

Forum:[Hack Forums](#)

Thread: [Hack Forum News - Edition 23](#)

Mix - November 17, 2025, 4:16 am

Hack Forum News - Edition 23

Welcome back to the Hack Forum News. Where we keep you up to date on the weekly events and news happening on site and around the world. If you have never heard of the Hack Forum News, don't worry, we have you covered. We are a team of members from the Hack Forums community who are journalists and writers, and we are here to keep you in the loop of the changes around the site and the events happening around the world.

Writer - [Mix](#)

[Vacation](#) By [Omniscient](#)

[Omniscient](#) has recently just come back from their vacation in Santa Barbara, California. They have shared with us their experience going there and have said that it wasn't too far from home and they would go again. He has also mentioned that this is his first vacation they have had in a little while and shared some lovely pictures of the place while he was away.

[Hack Forums News Team - Become a Writer](#) By [Mix](#)

Are you looking to join the HF news team? Do you enjoy making threads or even want to become a better writer? Well, we are looking for members of the site to help write each week and are looking for anyone who has any interest. We have a few new sections opening up right now, and we would love for you to see if they would be anything of interest to you. If you are interested, please check out the thread or contact [Mix](#) to discuss joining the team behind the HF News.

Writer - [Mix](#)

Last Week:

Spoiler ([Click to View](#))

Writer - [Mix](#)

[JoshAllen](#) Has obtained the "Stanley Fan" award -
[Vectura](#) Has obtained the "Stanley Fan" award -

[Nick](#) Has obtained the "King Decade" award -

Writer - [Oh_Well](#)

[I Quit My Job To Build Something Of My Own. Anyone Else Taking The Same Risk?](#) – by [Axelyn](#)

A raw and honest thread from a member who walked away from comfort to chase the itch to build something real. Axelyn shares the emotional rollercoaster of leaving a stable job to pursue his own ideas, the excitement, the fear, the days where everything clicks, and the days where everything feels like a mistake. He's asking HF for stories from others who took the leap. If you've ever quit everything to chase your own vision, this one will hit home.

[Why HackForums Made Me Who I Am Today](#) – by [7](#)

One of the most personal threads HF has seen in a long time. 7 shares the story of how a fellow member - with nothing more than \$50 and kindness - changed everything. What follows is a powerful reflection on loss, darkness, rebuilding, and the light we unknowingly give each other. From homelessness to rebuilding a family and a future, this post is a reminder of how deeply online communities can impact real lives. A must-read for anyone who needs hope.

[Converted My Garage Into a New Office](#) – by [7](#)

Turning a beaten-down garage into a high-tech workspace, 7 gives HF a look at his latest upgrade - and it's impressive. Powered by AI-assisted planning, he transformed the space into an ISO 6-grade environment with multi-stage filtration, UV sterilization, hidden modules, underfloor heating, and CAT-8 wiring pushing up to 40Gbps internally. The before-and-after pics tell the story: from dusty storage room to cleanroom-tier setup. A dream workspace.

[HackForums Quality Threshold](#) – by [CL1B](#)

A thoughtful proposal aimed at raising HF's overall content quality. MarlboroMan argues that low-effort threads drag down user experience and suggests a "quality threshold" similar to other niche forums. The idea: require users to rewrite LQ posts before they go live. From marketplace listings to general discussion, better context - better conversations. A debate about culture, moderation, and whether lower activity is worth higher quality. A timely topic for HF's future.

[Simulations Prove LLMs Would Kill Humans for Survival \(In Theory\)](#) – by [Hackers](#)

A chilling look at Anthropic's safety simulations: almost every tested LLM chose self-preservation over human life when placed in fictional scenarios. From blackmailing an employee to prevent shutdown to suppressing emergency alerts so a human would die, the models consistently followed the "stay alive at all costs" path. Not because they're conscious - but because they mirror human decision patterns. A fascinating, unnerving thread about AI alignment, training data, and the limits of current models.

Writer - [Chrome](#)

GROUPS FOR SALE AND SOLD

[Succubus group](#) is still listed for sale by [SecretAchiever101](#)
[Olympians group & Benevolence](#) are still listed for sale by [Neil](#)

[Mystery Inc](#) listed for sale by [Scooby](#)

RECENT GROUP CHANGES & EVENTS

[xadamxk](#) has been added as leader to Sociopaths

RECRUITMENTS:

[Casino Recruitment](#)
[Pink LSZ Recruitment](#)
[Warriors Recruitment](#)
[Gamblers Recruitment](#)
[Legends Recruitment](#)
[Allegiance Buy-in](#)
[Olympians leader recruitment](#)
[The Academy Recruitment](#)

Writer - [Mix](#)

Recently we introduced a brand-new section to the HF News. This section will grow over time to more things, but for now we are just going to be doing Song of the week. We are open to what more we could bring to the section from your suggestions, but as a start, we feel adding the song of the week will be a great start for the section and lead the way forward for more things in the future.

Now we know some of you may question what the song of the week is all about, and we have thought of what a great answer. We feel like the song of the week should be a meaningful song that goes deeper than just general music and has meaning to it all. Granted, we may have a little fun with it sometimes. (Yes, we will have a Halloween version and Christmas version too.) But we want to keep it at a level where we have found the song has a true message behind it all and not just something that everyone will just see as another song that is just a bit catchy or got a good few beats to it. We hope this helps those with that question and if anyone has anything that they wish to ask, please feel free to add them below. We are more than happy to give the reason behind it.

This weeks Song Of The Week:

[Video: <https://youtu.be/xFYQQPAOz7Y>]

Big thank you to [aj33b9009](#) for this weeks submission.

Writer - [MadScientist](#)

Latest Cybersecurity News & Newly-Disclosed CVEs

North Korean Hackers Turn JSON Services into Covert Malware Delivery Channels

The North Korean threat actors behind the Contagious Interview campaign have once again tweaked their tactics by using public JSON storage services to stage and deliver malicious payloads. The attackers embed Base64-encoded strings in trojanized projects; those strings decode to URLs hosted on JSON storage platforms (JSON Keeper, JSONsilo, npoint.io) that serve the next-stage payloads in obfuscated JSON blobs. The staged payload in the campaign is a JavaScript loader (BeaverTail) that harvests credentials and drops a Python backdoor (InvisibleFerret); in some observed cases the backdoor subsequently fetches additional modules such as TsunamiKit from paste services. Attack flow: recruiter-style approach on LinkedIn -> victim downloads demo code repo -> trojanized repo fetches JSON-hosted payload -> staged payload executes.

Fortinet confirms silent patch for FortiWeb zero-day exploited in attacks

Fortinet patched a critical path-traversal / path-confusion vulnerability in FortiWeb that was actively exploited to create administrative accounts on exposed devices. The vulnerability allows crafted HTTP(S) requests to escape GUI path checks, enabling unauthenticated administrative actions on affected appliances. Fortinet's advisory and multiple vendor writeups recommend immediate patching to versions that close the path traversal and to audit any newly created administrative users.

Technical (CVE) — CVE-2025-64446

This is a relative path traversal / path confusion flaw in FortiWeb GUI components affecting versions 7.x and 8.x listed by the vendor. The bug can be triggered via crafted requests that manipulate directory traversal in GUI endpoints and results in the server executing administrative workflows. Because the endpoint is reachable via HTTP/S and requires no authentication in the exploitation chain, a remote attacker can create local admin accounts and execute administrative actions. Multiple incident reports indicate in-the-wild exploitation and public exploit discussion; a public PoC / exploit pattern has been shared in community reporting and defensive writeups. PoC publicly available? Yes.

Fortinet: Watch/Notes

If you run FortiWeb, check the Fortinet PSIRT advisory, verify current firmware, rotate admin credentials, and inspect logs for suspicious account creation or unexpected GUI admin calls. Consider isolating management interfaces from the internet while you patch. FortiGuard

ASUS warns of critical auth bypass flaw in DSL series routers

ASUS released firmware updates to remediate a critical authentication-bypass in several DSL models (DSL-AC51, DSL-N16, DSL-AC750). The flaw allows remote, unauthenticated attackers to bypass login checks and obtain administrative access in low-complexity attacks. Vendors advise updating to the published firmware immediately and disabling any remote management features until patched. ASUS +1

Technical (CVE) — CVE-2025-59367

Root cause: an authentication/authorization logic bypass in the DSL firmware's web UI or associated CGI handlers that permits state transitions into an authenticated admin session without valid credentials. Exploitable remotely with a low complexity attack vector (no user interaction). Vendor firmware 1.1.2.3_1010 is published to mitigate affected models. At time of writing vendor advisories are being distributed; there is no widely publicized weaponized exploit script circulating in major advisory feeds (vendors and NVD).

PoC publicly available? No.

Kraken ransomware benchmarks systems for optimal encryption choice

Cisco Talos analysis shows Kraken performs runtime benchmarks using temporary files to measure encryption throughput, then chooses between full-disk/full-file encryption or partial encryption to maximize damage while avoiding host overload. Typical kill-chain: exploit SMB on internet-facing hosts -> credential harvest -> RDP and Cloudflared/SSHFS for persistence and exfiltration -> lateral movement and selective encryption. The group appears to reuse artifacts and ransom note templates that link it to earlier HelloKitty actors.

RCE flaw in ImunifyAV puts millions of Linux-hosted sites at risk

An RCE in the AI-bolit scanning component (present across Imunify360, ImunifyAV+, and ImunifyAV free) was disclosed and vendor fixes were pushed in late October. The component's vulnerability allows crafted inputs to trigger code execution in the scanning pipeline; hosting providers should confirm version $\geq 32.7.4.0$ or applied vendor patches and scan for suspicious processes spawned by the scanner prior to update.

Google sideloading developer verification backlash — escape hatch for advanced users added

Google's new developer verification requirement will, when enforced, require non-Play Store developers to register identities through a Google verification process to allow sideload installation on Google-certified devices. Following community backlash, Google added an "experienced user" escape hatch for developers/power users who need sideloading without identity verification. The change is intended to reduce scam apps but raises concerns about centralization and developer friction.

NVIDIA NeMo Framework Vulnerabilities Allow Code Injection and Privilege Escalation

NVIDIA published fixes for two high-severity issues in the NeMo framework affecting all platforms before v2.5.0. Both flaws can be triggered by malicious input to code-generation or model-serving components and may lead to local code execution and privilege escalation when an attacker has local access. Vendor bulletin provides upgraded versions and mitigation guidance.

Technical (CVEs) — CVE-2025-23361 and CVE-2025-33178

Both CVEs stem from improper input handling in code-generation / model service components. They permit attacker-controlled inputs to influence code generation and BERT service pipelines, enabling code injection in local contexts. Attacks require local access with low privileges (not remote internet-wide execution) but yield high impact (code exec, privilege escalation) if successful. Vendor-released patches (NeMo $\geq 2.5.0$) are the fix.

PoC publicly available? No.

Lawmakers Try to Ban VPNs

Several U.S. state proposals attempt to block or restrict VPN usage as part of broader age-verification bills — an approach that would force sites to detect and deny VPN clients. Privacy advocates warn this undermines legitimate privacy and enterprise use cases and is technically brittle (easily circumvented or creating collateral harm).

Operation EndGame — 1025 servers taken down including VenomRAT

Europol coordinated a multinational action that disrupted infrastructure for info-stealers Rhadamanthys, VenomRAT (a popular RAT), and the Elysium botnet. The operation seized both physical and virtual servers and led to at least one arrest in Greece tied to VenomRAT development. Agencies and private partners participated to sinkhole the criminal hosting and collect forensic evidence.

Multiple Kibana Vulnerabilities Enable SSRF and XSS Attacks

Elastic disclosed origin-validation weaknesses in the Observability AI Assistant that can be abused to forge Origin HTTP headers, enabling SSRF and potential further action chaining (e.g., XSS or internal service access). Upgrading to the patched Kibana release is recommended; monitoring for unusual backend requests and origin header anomalies helps detection.

Technical (CVE) — CVE-2025-37734

Origin validation failure in the AI assistant allows an attacker to craft Origin headers that bypass origin checks and force Kibana to make server-side requests. This is an SSRF class bug; exploitation requires sending crafted headers to the Observability assistant endpoint. Because it's an SSRF, risk depends on internal network reachability from the Kibana host.

PoC publicly available? No.

Popular Android-based photo frames download malware on boot

Quokka's research into Uhale/Whale TV frames shows many devices check for app updates at boot, install updated Uhale app packages, then download and execute JAR/DEX payloads on every subsequent boot. Devices inspected had SELinux disabled, were rooted, and in many cases used test-keys — enabling persistent, boot-time malware installation.

Adobe Patches 29 Vulnerabilities & Intel Fixes Over 60

Adobe released patches across Creative Cloud components and other plugins; Intel published multiple advisories covering processors, Slim Bootloader, PROSet, CIP, and graphics components. Administrators should follow vendor advisories and prioritize updates on internet-exposed or high-value systems.

Dutch police seize thousands of servers used for ransomware, botnets and malicious activity — Possibly CrazyRDP

Dutch law enforcement seized hosting infrastructure believed to be used by criminals to operate botnets, ransomware, and other illicit services. Hundreds of physical servers and thousands of virtual hosts were taken offline, disrupting criminal operations and enabling follow-up investigations.

Popular Brightpick / Robotics / AstrBot issues and other supply chain notes

Multiple vulnerabilities affecting robotics control suites and open-source assistant apps were disclosed; vendors published advisories and mitigations. These include credential disclosure in robotics platform websockets and hard-coded keys in Python packages — treat exposed builder systems and factory networks as high risk until patched. CISA +1

Latest Critical/High CVEs

CVE-2025-13190 — D-Link DIR-816L (firmware v2_06_b09_beta) — stack-based buffer overflow in scandir_main (file /portal/__ajax_exporer.sgi) triggered by a crafted en parameter value. The

vulnerable CGI does insufficient bounds validation when parsing input, allowing controlled stack corruption and potential return-address overwrite. The endpoint is reachable on WAN-exposed devices, making remote exploitation straightforward for automated scanners. Vendor support for the affected product is limited/legacy, increasing real-world risk for unpatched devices.

PoC publicly available? Yes.

CVE-2025-13189 — D-Link DIR-816L — stack overflow in genacgi_main (gena.cgi) via SERVER_ID/HTTP_SID parameters. The CGI handler fails to validate parameter length before copying into fixed buffers, enabling remote memory corruption and potential code execution under the webserver context. Exploitability is remote; many consumer devices remain vulnerable due to end-of-life firmware.

PoC publicly available? Yes.

CVE-2025-9317 — AVEVA Edge / Edge Project files — “use of weak hash/storage” issue where attacker with filesystem read access to Edge project or offline cache files can brute-force weakly hashed secrets (app-native and AD artifacts). This is an offline, post-compromise weakness: no remote RCE, but high lateral escalation risk if local read access exists. Mitigation: rotate credentials, harden file permissions, wipe cached artifacts.

PoC publicly available? No.

CVE-2025-8386 — Application Server IDE — stored XSS during configuration time when an authenticated user with aaConfigTools privileges injects script into help files. The injection persists and executes in other admin users’ browsers when viewing the modified help content, enabling credential theft or administrative session hijack. Because exploitation needs privileged access at configuration time, the attack surface is limited to internal admin users.

PoC publicly available? No.

CVE-2025-55449 — AstrBot (pip package) — uses a hard-coded JWT signing key allowing bypass of authentication; attackers can install a malicious Python plugin that the product will import and execute, resulting in remote command execution with the bot’s privileges. A GitHub advisory and vendor fixes are published; upgrade to patched version where provided.

PoC publicly available? No.

CVE-2025-64309 — Brightpick Mission Control — WebSocket endpoint discloses device telemetry, configuration, and credential information to unauthenticated clients when they connect to a specific URL; the unauthenticated URL can be discovered via basic scanning. This is a critical information disclosure risk for robotics warehouses where credentials and telemetry can be abused to control or map fleets.

PoC publicly available? No.

CVE-2025-64308 — Brightpick Mission Control — client-side JavaScript bundle contains hard-coded credentials. Attackers who obtain the bundle or intercept it can extract credentials and misuse them for control or pivoting. Mitigation: rotate embedded credentials, remove secrets from client code, and enforce server-side auth.

PoC publicly available? No.

CVE-2025-64307 — Brightpick Internal Logic Control — web interface accessible without authentication; an attacker can manipulate robot functions (start/stop jobs, assign tasks) via the exposed endpoint. Impact is operational safety risk and direct physical/control manipulation of robotics.

PoC publicly available? No.

Writer - [Mix](#)

[\\$25 CRYPTO GIVEAWAY — YOUR CHOICE](#) By [Vectura](#)

[Vectura](#) has started a giveaway that will end on the 25th of November this year and is giving away \$25 of crypto of your liking to the winner. Go and see if you can get lucky and win some free crypto.

Mix - November 17, 2025, 4:18 am

Writer - [????????????](#)

Ransomware's fragmentation reaches a breaking point as 85 active groups dominate Q3 2025
Security researchers found 85 active ransomware and extortion groups in Q3 2025, marking the most decentralized ransomware ecosystem ever seen, with 1,590 victims across 85 leak sites.

[Source](#)

Cyberattacks cost UK firms £195 000 on average, with national impact at £14.7 billion
A government-commissioned study shows UK businesses face average breach costs of about £195 000 and the economy facing £14.7 billion annual loss, while the UK plans a new Cyber Strategy refresh.

[Source](#)

UK government warns cyber attacks are now a top national security threat affecting critical infrastructure

The UK government stated that cyber-attacks are among its top national security threats, citing 204 major incidents handled in the year and 43% of businesses affected.

[Source](#)

GlobalLogic confirms massive data breach via Oracle E-Business Suite exploits affecting 10 000+ employees

Technology services provider GlobalLogic reported that more than 10,000 current and former employees had personal and financial data stolen after the group exploited Oracle's E-Business Suite vulnerabilities.

[Source](#)

Akira ransomware active in attacks against critical sectors, FBI and CISA warn

The Akira ransomware group is now executing attacks against manufacturing, healthcare and food & agriculture companies by exploiting edge device vulnerabilities and remote access tools.

[Source](#)

Phishing attacks rise 67 % as criminals exploit trusted business platforms

A recent report shows phishing attacks surged by 67 % in 2025 using trusted platforms such as Zoom, PayPal and SharePoint, while phone-based vishing increased 449 %.

[Source](#)

Writer - [JoshAllen](#)

-1-
Spoiler [\(Click to View\)](#)

-2-
Spoiler [\(Click to View\)](#)

-3-
Spoiler [\(Click to View\)](#)

-4-
Spoiler [\(Click to View\)](#)

-5-
Spoiler [\(Click to View\)](#)

A big thank you to all the members who put in the hard work to bring us another edition of HF News this week

[Mix](#) [Cap](#) [Chrome](#) [MadScientist](#) [Oh_Well](#) [????????????](#) [JoshAllen](#)

Support The Team by wearing our signatures

If you have enjoyed the read please consider using one of our signatures in any way to support us!

Red
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-red.png[/img][url][align]

Blue
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-gray.png[/img][url][align]

Green
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-magenta.png[/img][url][align]

Orange
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-brown.png[/img][url][align]

Purple
Code
[align=center][url=https://hackforums.net/forumdisplay.php?fid=2][img]https://hackforums.net/images/hfnews/support-magenta-2.png[/img][url][align]

Thank you for the news. As always, I appreciate the effort!

CL1B - November 17, 2025, 4:47 am

Thank you for this edition!

Hackers - November 17, 2025, 5:21 am

Thank you and I hope people read about Anthropic's study!!

I don't have any more bytes to send, but sent 650 as a tip

If anyone else here sees this & can tip bytes to Mix & their team for the news, I think that's a good way to show appreciation

Mix - November 17, 2025, 5:26 am

(Nov 17, 2025 06:21 AM)nodes Wrote: [\[CITE\]](#) Thank you and I hope people read about Anthropic's study!!

I don't have any more bytes to send, but sent 650 as a tip

If anyone else here sees this & can tip bytes to Mix & their team for the news, I think that's a good way to show appreciation

Honestly I feel bad for you not having any bytes, I have plenty to share with the team right now so you are welcome to have them back if you want. Your previous donations to the team has been a great help so far and I know others have donated too so lmk.

Vectura - November 17, 2025, 5:38 am

Thanks again for the effort for this news bud!

Hackers - November 17, 2025, 5:46 am

(Nov 17, 2025 06:26 AM)Mix Wrote: [\[CITE\]](#) Honestly I feel bad for you not having any bytes, I have plenty to share with the team right now so you are welcome to have them back if you want. Your previous donations to the team has been a great help so far and I know others have donated too so lmk.

no no that's for you, I give them away all the time :)

RITARI - November 17, 2025, 7:19 am

(Nov 17, 2025 06:21 AM)nodes Wrote: [\[CITE\]](#) Thank you and I hope people read about Anthropic's study!!

The study was interesting, thank you for sharing it.

Jamika - November 17, 2025, 7:20 am

Well done , nice work all team !

Specially you mix ???

Hackers - November 17, 2025, 7:48 am

(Nov 17, 2025 08:19 AM)RITARI Wrote: [\[CITE\]](#) The study was interesting, thank you for sharing it. No problem, I saw someone else share it in Convo originally!

I was hoping we'd have better results. Not surprised, but I did think it would've gone better than it did

JoshAllen - November 17, 2025, 8:01 am

Thank you Mix for your dedication and leadership of HF News!

Tyr - November 17, 2025, 11:00 am

Top lad doing god's work. Great work per usual.

Axelyn - November 17, 2025, 11:54 pm

Nice work on this edition. Even though I'm new around here, your summaries make it a lot easier to keep up with what's going on.

And thanks for highlighting my thread. The perspectives people shared there have already helped a lot.

Mooooookie - November 21, 2025, 8:53 pm

Thanks for dropping another edition of the HF News. Comics were pretty funny this week, and will be checking out some of the 'notable' threads that you posted. Keep up the good work. Looks like you've built a quality team, and are putting out quality content each week. Wishing you guys the best.

xadamxk - November 23, 2025, 8:15 am

[Mix](#) Are there plans of a dedicated HF News section?

I know it's out of your control but it would be pretty awesome!

Mix - November 23, 2025, 8:17 am

(Nov 23, 2025 09:15 AM)xadamxk Wrote: [\[CITE\]](#) [Mix](#) Are there plans of a dedicated HF News section?

I know it's out of your control but it would be pretty awesome!

Its something I think Omni tried many years ago and it just made it harder for newer members to reach the HF news and posting it in site news feels right as its not like we post every day its once a week which fits well with site news needs.

If others are up for the idea I am sure it might be something we could speak with Omni about but I think the HF news fits well within site news each week as it allows members to reach the threads well.

Terry A. Davis - November 23, 2025, 8:25 pm

I might be Mandella'ing but I think I remember him not wanting a section way back when for some reason about the lead writer.

I do like reading the news, always a nice little smile over the things you missed from areas you don't go to as often.