

Sysadministrivia

Linux, Lagers, and Late Nights

S2E1: "Like Files Caught in a Web"

Posted 2017-02-27 04:59
Modified 2017-03-10 16:32
Comments 0

Navigation

Previous Episode	Next Episode
S2E0: "I Think There's a Delay"	S2E2: "Ayyy, I Took Your Job"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-02-16 03:42:50	2017-02-27 04:59:00	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	7506e84a6852f5b9c4fb5ffac119a18325a0463bca705ef22080343788bd9e8e	click	click
OGG	9a7b0c1a25e59228cab170372e261fde1fc9b5c7916f5867e0ba6d3b5025a804	click	click

Quicklisten:

We talk about networked/clustered filesystems, running "bleeding-edge" software in production environments, and several important announcements!

- News
- Notes
- Sysbadmistration Award
- Errata
- Music

News

- A university's vending machines (and "smart" bulbs, and other IoT devices) were DDoSing ...themselves (see Errata).
- The exploit used to break into the San Bernardino shooter's phone has been leaked. No surprise here.
- A NASA engineer was 'compelled' by authorities to hand over the passcode to his iPhone.
 - Bonus points to Jthan for his "the government is stealing its own secrets" line.
- An IT professional was arrested simply for performing normal and standard business practices (namely, closing access when a client refuses to pay their bill).
- Windows 10's lockscreen leaks the clipboard.
- The Instapaper outage was due to them hitting the ext3 filesize limit.
 - For your records, that is **2TB**.
- Dubai wants to launch hover-taxi. But "hover" is a misnomer, we're talking actual flying cars (300m/1000ft) here.
 - And they'll be self-driving. What could go wrong? ;]
- Apple broke their ethernet with an update.
- Blackberry's market share has now hit 0% (well, specifically 0.0481%).
 - However, there is talk of them attempting resurrection of the brand. (Still. It's too late, guys.)
- CyanogenMod (and Cyanogen, Inc.) are **dead and gone**. We talked about it in S0E3. Anyways, the "spiritual reboot" of CyanogenMod is LineageOS which I've flashed and am immensely satisfied with. I didn't even need to start from scratch; they offer a "migration" firmware for a limited time only. It feels more clean/polished, and many of the bugs I had with CyanogenMod simply don't exist on Lineage.
 - Paden also flashed LineageOS onto his tablet from the vendor firmware he previously was running, and said it was incredibly easy and provided a much improved experience.
- Jthan is opening applications for his Sdayjob's hackathon. It will be from May 22 to May 24, 2017 in Boulder, CO. You can contact Jthan via our contact page (which also has our Twitter handle, etc.) or you can reach him directly via his bio.
- Please send in your questions you want answered on-air!

Notes

Starts at **16m09s**.

I was drinking Huyghe's Delirium Tremens. Paden was drinking water. Jthan was drinking a Fate Watermelon Kolsch, which we've linked to, mixed with vodka.

- Networked/clustered filesystems
 - CIFS / SMB (called "samba" in the opensource implementation)
 - CIFS/SMB vs. NFS
 - NFS
 - Yes, Virginia, Microsoft can use NFS, and map to a drive letter.
 - SSHFS
 - Uses FUSE
 - FTP
 - Technically in FTP's section (but not mentioned) is rsync (which we talk about at-length in S0E6), SCP, and SFTP
 - I also mention GPFS
 - Lustre
 - BeeGFS
 - Gluster
 - Ceph
 - Coda
 - I also mention AFS (and the opensource implementation)
 - ownCloud
 - NextCloud
 - I also mention TrueNAS / FreeNAS, and Syncthing
- When it's okay to run bleeding-edge in Prod (**39m00s**)
 - We define "non-bleeding edge" as typically "enterprise"-centric distros such as Debian, CentOS/RHEL, SuSE. They tend to have a long vetting process for packages included in the core repositories.
 - Arch or Gentoo in prod can be useful for cases where you're running source-based systems (and require very low-level binary optimizations) - Gentoo would be more ideal here.
 - Gentoo is very useful for slotted installs
 - Arch is good for up-to-date releases of software and implementations where resource consumption (storage space, RAM usage, etc.) is a concern.
 - Chromebooks are actually Gentoo-based!
 - e*Trade used to (and may still do) run Gentoo servers.
 - I also plug (yet again) the "Pink" Book
 - (Yes, it isn't actually pink. That refers to the 2nd ed.)
 - We talk about systemd at length in S0E8.

Sysbadmistration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. (**57m14s**)

Plone released a critical hotfix but their Cloudflare caching/CDN was, in some cases (namely if curl/wget was used) serving a file that didn't match the checksum. When Jthan addressed it, they told him he was wrong.

```
<jthan> Can anyone explain the reason for the sum mismatch on this file from what is listed? https://plone.org/security/hotfix/20161129
<REDACTED_0> jthan: I had that - try refreshing the page.
<REDACTED_1> jthan: very early after we published the fix there was a change to the zip file... check that you have the current zip file
<jthan> REDACTED_1: Just clicked download.
<jthan> also had two others confirm it's not just me
<REDACTED_0> REDACTED_1, jthan: I think for me - it was the page that had the wrong checksum, and was corrected later. The file didn't appear to change
<jthan> REDACTED_1: same results in chrome w/ incognito. no caching.
<REDACTED_1> jthan: I'm seeing PloneHotfix20161129-1.2.zip MD5: f78c6a6fb79421e5e05dc83cceedb191 SHA1: 1fe5909e22f6ba2a29712ec4c80725a33bcc6cd2 For all platforms (7364 bytes)
<REDACTED_1> $md5 PloneHotfix20161129-1.2.zip
<REDACTED_1> MD5 (PloneHotfix20161129-1.2.zip) = f78c6a6fb79421e5e05dc83cceedb191
```

```
<jthan> https://plone.org/security/hotfix/20161129/@download/hotfix
<jthan> ^ that link is still pushing 1.0
<REDACTED_1> for me https://plone.org/security/hotfix/20161129/@download/hotfix just sent 1.2
<REDACTED_1> huh
<REDACTED_1> well try going to pypi ... https://pypi.python.org/pypi/Products.PloneHotfix20161129/1.2
<REDACTED_1> jthan: well try going to pypi ... https://pypi.python.org/pypi/Products.PloneHotfix20161129/1.2
<jthan> Yeah that one is okay..
<jthan> I feel like if people are wgetting it right now though or using curl they're just getting a file called "hotfix" wih the wrong sum though
<REDACTED_1> jthan: you're right... anonymous Safari https://plone.org/security/hotfix/20161129 clicking on that link to https://plone.org/security/hotfix/20161129/@download/hotfix gets me the 1.0
<REDACTED_1> I'll ping folks :)
<jthan> Thanks.
* jthan is an alarmist :-p
<jthan> Just wanted to let someone know before too many people grabbed the wrong one without summing it
<REDACTED_1> nice catch jthan
<REDACTED_1> jthan should work now... we purged cache in the plone.org control panel. also, if you https://plone.org/security/hotfix/20161129?v=432 (some random string value) that forces CloudFlare to re fetch the page
<jthan> sum matches. thanks again
<REDACTED_1> thx jthan for catching that. we will see if we can fix the add-on for security fixes
<REDACTED_1> jthan: issue filed https://github.com/plone/plone.app.vulnerabilities/issues/8
<jthan> \o/
```

Welp.

Errata

- Turns out those vending machines and such seem to actually have been part of a botnet which we were a bit unclear on (and didn't realize until after); it wasn't part of their "normal" operation.
- SMB is the proper terminology, CIFS was only a specific implementation of SMB.
- I was mixed up- HTTP is **faster than FTP** for **large files** and **multiple small files**, and **FTP** is the one that's faster for **a single-shot small** download. (source)
- We got an email from a new listener who mentioned OES from Microfocus (previously Novell). It seems it's part of the Open Workgroup Suite but direct info can be found here. The listener mentions that it's rather solid, runs in SLES, and is scalable to 8Exabytes (from his recollection) with the NSS64 stack.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Got Me	Adrianna Krikl	click	CC-BY-NC-SA 4.0
Outro	Perfect Match	Kilyo	click	CC-BY-NC-SA 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.

Published with Textpattern CMS