

Forum:[Hack Forums](#)

Thread: [New week, new nonsense: Sneaky2FA, FortiWeb Oday, WhatsApp disaster and more](#)

JoseMar - November 19, 2025, 3:58 am

New week, new nonsense:

Sneaky2FA, FortiWeb Oday, WhatsApp disaster and more

Sneaky2FA Just Leveled Up and It's Getting Weird

Alright so apparently Sneaky2FA wasn't sneaky enough, so now it's using Browser in the Browser like it's trying to cosplay as your operating system.

You open some "Adobe PDF" crap, hit "Sign in with Microsoft," and boom, you're inside a fake window inside a window inside... whatever. Inception but for stealing your credentials.

The part that got me?

The pop-up morphs to look like whatever OS you're on. Windows, macOS, Chrome, Firefox, your grandma's toaster OS, doesn't matter. Looks real enough to fool even people who think they're paranoid.

And of course it hides behind Cloudflare Turnstile, obfuscated JS, and those 150-character URLs that look like a cat walked over the keyboard. Domains rotate like it's a DJ set.

Basically, phishing kits are now "premium SaaS products" for lazy criminals. Telegram support, licensed builds, code obfuscation as a service.
We're doomed.

Azure Firewall + Security Copilot = Skynet Junior

Microsoft finally did the mashup: Azure Firewall hooked up to Security Copilot.

You ask, "Hey why's that traffic sketchy?"

Copilot goes, "Here's the IDPS hit list, here's the actors, here's what to do... oh and here's a recommendation because you clearly weren't going to read the docs."

Lowkey feels like cheating.

Like these analysts went from "writing Kusto queries at 3AM" to "talk to my firewall like it's ChatGPT."?

Whole point:

Copilot watches all your firewall groups, pulls threat intel, spits out a whole briefing like it's your personal SOC intern but without the burnout.

You just need the logs sent to Log Analytics + the magic SCU compute credits. Because Microsoft always finds a way to bill you for the future.

SolarWinds Serv-U Still Getting Beat Up

SolarWinds can't catch a break.

Three new RCE vulnerabilities in Serv-U 15.5.3. All need admin access but once you're in, you can basically run whatever code you want.?

Windows = medium severity.

Linux = full panic mode.

Three CVEs, all 9.1 severity,? all basically "you trusted the wrong admin."

They patched it though, and threw in a whole buffet of security goodies like:ED25519 support

Better IP blocking

HSTS

Mandatory password length

Angular 19 (they're really trying)

If you're stuck on old versions cause "business reasons," you better be restricting admins and watching logs like a hawk because someone's out there scanning for this stuff 100%.

Defender Just Got a Threat Intelligence Brain Implant

Microsoft dropped the Threat Intelligence Briefing Agent right into the Defender portal.?

As in, your dashboard now gives you a personalized newspaper of "Here's everything trying to ruin your day."Daily custom briefings.

IOC lists.

MITRE mapping.

Risk scores.

Links to assets.

Threat actor origins.

Tools. Techniques.

Basically the works.

This is the kind of thing analysts used to spend hours collecting through Twitter feeds, private channels, three PDFs, and a cup of despair. Now Defender just... hands it to you.

You can even link cases directly to the IOCs so nothing gets lost in the shuffle.

Honestly starting to feel like defenders might finally get a slight advantage.

Maybe.

9M Users Got Owned by a "Free VPN" Extension... Again

Who TF still installs "Free Unlimited VPN" Chrome extensions in 2025??

Apparently 9 million people.

Turns out it wasn't a VPN at all.

It was a remote-controlled proxy botnet glued into your browser, watching every site you visit, stealing login attempts, injecting PAC scripts, and even erasing your history to cover its tracks.

This thing lived SIX years in the Chrome Web Store.

Two versions from 2019 + 2020, both shady.

2025 version? Even worse.

Two-second delay to dodge sandbox detection, dynamic code downloading, auto-disabling

competing proxy extensions, hashing your visited URLs, the whole spy kit.

Basically:

If the extension can “change your proxy settings,” congratulations, you just handed your traffic to a stranger in Belarus.?

WhatsApp Leaked 3.5 Billion Phone Numbers Because... Rate Limiting?

This one is WOOOW ?.

Researchers scraped 3.5 billion WhatsApp numbers just by querying the contact discovery feature. No hacks, no zero-days, just sending numbers to WhatsApp at 100M/hour and the app happily goes “yep this number’s on WhatsApp, here’s their picture, status, key, timestamp...”

Meta was warned in 2017.

Seven. Years.

And they finally patched it in October 2025.

They used only FIVE accounts on one server to probe 63 billion numbers.

Encryption keys, “about” status texts, profile pics, everything.

29% had personal data in their bios like political opinions or full names.

Some reused keys.

Twenty U.S. users even had a key of all zeros. I don't even know how you manage that.

Meta’s response: “It was public anyway.”

Sure man, thanks.

FortiWeb 0-Day Getting Actively Exploited

And the cherry on top:

Fortinet’s got a fresh zero-day, NOW: CVE-2025-58034.

Command injection, authenticated attacker, run system-level commands, game over.

Affects basically every version of FortiWeb unless you’re on the latest patch.

Exploit kits already floating around in the usual places since October.

People are getting popped, attackers are adding new admin accounts for persistence, the whole routine.

Fortinet is telling everyone to?:Patch NOW

Stop exposing management to the internet

Audit all accounts

Which honestly should’ve been SOP already.

SIM-4331310 - November 19, 2025, 4:03 am

Very interesting..especially the WhatsApp part..thanks for the read....

CL1B - November 19, 2025, 4:57 am

This evil extension.. I remember reading [loadman](#) his thread which elaborates on spreading malware.

One clever tactic was to buy already existent apps (but also extension) to then turn them into loaders.

9M is 1 hell of a load.

Thanks for the read.

Edit: Still one of my favorite reads on this forum

<https://hackforums.net/showthread.php?tid=6219272>