

Forum:[Hack Forums](#)

Thread: [Latest Cybersecurity, APT Attacks, Zero-Day Vulnerabilities, AI Exploits & Ransomware](#)

JoseMar - March 18, 2026, 3:59 am

Latest Cybersecurity, APT Attacks,
Zero-Day Vulnerabilities, AI Exploits & Ransomware 2026

So yeah... been going through a bunch of recent cybersec articles and honestly it feels like everything is getting quieter, sneakier, and kinda... weirder? Not louder attacks.

Not big flashy ransomware headlines (well, still some).

More like... subtle abuse, legit tools, trust hijacking, AI doing questionable stuff.

Anyway, read this latest news? ...:

Boggy Serpens Is Back,
Targeting Diplomats Like It's 2005

So apparently, this Boggy Serpens gang is still at it, yeah, the APT-style espionage crew that doesn't sleep.

They've been hitting diplomats and critical infra, multi-wave campaigns like it's some kind of chess game nobody asked for.

They're not just poking email servers, they're going after the usual juicy targets, plus some infrastructure nodes that make you go "wait, how did they even get there?"

From what I read, it's a combo of spear-phishing and these insanely tailored malware drops, basically giving them a full map of the networks they compromise.

The weird part, diplomats are usually warned about cyber threats, right?

And yet these guys are slipping in anyway, almost like the cybersecurity briefings are optional. I can't stop thinking about the scale too, this isn't one embassy getting hit, it's multiple countries, multiple layers.

They're patient, sneaky, the kind of stuff that makes you double-check every attachment you click.

Honestly, if you're in that line of work, I'd probably start questioning every device in your office/Home, every VPN hop, every "safe" network. And yeah, for the regular folks reading, this is probably overkill, but still, there's a lesson in how determined this can remain and invisible while collecting insanely sensitive intel.

Makes me wonder if anyone outside their immediate targets even notices until months later.

Court Docs Used to Sneak RATs? Judicial Malware Madness

So get this, hackers are literally using court documents and GitHub payloads to drop something called COVERT RAT on judicial targets.

Yeah, like they email a PDF or a court filing and suddenly your system is fully owned.

Makes you wonder about the irony, “we trust this document because it’s from a court” and boom, full RAT access. The thing is, it’s not just some random zero-day spam.

They’re chaining this with GitHub repos and scripts to make the infection cleaner, harder to spot, like a ghost. And they specifically target judicial systems, so the victims are basically people who should know better about security, but apparently, the “trusted source” effect is too strong.

What’s strange is that these RATs can exfiltrate data silently, so by the time anyone notices, they’ve been living rent-free in the system, makes you think about how much we trust digital docs without question.

I wouldn’t be shocked if we start seeing similar tricks in corporate law firms or maybe even smaller courts.

Honestly, it’s the perfect storm: high-trust environment

malicious payload

people thinking “oh it’s safe, it’s official.”

Custom Fonts Poisoning AI? Really?

Apparently, just feeding an AI a specially crafted font can mess it up, ChatGPT, Claude, Gemini, all of them.

Like you don’t even need code injection, just text that looks normal but carries a hidden payload.

Honestly, this feels like the next frontier in adversarial AI attacks, sneaky, invisible, and most people won’t notice until the AI does something totally wrong.

Makes you wonder if every AI model we trust has a blind spot like this.

RegPwn: Windows Registry Nightmare

So apparently, this RegPwn thing is worse than it sounds.

Full system access just by exploiting the Windows registry?

Yeah, that's basically giving root to anyone who knows the trick.

The vuln lets attackers escalate privileges in ways that feel like it was written for a hacker demo, not a production environment. The scary part, no complex chains needed, just trigger this and suddenly you own the box.

Makes me think about how many machines out there never get patched, and the registry is basically the spine of Windows. Once that's compromised, there's almost no turning back without a rebuild.

Honestly, I wouldn't be surprised if we start seeing mass scans for this soon.

FortiClient SQL Injection Hits Hard

FortiClient just got hit with a critical SQLi vuln that lets attackers do arbitrary DB stuff.

Like, everything that touches the database could be at risk.

It's classic injection, but in enterprise software, so it's serious.

Think about the kinds of secrets stored in these systems, credentials, configs, logs, you name it.

Patch immediately if you care about your network staying sane.

The scary part? People still run outdated appliances thinking "it's fine, nothing happened yet."

Yeah, until someone wipes your DB or drops malware, then it's too late.

Ubuntu Desktop RCE, Root Access Just Like That

Apparently, Ubuntu desktop users need to double-check their patches, there's a vuln giving attackers full root access.

Not just a token exploit, full control, like sudo without the password. It's the kind of thing that makes you question if Linux is "safe" or just less targeted. Honestly, it's probably a mix: fewer exploits in the wild, but when one pops, it's game over.

For sysadmins and devs, this is a wake-up call, update, patch, audit your logs.

Teams Support Call Turns Into Vishing Nightmare

So people are getting pwned via Teams support calls.

Not phishing, not email, literal voice calls that get you to open Quick Assist.

Attackers use social engineering to convince users to start the remote session.

Then boom, your system is compromised.

Makes you rethink every IT support call you take.

Honestly, I'd start verifying the number, the person, everything before touching anything.

Ransomware Actors Pivot as Google Watches

Ransomware groups apparently are losing steam on pure extortion and shifting toward data theft.

Google's telemetry shows profit drop, so now it's about stealing data and selling it rather than just locking files.

Makes sense in a way, but scary, it's harder to detect data exfiltration than file locks. If you run a business, maybe rethink your detection strategy.

Can't rely on old ransomware habits anymore.

Microsoft 365 Copilot Can Chill, No More Forced Installs

Microsoft finally admitted people are annoyed and decided to stop force-installing the 365 Copilot app on Windows.

Honestly, who hasn't opened a machine only to find some corporate AI tool just shoved in there like it's nobody's business?

They said users now get to opt-in, which feels like a common-sense move but somehow wasn't.

The kicker, Copilot is still integrated, but at least your Start menu isn't crowded with something you didn't ask for.

I guess IT admins might cry because rolling this back isn't always trivial, but from a personal perspective, it's refreshing. Makes me think about all the apps companies force-install that no one actually uses, quietly running in the background, collecting data, or slowing things down.

Kind of a microcosm of modern Windows life, features you never asked for, permissions you never agreed to.

At least now, you can click "nah, not today" without starting a small war with the update system.

Glassworm Hits React Native Packages, Supply Chain Nightmare

Glassworm hit npm hard, two popular React Native packages got backdoored.

Install them and suddenly your Windows box is sending creds and wallet info to attackers. No clicks, no exploits, just npm doing its thing.

The malware even checks for Russian locales and stops if it sees them, which is kind of a weird signature but typical for these guys.

Anyone building apps with phone number inputs or country selectors might be compromised already.

Rotate creds, check logs, audit dependencies, seriously, this is the kind of supply chain attack you dream of avoiding until it's too late.

InspectorGadget - *March 18, 2026, 4:21 pm*

Honestly expected to see more from Iran's Cyber Army after the war started, but aside from Stryker Intune hack there hasn't been much.