

Forum:[Hack Forums](#)

Thread: [Hack Forum News - Edition 22](#)

Mix - November 10, 2025, 7:48 am

Hack Forum News - Edition 22

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.

[Octoberfest Winners](#) By [Omniscient](#)

We somehow missed this thread last week sadly, but it's still worth a mention this week as there have been a few massive winners announced on this thread since Octoberfest, and it appears that the \$500 reward could still be up for grabs as it's not been claimed by the winner. If you haven't seen the winners, it's for sure worth checking out.

[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](#)

[Incognito™](#) Has obtained the "King Decade" award -
[Traid](#) Has obtained the "King Decade" award -
[_wind](#) Has obtained the "King Decade" award -
[splinter7](#) Has obtained the "King Decade" award -
[megathescientist](#) Has obtained the "King Decade" award -
[Pimping](#) Has obtained the "Lounge Head" award -
[Palestine](#) Has obtained the "Lounge Head" award -

Writer - [Mix](#)

[What was the most outrageous lie you believed as a child?](#) - by [The Pact](#)

[The Pact](#) has bought us another great thread talking about outrageous lies we all believed when we were young, and we have been reading through some of the replies and seen some pretty great responses. We all believed in silly things when we were much younger but some of the responses are crazy, and we had to add that to this week's edition.

[Are you still using Windows 10 ?](#) - by [Chorozon](#)

As Windows 10 support is coming to an end, the user known as [Chorozon](#) has raised the question for those who still haven't updated to Windows 11 and to find out the reason why they haven't moved over just yet, even when support is pretty much ended.

[How Has 2025 Been For You So Far?](#) - by [DemonAsylum](#)

As the year is slowly coming to an end, each day goes by and feels shorter and shorter. [DemonAsylum](#) has raised a good thread talking about how the year has treated everyone and shared how the year has treated them so far, with a few rough times but also a few good times as well.

[Do you use fidget toys](#) - by [Fish](#)

Fidget toys. We all remember the peak of them with the fidget spinners a few years back. [Fish](#) has created a thread talking about fidget toys as they were playing with their pen and thought they should buy one and ended up getting a fidget toy from Aliexpress. In the end, they have found they are being more productive now that they have bought a toy.

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

[Lavish Living](#) has been removed as leader from Pink

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/TW9RirTCbcM>]

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

Writer - [MadScientist](#)

Russian spies pack custom malware into hidden VMs on Windows machines

Bitdefender researchers attribute a campaign to the threat actor "Curly COMrades" that abuses Hyper-V on compromised Windows hosts to spin up a tiny, stealth Alpine Linux VM (?120 MB disk, 256 MB RAM) hosting custom C++ implants (CurlyShell and CurlCat) built on libcurl. By disabling Hyper-V management and using the Default Switch network adapter, the attackers route VM traffic

through the host stack so malicious C2 and proxy traffic appears to originate from legitimate host IPs, effectively evading host-based EDR. CurlyShell provides a cron-backed root-level reverse shell over HTTPS for persistence and remote command execution, while CurlCat implements an SSH reverse-proxy that tunnels SSH over HTTP payloads; supporting tooling includes PowerShell scripts for LSASS Kerberos ticket injection and GPO-deployed account creation for lateral movement. The technique highlights a growing trend of VM isolation as an EDR evasion vector and reinforces the need for defense-in-depth (hypervisor auditing, network telemetry, least-privilege, and cross-layer detection) to detect and disrupt such hidden-VM implants. Read More -

https://www.theregister.com/2025/11/04/russian_spies_pack_custom_malware/

Claude Desktop Extensions Vulnerable to Web-Based Prompt Injection

Security researchers at Koi Security uncovered critical vulnerabilities in three official Claude Desktop extensions that allowed prompt injection attacks via malicious web content. The flaws enabled arbitrary command execution on local systems due to the extensions' elevated OS-level permissions and inadequate input sanitization. Although Anthropic has since patched the issues, the incident underscores a broader systemic risk in AI desktop agents—where integrations with full system access can be weaponized through crafted prompts or browser-based payloads, effectively bridging web-origin threats into local execution environments. Read More -

<https://www.infosecurity-magazine.com/news/claude-desktop-extensions-prompt/>

US gives local police a face-scanning app similar to one used by ICE agents

The Department of Homeland Security has quietly rolled out a mobile biometric app—reported as “Mobile Identify” and likened to ICE’s Mobile Fortify—that gives local law enforcement a field-capable facial-comparison and fingerprint-matching capability against federal immigration and biometric holdings; the app appeared on the Google Play store and is being distributed to agencies working under authorities such as Section 287(g). Technical concerns raised by reporters and civil-liberties researchers include lack of meaningful oversight or audit trails, the ability to capture and query biometric images in-the-field (with no practical opt-out), potential data-sharing with commercial or federal databases, and algorithmic bias/false-positive risks that can disproportionately affect marginalized groups — all of which materially increase the risk that routine encounters will be turned into remote biometric identification events without warrants or local policy safeguards. Read More -

<https://arstechnica.com/tech-policy/2025/11/us-gives-local-police-a-face-scanning-app-similar-to-one-used-by-ice-agents/>

Google warns of new AI-powered malware families deployed in the wild

Google’s Threat Intelligence Group (GTIG) has identified multiple new malware families that integrate large language models (LLMs) directly into their execution chains to enable adaptive, self-modifying behavior. One strain, PromptFlux, is a VBScript dropper that queries an embedded LLM API to continuously regenerate and obfuscate its payload code in real time, allowing polymorphic evolution and evasion of static detection. Another, QuietVault, is a JavaScript credential stealer that leverages AI-driven code synthesis to locate and exfiltrate developer tokens and secrets from local environments to dynamically created remote repositories. A third variant, PromptLock, is a Lua-based ransomware framework capable of cross-platform execution on Windows, macOS, and Linux, generating encryption logic on-demand from contextual AI prompts. GTIG also observed state-aligned threat actors weaponizing LLMs for reconnaissance, phishing lure automation, vulnerability scanning, and code obfuscation. Collectively, these findings signal a shift toward AI-assisted, modular malware ecosystems where real-time prompt generation replaces hardcoded logic, posing major challenges to traditional signature- and heuristic-based defenses. Read More -

<https://www.bleepingcomputer.com/news/security/google-warns-of-new-ai-powered-malware-familie>

[s-deployed-in-the-wild/](#)

Hundreds of Malware-Laden Apps Downloaded 42 Million Times From Google Play

A recent report by Zscaler reveals that approximately 239 malicious Android apps on the Google Play Store were collectively downloaded over 41 million times in the one-year span between June 2024 and May 2025. These apps primarily delivered spyware and banking-trojan payloads and represent a 67% year-on-year increase in mobile-malware volume. Many of the threats bypassed normal protections and shifted tactics from card-fraud towards mobile-payment vectors, abusing social engineering (smishing, fake apps, SIM-swaps) combined with privilege escalations via accessibility APIs. The study underscores that malware authors are targeting the Android ecosystem with applications from legitimate stores, leveraging permission creep, sandbox-escape techniques and bank-app overlays — meaning defenders must monitor behavioral anomalies (unexplained data exfiltration, background active services, unusual permission usage) rather than rely solely on signature-based detection. Read More -

<https://www.infosecurity-magazine.com/news/apps-download-41-million-times/>

Attackers exploit critical bypass flaw in WordPress JobMonster theme

A critical authentication-bypass flaw in the JobMonster WordPress theme (CVE-2025-5397) allowed attackers to bypass normal login mechanisms and gain administrative privileges. Exploitation provides full site control, enabling data exfiltration of sensitive user information such as resumes and recruiter details, content manipulation, and deployment of malicious job listings for phishing campaigns. The vulnerability resides in the theme's authentication and social-login workflow, which fails to properly validate user sessions. Immediate mitigation includes updating to the patched version, disabling the social-login feature if updates are not possible, enforcing MFA on admin accounts, auditing access logs for unauthorized activity, rotating exposed credentials, and checking for injected content or rogue administrator accounts. Given JobMonster's widespread use, compromised instances should be treated as high-risk breach candidates. Read More -

<https://www.scworld.com/news/attackers-exploit-critical-bypass-flaw-in-wordpress-jobmonster-theme/>

Apple Patches 19 Critical WebKit Vulnerabilities

Apple has released iOS 26.1 and macOS Tahoe 26.1 which address over 100 security issues across the platforms—most notably 19 critical vulnerabilities in the WebKit browser engine. Many of these WebKit flaws could allow a website to bypass same-origin protections and exfiltrate data, crash or corrupt memory in processes, or monitor keystrokes. Beyond WebKit, the updates also patch kernel-level memory corruptions, sandbox escapes, elevation of privilege and file tampering bugs in macOS, and a broad range of component flaws in iOS/iPadOS. None of the disclosed issues are publicly known to have been exploited in the wild, but due to their severity, administrators and users are strongly advised to apply the updates without delay. Read More -

<https://www.securityweek.com/apple-patches-19-webkit-vulnerabilities/>

DeFi Protocol Balancer Loses Over \$120m in Cyber Heist

The Balancer protocol suffered a major exploit in its V2 composable stable-pool architecture resulting in a loss of over US \$120 million in crypto assets. Initial chain forensics indicate the attack targeted a rounding error or imbalance within the pool swap calculation logic, enabling the attacker to drain funds across multiple pools and chains including Ethereum and Polygon. The protocol's internal authorization controls for the vault and batchSwap operations also appear to have been bypassed, enabling unauthorised fund transfers. On-chain data shows large volumes of tokens (e.g., wstETH, WETH, osETH) shifted to controlled exploiter addresses. The incident exposed that

even heavily audited DeFi systems remain vulnerable to economic-logic and complex multi-transaction exploits, underscoring the need for continuous simulation, anomaly detection, and fast response mechanisms across smart-contract stacks. Read More -

<https://www.infosecurity-magazine.com/news/defi-protocol-balancer-loses-120m/>

Latest High Severity CVEs

CVE-2025-63601 - In Snipe-IT versions prior to 8.3.3, an authenticated attacker can upload a malicious backup archive containing arbitrary files, which can then be used to execute system commands. This effectively enables remote code execution via the backup-upload functionality.

CVE-2025-64164 - In DataEase versions <= 2.10.14, the JDBC connection logic fails to properly sanitize user-provided input, resulting in a JNDI injection vulnerability that can be abused to trigger remote lookups, execute code, or steal credentials.

CVE-2025-64163 - In DataEase versions <= 2.10.14, insufficient protocol filtering allows dns:// URIs to bypass blacklists intended for ldap:// and ldaps://, producing a server-side request forgery (SSRF) that can force access to internal network resources or metadata endpoints.

CVE-2025-64110 - In Cursor (code editor) versions <= 1.7.23, a logic flaw in the “.cursorignore” handling can be manipulated—via crafted project files or prompt injection—to read sensitive files that should be excluded, leading to potential data exposure and local code-execution chains.

CVE-2025-64109 - In Cursor CLI Beta, a malicious MCP (Model Context Protocol) configuration hosted in a cloned repository can be executed when the project is opened, allowing arbitrary command execution on the developer’s machine due to unsafe loading of remote MCP servers.

CVE-2025-64108 - In Cursor versions <= 1.7.44 on Windows, NTFS path-handling quirks (notably backslash handling) allow prompt-injection attackers to bypass protections and overwrite sensitive editor files, enabling remote code execution and integrity compromise.

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

Nagpur Municipal Corporation servers hit by over 2,000 hacking attempts in a single day
Nagpur’s civic IT systems faced more than 2,000 hacking attempts targeting its property tax and water billing portals. Officials say attempts originated from foreign IP addresses, but no data loss was reported.

[Source](#)

Hackers team up with organized crime rings to hijack physical cargo shipments
Proofpoint researchers warn that cybercriminals are partnering with traditional crime rings to hijack shipments through phishing, social engineering, and manipulation of freight systems.

[Source](#)

Iran-linked group Cyber Toufan leaks Australian defense vehicle schematics
A pro-Hamas hacking group tied to Iran claims responsibility for breaching Elbit Systems, leaking designs for Australia’s \$7 billion Redback infantry fighting vehicle project. Authorities are investigating possible espionage motives.

[Source](#)

ESET report highlights surge in APT activity by Russia, China, Iran, and North Korea
ESET's new Global APT Activity Report shows nation-state groups escalating espionage and disruption operations worldwide, particularly in energy, defense, and telecom sectors.

[Source](#)

Cybercriminals exploit remote monitoring tools to steal digital cargo
Hackers are increasingly abusing remote access tools and supply-chain software in the logistics industry to reroute or steal valuable cargo, creating a new cyber-physical threat landscape.

[Source](#)

Industrial cybersecurity sector faces reckoning as ransomware surges 25%
A new report finds ransomware incidents in the industrial sector surged 25% in October, with attacks targeting grain, energy, and manufacturing systems. Analysts say compliance must shift to real resilience.

[Source](#)

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.

[Win 5,000 Bytes! Easy Entry](#) by [PacketPilot](#)

Are you after some free bytes? Well [PacketPilot](#) has got you covered with their 5,000 bytes giveaway. As the title says, to enter is a very easy process and only takes a few seconds to get your chance to win.

[100,000 Bytes Contest : \\$250 Value](#) by [Mooooookie](#)

100,000 bytes are up for grabs with [Mooooookie](#) giveaway. The giveaway ends on November 16, 2025, so not too far away and this could be a life changing amount of bytes to someone who may be in need. We hope you all the best of luck to whoever wins.

Mix - November 10, 2025, 7:50 am

Writer - [Mix](#)

Natural disaster in the Philippines

A powerful typhoon named Typhoon Fung-wong struck the Philippines, prompting large-scale evacuations and significant damage. It's a reminder of how vulnerable coastal communities remain to extreme weather events.

[Source](#)

Saudi Arabia and Israel

Donald Trump has been promoting the idea that Saudi Arabia might normalise relations with Israel, but Riyadh says such a step depends on a roadmap to a Palestinian state. This illustrates the complexity of Middle-East diplomacy: major moves depend on broader political conditions.

[Source](#)

New leadership in Bolivia amid economic crisis

Rodrigo Paz has been sworn in as the president of Bolivia, promising “capitalism for all” as the country faces its worst economic crisis in decades (inflation, fuel & dollars shortage).

[Source](#)

Global climate summit in Brazil

The COP30 climate talks are underway in Belem, Brazil — located near the Amazon rainforest. Leaders, activists and scientists are meeting amid growing recognition that the 1.5 °C global warming target may now be out of reach.

[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 workto 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]

CL1B - November 10, 2025, 8:01 am
Thank you for this week's edition!

Tor - November 10, 2025, 8:07 am
Thank you for tagging me in this news edition.
Glad you liked the song.

Jamika - November 10, 2025, 8:23 am
Nice edition as usual, good work ??
Thanx for u and the excellent team

JoshAllen - November 10, 2025, 9:20 am
Another great read as always. Thank you Mix and team for your work.

Bastille - November 10, 2025, 11:00 am
Thanks for the news ! Always pleasant to read these threads, a lot of King Decade awards have been granted, I guess will see more and more over time.

Mix - November 10, 2025, 11:04 am
(Nov 10, 2025 12:00 PM)Bastille Wrote: [\[CITE\]](#) Thanks for the news ! Always pleasant to read these threads, a lot of King Decade awards have been granted, I guess will see more and more over time.

I think more and more people have been returning and opening up the award goals page to let it grant the awards. Thank you as always for the support and repping the signature too.

JoseMar - November 10, 2025, 11:15 am

Cheers for this week's edition, always something interesting in here.??

xadamxk - November 10, 2025, 1:09 pm

If I wrote a user script for you to help, would you report the site stats via text values rather than a screenshot?

Screenshots expire but text lives forever <3

Mix - November 10, 2025, 2:01 pm

(Nov 10, 2025 02:09 PM)xadamxk Wrote: [\[CITE\]](#) If I wrote a user script for you to help, would you report the site stats via text values rather than a screenshot?

Screenshots expire but text lives forever <3

We tried using the mybb format before and now just use the stat images that are custom to the site. With the images I feel that it does a cleaner job than a span of text these days also fits the sites themes better but I would consider making 2 versions if people want such each week.

xadamxk - November 10, 2025, 7:34 pm

Fun fact, this would be the 561st Edition of the HF News.

RITARI - November 11, 2025, 3:27 am

Thank you for this great edition!

Astaroth - November 11, 2025, 8:33 am

Another fabulous edition by our dear friend, Mix.

???