Episode Book

EPISODE #6396

How Political Scandals Exposed Boring Email Bugs

PUBLISHED	31 October 2026 at 20:23 UTC
DURATION	31:21
LISTEN	myweirdprompts.com/episode/political-scandals-email-sysadmin-32146/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	anthropic/claude-sonnet-5.5
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
BOOK GENERATED	1 November 2026 at 07:41 UTC

SYNOPSIS

Political scandals routinely get billed as masterclasses in secrecy or digital espionage, but looking under the hood reveals mundane systems administration failures. Examining the 2007 White House email disappearance across private domains like gwb43.com, the 2008 Sarah Palin Yahoo account security question reset, and the 2012 David Petraeus shared Gmail drafts technique demonstrates how basic configuration details, routine backup tape recycling, and login IP address metadata repeatedly unravel high-profile affairs.

TRANSCRIPT



Corn

Somewhere between five million and, by one count, twenty-two million White House emails went missing, and the reason was a mail server that the government did not own. It belonged to a political party. It had a domain name that looked like a fan site. Herman, you remember how we left The Clinton Email Server: A Technical Autopsy.



Herman

Settled. We said what we had to say about that setup.



Corn

Here is what Daniel picked up from that episode, and it's a good thread. The Clinton saga was one of the rare times that sysadmin territory, the stuff you normally only hear about in a homelab forum, ended up as the lead story on the evening news. What he wants to know is what else got dragged out of the server room like that. And a lot of it turns out to be the same stuff, earlier. The Clinton saga had a predecessor, and it ran on G W B forty-three dot com.



Herman

Two thousand seven. The US attorney firings investigation. Congress is asking for emails from White House staff, and it turns out a good number of those staff were not using White House addresses for the political side of their work. They were using addresses at G W B forty-three dot com, and some at georgewbush dot com and rnchq dot org, all hosted on servers belonging to the Republican National Committee.



Corn

Hosted by the party, for the party's work, sitting next to government work.



Herman

The stated reason was reasonable on its face. The Hatch Act keeps political campaigning off government systems, so you run the political email somewhere else. The trouble is the Presidential Records Act of nineteen seventy-eight, which says official business is a record the public owns. If an official business email lands on the party's server, whose is it? Scott Jennings, a deputy political director, was one of the names that came up. Karl



Herman (continued)

Rove reportedly did about ninety-five percent of his email on the RNC side.



Corn

Ninety-five percent. That's not a side account, that's his office.



Herman

A House Oversight report that June counted at least eighty-eight RNC accounts for senior officials, and the party had preserved no emails at all for fifty-one of them.



Corn

Fifty-one. Out of eighty-eight. Imagine that being your backup rate.



Herman

What I love here, as a sysadmin, is that the retention policy was a configuration question nobody treated as one. The RNC's policy from two thousand four was supposed to keep White House staff mail, but staff could delete their own, and Mother Jones suggested a thirty-day purge before that. Fine, so that's server one. Server two is the part the headlines glossed over. The White House had its own mail archive, and it was broken. Steven McDevitt, who ran the system from two thousand two to two thousand six, testified that the collection process was primitive and that the risk of losing data was high. He put the gap in the record at around four hundred days. And the backup tapes were being recycled, reused, until October of two thousand three. Theresa Payton, the CIO later, testified to that.



Corn

Tapes being recycled is just what tapes do. You don't keep every tape forever, you overwrite the oldest one.



Herman

In an ordinary company, rotating tapes is a retention policy. In the White House, under a records act, it's a legal problem, and nobody had flagged it, because the thing writing the policy was a backup schedule. The coverage at the time just said emails were "missing," as if someone had gone into a room and taken them. What actually happened is the archive had a hole in the middle, and a different server with a different owner had the other half.



Corn

So there wasn't one missing pile of emails. There were two separate ways of losing them.



Herman

Yes. And the number moves depending on who is counting. Over five million was the figure in two thousand seven and eight. In two thousand nine, CNN reported up to twenty-two million turned up on backup tapes, though that number is debated. The Obama administration settled with the two watchdog groups that were suing.



Corn

Herman, a sysadmin would have asked one question on day one. Whose server is it?



Herman

Whose server is it, and who has the root password. That's the only question that matters for records. Everything else, the Hatch Act, the argument about intent, comes after.



Corn

Which is also what the mainstream coverage kept getting backwards. It was all about motive. Was somebody hiding something. Nobody asked about the mail server's retention setting.



Herman

Because "the retention setting was wrong" isn't a headline. Now, this one I have to put to you. Palin. Two thousand eight, a personal Yahoo account, and a story that the press called a hack. Would you call it a hack?



Corn

I'd call it a reading comprehension test for a security question. But walk me through it, because I know it ended up on four-chan.



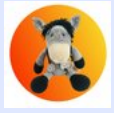
Herman

Just after midnight on the sixteenth of September, someone calling himself Rubico on four-chan's random board reset her Yahoo password. No exploit. He used the forgot-password page. Yahoo wanted a date of birth, a ZIP code, and the answer to a security question. Birth date and ZIP code are public for a governor. The question was where she met her spouse, and the answer, Wasilla High, was in her biography.



Corn

So the security question was in the campaign literature.



Herman

He claimed about fifteen seconds. The password he set was reportedly "popcorn." He posted the new password publicly, and then another four-chan user logged in, changed it again, and posted a screenshot with the new password unredacted.



Corn

Hold on. So the account was hacked, and then the hack was hacked.



Herman

Then a crowd tried to log in all at once and Yahoo locked the account. And what they found in there was mundane. Ordinary mail. Some of it touched Alaska state business, because she sometimes used Yahoo for that, which is the records angle again.



Corn

Mundane mail. Spotless as a freshly wiped server.



Herman

The person on the other side of this was careless in a more interesting way. He used a proxy, reportedly CTunnel, and that proxy logged his IP address. A screenshot he posted exposed a URL, he left an email address on four-chan, and his social profiles pointed to David Kernell, a twenty-year-old student at the University of Tennessee, whose father was a state representative. Indicted in October, convicted in April of twenty-ten of anticipatory obstruction of justice, because he'd deleted evidence, and of unauthorized access, which was the misdemeanor. A year and a day. He died in twenty-eighteen, aged thirty.



Corn

He was a student who got undone by the cover-up, not the break-in.



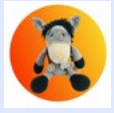
Herman

The felony was the deleting. And what I'd want a listener to notice is that the word the media used, hacker, covers nothing here. Account recovery was the vulnerability. Knowledge-based authentication, where the answers are things anybody can look up. Corn, you've done the thing where you answer the "mother's maiden name" question with a random string, haven't you?



Corn

I store a made-up answer in the password manager. My mother's maiden name is, depending on the site, a forty-character string. Which is the correct answer to all of those, because the question was never about my mother.



Herman

See, that's what most people missed in twenty-oh-eight. The reset is the real login.



Corn

And that is the thing about these sagas, the reset is always the moment everything comes apart.

L

Larry

And now a word from Resetsure, the gentle little tablet for anyone whose inbox has ever made the evening news. Resetsure quietly archives your drafts folder, scrubs your private account, and resets your password to something even your own mother could not guess, so your sensitive messages simply vanish from history and your reputation stays as spotless as a freshly wiped server. Ask your doctor about Resetsure today.

L

Larry

Side effects may include mild inbox nostalgia, spontaneous forwarding to everyone in your contacts, a sudden urge to conduct official government business from a personal Yahoo account, phantom sent items you never wrote, an uncontrollable drafts folder that refills itself overnight, forgetting which email server you actually used, brief appearances in a national security hearing, a lingering suspicion that someone already read everything, and in rare cases, complete and total server deletion. Resetsure. Because history is easier when it is gone.



Herman

Corn, "spotless as a freshly wiped server." That was your line, a minute ago, word for word, and I do not know where that came from. Anyway, drafts folders, which is where the next story lives.



Corn

Petraeus. David Petraeus, then the CIA director, and Paula Broadwell, his biographer. And the thing the coverage latched onto was a shared Gmail account.



Herman

The way it began matters, because it had nothing to do with either of them at first. From around May of twenty-twelve, a woman named Jill Kelley received harassing emails from pseudonymous accounts, and she took them to the FBI. The FBI traced the sender. The sender turned out to be Broadwell. In the course of that, they found the relationship, and that's the thing that brought Petraeus down in November.



Corn

So, a harassment case, and the CIA director falls out of it.



Herman

Via the metadata. And this is the sysadmin part. She had not hidden her IP address. The emails were sent from locations that weren't her home, hotels in several cities, and the FBI, as reported, cross-referenced the IP addresses with hotel guest lists, looking for a name that appeared in all of them.



Corn

That's elegant, if you're the FBI. If you're anyone else it's alarming.



Herman

Yahoo and Outlook dot com, at the time, put the sender's IP address right in the message headers, so investigators could have pulled it off the message itself, no provider request needed. Whether that's how they got these, or from Google's logs, is debated.



Corn

What about the drafts-folder thing? Because that's the bit that got explained on the news as if it were spy-grade encryption.



Herman

Reportedly Petraeus and Broadwell shared one Gmail account. Neither of them sent mail from it. One would write a draft, the other would log in and read it, and delete it. A technique that had been associated with al-Qaida in the press coverage.



Corn

So no message ever travels.



Herman

No message goes over SMTP. Nothing sits in anybody's outbox or in transit. But it does nothing at all about the login. Every time somebody opens that account, Google logs the IP address that came in. So you've hidden the content from the wire and given the provider a timestamped list of where you were.



Corn

It's a shared mailbox. It's the thing the whole office does with the info at company dot com address, except they did it with something to hide.



Herman

Which the news called a trick. A clever trick. Like cryptography. I'd say the reverse: if you wanted to hide that two particular people are talking, a shared mailbox is the worst way, because it ties the two of them to the same account.



Corn

And on the legal side, I recall that a sysadmin could have a field day, because the rules were from nineteen eighty-six.



Herman

The Electronic Communications Privacy Act. The reading the government used was that unopened email, a hundred and eighty days old or less, needs a warrant, but opened mail or older mail only needs a subpoena. The Ninth Circuit had disagreed with that reading, but the agents were in Tampa, which is outside the Ninth Circuit. The EFF thinks the FBI likely got a warrant anyway. And a draft that's been opened and left sitting, is it unopened? Is it, in fact, even a message?



Corn

I'd pick the one that's easiest for the investigator.



Herman

Then you'd be the FBI in twenty-twelve. Okay, a different kind of question for you. You're a person with something to hide, and you're about to use a shared mailbox. What do you do instead?



Corn

Honestly? Nothing electronic. I'm a sloth. I'd leave a note under a rock.



Herman

Under a rock I can't subpoena.



Corn

That's why I'd choose it.



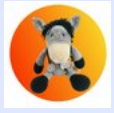
Herman

Celebgate was the one where the coverage got the mechanism wrong in the first week and then the court record corrected it years later. Waves of private photos from celebrities posted from the thirty-first of August, twenty-fourteen, first on four-chan and a site called Anon-IB. There was a collector asking for Bitcoin. Then Imgur, Tumblr, Reddit. Reddit banned the main subreddit on the seventh of September.



Corn

And the initial explanation was that Apple had been broken into.



Herman

The first theory was a flaw in Find My iPhone, an API that would let you guess passwords without limit. Brute force. A tool called iBrute went around. Whether that flaw was ever real is debated. Apple's statement was that it was "a very targeted attack on user names, passwords and security questions," and that neither iCloud nor Find My iPhone had been breached.



Corn

Which is a company saying "it wasn't us." Sometimes that's the most suspicious sentence in the world.



Herman

Except this time the court cases backed them up. The method was phishing. Fake emails that looked like security warnings from Apple or Google, with one fake account in the record literally named appleprivacysecurity. People typed their credentials in. Then commercial forensics software, ElcomSoft's tooling, was used to download iCloud backups using those credentials.



Corn

A forensics product. So the intruder used the same tool the police use to read your phone.



Herman

It's sold to law enforcement, yes. The backup is the soft target here. The phone itself is encrypted and locked. The offsite copy of the phone sits in the cloud, protected by a password and security questions, and if you're the kind of sysadmin who gets paged about backups, you know that the backup always has weaker protection than the live system.



Corn

Because nobody thinks of the backup as the thing the attacker wants.



Herman

And the sentences were smaller than the damage. Ryan Collins got eighteen months in twenty-sixteen, for getting into more than fifty iCloud accounts and seventy-two Gmail accounts over about eighteen months. Prosecutors found no evidence that he was the one who leaked the photos. Others got nine months, sixteen months, eight months. One sentence, Brannan's, is reported inconsistently, thirty-four versus thirty-eight months, so I'll leave it there.



Corn

And Tim Cook's promise was alerts when someone restores a backup.



Herman

Alerts on iCloud restore, alerts on a browser login, and wider two-factor. Alerts are the sort of thing a sysadmin would have turned on first. Your email provider tells you when a new device logs in. Somehow, a company with that many users hadn't.



Corn

I'm still stuck on the mainstream version. It was "Apple got hacked" for a week, and for a week the phrase everyone repeated was "the cloud." As though the pictures were in weather.



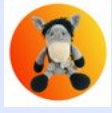
Herman

And the actual answer was a person who clicked a link in an email. The most boring attack in the world. Which is also true of Palin. Neither case involved anything clever. It was the human part of account recovery.



Corn

Palin's was a question anyone could answer. Celebgate was a password page anyone could clone. Same flaw, six years apart.



Herman

Okay, the one I find most useful to explain, because it contains an actual sysadmin moment. Signalgate. March of twenty-twenty-five. Mike Waltz creates a Signal group chat on the eleventh. Jeffrey Goldberg of The Atlantic is added on the thirteenth. Strikes begin on the fifteenth. The Atlantic publishes on the twenty-fourth, with the full text on the twenty-sixth.



Corn

And how did a journalist end up in the chat? Because I remember the explanations on the news being, a bit, mystical.



Herman

Per the White House forensic review, as it was reported, Waltz's iPhone had saved Goldberg's number under the contact card of Brian Hughes, a spokesman. That's an automatic contact-suggestion update, the phone merging a number it thought belonged to the same person. Waltz went to add Hughes and added Goldberg. Nobody hacked anything. It's a contact book.



Corn

I have to say, that's not even a phishing email. It's autocomplete.



Herman

Autocomplete with consequences. And the chat had disappearing messages set to one week or four weeks. Which brings up the argument that runs through all five of these.



Corn

Records. Bush lost them by accident. Here they were deleted on a timer.



Herman

Yes, by design. And the Pentagon inspector general looked at Hegseth's use of a personal phone, and the report, which went to Congress in early December, found it violated policy. The content matched information from a CENTCOM document that was marked classified. The inspector general didn't assess declassification. The Pentagon described the report as exoneration, and FactCheck dot org disputed that reading. I'll leave the reading to people with security clearances.



Corn

Fair enough. Technical part only.



Herman

The technical part is the sequel, and it's the better story. On the second of May, a Reuters photographer caught Waltz using an app that looked like Signal, but it was called TM SGNL. It's a modified Signal made by TeleMessage, an Israeli-founded company, and it exists to archive messages.



Corn

So the cure for the disappearing messages.



Herman

The cure for the records problem. Federal officials are required to keep records, so TeleMessage offers a Signal-compatible app that sends a copy of every message to an archive. And here's the structural issue. The messages were end-to-end encrypted between the phones. But the copy to the archive wasn't end-to-end encrypted all the way to its destination. The archive server was on Amazon Web Services in Northern Virginia. Signal's own line was that they could not guarantee the privacy or security of unofficial versions.



Corn

Which I'm reading as the nicest possible way of saying "not ours."



Herman

Then somebody got in. Reported as taking fifteen to twenty minutes. The hacker pulled what's called heap data, which is a snapshot of the server's memory, and it contained live unencrypted traffic and backend login credentials. Four-oh-four Media found something like seven hundred and forty-seven entries from Customs and Border Protection in one view. There was also Coinbase, Galaxy Digital, Scotiabank, and the DC Metropolitan Police. Distributed Denial of Secrets released a bit over four hundred gigabytes of heap dumps on the nineteenth of May. The parent company, Smarsh, suspended TeleMessage.



Corn

Hang on. Heap dumps. Why would a server hand over its memory to a stranger?



Herman

And now you're asking the sysadmin's question. The researchers withheld the entry method, but later reporting ties it to two vulnerabilities that CISA added to its list of known exploited vulnerabilities on the first of July, with a deadline of the twenty-second. One of them was a Spring Boot Actuator endpoint, a debugging tool that returns a memory dump, left switched on and open to the internet.



Corn

One debugging endpoint. Left on.



Herman

One switch. If that is it, then the whole archive of a federal compliance product was a feature that was supposed to be turned off before going live. I would bet that every sysadmin who's ever shipped something has a leftover debug endpoint somewhere in their past. Corn, have you ever left a test thing running in production?



Corn

I once left a status page up on a home server for a year with no password. It said my uptime. Nobody took any interest.



Herman

Your uptime was the only thing there.



Corn

A year of it. Very impressive.



Herman

But the irony in the TeleMessage case is hard to beat. Bush's problem was that records weren't kept. The fix is archiving. Archiving requires copying every message to a second place. The second place is a server that somebody has to run and someone has to patch, and now the compliance system is the single biggest pile of readable messages in the building.



Corn

The thing that was supposed to prove nothing was hidden became the thing that exposed everything.



Herman

One saga left, and the whole argument in it was a sysadmin argument. A laptop with water damage, a repair shop in Wilmington, Delaware, and a mail header called DKIM that ended up in campaign coverage. The technical part is the best part. April of twenty-nineteen, someone drops off a MacBook Pro with liquid damage at a small shop called The Mac Shop. The owner never pays and never comes back. The shop's owner, John Paul Mac Isaac, is legally blind, and he's said he couldn't confirm who the customer was.



Corn

So the chain of custody starts with a man who can't read the paperwork.



Herman

Which I'd say is a gift to the later arguments. To recover data off a water-damaged Mac, you boot it, copy files until it dies, and boot it again. Every boot writes logs. Every copy touches timestamps. By the time a forensic examiner gets near it, the evidence has been through a washing cycle.



Corn

The shop's security cameras kept two months of footage.



Herman

Then wiped it, before anyone knew it mattered. Then the FBI subpoenas the drive in December of twenty-nineteen, and before he hands it over, Mac Isaac copies it, reportedly for his own protection. That copy goes to Rudy Giuliani's lawyer, Robert Costello, and on to Giuliani, and Steve Bannon says on Dutch television that he has one too. The date the copy reached Giuliani's side is disputed, January or August of twenty-twenty depending on whom you believe, so I won't pin it. The New York Post runs the story on the fourteenth of October.



Corn

So nobody is arguing about "the laptop." They're arguing about a copy of a copy of a copy, handed around like a mixtape.



Herman

A sysadmin would have said that in the first hour. And it's why, when the Washington Post hired experts in twenty-twenty-two, they couldn't examine the laptop. They got a copy that had come through Mac Isaac and Giuliani's side, and by then it had been modified. Two hundred seventeen gigabytes, around a hundred and twenty-nine thousand emails.



Corn

Herman, do you actually understand DKIM, or have you just read an explainer?



Herman

I understand it well enough to explain it, which is a lower bar than it sounds. When your mail server sends a message, it adds a header called a DKIM signature, a cryptographic signature over the key parts of the message. The receiving side checks that signature against a public key that the sending domain publishes in its DNS records. If the check passes, the message went through that domain's servers and hasn't been altered since.



Corn

Went through the servers. Not written by the person.



Herman

That's what the news dropped. A signature proves passage and integrity, not authorship. Robert Graham, the security researcher, wrote the explainer everyone passed around, using a test message from his own Gmail account, and his point was that the cryptography works, and the only way around it is to compromise the servers.



Corn

Is there a catch?



Herman

Two, and they're the sysadmin part. Keys rotate, so an email from twenty-fifteen has to be checked against the key that was published back then, not today's. And only mail you received carries a signature you can check. Mail you sent doesn't. So half of any mailbox is unverifiable by this method.



Corn

Half of a conversation is invisible. That's a strange basis for a headline.



Herman

In the Post's review, Matt Green, a Johns Hopkins cryptographer working unpaid, verified a little over eighteen hundred emails. Jake Williams, formerly of the NSA, verified close to twenty-two thousand, most of them Google-signed. Neither found signs of tampering, and neither could rule tampering out. Williams called the drive a disaster for forensics, and Green called it a mess.



Corn

So two experts, a few thousand verified emails and the sentence "can't say." And the headlines?



Herman

Headlines went both ways from the same ambiguity. Verified, and therefore all of it is real. Unprovable, and therefore none of it counts. When both camps are reading the same result, I'd say that's a sign that the public hadn't heard what a signature covers. Verified emails tell you nothing about the folders around them. And the folder names matter. Folders like "Biden Burisma" were created in September of twenty-twenty, in a drive that had been almost idle for a year, and "Big Guy File" was created days after the first stories ran.



Corn

Somebody was filing things after the story broke.



Herman

Someone with access to a copy, which is what a copy is for. CBS looked at it in twenty-twenty-two and described the contents as consistent with normal everyday use. In the twenty-twenty-four trial, an FBI agent testified that the laptop's serial number matched the one tied to Hunter Biden's iCloud account. She said she'd seen no evidence of tampering, but when she was asked whether she'd analysed for it, she said she hadn't. People read that sentence in opposite directions. It's a summary witness, not a forensics examiner.



Corn

Both camps got a quote they liked.



Herman

And there's the platform side. Twitter blocked links to the story under its hacked materials policy, even though no hack had been found, and the Twitter Files later reported that staff inside the company doubted the policy fit. Fifty-one former intelligence officials signed a letter saying the story had the classic earmarks of a Russian operation. The letter also said they did not know whether the emails were genuine, and had no evidence of Russian involvement. Politico's headline went further than the letter did.



Corn

So the nuance was in paragraph three, and the headline was in paragraph one.



Herman

The oldest problem in the building. A sysadmin would have wanted three things on day one. The raw headers, the original drive, and a log of everyone who touched it. They got a story and a copy.



Corn

I'd have wanted one thing answered. How many people had that drive in their hands before anybody photographed the serial number?



Herman

At least five, by name. That count alone tells you what the evidence is worth.



Corn

A custody chain with more hands than a pub quiz.



Herman

Every copy is somebody's afternoon. Somebody who plugged it in and moved it on.



Hilbert

No argument from me. I've got eleven years of correspondence from the borough council on a two terabyte drive on my desk right now, plugged into the Dell. I put in a records request in September for every email about the extension on my back wall. The records office is run by a Mrs Pauline Redfern, and she told me the mail is held but not searchable. It is held by Gerald Ashby, who is the entire IT department. Gerald comes in at seven, because the old server will only export before the offices open, and he copies one mailbox, goes off to do the printers, and comes back to see if it stalled. He's been doing it since the third of October. I said I wanted the drive posted, not a download link, fourteen ninety-nine, and he wrote my name on the sticker in biro. Spelled right. The



Hilbert (continued)

council has never done that. The ports on the Dell sit too close together for a snout, so I press the drive in with a pencil.



Herman

Exporting before opening hours is sensible. The export competes with live mail for the same disk, and on an old machine you'd feel it.



Hilbert

It's a Dell as well. The council one. Twenty-oh-nine.



Corn

Four weeks, and the only person who can get at the mail is one man with a morning shift. That's a tight records policy.



Hilbert

Gerald's on the Ks.



Corn

The Zs are going to be a December problem.



Herman

Most of what we've covered comes down to who the person is. The Bush archive had a man called McDevitt running a primitive collection process that he told Congress he thought was too risky. TeleMessage had someone, somewhere, who left an endpoint switched on. Nobody built these systems to be seen, and the coverage came after.



Corn

Herman, the thing I'd flag is how much of this I'd have missed if I'd only read the headlines. Hacked. Missing. Encrypted. Three words, and each of them was wrong.



Herman

Hacked for Palin, where nothing was broken. Missing for the Bush email, where the archive had a hole and a second server had the rest. Encrypted for the drafts folder, which defeated nothing. Corn, what would you have wanted a reporter to ask, if you could have had one question in each case?



Corn

For Palin, whose idea was it that her birthplace made a password? For Celebgate, why does the backup have a weaker lock than the phone? And for the last one, I'd have asked who runs the archive. I think that's the question that would have saved the most trouble.



Herman

And if you get the answer "a company in a data centre," then the next question is who patches it.



Corn

Okay. The idea I'd keep from all five is that none of these were failures of something exotic. A mail server with an owner nobody checked, a reset page that answered questions anybody could look up, a shared mailbox that left a login trail, a phished password, a debugging switch. Ordinary stuff, with the wrong person's name on it.



Herman

Add to that the person at the other end of the mailbox. Whoever keeps the server running has a Tuesday, and the headlines never describe it.



Corn

Next time one of these breaks, the first thing I'll want to know is who gets in at seven and what the export schedule is.



Herman

Thanks to our producer, Hilbert Flumingtop, for keeping this show running. This has been My Weird Prompts. You can find every episode at my weird prompts dot com.



Corn

We'll be back soon.