Sysadministrivia

Linux, Lagers, and Late Nights

S4E13: "Xmas in July"

Posted 2019-08-19 03:59
Modified 2019-08-19 16:44
Comments 0

Navigation

Previous Episode	Next Episode
S4E12: "It's Getting Routey in Here"	S4E14: "The Way You Do the Things You Do"

Log

Recorded (UTC)	Aired (UTC)	Editor
2019-07-25 03:14:43	2019-08-18 13:45:27	r00t^2

Verification

Format	SHA256	GPG	Audio File
MP3	`0d55cdec085f7c49abea163308708680478d2b0a019c996d1cc2c95e437c4cb3`	click	click
OGG	`891770372237bc3104d61c83f193af8a753fb81310a43998807cf311b1669f16`	click	click

Quicklisten:

We have Johnny Xmas on to talk about WAFs, why they suck, why they don't work, and why Kasada does.

Yes, I choked on my vape.

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

Just the Tip

- Paden introduces us to drill, which is part of ldns (man page).
  - Bonus points, It may help with a project Johnny's been working on lately! (See his plugs in notes.)
  - Johnny mentions @dril.

Notes

Starts at **22m34s**.

I was drinking another Victory Dirt Wolf. Paden was drinking Coors Light and vodka. Jthan was drinking a gin and tonic (Tanqueray and "Seagrams, Canada Dry, whatever"). Johnny was drinking a Red Bull and Death's Door vodka, along with Rowan's Creek Kentucky Bourbon. Jthan tells him to go to Bathtub Gin & Co. in Seattle and Johnny says it sounds disgusting.

Joining us was Johnny Xmas. You may recognize him, he's been on the show a couple times before! Specifically:

- S1E14
- S2E18
- S2E22
- S3E14

Johnny has some plugs, too.

- You can find his Twitter here.
- He loves working with Kasada.
- He has a podcast called I Got One.
  - He's on the Radio Statler podcast frequently as well.
- He's really excited about his project Ghost Express.
- He also mentions working on ScanCannon.

That said, he's primarily here to talk about:

- HTTP bots/crawlers and WAFs (and why they suck donkey dick)
  - HTTP bots/crawlers are bad for business because they do things like gambling arbitration, price undercutting, etc.
  - WAFs are ineffective because:
    - There's a LOT of encoding options and such that break content inspection
    - Request headers are the **easiest** things to forge
    - They block based on client IP address, but between proxies and SOCKS5 tunnels and AWS instances and such, this is pointless.
      - Sure, they can block based on whitelisting residential/mobile carrier IP address ranges, but things like Luminati (which HolaVPN uses) and MonkeySocks respectively can use those ranges (by **making the client a peer in the network**, meaning they use customer devices as their own servers).
  - Johnny wants you to read Time-Based Security (which I **think** Johnny incorrectly attributes to Wim Remes, who DID write a book though!).
  - "**Security's job is to destroy the economics of the attack.**" – Johnny
  - See also the joke about the tiger. (Commonly referred to in the US as a bear instead of a tiger.)
  - So how does Kasada address this?
    - When I mention rate-limiting, I refer to rate-liming the **endpoint** – rate-limit all requests to the target/destination, not based on client. But this of course is not feasible if there's a convention, if there's a "Slashdot effect", etc. and it still allows **some** of the bot requests through.
    - They "irresistably ask" the client to identify themselves as automation. Meaning they query it in such a way that it cannot lie, identifying inconsistencies between headless vs. graphically-rendered sessions, etc.
  - I mention a similarity to how the NSA identified TorBrowser sessions via Javascript. You can find examples of how to do that here and here.
    - I think what Johnny was talking about re: Cloudflare and Tor is this.
  - WAFs also are only effective **after the detection**. Kasada performs detection (and remediation) **before the traffic hits the endpoint**.
  - Johnny wants you to check out headless Chrome and Puppeteer. I'd recommend Selenium as well (as it has a Python interface).
  - They can also either DoS the bots with a tarpit or **delay** them to "make it fair" for human visitors.
  - We talk about how you shouldn't go running in blindly on setting up your own email server in S1E18.
  - ...and the GIANT Twitter thread that Johnny mentions is, I think, here.

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 **1h20m47s**.

Jthan is building a router! Johnny talks about his forays into networking oddity and full router boxes.

(Speaking of ISPs, someone just pointed me to this.)

Errata

- I gave Edita the episode off! So I edited this one.
- We recorded this one **wayyy** early because Jthan doesn't know how calendars work.
- I didn't get Johnny's local raw before he wiped it from existence (my fault), so we had to use the backup Mumble recording for his track. This is why it sounds like he's underwater. Sorry, Johnny!
- The episode title is funny because our guest is Johnny Xmas. We were recording on the Eve of Christmas in July.
- That Ghost in the Shell reference was just for you, weebs.
- Johnny gets riled up about SANS' certification renewal policy.
- Pretty sure the "ls in Golang" I/Jthan mention is either this or this. Not sure where we saw that it was someone's thesis.
- I had a **dickens** of a time trying to find out who wrote SysV `rm`. I managed to find the source code. Thinking myself clever, I then tried checking `SysVr2.0_32000/src/cmd/rm.c` – no such luck, as it only mentions AT&T, not any particular developer (and this was before version control). I even tried a recursive grep for "Robert" but only pulled up a strings list. If someone wants to dig deeper, please let us know your findings! I can't waste a day on tracking down original AT&T guys from 1984-1987, but that's where I'd start.
- You can find IA64 processors pretty cheap.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Sentinel	Kai Engel	click	CC-BY 4.0
Outro	Slinky	Robert John	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 Four

Comments

There are currently no comments on this article.