLY aren't engaging in (illegal) counter-ops or anything…
  - You really need to not give your social media credentials out.
  - And also, don't trust social media website staff.
    - Hell, don't trust dating websites either.
  - Oh hey, and something like this can totally happen to you. Don't make it any easier- use different passwords for ALL your accounts.
  - And shitty internet political activists/"social justice warriors" do some REALLY shitty things sometimes, and destroy the lives of totally innocent people, simply because they have a *perceived difference in politics or values* (even when the difference in values **isn't even there**). I should note that this would be a classic example of a widescale social engineering attack (DSE? Distributed Social Engineering?).
  - Ello, lolol.
- This has an awesome introduction to steganography.
  - You can even steg tweets.
  - Some handy steganography tools (in GNU/Linux at least are OpenStego, StegHide, SNOW, Stepic…
    - You can even convert text to image stegs (think along the lines of QR codes)! Check out PhotoCrypt.
  - You can find an archive/mirror of PoC||GTFO here
  - Just be sure you remember that stegs are not encryption, they're obfuscation. With a little luck, they can even be automatically detected.

- For my drive encryptions, I use cryptsetup with LUKS (via dm-crypt).
- Social media can indeed be used as an alibi.
  - Plausible deniability
  - Related (especially to topic before this one): deniable encryption

Errata

- If you listen closely, you may hear the hum of my window A/C unit (and the distortion I caused trying to remove it as much as realistically possible). Sorry about that; I tried to edit it out best I could. Future episodes I'll try to not keep it on while recording. :)
- The episode we were *supposed to* talk about documentation in was S0E5.
- VENOM does **not** affect VMWare despite what I had suspected.
- Yay! Employers engaging in social media snooping actually **is** now illegal in six states.
- The Internet is, indeed, 25 years old.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Peer Gynt Suite No. 1, Op. 46 - I. Morning	Composed by Edvard Grieg (Performed by Czech National Symphony Orchestra)	click	CC0 1.0
Outro	Naraina	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 (Pilot Season)

Comments

There are currently no comments on this article.