Sysadministrivia

Linux, Lagers, and Late Nights

S2E18: "Dueling Banditos"

Posted 2017-10-23 03:59
Modified 2018-04-18 16:06
Comments 1

Navigation

Previous Episode	Next Episode
S2E17: "Garden of Deloittes"	S2E19: "Patching the KRACKs in the (Fire)Wall"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-10-12 03:36:01	2017-10-22 19:57:55	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	7f2a8960518337869478447899f713751e0c76df2c4a376c98a283ede5c1f914	click	click
OGG	2e699cf20158a12ee64f443310fa2615168f87c087a7af5be074e978dc1dc5ef	click	click

Quicklisten:

In this episode we have two guests involved in the InfoSec industry, Johnny Xmas, who is with The Faction and Uptake, and Daryl Kellison (who didn't give us any contact info to release).

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- China has used quantum encryption for a video call
- Google Chrome (for once) has copied Mozilla Firefox – it will now warn when entering data into an insecure field (as Firefox has been doing)
- Confidential NSA material has been leaked via a bizarre Telephone-Game-esque traversal of Israeli intelligence officers compromising a Russian intelligence operation compromising Kaspersky and via this, targeting an exfiltrating NSA contractor…
  - Confused? I don't blame you. The article spells it out a bit better.
- Outlook, due to a bug, has not been properly applying S/MIME encryption
- There are heap buffer overflows in the Windows DNS resolver
- The Dow Jones erroneously reported that Google acquired Apple, which (of course) has massive effects on the stock market
  - Weekly World News is indeed still around
- Accenture kept highly-sensitive data on publicly-exposed servers
- The Equifax breach (this one's different, promise) led to the release of over 15 million records (we talk more in-depth about the whole Equifax ordeal in the Baddie for S2E16 and the News segment in S2E17)

Notes

Starts at **19m17s**.

Jthan was drinking Monkey Shoulder (SHAME ON YOU! At the time of shownote composition, their site is returning an expired cert. I've contacted them to attempt to rectify this…). Daryl was drinking Sam Adams' Octoberfest. Johnny was drinking Wild Turkey Master's Keep. Paden was drinking Glenlivet Founder's Reserve again. I was drinking Bulleit 10-year bourbon again.

The discussion segment in this episode was very free-flowing, so there's not much structure or specific timestamps in this. Our apologies!

- Johnny was on (along with Deviant Ollam) in S1E14.
  - Jthan was really close!
- The tweet I mentioned during the intro is here.
- This is the raw list of questions we had prepared (some were answered indirectly, some not):
  - At what point in the Equifax debacle did it cross from tragic to ludicrous for you? What should they have done better in terms of DFIR at each new "stage-o-fail" to mitigate or otherwise address? How do we, as citizens and people, ever use credit services again and how do we overcome this? How can a "normal" person evaluate giving their information away in exchange for something like credit?
  - So-called "hacking insurance" (including "ransomware insurance", etc.) – is this a good idea? bad idea? What do you see as a far-reaching effect of this?

- Should companies be held liable for damages as a result of breaches et. al. they incur? Is it just a monetary liability? Does it fall on the company or top-level executives?
- Everyone has different advice for this, so we want to know what you personally would recommend for someone to break into InfoSec from another technological career. Did you follow this same path? If not, why does your advice differ from what led you to where you are now/what, if anything, would you do differently in hindsight?
- How do you propose we bridge Operations and InfoSec? (Going back to S1E14 for Johnny; has your answer/position changed any?)

- Daryl and Johnny talk about Equifax's CISO having a degree in musical study, and whether that in and of itself is a valid criticism.
  - The episode with Matt Crape was S1E13, in which we discuss certs and their value in greater detail. We initially talk about them in S0E3.

- As for passwords/password policy, we talk about them in the following:
  - I briefly talk about **managing** passwords in S0E7
  - S1E2
  - And again more talk of managing them in S1E19
  - Briefly in the Baddie for S1E18
  - Quite a fair bit in S1E11
  - Also a ton in S1E15
  - And then **again** in S2E3
  - And a new(-ish) password management method in S2E11
  - And finally, we talk about Bill Burr rescinding his recommendations for passwords to NIST in S2E14.

- In discussing shaking up existing standards/certification organizations in the InfoSec world, Daryl mentions Chris Nickerson.
  - Johnny mentions Wim Remes and David Kennedy.
  - I mention that the CISSP has gotten (relatively) more respect lately.

- Johnny talks about how limited change application is in larger enterprises, and why "patch your shit" can't be the only answer.
  - In a future episode, I'd like us to delve further into this – **should** set patching windows be the case, even for larger corporate environments? Is there anything we can do to make this an obsolete practice?

- We also talk about the difference between accountability, responsibility/fault, and liability.
  - C-levels take their position with the **knowledge** that they're the "fall-guy" when shit goes down, even if it isn't their **fault** – it may not be their **responsibility**, but it's their **liability**.

- We also talk about why Social Security numbers generally mean nothing.
  - Johnny and I have a brief tiff because I posit we need **some** sort of unique individual identifier/verifier for citizens – SSN isn't the best for this, and it's broken, but if not SSN then what instead?
  - Johnny's only suggestion is a chip in the back of the neck. :P
  - Realistically, though, we **all** agree that current punishments (if ANY) levied against corporations in breach of privacy and security ethics and practices **are not being punished anywhere nearly severely enough**, full-stop.
  - An interesting question I ask, though: why do people care about HIPAA breaches but they don't about other PII?
    - Johnny points out the extremely short collective attention span in regards to breaches.
  - Daryl offers a good suggestion: in the cases of breaches, etc. – no "golden parachute" for resignations/firing in addition to severe fines. C-levels should not be "untouchable".

- Johnny and Daryl answer the question they hate the most – how to get started in InfoSec.
  - Johnny says for **us/our listeners**, we are in high-demand in the InfoSec field because we know things "under the hood", we don't just want to "hack into banks" and such.
  - Daryl agrees with Johnny – he wants people with Sysadmin/DBA/webdev experience.
  - They both specify the difference between a red team engagement (stealth) vs. a pentesting engagement (thoroughness).

- Phishing **always** works.
  - This can be fixed by *incentivizing* employees to *give a shit*.
  - Johnny mentions Ben 0xA and how he developed a program so effective that due to an employee's report, an ant trap was investigated as a potential bug device (best pun ever).

- I was right! The "pigeon RFCs" are RFC1149 and RFC2549.

- Johnny briefly talks about the type of work he does with The Faction and Uptake.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(1h37m54s)**

A home-monitoring service has had a leak of blood reports.

Johnny asks what the importance of it is; Jthan refers to a situation like this, in which Aetna leaked the HIV status of 100k+ patients. Which is the joint Baddie, but due to a clerical error was not mentioned on-air.

Errata

- When I mention we have "guests that fuck shit up" in the intro, I was referring to them being red teamers, but the fact that (after I had already planned the welcome tagline) Daryl goofed and THEN Johnny introduced himself in non-alphabetical order, well… it made the situation all the more hilarious as the phrase took on an entirely different meaning.

- You can find our PoC||GTFO mirror here.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	The Killer Carpenter (Main Title)	Lee Rosevere	click	CC-BY 4.0
Outro	In Memoriam: Halloween 2013	Future Sauce	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

1. ## Pawel

2017-10-31 22:27 (1360 days ago)

It should be noted that Bill Burr wrote the original NIST guidance on passwords in the early 2000's, when people using 1234 as a password seemed completely legit. While for today it is outdated and not a good practice, we are looking at the recommendation from a much different place than in 2003.