Sysadministrivia

Linux, Lagers, and Late Nights

S1E1: "GHOSTv2: The Re-Hauntening"

Posted 2016-02-29 05:16
Modified 2020-09-10 01:22
Comments 0

Navigation

Previous Episode	Next Episode
S1E0: "The Return of the Ping"	S1E2: "hunter2"

Log

Recorded (UTC)	Aired (UTC)	Editor
2016-02-18 03:33:48	2016-02-29 05:16:00	aaron k.

Verification

Format	SHA256	GPG	Audio File
MP3	`7fe7f7a24f2a68d3b9c47da7da391b705a75653648ce1170f901a202613ce165`	click	click
OGG	`41322fbb21571d13fd7000d4626b01a6962418508ab6cbb79e4e9a16122b1819`	click	click

Quicklisten:

Apple vs. the FBI, IPMI/DRAC, and mostly the new glibc bug.

We also introduce fixed segments to the show with designated hosts. Let us know how you feel about the format change! (This allows us to give timestamps for each segment as well!)

- News
- Notes
- Errata
- Music

News

2m27s

- The iPhone/iOS bricks if you set the year to 1970.
  - There's news of it all over, and I'm sure there's a patch coming if one doesn't exist already to prevent it from happening to devices that haven't been bricked- source is this, which mentions a patch in the next (presumably already released) iOS update. Anyways, this is presumably due to some sort of underrun and the Unix Epoch time (*0* in Epoch time is January 1, 1970).
- Not only did malevolent actors hold a hospital at ransom with cryptoware/ransomware, but they paid it. We talk about it more in the notes.
- In the San Bernardino shooting case, the FBI are demanding that Apple provide them with an iPhone backdoor. Apple has responded. And the FBI has responded.
  - But wait, there's more! After we recorded, it seems our predictions are coming true – even before any sort of PoC was **even delivered**. Orwell must be spinning in his grave.
- The glibc vulnerability we talk about more in the notes.

Notes

3m13s
I was drinking a PBR, Paden was drinking Pinnacle Vodka, and Jthan was drinking his homebrewed amber ale.

- IPMI/DRAC/etc. (**3m37s**)
  - IPMI is an acronym for **Intelligent Platform Management Interface**.
    - You may remember the report of widespread attacks on/through IPMI. This is why I say leaving it exposed to the WAN is a **bad** idea. (If you see reference to *BMC*, that's the *Baseboard Management Controller*- basically the "brains" of the IPMI and the actual hardware integration.)
  - IPMI can do some pretty awesome things.
  - *DRAC* is **Dell Remote Access Controller**.
  - Some handy clients are ipmitool, FreeIPMI, IPMIview/IPMIcfg, and IPMIutil. There's even a Nagios plugin (because of course there is). And hey, if you're an LDAP nerd, there's a Fusiondirectory plugin, too. And Jthan thought there "weren't any Linux IPMI clients". HAH.
  - And yes, Victoria, there is indeed a Linux client for DRAC too. I recommend DRAC-KVM though, as it's fully opensource and comes without all the bloat.
  - And like I said, you can get KVM over IP/IP-KVM switches as well.
  - Remember, it's not just a toy to make you more lazy- it's a valid uptime and maintenance tool that will save your company money.
- The Android encryption "spec" (**10m42s**) can be found here.

- Clickbait ahoy! (**11m42s**). There's some solid tips, but we read (and talk about!) the entire article on-air so you know.
  - I talk about disaster recovery in S0E6, S0E14, and S0E17.
  - We talk about the Linode outage/attack in S1E0.
  - Infosec advice via twitter was S0E11.
  - If you're wondering what was bleeped, this is a clue. So is this.
    - I love that Aaron didn't censor the actual indicting part.

- Paden mentions these, **28m01s**.
  - I mention my shining glory.

- I still can't believe the hospital paid the ransom (**32m02s**).
  - The sheriff station that paid off multiple infections of ransomware? Hilarious and tragic.
  - Remember to MAKE YOUR BACKUPS! It renders ransomware ineffective.
  - Does anyone else remember the ILOVEYOU virus?
  - We also talk about DIY infosec research in S0E6.

- The glibc bug is a mess. (**41m20s**)
  - It's *very* similar to GHOST (S0E1), except…
  - It's a **much** wider scope and not limited to several services.
  - A fix has been incorporated, and is in glibc 2.23. It has been backported to most major distributions' releases.
  - It affects glibc versions 2.9-2.22.
  - The following are the associated bug reports, mailing list posts, etc.:
    - googleonlinesecurity.blogspot.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html
    - access.redhat.com/errata/RHSA-2016:0176
    - sourceware.org/bugzilla/show_bug.cgi?id=18665
    - sourceware.org/ml/libc-alpha/2016-02/msg00416.html
    - access.redhat.com/security/cve/cve-2015-5229
    - access.redhat.com/security/cve/cve-2015-7547

- We neglected to mention it in the news segment, but GMail's new padlock shit fucking sucks. It's a terrible idea. (**46m24s**)
- Lastly, (**51m28s**) we have an article on our Cards Against Humanity deck, but we need more cards! So give us some suggestions!

Errata

We need some more topics! please get in touch and give us some suggestions!

- Now I'm wondering if at **4m27s** Paden is giggling because it sounds like I'm saying "in Iraq somewhere". I'm actually saying "in a rack somewhere".

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Disco Medusae	Kevin MacLeod	click	CC-BY 3.0
Outro	Vadadora	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.